**BÜRGERSCHAFT
DER FREIEN UND HANSESTADT HAMBURG**

Drucksache 17/352

17. Wahlperiode

13. 02. 02

Der Hamburgische Datenschutzbeauftragte

**An die
Frau Präsidentin der Bürgerschaft**

Betr.: 18. Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten

Gemäß § 23 Hamburgisches Datenschutzgesetz übersende ich der Bürgerschaft den 18. Tätigkeitsbericht.*

Dem Senat leite ich den Tätigkeitsbericht gleichzeitig zu.

Dr. Schrader

* Verteilt nur an die Abgeordneten der Bürgerschaft.

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

18. Tätigkeitsbericht
des
Hamburgischen Datenschutzbeauftragten
zugleich
Tätigkeitsbericht der Aufsichtsbehörde
für den nicht öffentlichen Bereich
2000 / 2001

vorgelegt im Februar 2002

(Redaktionsschluß: 5. Dezember 2001)
Dr. Hans-Hermann Schrader

Diesen Tätigkeitsbericht können Sie abrufen unter
www.hamburg.datenschutz.de

Herausgegeben vom Hamburgischen Datenschutzbeauftragten
Baumwall 7 · 20459 Hamburg · Tel. 4 28 41 20 47 · Fax 4 28 41 23 72
mailbox@datenschutz.hamburg.de

Vertrauliche Informationen sollten uns elektronisch nur verschlüsselt übermittelt werden; wir geben dazu nähere Hinweise.

Auflage: 2.500 Exemplare

Druck: Lütcke & Wulff, 20097 Hamburg

INHALTSVERZEICHNIS

Datenschutz im öffentlichen Bereich

Datenschutz im nicht öffentlichen Bereich

Bürgerservice und die Dienststelle

Einleitung

Datenschutz und Terrorismusbekämpfung

Dieser Tätigkeitsbericht steht unter dem Eindruck der Ereignisse und Folgen des 11. September 2001 mit den Terroranschlägen auf das World Trade Center und weitere Ziele in den USA. Danach hat sich sehr bald eine intensive Auseinandersetzung um das Verhältnis von Sicherheit und Datenschutz entwickelt. Auf der Internationalen Datenschutzkonferenz von Ende September 2001 mit Teilnehmern aus rund 50 Ländern wurde eingehend diskutiert, wie ein neues Gleichgewicht zwischen den Sicherheitsbedürfnissen und den Datenschutzbelangen der Menschen gewährleistet werden kann. Das Selbstbestimmungsrecht (Rückseite des 17. Tätigkeitsberichts) und die Menschenwürde (Rückseite dieses Tätigkeitsberichts) müssen dabei ihren hohen Rang behalten.

Die Datenschutzbeauftragten des Bundes und der Länder haben am 1. Oktober 2001 diese Thematik erörtert. Sie haben dazu folgende Entschließung gefasst:

Bonn, den 1. Oktober 2001

Entschließung

Sondertreffen der Datenschutzbeauftragten des Bundes und der Länder zur Terrorismusbekämpfung

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen mit Nachdruck den Kampf des demokratischen Rechtsstaats gegen Terrorismus und organisierte Kriminalität. Sie sind heute zu einem Sondertreffen in Bonn zusammengekommen, um die aktuelle Situation nach den Terroranschlägen zu erörtern. Im politischen Raum werden zahlreiche Forderungen und Vorschläge zur Verbesserung der inneren Sicherheit diskutiert, die auch Auswirkungen auf den Datenschutz haben.

Die Datenschutzbeauftragten weisen darauf hin, dass die Sicherheits- und Strafverfolgungsbehörden zur Terrorismusbekämpfung bereits über weitreichende Befugnisse zur Datenverarbeitung verfügen. So ist z.B. die Rasterfahndung zu Strafverfolgungszwecken generell möglich, in den meisten Ländern auch zur Gefahrenabwehr durch die Polizei. Das Bundesamt für die Anerkennung ausländischer Flüchtlinge kann bereits heute Erkenntnisse über terroristische Aktivitäten an den Verfassungsschutz und die Polizei übermitteln. Auch ist eine effektive Zusammenarbeit zwischen Polizei und Verfassungsschutz durch die geltende Rechtslage gewährleistet; Vollzugsdefizite sind kein Datenschutzproblem. Zu pauschalen Forderungen nach Einschränkung des Bürgerrechts auf Datenschutz besteht deshalb kein Anlass. Die Datenschutzbeauftragten betonen, dass Datenschutz nie Täterschutz war und auch in Zukunft nicht sein wird.

Die Datenschutzbeauftragten sind zu einem offenen und konstruktiven Dialog über etwa notwendige Anpassungen an die neue Bedrohungslage bereit. Sie erwarten, dass sie rechtzeitig beteiligt werden. Die Datenschutzbeauftragten warnen vor übereilten Maßnahmen, die keinen wirksamen Beitrag zur Terrorismusbekämpfung leisten, aber die Freiheitsrechte der Bürgerinnen und Bürger einschränken. Sie sprechen sich dafür aus, alle neu beschlossenen Eingriffsbefugnisse zu befristen und tiefgreifende Eingriffsbefugnisse, damit auch die laufende Rasterfahndung, einer ergebnisoffenen Erfolgskontrolle zu unterziehen.

Bei der künftigen Gesetzgebung sind die grundlegenden Rechtsstaatsprinzipien, das Grundrecht der freien Entfaltung der Persönlichkeit, das Verhältnismäßigkeitsprinzip, die Unschuldsvermutung und das Gebot besonderer gesetzlicher Verwendungsregelungen für sensible Daten selbstverständlich zu beachten. Diese verfassungsrechtlichen Garantien prägen den Rechtsstaat, den wir gemeinsam zu verteidigen haben.

Diese Grundsatzerklärung wurde mit der Entschließung der Datenschutzkonferenz vom 24. bis 26. Oktober 2001 „Freiheits- und Persönlichkeitsrechte dürfen bei der Terrorismusbekämpfung nicht verloren gehen“ aktualisiert und konkretisiert. Die Forderungen der Datenschutzbeauftragten sind ebenso wie ihre weiteren Entschließungen zu dem Themenkomplex unter www.hamburg.datenschutz.de abrufbar.

In diesem 18. Tätigkeitsbericht (18. TB) haben wir insbesondere Gesetzesvorhaben aufgegriffen, die bei der Terrorismusbekämpfung eine große Zahl von Bürgerinnen und Bürgern betreffen, häufig ohne dass die Regelungen irgendwelche tatsächlichen Anhaltspunkte hinsichtlich der Beteiligten voraussetzen. Anders als bisher werden damit alle Beteiligten unter einen Generalverdacht gestellt und in ihrer Freiheit ohne konkrete Gründe weitgehend eingeschränkt. Beispiele sind dafür insbesondere:

- Befugnisse von Strafverfolgungsbehörden zur Internet-Überwachung (3.5.3),
- Fingerabdruck und sonstige biometrische Merkmale in Personalausweisen und Pässen (6.1),
- Auskunftsbefugnisse des Verfassungsschutzes (17.1).

Gegenüber den ursprünglichen Entwürfen des Bundesinnenministeriums sind in der Kabinettsvorlage vom 7. November 2001 für ein Terrorismusbekämpfungsgesetz mehrere pauschale Regelungsvorschläge erheblich korrigiert und teilweise auch befristet worden. Andererseits gibt es neue problematische Vorhaben wie das Abhören von Wohnungen durch den Verfassungsschutz und die Einbeziehung von Sozialdaten in die Rasterfahndung.

Bei diesen wesentlichen Eingriffen haben wir jeweils den Sachstand bis zu unserem Redaktionsschluss am 5. Dezember 2001 berücksichtigt. Wir werden die weitere Entwicklung in unsere Presseerklärung zur Veröffentlichung des Tätigkeitsberichts am 21. Februar 2001 aufnehmen.

Schon vor den Ereignissen vom 11. September 2001 hatten wir uns eingehend mit der zunehmenden personenbezogenen Überwachung der Bürgerinnen und Bürger befasst. Angesichts der weitreichenden Vorhaben, den Datenschutz einzuschränken, hat das Schwerpunktthema dieses Tätigkeitsberichts „Alles unter elektronischer Kontrolle?“ noch an Aktualität gewonnen.

Den sich bedenklich ausweitenden Überwachungsbereich stellen wir anhand gravierender Kontrolltechniken zusammenfassend dar: hinsichtlich der Ortungstechniken, der Videoüberwachung, der Biometrie und der Genom-Kontrolle.

Diese Entwicklung widerspricht den Bemühungen bei der Novellierung des Bundesdatenschutzgesetzes und der bereits 1997 erfolgten Änderung des Hamburgischen Datenschutzgesetzes, die Verarbeitung personenbezogener Daten so weit wie möglich zu vermeiden. Wir werden deshalb bei Vorhaben der Verwaltung und der Wirtschaft darauf achten, dass die verantwortlichen Stellen zunächst die Möglichkeiten der Datenvermeidung konkret prüfen – insbesondere durch eine entsprechende Systemgestaltung mit Anonymisierung und Pseudonymisierung. Dazu werden wir auch auf die bereits seit Jahren bestehenden Anforderungen an eine Risikoanalyse und auf die neuen rechtlichen Vorgaben für eine Vorabkontrolle verweisen.

Schwerpunktthema

1. Alles unter elektronischer Kontrolle?

Wissenschaftliche Erkenntnisse und neue Techniken ermöglichen die umfassende Überwachung vieler Lebensbereiche. Technische Systeme und rechtliche Rahmenbedingungen müssen deshalb so gestaltet werden, dass die Überwachungspotenziale begrenzt werden.

„Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. ... Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhal-

tensweisen aufzufallen. Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist." (Bundesverfassungsgericht, Volkszählungsurteil BVerfGE 65, 1ff. – 43 -)

Die Aussagen des Bundesverfassungsgerichts im sog. „Volkszählungsurteil" sind heute aktueller denn je – fast 20 Jahre, nachdem sie formuliert wurden. Die technische Entwicklung hat dazu beigetragen, dass elektronische Datenerfassungs- und Auswertungssysteme immer intensiver im öffentlichen Bereich eingesetzt werden. Auch in vielen Haushalten befinden sich derartige elektronische Systeme, von der automatischen Temperatursteuerung und Verbrauchsablesung für Gas, Wasser oder Strom über Telefon-, Kabel- und Mobilfunkdienste bis zum PC mit Internetanschluss: Technik, die unser Leben erleichtert, birgt in sich auch das Potenzial einer umfassenden Überwachung des Verhaltens.

Neue wissenschaftliche Erkenntnisse der Medizin und Genomforschung bieten nicht nur große Chancen zur Erkennung von gesundheitlichen Dispositionen und Erkrankungen sowie deren Therapie. Sie könnten auch missbraucht werden, um biologische Dispositionen zu registrieren, zu katalogisieren und mit Verhaltensdaten abzugleichen.

Diese Entwicklungen haben uns veranlasst, das Thema „Überwachung" einer differenzierten Betrachtung zu unterziehen. Ausgehend von äußeren Verhaltenskontrollen (Lokalisierung, Videoüberwachung) wird ein Bogen zur Auswertung von persönlichen Merkmalen (Biometrie, Genomanalyse) gespannt. Die Darstellung muss sich auf einige Beispiele beschränken, wobei weitere, ebenfalls bedeutsame Überwachungsmöglichkeiten (etwa Überwachung der Telefon- und E-Mail-Kommunikation, akustische Überwachung, elektronische Kontrolle des Zahlungsverkehrs) außer Betracht bleiben.

Besonders problematisch sind die Möglichkeiten, die sich aus der Kombination unterschiedlicher Kontrolltechnologien ergeben, etwa durch die Verbindung von Videotechnik und Biometrie, die eine automatische Erkennung und Verfolgung bestimmter Personen ermöglichen. Damit verbunden ist die Gefahr einer „Totalüberwachung", d.h. einer umfassenden Katalogisierung der Persönlichkeit, die mit der Menschenwürde (Art. 1 GG) nicht zu vereinbaren wäre.

In diesem Zusammenhang gibt es bei Behörden und Unternehmen ernst zu nehmende Motive, die Überwachungen noch zu verstärken. Bei staatlichen Stellen steht die Aufklärung von Straftaten und die Aufdeckung sonstiger unrechtmäßiger Handlungen im Vordergrund. Unternehmen haben häufig ein Interesse daran, Kundenbindungen zu intensivieren oder Risiken (etwa das Krankheitsrisiko von Arbeitnehmern oder Versicherten) durch möglichst umfassende Kenntnis der betroffenen Arbeitnehmer oder Vertragspartner zu reduzieren. Dazu gehören Aspekte der Servicefreundlichkeit und Kosteneinsparung durch E-Commerce und E-Government.

Für den Datenschutz stellen die beschriebenen Tendenzen und Entwicklungen erhebliche Herausforderungen dar. Das Recht muss diesen Gefahren begegnen und – auch für nicht-öffentliche Stellen – klare Grenzen für die Registrierung von Verhaltens- und Persönlichkeitsmerkmalen definieren und dabei insb. dem Grundsatz der Verhältnismäßigkeit Rechnung tragen. Dabei ist nicht allein auf die „Sensibilität" der einzelnen Daten abzustellen; vielmehr sind alle denkbaren Verwendungs- und Verknüpfungsmöglichkeiten mit einzubeziehen, die in der Gesamtschau häufig zu völlig anderen Risikobewertungen führen. Die Aussage des Bundesverfassungsgerichts, dass es im Zeitalter der automatisierten Datenverarbeitung kein wirklich unsensibles personenbezogenes Datum gibt, hat in diesem Zusammenhang einen hohen Aktualitätsgrad.

Die Abwägung der konkurrierenden Interessen muss bereits bei der Technikgestaltung und Systemkonzeption beginnen und nicht erst bei der konkreten Einsatzplanung. § 3a des im Mai 2001 novellierten Bundesdatenschutzgesetzes (BDSG) enthält bereits die Vorgabe, dass sich die Gestaltung und Auswahl von Datenverarbeitungssystemen an dem Ziel auszurichten haben, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Diese Vorschrift, der in dem hier betrachteten Zusammenhang besondere Bedeutung zukommt, muss indes vielfach noch mit Leben gefüllt werden. Nicht jede technische Möglichkeit, nicht jeder Komfortgewinn – und sei er noch so groß – rechtfertigt die Erhebung oder Registrierung persönlicher Daten.

1.1 Wo bin ich? – Ortungstechniken

Familie Mustermann steht neuen Techniken aufgeschlossen gegenüber. Inzwischen haben alle Familienmitglieder ihr eigenes Handy. Kürzlich hat sich Herr Mustermann sogar einen mobilen „personal digital assistent" (PDA) gekauft, der direkt mit dem Mobilfunknetz verbunden ist. Trotzdem wundert sich Herr Mustermann, dass er beim Eintritt in das Blumengeschäft, in dem er bislang noch nie Kunde war, von der Verkäuferin mit dem Satz begrüßt wird: „Schön, dass Sie nun auch zu uns kommen. Nach

einer längeren Shopping-Tour in unserem Einkaufszentrum sind Blumen genau das Richtige. Ihre Frau mag übrigens Rosen besonders gern.“ Als er an dem Supermarkt vorbeigeht, erscheint auf dem Display seines PDA die Meldung: „Lieber Herr Mustermann, Ihr Kühlschrank ist ziemlich leer. Milch und Eier müssen gekauft werden.“ Im Supermarkt wird er von einer angenehmen Stimme aus dem Einkaufswagen angesprochen: „Wie wäre es mit einer Blumenvase im Art Deco Stil? Wir haben gerade einige sehr schöne Exemplare im Angebot, die Ihnen bestimmt gefallen werden.“ Herr Mustermann überlegt, ob diese Angebote bloß Zufälle waren.

1.1.1 Überall unter Kontrolle?

Mobilität, Flexibilität und Individualität gehören – gekoppelt mit einer jederzeitigen Erreichbarkeit – zu den Kernbotschaften der Ökonomie des 21. Jahrhunderts. Gebrauchsgegenstände wie Autos, Kühlschränke, Waschmaschinen und auch Kleidung werden zunehmend „intelligente Techniken“ enthalten, die in umfassende Netzwerke integriert sind.

Bisher erfolgt die Lokalisierung ausschließlich zur Gewährleistung der Erreichbarkeit von Handys in GSM-Netzen.

GSM (Global System for Mobile Communications)

Die derzeitigen D- und E-Netze funktionieren nach dem GSM-Standard. GSM-Netze setzen sich aus einer Vielzahl von Funkzellen zusammen, damit die knappen Frequenzen mehrfach genutzt werden können. Der Durchmesser der Funkzellen liegt zwischen 200 Metern und 50 Kilometern. Damit ein mobiles Gerät erreichbar ist, muss dem Netz bekannt sein, in welcher Funkzelle es sich befindet. Deshalb senden eingeschaltete Mobilteile laufend „Aktivmeldungen“. Aufgrund der Aktivmeldungen wird der Standort des jeweiligen Teilnehmers ermittelt und an zentraler Stelle im Netz gespeichert. Sofern eine Verbindung zu Stande kommt, werden die Standortdaten (insb. zur Ermittlung der Telefongebühren) in einem Verbindungsdatensatz gespeichert.

Für die Erreichbarkeit genügt die relativ grobe Bestimmung des Aufenthaltsortes. Damit der Nutzer mobil telefonieren kann, muss dem Netzbetreiber lediglich bekannt sein, in welcher Funkzelle sich das jeweilige Gerät gerade befindet. In den Fällen, in denen eine Verbindung zu Stande gekommen ist, kann es – abhängig von der Tarifgestaltung des Diensteanbieters – darüber hinaus erforderlich sein, die Standortinformationen als Verbindungsdaten für die Entgeltermittlung zu speichern.

Im Hinblick auf die Datensparsamkeit (§ 3a BDSG, s. 1.1) muss bereits bei der Tarifgestaltung der Umfang der für die Entgeltabrechnung erforderlichen Daten berücksichtigt werden. So ist bei Tarifen, die keine Differenzierung der Entgelte je nach Entfernung vorsehen, die Speicherung von Standortdaten im Verbindungsdatensatz nicht erforderlich. Keinesfalls erforderlich ist es für Abrechnungszwecke, die Standortmeldungen von Mobiltelefonen für einen längeren Zeitraum auf Vorrat zu speichern und auszuwerten.

Neue Mobilfunknetze werden eine wesentlich genauere Ermittlung des Standortes der mobilen Geräte gestatten. Dies wird zum einen durch Nachrüstung der herkömmlichen, GSM-basierten Mobilfunktechniken um besondere Lokalisierungsmodule ermöglicht. Dabei erfolgt eine Peilung anhand der Auswertung der Signallaufzeiten durch mindestens drei Basisstationen. Diese Standortdaten können an zentraler Stelle durch den Netzbetreiber oder in dem mobilen Gerät gespeichert werden. Zum anderen funktionieren die Lokalisierungsdienste durch Kombination von GSM mit der Ortung durch GPS, wodurch eine metergenaue Standortbestimmung (mit Stockwerksangabe) möglich wird.

GPS (Global Positioning System)

GPS ist ein System zur satellitengestützten Bestimmung der eigenen Position an einem beliebigen Ort auf der Erde bis auf wenige Meter genau. Es besteht aus 21 Satelliten, die die Erde in großer Höhe umkreisen. Mit einem GPS-Empfangsgerät werden die vier dem Standort am nächsten befindlichen Satelliten angepeilt. Auf der Grundlage der Signallaufzeiten wird der Standort berechnet. GPS wurde im Auftrag des amerikanischen Verteidigungsministeriums entwickelt. GPS selbst ist ein „passives“ System; die Positionsdaten werden zunächst nur an das abfragende Empfangsgerät gesandt. Dies geschieht nicht ständig, sondern nur auf Anforderung durch das Empfangsgerät. Personenbezogene oder -beziehbare Daten, die ohne eine Kontrolle des Betroffenen erhoben oder verarbeitet werden, fallen daher zunächst nicht an. Das System wird jedoch im Rahmen von anderen Diensten (Ortung gestohlener Fahrzeuge, Flottenmanagement) zur Positionsbestimmung genutzt. Die mit GPS gewonnenen Informationen können in diesen Systemen zur Erzeugung von Bewegungsbildern genutzt werden.

Bei dem neuen „universalen Mobilfunkstandard“ UMTS sind genaue Lokalisierungsmechanismen und darauf basierende Dienste von vornherein vorgesehen. Dabei arbeiten die Betreiber der Ortungstechnik mit Dritten zusammen, die sich der Standortinformationen bedienen. Die Ortung wird von den Betreibern der Mobilfunkdienste durchgeführt, die die Standortdaten zum Abruf

bereit halten. Die Nutzer der Standortdaten (sog. „Mehrwertdienste“) – etwa Kaufhäuser, Rettungsdienste, Pannenhilfsdienste – greifen auf die Standortdaten zu und verwenden sie weiter – etwa, indem sie die Standortdaten mit anderen Daten (z.B. Kundendaten) verknüpfen. Auf diese Weise sollen etwa eine persönliche Ansprache von Kunden ermöglicht und Hilfeleistungen oder sonstiger Service erleichtert werden.

Die eigentliche Neuigkeit besteht also weniger darin, dass bei der mobilen Kommunikation überhaupt eine Lokalisierung stattfindet (dies geschieht bereits jetzt), sondern in der Exaktheit der Ortung, die völlig neue Dienste bzw. Anwendungen ermöglicht:

- Die Standortdaten ermöglichen die automatische Benachrichtigung von Rettungs- und Pannendiensten bei Unfällen.
- Navigationshilfen erleichtern die Orientierung in fremden Städten.
- Unternehmen versenden gezielt Werbung an Personen, die sich in der Nähe ihrer Geschäfte aufhalten.
- Eltern erhalten Kenntnis von dem jeweiligen Aufenthaltsort ihrer Kinder und umgekehrt.

1.1.2 Datenschutzrechtliche Problematik von Lokalisierungstechniken

Bereits die bisherigen (verhältnismäßig ungenauen) Lokalisierungsmöglichkeiten lösen Datenschutzprobleme aus. Standortdaten, die bei der Bereitstellung und Erbringung von Telekommunikationsdiensten erhoben werden, sind Verbindungsdaten (§ 2 Nr. 4 Telekommunikations-Datenschutzverordnung – TDSV). Wenn die Daten nicht für die Erbringung eines Telekommunikationsdienstes erhoben, jedoch mittels Telekommunikation übertragen werden, handelt es sich um Inhaltsdaten. Sowohl Verbindungs- als auch Inhaltsdaten stehen unter dem Schutz des Fernmeldegeheimnisses (Art. 10 GG, § 85 Telekommunikationsgesetz – TKG). Sie dürfen für andere Zwecke nur verwendet werden, wenn dies ausdrücklich durch ein Gesetz erlaubt wird.

So dürfen Strafverfolgungsbehörden Standortdaten aus Mobilfunknetzen verwenden, um bestimmte Straftaten aufzuklären. Über Verbindungsdaten, die für Zwecke der Gebührenermittlung von Telekommunikations-Anbietern gespeichert wurden, können gemäß § 12 Fernmeldeanlagengesetz (FAG – siehe 3.5.3) auf richterliche Anordnung (bei Gefahr im Verzuge auch durch die Staatsanwaltschaft) in strafgerichtlichen Untersuchungen Auskünfte verlangt werden, wenn der Beschuldigte mutmaßlich an einem Kommunikationsvorgang beteiligt war und die Auskunft für die Untersuchung Bedeutung hat. Der Bundesgerichtshof (BGH) hat in einer kürzlichen Entscheidung festgestellt, dass Betreiber von Mobilfunknetzen sogar verpflichtet werden können, die aus den Aktivmeldungen von Handys stammenden Standortdaten aufzuzeichnen und im Rahmen von Telefonüberwachungen gem. §§ 100a, b Strafprozessordnung

(StPO) an Strafverfolgungsbehörden weiterzugeben und zwar auch dann, wenn über die mitzuteilende Funkzelle keine Verbindung abgewickelt wird (BGH Beschl. v. 21.2.2001-2 BGs 42/2001, StV 4/2001, S. 214). Auch ist es zulässig, dass Strafverfolgungsbehörden auf Grund der Befugnis gemäß § 100c StPO heimlich GPS-Empfänger an Fahrzeugen von Verdächtigen anbringen und die so gewonnenen Bewegungsdaten per Funk auslesen (BGH Urt. v. 24.1.2001 – 3StR 324/00, StV 4/2001 S. 216).

Die Einführung neuer Lokalisierungstechniken ermöglicht es, dass mobile technische Geräte – und damit auch deren Nutzer – in Zukunft noch weitaus präziser lokalisiert werden. Diese metergenauen Angaben über den Aufenthaltsort sind für die Telekommunikation selbst im Regelfall nicht erforderlich. Im Vordergrund stehen vielmehr neuartige Dienste (etwa Navigationshilfen, s.o.) und wirtschaftliche Interessen an dem Bewegungsverhalten von Nutzern (Bewegungsprofile). Standortdaten könnten auch mit anderen Informationen über die Betroffenen zusammengeführt werden, etwa mit soziographischen Daten aus den Telekommunikationsverträgen, mit Angaben über das Kaufverhalten und mit Nutzungsprofilen aus dem Internet.

Die rechtliche Einordnung der Standortdaten hängt von dem jeweiligen Dienst ab. Werden die Daten für die Erbringung eines Telekommunikationsdienstes erhoben, handelt es sich um Verbindungsdaten der Telekommunikation, die durch das Fernmeldegeheimnis geschützt werden. In den Fällen, in denen die Daten zwar durch einen Telekommunikationsdienst übertragen werden, bei denen jedoch anderweitige Nutzungsmöglichkeiten im Vordergrund stehen – etwa bei Navigationshilfen –, handelt es sich um Teledienste, für den das Teledienstedatenschutzgesetz (TDDSG) einschlägig ist. Auch diese Daten stehen unter dem Schutz des Fernmeldegeheimnisses, weil sie als Inhaltsdaten mittels Telekommunikation übertragen werden. Soweit die Daten allerdings ohne Einschaltung eines Telekommunikationsdienstes von Dritten verwendet werden (etwa durch ein Abschleppunternehmen), gelten hierfür die Bestimmungen des BDSG.

Personenbezogene Daten dürfen nur erhoben, verarbeitet oder genutzt werden, wenn der Betroffene eingewilligt hat oder wenn ein Gesetz dies vorsieht. Gemäß § 28 Abs. 1 Satz 1 Nrn. 1 und 2 BDSG dürfen Daten durch nicht-öffentliche Stellen nur erhoben, verarbeitet und genutzt werden, wenn es der Zweckbestimmung eines Vertragsverhältnisses dient oder soweit zur Wahrung sonstiger überwiegender Interessen der verantwortlichen Stelle erforderlich ist. Nutzungsdaten von Telediensten dürfen gemäß § 6 Abs. 1 TDDSG nur erhoben oder verwendet werden, soweit dies erforderlich ist, um die Inanspruchnahme von Diensten zu ermöglichen oder diese abzurechnen. Die präzisen Standortdaten dürfen dem entsprechend nur dann generiert werden, wenn der Nutzer einen Dienst, der eine präzise Lokalisierung voraussetzt, in Anspruch nehmen will. Die genaue Ortung des Nutzers bzw. des mobilen Geräts „auf Vorrat“ ist unzulässig.

1.1.3 Gewährleistung des Datenschutzes

Aus Datenschutzsicht müssen wegen der erheblichen Überwachungsmöglichkeiten durch neue Ortungstechniken die folgenden Prinzipien beachtet werden:

- **Datenvermeidung/Datensparsamkeit:** Die Gestaltung und die Auswahl von technischen Verfahren zur Lokalisierung von mobilen Geräten müssen sich daran orientieren, dass so wenig personenbezogene Daten wie möglich erhoben, verarbeitet und genutzt werden. Dies bedeutet in erster Linie, dass präzise Lokalisierungsdaten nur dann generiert werden, wenn der Nutzer einen entsprechenden Dienst in Anspruch nehmen will. Anbieter von Mobilfunkdiensten sollten Ortungsdaten nicht zusammen mit persönlichen Identifikationsdaten (z.B. Name des Nutzers, Mobilfunknummer oder Seriennummer des Geräts) an Dritte übermitteln. So weit wie möglich sollten Mehrwertdienste (etwa Navigationshilfen) anonym erbracht oder zumindest Pseudonyme verwendet werden.

- **Vertraulichkeit:** Standort- und Bewegungsdaten sind hochsensibel. Durch gesetzliche Vorschriften sollte ihr Schutz auf dasselbe Niveau gehoben werden wie der Schutz von Inhaltsdaten der Telekommunikation, etwa durch ausdrückliche Aufnahme der Standortdaten in das Fernmeldegeheimnis.

- **Transparenz:** Die Nutzer müssen darüber informiert werden, ob und in welcher Weise sie bei der Nutzung oder durch das Mitführen mobiler Geräte lokalisiert werden können und wie die Standortdaten verwendet, insbesondere an wen sie für welchen Zweck übermittelt werden. Das Auskunftsrecht des Betroffenen über seine personenbezogenen Daten muss sich auch auf alle Standortdaten beziehen und durch den Betroffenen auch ohne Medienbruch (ggf. von seinem mobilen Gerät aus) ausgeübt werden können.

- **Selbstbestimmung:** Eine präzise Lokalisierung und die Übermittlung an Anbieter zusätzlicher Dienstleistungen (z. B. Navigationshilfen, Pannendienste) sollte nur mit ausdrücklicher Einwilligung des Nutzers erfolgen. Der Nutzer muss die Möglichkeit haben, den Umgang mit seinen Standortdaten effektiv zu kontrollieren. Deshalb sind Lösungen, bei denen die personenbezogenen Standortdaten dezentral auf Grund einer besonderen Anforderung der Nutzer generiert werden, besser als netzwerkbezogene Lösungen, bei denen die Nutzer lediglich darüber entscheiden können, wie die Daten verwendet und an Dritte übermittelt werden. Die Nutzer müssen in der Lage sein, die präzise Lokalisierungsfunktion jederzeit zu deaktivieren und den Präzisionsgrad der Übermittlung ihrer Standortinformationen (z. B. Gebäude, Straße, Ort) zu steuern. Mobilfunkanbieter dürfen den Vertragsabschluss mit dem Nutzer nicht davon abhängig machen, dass die Nutzer in die Generierung und Verwendung genauer Ortungsdaten einwilligen, soweit diese Daten für den jeweiligen Dienst nicht erforderlich sind (Koppelungsverbot).

– **Keine Bewegungsprofile:** Die Erzeugung von Bewegungsprofilen sollte gesetzlich verboten werden, soweit nicht der Betroffene hierin ausdrücklich eingewilligt hat. Die Möglichkeit der Nutzung von Diensten darf nicht von der Einwilligung in Bewegungsprofile abhängig gemacht werden.

1.2 Wie verhalte ich mich? – Videoüberwachung

Frau Mustermann muss heute nach der Arbeit noch einkaufen. Um unnötige Wartezeiten zu vermeiden, sieht sie sich von ihrem Arbeitsplatz die ins Internet übertragenen Webcam-Aufnahmen von der Lebensmittelabteilung des Kaufhauses an. Da es dort gerade nicht so voll zu sein scheint, verlässt Frau Mustermann ihren Arbeitsplatz, winkt vor der Tür zum Abschied in die Kamera, mit der der Pförtner den Außenbereich des Gebäudes und den Parkplatz überwacht, und eilt zum Kaufhaus. An vielen Stellen im Kaufhaus hängen Videokameras. Nach dem Einkauf fährt Frau Mustermann mit öffentlichen Verkehrsmitteln nach Hause. Da sie vor kurzem Zeuge einer Schlägerei in der U-Bahn wurde, achtet sie darauf, dass sie in einen videoüberwachten Wagen steigt, weil sie sich dort sicherer fühlt. Im Bus setzt sie sich in den hinteren Teil. Der Busfahrer erkennt auf dem Monitor, was hinten im Wagen vor sich geht. Auf dem Spielplatz vor ihrem Haus sieht Frau Mustermann ihre Tochter in der Sandkiste, begrüßt sie und plaudert kurz mit der Nachbarin. Da der Spielplatz videoüberwacht ist, hat ihr Mann auf der hauseigenen Videoanlage alles im Blick. Die Haustür öffnet sich automatisch, nachdem Frau Mustermann in die darüber angebrachte Kamera gesehen hat. Nach ihrem anstrengenden Tag entspannt sie sich abends bei der Fernsehsendung „Big Brother“.

1.2.1 Videoüberwachung in der Praxis

Die Beobachtung öffentlicher und öffentlich zugänglicher privater Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist ein fester Bestandteil unseres täglichen Lebens geworden. Dabei wird die Erforderlichkeit der Überwachung im Einzelfall häufig gar nicht mehr näher geprüft.

Videoüberwachungen erfolgen in Kaufhäusern, öffentlichen Verkehrsmitteln, Banken, auf Tankstellen, Bahnhöfen und Flugplätzen sowie in Unternehmen und Behörden. Im Sicherheitsgewerbe wird Videoüberwachung zur sogenannten „Außenhautüberwachung“ genutzt, um Einbrüche zu erkennen bzw. aufzuklären. Alten- und Pflegeheime und Krankenhäuser werden videoüberwacht. In Schwimmbädern reicht die Überwachung bis in die Umkleidekabinen. Die Polizei und Verkehrsgesellschaften setzen Videoüberwachung zu Zwecken der Verkehrsüberwachung und -lenkung ein. Web-Cams, die Bilder ins Internet übertragen, werden bei Kunstausstellungen, in Diskotheken und vor Touristenattraktionen installiert. Fernseh- und Internetshows mit Livebildern ziehen ein großes Publikum an.

Um der Kriminalität vorzubeugen und das Sicherheitsgefühl der Passanten zu stärken, wird der Ruf nach Videoüberwachung auf öffentlichen Plätzen und in Einkaufszonen durch Medien und von politischer Seite immer lauter. Einige Bundesländer haben mittlerweile Vorschriften zum Einsatz von Videotechnik insbesondere zur Videoüberwachung sogenannter Kriminalitätsschwerpunkte erlassen. In Großbritannien sind aus diesen Gründen bereits mehrere Millionen Kameras im Einsatz; viele Innenstädte sind dort flächendeckend videoüberwacht, ohne dass die Wirksamkeit der Überwachung im Hinblick auf die angestrebten Ziele jeweils überprüft wird.

Die Videotechnik entwickelt sich rasant und bietet immer neue Einsatzmöglichkeiten. Während bis vor kurzem Videokameras groß und daher auffällig waren, sind mittlerweile neuartige kleine und unauffällige Geräte im Einsatz. Sogenannte „Dome-Kameras“ sind voll schwenkbare Kameras, die eine starke Zoomfunktion haben und noch auf hundert Meter Details erkennen lassen. Da sie in ihrer äußerlichen Gestalt Deckenlampen ähneln, weil sie unter Glaskuppeln verborgen sind, werden sie kaum als Kameras wahrgenommen.

Videokameras werden zudem verstärkt mit technischen Zusatzverfahren ausgerüstet. Die Koppelung mit biometrischen Verfahren führt z.B. dazu, dass die Speicherung von Aufnahmen erst dann begonnen wird, wenn die Anlage bestimmte Körperbewegungen oder Gesichtbilder registriert (siehe 1.4.2 und 1.4.3). Die so gewonnenen Daten können mit Bilddatenbanken abgeglichen werden, was zu weiteren datenschutzrechtlichen Problemen führt.

Als Gründe für die Videoüberwachung im öffentlichen Bereich werden vor allem Sicherheitsaspekte angeführt. Die polizeiliche Videoüberwachung soll hier entweder der „vorbeugenden Bekämpfung künftiger Straftaten“ oder in Einzelfällen der Aufklärung begangener Straftaten dienen. Im privaten Bereich spielt daneben die Wahrnehmung des Hausrechts eine Rolle. Webcam-Aufnahmen im Internet werden von Unternehmen als Service für die Kunden angeboten und haben daneben auch Werbecharakter. Auch wenn Videoüberwachungen in vielen Fällen zweckdienlich und sinnvoll sein können, führt der verstärkte Einsatz von Videotechnik zu einer Reihe von datenschutzrechtlichen Problemen.

1.2.2 Datenschutzrechtliche Probleme

Im Vordergrund steht die Bedrohung des Persönlichkeitsrechts des Einzelnen durch eine flächendeckende Überwachung, die keinen Lebensbereich ausspart und zu einer lückenlosen Kontrolle sowohl durch öffentliche als auch private Stellen führt. Neben diesem Risiko der Totalüberwachung steht das Risiko eines Autonomieverlustes des Betroffenen. Das Gefühl, möglicherweise oder tatsächlich beobachtet zu werden, verunsichert und schränkt subjektiv

die Verhaltensalternativen ein. Die Gefahr, dass der Betroffene nicht weiß, wer wann was über ihn durch Videobeobachtung erfahren hat, und sein Verhalten auf eine ständige Beobachtung einstellt, besteht auch bei einer nur teilweisen tatsächlichen Überwachung. Das Gefühl des „Überwachtwerdens“ verstärkt sich mit der Miniaturisierung und Leistungssteigerung der Aufnahmetechnik und der daraus resultierenden Unsicherheit darüber, ob ein bestimmter Ort elektronisch beobachtet wird.

Wesentlich größer als bei der bloßen Videobeobachtung sind die Risiken für die informationelle Selbstbestimmung, wenn die Videoaufnahmen aufgezeichnet werden, da Videoaufzeichnungen auch zweckentfremdet und missbräuchlich verwendet werden können. Die Datenschutzbeauftragten des Bundes und der Länder sowie die Datenschutzaufsichtsbehörden haben wegen der Gefahren für das informationelle Selbstbestimmungsrecht Regelungen für den Einsatz von Videoüberwachung gefordert, die die Interessen angemessen ausgleichen und zu einer restriktiven Verwendungspraxis dieser Technik führen. Diese Forderungen hat der Bundesgesetzgeber nun aufgegriffen und in der neuen Vorschrift § 6 b BDSG zur Videoüberwachung umgesetzt.

1.2.3 Gesetzliche Regelung der Videoüberwachung

§ 6 b Bundesdatenschutzgesetz

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie

1. zur Aufgabenerfüllung öffentlicher Stellen,
2. zur Wahrnehmung des Hausrechts oder
3. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke

erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

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

(3) Die Verarbeitung oder Nutzung von nach Abs. 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Für einen anderen Zweck dürfen sie nur verarbeitet oder genutzt werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über eine Verarbeitung oder Nutzung entsprechend §§ 19a und 33 zu benachrichtigen.

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

Diese Vorschrift soll den Gefahren einer ausufernden Videoüberwachung begegnen. Da bereits eine reine Beobachtung (ohne Aufzeichnung) Risiken eines Autonomieverlustes und der Totalüberwachung für den Betroffenen birgt, hat der Gesetzgeber die Beobachtung mittels Videotechnik als Videoüberwachung definiert und in den Anwendungsbereich des BDSG gestellt. Diese Beobachtung ist künftig nur in den gesetzlich geregelten Fällen unter Beachtung einer strikten Zweckbindung und Einhaltung des Erforderlichkeitsgrundsatzes möglich (§ 6b Abs. 1). Auch die weitere Verarbeitung oder Nutzung der durch eine Videoüberwachung erhobenen Daten muss erforderlich sein und ist zweckgebunden (§ 6b Abs. 3).

In jedem Einzelfall einer Videoüberwachung und einer anschließenden Verarbeitung oder Nutzung der erhobenen Daten schreibt die gesetzliche Regelung eine Abwägung mit den schutzwürdigen Interessen der Betroffenen vor. Dies setzt eine umfassende Güter- und Interessenabwägung unter Beachtung der rechtlich geschützten Positionen sämtlicher Beteiligten unter Würdigung der Umstände des Einzelfalls voraus. Im Rahmen dieser Abwägung wird u.a. zu berücksichtigen sein, wie oft der überwachte Raum von den Betroffenen aufgesucht wird bzw. aufgesucht werden muss oder um welche Art von Räumlichkeit es sich handelt. Eine dauerhafte, wiederholte und ständige Videoüberwachung, der sich ein Betroffener nicht entziehen kann, greift stärker in das allgemeine Persönlichkeitsrecht ein als eine nur punktuelle und gelegentliche Überwachung und kann nur in wenigen Ausnahmefällen, z.B. im überwiegenden öffentlichen Interesse, zulässig sein.

Bei der Prüfung sind – im Sinne von Datenvermeidung und -sparsamkeit (§ 3a BDSG) – auch Alternativen einzubeziehen, die ohne Videoüberwachung und -aufzeichnung auskommen. So kann die Ausstattung einer U-Bahnhaltestelle mit Personal eine dauernde zentrale Videoüberwachung überflüssig machen. Bauliche Veränderungen und gute Beleuchtung können das subjektive Sicherheitsgefühl und die objektive Sicherheit ggf. stärker verbessern als die Installation einer Videokamera.

Die schutzwürdigen Interessen der Betroffenen sind auch bei der Videoüberwachung in öffentlichen Verkehrsmitteln zu berücksichtigen. Auch wenn eine Videoüberwachung aus Sicht des Betreibers erforderlich erscheint, z.B. aus

Sicherheitsaspekten oder zur Abwehr von Vandalismus, können die schutzwürdigen Interessen der Betroffenen die Einrichtung einer nicht überwachten Zone (z. B. einzelner U-Bahnwagen ohne Videokameras) notwendig machen.

Schutzwürdige Interessen der Betroffenen sind dann in besonderer Weise berührt, wenn die durch Videoüberwachung erzielten Aufnahmen weiter verarbeitet werden oder durch automatisierte Verfahren beispielsweise zum Vergrößern oder Herausfiltern einzelner Personen, zur biometrischen Erkennung, zum Bildabgleich oder zur Profilerstellung genutzt werden. Da derartige Maßnahmen in gravierender Weise in das informationelle Selbstbestimmungsrecht eingreifen, kommt der Einsatz automatisierter Systeme zur Erkennung von Personen nach erfolgter Videoüberwachung nur in Ausnahmefällen in Betracht.

Der Forderung der Datenschutzbeauftragten, dass es grundsätzlich keine heimlichen Videoüberwachungen geben darf, hat der Bundesgesetzgeber dadurch entsprochen, dass künftig der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen ist. Dies kann durch entsprechende schriftliche Hinweise oder Piktogramme geschehen (§ 6 b Abs. 2).

Zur Verhinderung einer missbräuchlichen Nutzung hat der Gesetzgeber zudem festgelegt, dass durch Videoüberwachung erhobene Daten unverzüglich zu löschen sind, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind (§ 6b Abs. 5).

Es bleibt abzuwarten, ob die Regelung insgesamt geeignet ist, zu einer restriktiveren Verwendung der Videoüberwachung beizutragen, und ob sie den durch die Videoüberwachung aufgezeigten Gefahren wirksam begegnen kann. Im Hinblick auf die Alltäglichkeit des Einsatzes von Videotechnik sollten sich Betroffene nicht scheuen, die jeweils verantwortlichen Stellen nach Sinn und Zweck der Überwachung und nach dem Umfang von Aufzeichnungen zu fragen.

1.3 Wie erkennt man mich? – Biometrie

Frau Mustermann hat heute einen wichtigen Termin bei einem Firmenkunden in Süddeutschland. Bevor sie zum Flughafen fährt, loggt sie sich nochmals von Zuhause im Netzwerk ihrer Firma ein, um einige aktuelle Informationen abzurufen. Statt wie früher ein Passwort eingeben zu müssen, genügt es mittlerweile, den Zeigefinger auf ein Sensorfeld der Maus zu legen, um sich als Mitarbeiterin auszuweisen. Am Flughafen hat Frau Mustermann noch etwas Zeit und kontrolliert bei einem Bankautomaten ihren Kontostand. Da ihre Bank flächendeckend auf Systeme mit Iriserkennung umgestellt hat, hat Frau Mustermann ihre PIN (Persönliche Identifi-

kationsnummer), die sie sich sowieso nur schwer hatte merken können, endgültig vergessen. Während sie auf dem Weg zum Flugzeug die Personenschleuse durchschreitet, wird mit Hilfe eines Systems zur automatischen Gesichtserkennung in Echtzeit überprüft, ob sie sich auf einer internationalen Fahndungsliste befindet. Frau Mustermann hat sich weder etwas zu Schulden kommen lassen noch ähnelt sie einer der gesuchten Personen und kann daher unbehelligt passieren.

1.3.1 Biometrische Verfahren

Biometrische Verfahren erfassen spezifische Eigenschaften oder Fähigkeiten von Personen mit dem Ziel, sie auf diese Weise möglichst eindeutig – positiv oder negativ – zu identifizieren. Dabei werden Merkmale zur Auswertung herangezogen, die weitgehend unlösbar mit der Person verknüpft sind und daher weder willentlich noch aus Versehen auf einen Anderen übertragen werden können. Durch diese enge Verknüpfung kann im Idealfall eine höhere Sicherheit als durch herkömmliche, an Wissen (Passwörter, PIN) oder Besitz (Ausweiskarten) gebundene Authentisierungsmechanismen erzielt werden.

Hinsichtlich der Aufgabenstellung biometrischer Systeme wird zwischen der Identifikation, d.h. der Zuordnung einer Person zu einer bestimmten Gruppe mit z.B. gewissen Zugangsrechten und der Verifikation, d.h. der eindeutigen Erkennung einer bestimmten Person unterschieden. Diese unterschiedlichen Anforderungen führen zu verschiedenen technischen Lösungsmöglichkeiten und datenschutzrechtlichen Folgen.

Nach dem heutigen Stand der Technik sind folgende biometrische Verfahren (mit unterschiedlichem Grad der Entwicklung und Marktreife) unterscheidbar:

Körpermerkmale

- Fingererkennung (optische/kapazitive Analyse des Fingerabdrucks)
- Iriserkennung (optische Analyse des Augengewebes)
- Gesichtserkennung (optische Analyse spezifischer Gesichtsregionen)
- andere Körpermerkmale (Ohrgeometrie, Geruch, DNA)

Verhaltensmerkmale

- Tastenanschläge (Rhythmus und Geschwindigkeit von Anschlägen auf der Tastatur)
- Schrifterkennung (Geometrie und Dynamik des Schreibverhaltens)
- Stimme (verschiedene Merkmale vorgegebener oder frei gesprochener Texte)
- Bewegung (Gang, Mimik, Gestik)

Diese verschiedenen Merkmale führen zu sehr unterschiedlichen Systemen hinsichtlich Qualität, Benutzungsfreundlichkeit, Akzeptanz, Transparenz und nicht zuletzt Datenschutz. Doch auch wenn aus bestimmten Gründen in einem Anwendungszusammenhang nur ein bestimmtes biometrisches Merkmal in Frage kommt, sind die Systeme zu dessen Erfassung und Auswertung – auch im Hinblick auf den Datenschutz – weitgehend gestaltbar.

1.3.2 Biometrie in der Praxis

Noch befinden sich biometrische Systeme vielfach in der Phase der Entwicklung und Erprobung. Die Durchdringung des Massenmarkts scheitert bislang häufig an einer Kombination aus mangelnder technischer Reife, fehlender Akzeptanz und hohem Preis. Gleichwohl sind eine Reihe von Systemen bereits im Einsatz, von denen hier einige genannt werden:

- Für PC sind im Einzelhandel in die Tastatur oder die Maus integrierte Fingerabdrucksysteme verfügbar, die eine Authentisierung (d. h. die eindeutige Identifizierung des Nutzers) sowohl gegenüber dem Betriebssystem als auch gegenüber Anwendungssoftware unterstützen. Die Eingabe von Kennwörtern wird dadurch entbehrlich siehe 3.2.4.
- Einige größere Firmen verwenden seit längerem Systeme auf Grundlage von Fingerabdrücken zur Zugangskontrolle an Türschleusen.
- Eine Reihe von Banken arbeiten mit Zugangssystemen auf Grundlage optischer Gesichtserkennung für sicherheitskritische Bereiche.
- Eine auf Stimmerkennung des Fahrers basierende elektronische Wegfahrsperre für PKW ist seit einiger Zeit am Markt erhältlich.
- Im Rahmen des vom Bundeswirtschaftministerium geförderten Forschungsprojekts „BioTrusT“ werden biometrische Verfahren im Bankwesen, insbesondere an Geldausgabeautomaten, entwickelt und erprobt.
- In einigen Staaten werden biometrische Merkmale (insbesondere Fingerabdrücke) bei Ausweisdokumenten verwendet. Zur Situation hier zu Lande siehe 6.1

1.3.3 Datenschutzrechtliche Probleme

Sowohl die Art der verwendeten Daten als auch die Form ihrer Verwendung lassen eine Reihe datenschutzrechtlicher Problemfelder biometrischer Verfahren erkennen.

Problemfeld überschießende Information

Um im Ergebnis zu einer einfachen Ja-Nein-Entscheidung zu kommen („Handelt es sich um Person X?“) werden bei der Biometrie vergleichsweise große Datenmengen erhoben, die neben dem Rückschluss auf die Identität unter Umständen eine Vielzahl anderer Auswertungsmöglichkeiten eröffnen, z.B.

- Körpermaße und Körperzustand (insbes. Gesicht und Finger)

– Anzeichen akuter Krankheit oder genetischer Dispositionen (insbes. Gesicht und Finger)
– Rückschlüsse auf Stimmungslage und andere psychologische Faktoren (insbes. Stimme und Bewegung)

Auch in Fällen, in denen die Identität für sich genommen ein vergleichsweise harmloses Datum darstellt, tangiert die Biometrie insofern immer auch datenschutzrechtlich hochsensible Bereiche. Erschwerend kommt hinzu, dass einmal erfasste Merkmale (z.B. Fingerabdrücke) durch zukünftige Erkenntnisse etwa im Bereich der Genetik erst nach Einführung eines biometrischen Verfahrens in diesem Sinne relevant werden können. Eine datenschutzgerechte Gestaltung bedeutet hier daher, die Nutzbarkeit solch überschießender Information möglichst prinzipiell zu unterbinden.

Problemfeld Zweckdurchbrechung

Insbesondere bei Verfahren auf Grundlage der Fingererkennung liegt der Gedanke an ähnliche Praktiken im polizeilichen und asylbehördlichen Bereich nahe. Gerade der Abgleich mit dort vorliegenden AFIS-Dateien (Automatisches Fingerabdruck-Identifizierungs-System) stellt ein besonderes datenschutzrechtliches Problemfeld dar. Werden im Zuge biometrischer Verfahren große Datenbestände angelegt und insbesondere zentral gespeichert, sind entsprechende Begehrlichkeiten nahezu zwangsläufig. Gerade dort, wo die Zielsetzung (Identitätsfeststellung) vergleichbar ist und das selbe biometrische Merkmal verwendet wird, sind die Risiken am größten.

Aus Datenschutzsicht sind daher solche Systeme vorzuziehen, die bereits aus prinzipiellen Gründen voneinander isoliert sind und insofern einer Zweckdurchbrechung entgegenwirken.

Problemfeld Dauerkontrolle

Bereits die Verwendung kombinierbarer Techniken im Bereich der Biometrie und bei der Videoüberwachung lässt Parallelen erkennen. Eine Kamera, die am Eingang eines Gebäudes der biometrischen Gesichtserkennung dient, kann auch der Überwachung des Eingangsbereichs dienen und dabei womöglich bereits zwischen bekannten und unbekannten Personen unterscheiden. Eine solche Technik kann problemlos rund um die Uhr betrieben werden.

Zumindest dort, wo biometrische Zugangsverfahren gegen traditionelle (z.B. mechanische Schlüssel) getauscht werden, ergeben sich neue Möglichkeiten der automatisierten Erfassung von Anwesenheiten etc. Dies ist zwar kein Merkmal, das biometrische von anderen automatisierten Zugangsverfahren (etwa mit Chipkarte oder Kennwort) unterscheidet; allerdings kann aufgrund der leichten Bedienbarkeit biometrischer Verfahren eine deutliche Ausweitung automatisierter gegenüber nicht-elektronischen Systemen und damit zusätzlicher personenbezogener Datenverarbeitung erwartet werden.

1.3.4 Datenschutzgerechte Biometrie

Das Prinzip der Datenvermeidung bzw. -sparsamkeit (§ 3a BDSG) muss auch bei der Biometrie konsequent umgesetzt werden. Bereits bei der Systemgestaltung und -auswahl sind Systeme zu favorisieren, die ohne bzw. mit wenigen personenbezogenen Daten auskommen. Ggf. muss auf den Einsatz biometrischer Systeme verzichtet werden, wenn der Zweck (etwa Zugangskontrolle) ohne oder mit weniger personenbezogenen Daten erreicht werden kann.

Aus den genannten Problemfeldern sowie allgemeinen datenschutzrechtlichen Überlegungen lassen sich eine Reihe von Forderungen an biometrische Systeme aufstellen.

- Daten über die Nutzung von biometrischen Systemen sind nur im erforderlichen Umfang zu erheben und zu nutzen. Bereits in der Konzeptions- und Planungsphase müssen ggf. alternative Lösungsmöglichkeiten untersucht und hinsichtlich ihrer Datenschutzfreundlichkeit bewertet werden.

- Biometrische Rohdaten (Finger- und Gesichtsbilder, Stimmaufzeichnungen etc.) sind möglichst frühzeitig im Verarbeitungsprozess auf diejenigen Merkmale zu reduzieren, die für den Identifikationszweck erforderlich sind. Eine dauerhafte Speicherung der Rohdaten ist zu vermeiden. Die Daten sind zu löschen, wenn der Erhebungszweck erreicht wurde (z.B. nach erfolgreicher Identifizierung).

- Die dezentrale Speicherung von Referenzdaten (z.B. auf einer Chipkarte in der Verfügungsgewalt des Benutzers) ist einer zentralen Speicherung in der Regel vorzuziehen, weil auf diese Weise eine unberechtigte Auswertung der Daten ohne Kenntnis des Betroffenen deutlich erschwert wird.

- Biometrische Daten sind sicher, d.h. gegen unbefugten Zugriff geschützt, zu speichern und zu übertragen.

- Die biometrischen Systeme sind so zu gestalten, dass sie möglichst überwindungssicher sind. Insbesondere wenn eine Falscherkennung mit nachteiligen Folgen für den Benutzer oder Dritte verbunden ist, sollte die Erkennungsqualität möglichst hoch sein.

- Die Kombination von biometrischen Verfahren mit anderen Überwachungsmechanismen (etwa Videoüberwachung) muss im Regelfall unterbleiben.

- Eine zweckfremde Nutzung biometrischer Daten ist grundsätzlich unzulässig. Sollen die Daten ausnahmsweise für einen anderen Zweck verwendet werden, ist dies nur auf Grund einer ausdrücklichen gesetzlichen Erlaubnis zulässig. Die Zweckbindung ist durch geeignete technische und organisatorische Maßnahmen abzusichern.

– Transparenz für den Nutzer stellt ein wichtiges Gebot dar. Dies betrifft zum einen die Systeme und die dort implementierten Verfahren und Sicherheitsvorkehrungen. Zum anderen bedeutet dies, dass für den Nutzer erkennbar sein muss, wann und durch wen eine Datenerhebung und Identitätsfeststellung erfolgt und was mit den Daten weiter geschieht.

– Die Einführung biometrischer Verfahren darf nicht zu einer Diskriminierung führen. Nicht alle Menschen verfügen über die körperlichen Fähigkeiten bzw. Eigenschaften, die die Biometrie voraussetzt. Es gibt Menschen ohne ausgeprägte Fingerabdrücke, ohne Iris, ohne Stimme oder auch Analphabeten. Solche Personen dürfen datenschutzrechtlich nicht benachteiligt werden, indem sie etwa einer besonderen Kontrolle ausgesetzt werden oder durch häufige Fehlerkennungen auffällig werden.

1.4 Wer bin ich? – Genom-Kontrolle – die Zukunft hat begonnen

Herr Mustermann hat einen Verdacht: Woher hat sein Sohn die schwarzen Haare? War seine Frau Erika untreu? Im Internet findet er, was er sucht: Das Labor Gen-Diagnose GmbH (Name geändert) bietet für 790 DM incl. MWSt. einen DNA-Vaterschaftstest an, um sog. Kuckuckskinder herauszufinden. Es ist nicht schwer, den Schnuller des Kleinen verschwinden zu lassen, bei sich eine Speichelprobe zu entnehmen – und ab zum Labor. Das Ergebnis: Vertrauen war gut, Kontrolle war besser: Erika ist überführt: Die DNA des Kleinen und von Herrn Mustermann passen nicht zusammen.

Herr Mustermann ist Betriebsrat. Mit einem anonymen Brief an seinen Arbeitgeber beschwert er sich über einen Vorgesetzten. Der Arbeitgeber verdächtigt Herrn Mustermann der Anschwärzung. Er lädt ihn zu einer Besprechung in anderer Sache ein. An der Kaffeetasse hinterlässt Herr Mustermann Speichelreste. Tasse und Klebefalz des Beschwerdebriefes schickt der Arbeitgeber an ein Genlabor. Dieses bestätigt: Die Proben stammen von derselben Person. Herrn Mustermann wird gekündigt.

1.4.1 Die DNA als Kontroll-Material

Es gibt wohl kaum etwas Persönlicheres als die eigenen Erbinformationen. Die Säurekette DNS (oder englisch DNA), die in jeder Körperzelle auf den 23 Chromosomenpaaren „aufgewickelt“ ist, enthält in einer Abfolge von 3 Milliarden „Buchstabenpaaren“ ca. 30.000 Gene und dazwischen „nicht codierende“ Buchstaben-Sequenzen. Die Struktur der DNS und die Abfolge der Buchstaben wurden im Jahre 2000 entschlüsselt. Wieviel und welche Gene es gibt,

wie sie zusammengesetzt sind, welche Funktionen sie haben, wie und wann sie „aktiviert“ werden, kann dagegen nur in wenigen Einzelfällen beantwortet werden.

Von Mensch zu Mensch weichen die Gene, die zusammen das Genom bilden, nur in etwa jedem 1000. Buchstabenpaar voneinander ab. Mutationen, „Gendefekte“, können dazu führen, dass die betroffene Person eine erhöhte Krankheitsanfälligkeit hat. Einige Hundert solcher Krankheitsanlagen wurden inzwischen entdeckt. Weitgehend unklar ist, welche Persönlichkeitsmerkmale in welchem Ausmaß durch Gene vorgeprägt sind.

Die Genforschung arbeitet jedoch mit Hochdruck an der weiteren Entschlüsselung des menschlichen Genoms. Immer neue Erkenntnisse zu erblich bedingten Krankheiten, Merkmalen und Eigenschaften stehen der Menschheit ins Haus.

Wie beim kürzlich gefundenen sog. Brustkrebs-Gen und dem Alzheimer-Gen bedeutet das Vorliegen der entsprechenden DNS-Besonderheit jedoch in aller Regel nur eine erhöhte Anfälligkeit. Die Aussagekraft entsprechender Gentests ist damit relativ gering. Umwelteinflüsse, Ernährung und Lebensweise haben meist einen mindestens ebenso großen Einfluss darauf, ob die Erbanlage tatsächlich zum Ausbruch der Krankheit führt oder nicht.

Anders ist dies bei den „nicht-codierenden“ DNS-Sequenzen, die nach bisherigen Erkenntnissen keine Gene bilden, aber bei jedem Menschen einmalig sind. Ihre Zusammensetzung ist aus der DNS der Eltern ableitbar. Solche DNS-Identifikationsmuster sind als „genetische Fingerabdrücke“ sowohl zur Klärung der Abstammung als auch zur Zuordnung von Spuren humanbiologischer Substanzen geeignet.

Die Analysen der DNS werden heute weitgehend elektronisch unterstützt. Ohne die Informationstechnik sind Gentests – jedenfalls in größerer Zahl – nicht denkbar. Eine neue Stufe in der Verschmelzung von Gentechnik und Informationstechnik bedeutet die Erfindung des sog. Gen-Chips: Wenige Quadratzentimeter große Platten mit mehreren tausend kleinsten Vertiefungen werden mit unterschiedlichen DNS-Sequenzen „beladen“, die mit einer fluoreszierenden Farbe gekennzeichnet sind. Zu diesen werden ebenfalls farblich gekennzeichnete Teile der Proben-DNS hinzugegeben. Die entstehenden Mischfarben, die den Grad der Übereinstimmung zwischen Standard-DNS und Proben-DNS offenbaren, werden elektronisch dargestellt und unmittelbar digital gespeichert. Damit können Genanalysen einerseits erheblich beschleunigt, andererseits auf viele gleichzeitige Untersuchungen ausgeweitet und drittens direkt elektronisch weiterverarbeitet werden. Noch ist der Gen-Chip der Grundlagen- und der Arzneimittelforschung („Pharmakogenetik“) vorbehalten. Sein Einsatz in der Transplantationsmedizin und der pränatalen Diagnostik ist jedoch bereits angekündigt.

1.4.2 Kontroll-Interessen

Die Struktur der DNS mit codierenden Sequenzen (Gene) und nicht-codierenden Sequenzen („genetischer Fingerabdruck“) eröffnet ganz verschiedenen Interessen und Interessenten Kontrollmöglichkeiten:

Die Strafverfolgungsbehörden haben die DNS-Analyse schon seit einigen Jahren in ihr kriminaltechnisches Instrumentarium aufgenommen. Der genetische Fingerabdruck hat einige Straftäter überführt, viele andere Personen vom Verdacht entlastet. Die Strafprozessordnung (StPO) regelt das dafür vorgesehene rechtsstaatliche Verfahren. Höchst problematisch ist jedoch der psycho-soziale Druck, der dann entsteht, wenn zur Aufklärung einer Straftat große Personengruppen mit bestimmten Merkmalen um einen „freiwilligen“ DNS-Test gebeten werden. Wer sich dagegen wehrt, macht sich verdächtig. Das Interesse, durch DNS-Test einmal ermittelte Identifikationsmuster vorsorglich elektronisch zu speichern – man kann ja nie wissen, zu welcher Kontrolle es einmal gut sein kann –, ist groß. Es muss deswegen regelmäßig überwacht werden, ob die strengen gesetzlichen Einschränkungen hinsichtlich des Personenkreises, des Analyse-Gegenstandes und der Speicherung eingehalten werden.

An der Identitätsfeststellung haben neben den Strafverfolgungsbehörden z.B. auch die Ausländerbehörden ein großes Interesse. Gegenwärtig werden allen Asylbewerbern Fingerabdrücke abgenommen, um neue Asylanträge unter falschem Namen zu verhindern. Der genetische Fingerabdruck würde es ermöglichen, die Identität eines Ausländers auch in seiner Abwesenheit – etwa anhand eines Haares oder eines Speichelrestes an einem Glas oder einer Zigarette – zu prüfen. Angesichts der Probleme mit dem „Familiennachzug“, der Höhe der Unterbringungskosten für Flüchtlinge und der Anstrengungen, die bereits heute zur Sicherung von Abschiebungen unternommen werden, liegt eine DNS-Kontrolle mit anschließender Ergebnis-Speicherung in der Ausländerakte und im Ausländerzentralregister zumindest nicht fern.

Dass Väter von sog. „Kuckuckskindern“ (siehe Kasten vor 1.4.1) ein Interesse an der Klärung ihrer Vaterschaft und damit an der Kontrolle ihrer Ehefrau haben, ist tagtägliche Erfahrung von vielen Genlabors und Familiengerichten. Die Datenschutzbeauftragten halten es rechtspolitisch für nicht vertretbar, dass sich diese heimliche Treue-Kontrolle gegenwärtig in einem rechtsfreien Raum abspielt, und fordern ein strafbewehrtes Verbot von Gentests ohne die Einwilligung der betroffenen Person. Betroffen im datenschutzrechtlichen Sinne ist hier zwar das Kind, dessen Probe untersucht wird. Einwilligen müsste jedoch auch die Mutter als Sorgeberechtigte und gesetzliche Vertreterin des Kindes.

Innerhalb der Familie bzw. vor ihrer Gründung ist nicht nur das DNS-Identifikationsmuster interessant, sondern auch das Genom: Ein skeptischer Schwiegervater in spe kann durchaus ein dringendes Interesse haben, den Speichelrest am Bierkrug daraufhin analysieren zu lassen, ob der angehende Schwiegersohn überhaupt genetisch „geeignet" ist, in sein Unternehmen einzuheiraten. Je mehr die Genforschung und Gentechnik über Erbanlagen für häufige Krankheiten und Persönlichkeitsmerkmale in Erfahrung bringen, desto größer wird das Kontrollinteresse vor einer familiären Bindung. Mag man bei zukünftigen Ehepartnern noch von einem vertrauensvollen Einverständnis bei einer (gegenseitigen) Genomanalyse ausgehen – den Schwiegereltern, weiteren Verwandten oder abgewiesenen Liebhabern muss man diese Vertrauensbindung nicht unterstellen. Man will ja nur das Beste für die Braut.

Was als Vorsorgeuntersuchung in der Schwangerschaft gilt, kann auch als heimliche Kontrolle des Nachwuchses gedeutet werden: die pränatale Diagnostik. Für den Embryo ist die Kontrolle in der Regel die Entscheidung über Leben und Tod. Je mehr Gene entschlüsselt werden, je einfacher, umfassender und kostengünstiger die Gentests mit Hilfe von Gen-Chips werden, desto größer wird für den Nachwuchs die Gefahr, dass auch Anlagen zu leichten Krankheiten oder Behinderungen, ja zu bestimmten Körper- oder sogar Persönlichkeitsmerkmalen den Tod bedeuten. Das „Designer-Baby" ist zwar noch Science Fiction, Tendenzen in diese Richtung sind jedoch unverkennbar. Die Datenschutzbeauftragten und Ethik-Beiräte haben mehrfach auf einen entsprechenden Handlungsbedarf des Gesetzgebers hingewiesen.

Außerhalb der Familie können viele Bezugs- und Kontaktpersonen eines Menschen ein Interesse daran haben, zumindest über bestimmte Erbanlagen ihres Gegenüber etwas zu erfahren. Viel diskutiert wird gegenwärtig die Frage, ob private Kranken- und Lebensversicherungen ein Recht haben, von einem Versicherungsbewerber einen Gentest zu verlangen. Diese Art der Risikokontrolle, die z.B. in Großbritannien durchaus zugestanden wird, wäre jedenfalls nicht geheim, wird aber derzeit in Deutschland auch von den Versicherern selbst nicht gefordert. Der Bundesrat forderte die Bundesregierung auf, ein entsprechendes gesetzliches Verbot vorzubereiten. Dagegen besteht nach dem geltenden Versicherungsvertragsgesetz eine Pflicht des Bewerbers, früher einmal eingeholte Gentest-Ergebnisse vorzulegen, wenn diese das Versicherungsrisiko beeinflussen.

Als besonderes Bedrohungs-Szenario kann ein „genetischer Score-Wert" der Versicherungen gelten: Entsprechend dem Ergebnis eines umfassenden Gentests erhält jeder Versicherungsbewerber bzw. Versicherte einen Risiko-Einstufungs-Wert, der dann als elektronisches Datum in branchenüblichen Warn- und Hinweissystemen abrufbar ist – elektronische Kontrolle total.

Wie das zweite eingangs dargestellte Beispiel zeigt (siehe Kasten vor 1.4.1), nutzen auch Arbeitgeber Gentests zu Kontrollzwecken. In diesem tatsächlich geschehenen Fall hat der Verwaltungsgerichtshof Mannheim die Kündigung für unwirksam erklärt. Der geheime Gentest sei ein unzulässiger Eingriff des Arbeitgebers in die Persönlichkeitsrechte des Betroffenen.

Aber auch in anderer Beziehung kann ein Arbeitgeber Interesse an genetischen Informationen über seine Beschäftigten haben. Mit der Anstellung geht er ein gewisses Risiko ein: Wird der Arbeitnehmer krank, muss der Arbeitgeber eine Zeit lang trotzdem das Entgelt zahlen. Arbeitsunfälle und Berufskrankheiten betreffen nicht nur die Unfallversicherung, sondern möglicherweise auch Kollegen oder Kunden. Bei Berufen, die eine hohe Verantwortung für Dritte mit sich bringen, wie Piloten oder Zugführer, können plötzlich ausbrechende Erbkrankheiten zu Katastrophen führen. Da liegt es nahe, Bewerber auf ihre Anfälligkeit gegenüber bestimmten Stoffen, die in dem Unternehmen verarbeitet werden, oder auf Erbanlagen für unvorhersehbar auftretende Krankheiten zu testen. Das hat zwar nichts mit der üblichen Betriebsarzt-Untersuchung auf den gegenwärtigen Gesundheitszustand zu tun, könnte den Arbeitgeber aber entlasten: Es ist einfacher, anfällige Arbeitsplatzbewerber gar nicht erst einzustellen, als den Produktionsprozess so umzugestalten, dass auch erblich bedingt empfindliche Personen keinen Schaden nehmen.

Mit den Möglichkeiten der geheimen Probennahme (die Kaffeetasse beim Bewerbungsgespräch) wächst für den Arbeitgeber die Versuchung, die Proben zu verwenden und auszuwerten.

1.4.3 Maßnahmen gegen Genom-Kontrollen

Nicht erst die eingangs dargestellten Beispielsfälle, die im Jahr 2001 die Öffentlichkeit beschäftigten, haben die Datenschutzbeauftragten auf den Plan gerufen. Bereits 1989 hatten sie in einer gemeinsamen Entschließung Schutzmaßnahmen für das Selbstbestimmungsrecht der betroffenen Personen gefordert: Außer bei Straf- und Abstammungsverfahren sollen Genomanalysen nur auf freiwilliger Basis nach umfassender Aufklärung der Betroffenen vorgenommen werden dürfen. Genomanalysen im Arbeitsverhältnis und im Versicherungswesen sollten gesetzlich verboten werden. Pränatale Untersuchungen sollten auf heilbare und besonders schwere Gesundheitsschädigungen beschränkt werden. Auch das Recht auf Nichtwissen müsse berücksichtigt werden.

Der Gesetzgeber hat seitdem in der Strafprozessordnung (§§ 81e-g) und dem DNA-Identitätsfeststellungsgesetz von 1998 die Nutzung von „genetischen Fingerabdrücken“ im Einzelnen geregelt.

Im Übrigen blieb der Gesetzgeber dagegen bislang untätig. Der Bundesrat forderte die Bundesregierung im November 2000 auf (Bundesrats-Drs.

5300/00), einen Gesetzentwurf vorzulegen, nach dem „es Versicherern verboten ist, eine Genomanalyse zur Voraussetzung des Abschlusses eines Versicherungsvertrages zu machen, (und) der Versicherer nicht berechtigt ist, nach genetischen Dispositionen zu fragen, die dem Antragsteller ... bekannt sind; Ausnahmen sollten nur unter eng begrenzten Voraussetzungen insbesondere zur Vermeidung missbräuchlicher Ausnutzung des Versicherungssystems zugelassen werden."

Sowohl der Ethik-Beirat beim Bundesgesundheitsministerium als auch die Enquete-Kommission „Recht und Ethik der modernen Medizin" des Deutschen Bundestages äußerten sich besorgt und kritisch zu Genomanalysen an heimlich entnommenen (Haar-, Speichel-) Proben. Insbesondere zu den verbreiteten Gentests beim Zweifeln an der Vaterschaft forderte auch der Bundesbeauftragte für den Datenschutz eine eindeutige Vorschrift, die heimliche Genomanalysen verbietet und unter Strafe stellt.

In einer Bund-Länder-Arbeitsgruppe unter Vorsitz des Hamburgischen Datenschutzbeauftragten wurde ein Vorschlag für eine gesetzliche Regelung zum Schutz der Selbstbestimmung bei genetischen Untersuchungen beim Menschen erarbeitet. Er greift Fragen von Gentests zu medizinischen Zwecken, zu Zwecken der Identifizierung und Abstammung, im Zusammenhang mit Arbeits- und Versicherungsverhältnissen sowie zu Forschungszwecken auf und schlägt Regelungen im Sinne möglichst weitgehender Selbstbestimmung der betroffenen Personen vor. Die Arbeitsgruppe konnte dabei auf das geltende österreichische Gentechnikgesetz und einen ausführlichen Gesetzentwurf aus der Schweiz zurückgreifen (zu den Vorschlägen der Datenschutzbeauftragten siehe unten 21.3)

Datenschutzrecht und -technik

2. Neues Datenschutzrecht

2.1 Europa- und Bundesrecht

2.1.1 Grundrechte-Charta der Europäischen Union

Das Grundrecht auf Datenschutz ist in Art. 8 der Charta erfreulich deutlich gefasst worden.

Der Europäische Rat hat am 7. Dezember 2000 die „Charta der Grundrechte der Europäischen Union" proklamiert. Nach Beteiligung der Datenschutzbeauftragten des Bundes und der Länder ist das Grundrecht auf Datenschutz zufriedenstellend formuliert worden.

Artikel 8

Schutz personenbezogener Daten

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

In Art. 8 Abs. 2 der Charta ist die Aufzählung konkreter Schutzrechte allerdings nicht abschließend gemeint. Auch Ansprüche auf Sperrung und Löschung von Daten sowie Widerspruchs- und Informationsrechte usw. können geltend gemacht werden.

Der Grundrechtsartikel für den Datenschutz ist – wie die gesamte Charta – insgesamt so formuliert, dass er ohne Wortlautänderung jederzeit rechtlich verbindlich werden kann. Für eine künftige europäische Verfassung gibt es damit bereits konkrete Grundlagen auch für ein Grundrecht auf Datenschutz.

2.1.2 EG-Datenschutzrichtlinie und Bundesdatenschutzgesetz

Zur Umsetzung der Richtlinie ist die Novellierung des Bundesdatenschutzgesetzes im Mai 2001 in Kraft getreten.

Nachdem die dreijährige Umsetzungsfrist für die EG-Datenschutzrichtlinie schon im Oktober 1998 abgelaufen war, ist das Bundesdatenschutzgesetz schließlich mit großer Verspätung verabschiedet worden. Die Bundesregierung hatte den Gesetzentwurf Mitte August 2000 eingebracht und dabei in erheblichem Umfang Anliegen der Datenschutzbeauftragten und der Aufsichtsbehörden berücksichtigt. In der Stellungnahme des Bundesrates von Ende September 2000 waren wiederum Vorschläge der Datenschutzbeauftragten und der Aufsichtsbehörden aufgegriffen worden. Nach der Gegenäußerung der Bundesregierung von Ende Oktober 2000 sind bei der Schlussberatung von Bundestag und Bundesrat Ergänzungen in das Gesetz eingefügt worden, insbesondere die Regelung zur Videoüberwachung in § 6b BDSG und eine stark überarbeitete Fassung der Bußgeld- und Strafvorschriften in §§ 43 und 44 BDSG; dabei wurden Anregungen der Datenschutzbeauftragten und Aufsichtsbehörden jedenfalls teilweise einbezogen.

Die Umsetzung der Novellierung stellt erhebliche Anforderungen an die Aufsichtsbehörden für den Datenschutz, insbesondere wegen der neu eingeführten Daueraufsicht über die Wirtschaft (siehe 2.2.1 und auch 31.). Während dessen wird bereits an der sog. 2. Stufe zur Novellierung gearbeitet, mit der eine verständliche, moderne und effektivere Fassung des Bundesdatenschutzgesetzes angestrebt wird. Die Datenschutzbeauftragten beteiligen sich auch an diesem wichtigen Vorhaben weiterhin aktiv.

2.2 Hamburgische Datenschutzvorschriften

2.2.1 Hamburgisches Datenschutzgesetz

Die Novellierung ist Ende Januar 2001 von der Bürgerschaft beschlossen worden.

Mit der Novellierung ist für die hamburgischen öffentlichen Stellen die EG-Datenschutzrichtlinie umgesetzt worden. Zugleich wurde das Gesetz an weiteren Stellen modernisiert. Die Novellierung wird von uns weitgehend begrüßt. Dazu kann im einzelnen auf die Erläuterungen zum Hamburgischen Datenschutzgesetz in der neuen Broschüre „Hamburgisches Datenschutzrecht 2001“ verwiesen werden (siehe auch 30.3).

Zusätzlich zu der bereits geregelten Risikoanalyse ist bei der Novellierung des Gesetzes die Vorabkontrolle in § 8 Abs. 4 HmbDSG eingefügt worden. Dazu haben wir Hinweise erarbeitet, die in unserem Internet-Angebot www.hamburg.datenschutz.de zur Verfügung stehen.

Zur Umsetzung der Daueraufsicht über die Wirtschaft ist das Hamburgische Datenschutzgesetz erneut Mitte Juli 2001 geändert worden. Dabei wurde zusammen mit der Bewilligung einer personellen Verstärkung der Dienststelle (siehe dazu 31.) ein § 34 HmbDSG über Verwaltungsgebühren für die neue Daueraufsicht (siehe 2.1.2) eingefügt. Demnach haben die von uns überprüften Stellen der Wirtschaft in Hamburg für die Kontrolle grundsätzlich Gebühren zu zahlen, wie dies in drei anderen Bundesländern auch schon geregelt ist. Die Gebühren sind im einzelnen in der Gebührenordnung des Senats vom 11. September 2001 festgelegt worden.

2.2.2 Bereichsspezifische Datenschutzvorschriften

Bei den neuen Rechtsvorschriften sind unsere Vorschläge vielfach aufgegriffen worden.

Die Datenschutzordnung der Hamburgischen Bürgerschaft (vgl. 17. TB, 2.2.2) wurde am 12. September 2001 geändert. Die Öffentlichkeit erhält damit über das Internet im Wege der Volltextrecherche Zugriff auf Bürgerschaftsdrucksachen und Plenarprotokolle. Datenschutzrechtlich zuständig ist in erster Linie das Datenschutzgremium der Bürgerschaft. An der Vorbereitung der Rechtsänderung waren wir beteiligt.

Der Senat hat am 26. Juni 2001 die Fünfte Verordnung zur Änderung der Wahlordnung für die Wahlen zur Bürgerschaft und zu den Bezirksversammlungen erlassen. Danach können Wahlscheine auch durch Telegramm, Telefax oder über das Internet beantragt werden. Das elektronische Verfahren zur Antragstellung wurde mit uns abgestimmt (siehe dazu 3.1.3) und fand bereits bei der Bürgerschaftswahl am 23. September 2001 Anwendung. Ferner wurden durch die Änderung der Wahlordnung die Wahlumschläge abgeschafft; Vorkehrungen gegen Beeinträchtigungen des Wahlgeheimnisses wurden getroffen.

Das Hamburgische Gesetz über Volksinitiative, Volksbegehren und Volksentscheid wurde am 6. Juni 2001 geändert. Die Volksinitiatoren sind danach verpflichtet, über die Herkunft und Verwendung der Mittel, die ihnen zum Zweck der Durchführung der Volksgesetzgebung zugeflossen sind, Rechenschaft zu legen. Den Inhalt des Rechenschaftsberichts hat der Senat durch eine am 11. September 2001 beschlossene Änderung der Volksabstimmungsverordnung festgelegt. Die inhaltliche Konkretisierung der Rechenschaftslegung geht über die dem Senat erteilte gesetzliche Verordnungsermächtigung hinaus (näher dazu unsere Kritik unter 4.1.1).

Nach dem „Gesetz zur Umsetzung von Artikel 13 Absatz 6 des Grundgesetzes“ vom 19. Juli 2000 hat der Senat die Bürgerschaft jährlich über die durchgeführten Maßnahmen zum Abhören von Wohnungen (sog. Lauschangriffe, s. 17. TB, 14.2) zu unterrichten. Die parlamentarische Kontrolle wird von einem Gremium aus sieben Mitgliedern der Bürgerschaft ausgeübt. Wir konnten durchsetzen, dass diese bürgerschaftliche Kontrolle sich nicht nur auf Lauschangriffe zu Zwecken der Gefahrenabwehr, sondern auch auf solche zu Zwecken der Strafverfolgung erstreckt (vgl. 20.3).

Die Erkenntnisse, die mit polizeilichen Personenschutzsendern beim Einsatz in Wohnungen gewonnen werden, dürfen nach dem am 19. Juli 2000 geänderten Gesetz über die Datenverarbeitung der Polizei über den Zweck des jeweiligen Einsatzes hinaus nur für die Strafverfolgung sowie zur Abwehr einer unmittelbar bevorstehenden Gefahr für Leben, Leib oder Freiheit genutzt werden. Diese Regelung halten wir für vertretbar.

Das Hamburgische Sicherheitsüberprüfungsgesetz (HmbSÜG) ist am 30. Januar 2001 geändert worden. Bei vereinfachten Sicherheitsüberprüfungen ohne Mitwirkung des Landesamtes für Verfassungsschutz (z.B. im Straf- und Maßregelvollzug sowie beim Landesamt für Informationstechnik) darf das Landeskriminalamt (LKA) Erkenntnisse aus abgeschlossenen Straf- und Ermittlungsverfahren über Vergehen nur insoweit übermitteln, als sie der Generalbundesanwalt im Wege der unbeschränkten Auskunft aus dem Bundeszentralregister mitteilen dürfte. Polizeiliche Mitteilungen über Einstellungen des Verfahrens, etwa wegen fehlenden Tatverdachts oder geringer Schuld, sind danach unzulässig, soweit ein Vergehen Gegenstand des Verfahrens war. Unsere Überprüfung im Oktober 2001 ergab, dass das LKA diese Rechtslage bei vereinfachten Sicherheitsüberprüfungen in mehreren Fällen

nicht beachtet hat. So erhielt das Strafvollzugsamt Kenntnis von einem eingestellten Verfahren wegen Beförderungserschleichung. Das Ergebnis unserer Kontrolle haben wir zum Anlass genommen, die Rechtsabteilung der Polizei um einen Hinweis an das LKA zu bitten.

Die Bürgerschaft hat am 21. November 2000 das Gesetz über das Versorgungswerk der Rechtsanwältinnen und Rechtsanwälte in der Freien und Hansestadt Hamburg (RAVersG) beschlossen. Die Auskunfts- und Mitwirkungspflichten der Leistungsberechtigten und der Hanseatischen Rechtsanwaltskammer gegenüber dem Versorgungswerk sind entsprechend unseren Anregungen begrenzt worden.

Bei der Novellierung des Hamburgischen Hochschulgesetzes vom 18. Juli 2001 haben wir insbesondere die Formulierung des § 111 beeinflusst, der die Verarbeitung von Studierenden- und Hochschullehrer-Daten regelt. So konnte eine abschließende Aufzählung der Verarbeitungszwecke erreicht und die Verordnungsermächtigung auf Regelungen über die Datenaufbewahrungsfrist und das Auskunfts- und Einsichtsrecht der Betroffenen erweitert werden.

Die Berufsordnung für Hamburger Ärztinnen und Ärzte wurde im Frühjahr 2000 von der Kammerversammlung geändert, nachdem die Behörde für Arbeit, Gesundheit und Soziales als Genehmigungsbehörde einem Kompromiss zu zwei lange diskutierten datenschutzrechtlichen Problempunkten zugestimmt hatte: Beim Praxisverkauf verzichtete sie auf die Bedenken, die wir hinsichtlich der Übergabe der Patientenkarteien ohne Patienteneinwilligung geäußert hatten. Beim Akteneinsichtsrecht der Patienten verzichtete die Ärztekammerversammlung auf die von uns kritisierte Einschränkung „ausgenommen sind diejenigen Teile (der Dokumentation), welche subjektive Eindrücke oder Wahrnehmungen des Arztes enthalten."

Das Psychotherapeutenkammergesetz vom 18. Juli 2001 ermächtigt die neu eingerichtete Kammer auch zur Verarbeitung der Daten ihrer Mitglieder. Hier konnten wir in § 4 eine Beschränkung auf bestimmte Zwecke und insbesondere eine klare Regelung zur Auskunftserteilung gegenüber anfragenden anderen Kammern erreichen. Für die Berufsordnung haben wir dafür gesorgt, dass das Recht auf Einsichtnahme der Patientinnen und Patienten in die therapeutischen Dokumentationen eingefügt wurde – ein Problem, das uns immer wieder beschäftigt.

10 Jahre nach unseren ersten Anregungen trat am 19. Juli 2001 das Gesetz über den öffentlichen Gesundheitsdienst in Hamburg in Kraft. Es enthält einen ausführlichen Abschnitt über den Datenschutz. In mehreren Stellungnahmen zu den Entwürfen konnten wir vor allem zu eindeutigen Formulierungen und mehr Normenklarheit beitragen. Insbesondere die deutlichere Trennung zwischen Beratungs- und Überwachungsaufgaben des öffentlichen Gesundheitsdienstes führte zu einer Stärkung der Datenschutzes im Beratungsbereich. Nur zum Teil durchsetzen konnten wir uns mit der Forderung, die Aus-

kunftspflicht der Bürgerinnen und Bürger bei Überwachungsaufgaben, z.B. auch umweltmedizinischen Maßnahmen, auf die Abwehr bedeutsamer Gesundheitsrisiken zu beschränken.

Durch das Sechste Gesetz zur Änderung des Hundesteuergesetzes vom 14. Juli 2000 ist die Befugnis zum Austausch personenbezogener Daten zwischen den Wirtschafts- und Ordnungsämtern der Bezirke und der Steuerbehörde geschaffen worden. Die Hundeverordnung des Senats vom 18. Juli 2000 regelt die Zuverlässigkeitsüberprüfungen bei Halterinnen und Haltern gefährlicher Hunde. Unsere Beteiligung bei der Vorbereitung der Hundeverordnung war unzulänglich. Im weiteren Verfahren wurde unseren erheblichen Bedenken gegen den Vollzug der Verordnung – insbesondere zum Umgang mit Auskünften aus dem Bundeszentralregister – Rechnung getragen.

Kurz vor Ablauf der letzten Legislaturperiode hat die Bürgerschaft das Hamburgische Gesetz über Schulen in freier Trägerschaft (HmbSfTG) vom 12. September 2001 beschlossen. Das Gesetz tritt am 1. Januar 2002 in Kraft und ersetzt das bisherige Privatschulgesetz. Mit § 3 des neuen Gesetzes wurde der Datenschutz parallel zu den §§ 98 ff. Hamburgisches Schulgesetz (HmbSG) im Bereich der freien Schulträger erstmals auf eine bereichsspezifische Grundlage gestellt. Die Regelung beschränkt sich auf den Schutz der personenbezogenen Daten im Verhältnis der Schulträger zur staatlichen Schulaufsicht. Im Verhältnis zu den Schülerinnen und Schülern, den Erziehungsberechtigten und ihren Beschäftigten sind die Schulträger an die Regelungen des Bundesdatenschutzgesetzes bzw. – soweit es sich um öffentlich-rechtliche Religionsgemeinschaften handelt – an das jeweilige kirchliche Datenschutzrecht gebunden.

2.2.3 Neue Datenschutzbestimmungen für das Presserecht

Die Vorschrift des § 41 BDSG, die die Verarbeitung und Nutzung personenbezogener Daten durch Medien regelt, ist als Rahmenvorschrift für die Landesgesetzgebung ausgestaltet worden. Auch in Hamburg ergibt sich deshalb die Notwendigkeit, zügig Datenschutzregelungen für die Presse zu formulieren, die den Schutz personenbezogener Daten gewährleisten, ohne die Pressefreiheit (Art. 5 GG) unangemessen einzuschränken.

§ 41 Abs. 1 BDSG

Die Länder haben in ihrer Gesetzgebung vorzusehen, dass für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Unternehmen und Hilfsunternehmen der Presse ausschließlich zu eigenen journalistisch-redaktionellen oder literarischen Zwecken den Vorschriften der §§ 5, 9 und 38a entsprechende Regelungen einschließlich einer hierauf bezogenen Haftungsregelung entsprechend § 7 zur Anwendung kommen.

Bei der Novellierung wurde der bisherige § 41 Abs. 1 BDSG durch eine Rahmenvorgabe für die Länder ersetzt. Dies wird mit der von Art. 75 GG vorgegebenen Kompetenzverteilung von Bund und Ländern begründet. Die Bundesregierung vertritt die Auffassung, dass die übrigen BDSG-Regelungen nicht auf die Presse anwendbar sind. Die Vorschrift, die damit auf dem Gebiet des redaktionellen Datenschutzes lex specialis zu § 1 Abs. 2 Nr. 3 BDSG sei, enthalte dementsprechend auch keine unmittelbar geltenden Regelungen. Sie gebe für die in die Zuständigkeit der Länder fallende Umsetzung lediglich den Mindeststandard der – in der Rechtprechung seit dem Volkszählungsurteil des Bundesverfassungsgerichts (BVerfGE 65, 1) – geforderten datenschutzrechtlichen Regelungen im Bereich der Medien vor und berücksichtige den Änderungsbedarf aufgrund von Art. 9 der EG-Datenschutzrichtlinie.

Über den früheren § 41 BDSG hinaus wird der Anwendungsbereich der Datenschutzbestimmungen in Umsetzung von Art. 9 EG-Datenschutzrichtlinie erweitert, insb. hinsichtlich der Haftung und zu den datenschutzfördernden Verhaltensregeln. Damit haben die Länder hinsichtlich der Datenverarbeitung von Unternehmen und Hilfsunternehmen der Presse ausschließlich zu eigenen journalistisch-redaktionellen oder literarischen Zwecken zumindest zu den folgenden Bereichen landesrechtliche Rechtsvorschriften zu erlassen:

- Datengeheimnis (§ 5 BDSG),
- technische und organisatorische Maßnahmen (§ 9 BDSG),
- Verhaltensregeln zur Förderung der Durchführung datenschutzrechtlicher Regelungen (§ 38a BDSG),
- Schadensersatz (§ 7 BDSG).

Für die Datenverarbeitung von Presseunternehmen, die nicht ausschließlich zu eigenen journalistisch-redaktionellen Zwecken erfolgt (etwa Personal- oder Abonnentendaten), ist das BDSG ohnehin voll anwendbar.

Der **Deutsche Presserat** hat inzwischen als Form der Selbstregulierung ergänzende Regelungen getroffen. Zunächst ist die Satzung des Deutschen Presserats dahingehend geändert worden, dass zu den Aufgaben des Presserats nunmehr auch die Selbstregulierung im Bereich des Redaktionsdatenschutzes einschließlich des präventiven Datenschutzes sowie der Anlassaufsicht gehört. Außerdem ist die Bindungswirkung der Grundsätze zum Redaktionsdatenschutz gegenüber den Mitgliedern des Deutschen Presserats verstärkt worden. Schließlich wurde ein Beschwerdeausschuss für den Redaktionsdatenschutz eingerichtet.

Der Deutsche Presserat hat inzwischen allgemeine Datenschutzleitlinien in den **Pressekodex** eingefügt. Darin werden Regeln zur Richtigstellung falscher Berichterstattung sowie deren Dokumentation, zur Auskunft über die der Berichterstattung zugrunde liegenden personenbezogenen Daten, zur Löschung

und Archivierung personenbezogener Daten sowie zum Umfang zulässiger Datenübermittlungen getroffen. Bei Verletzungen des Rechts auf informationelle Selbstbestimmung durch Veröffentlichungen haben die Betroffenen einen – aufgrund des Quellenschutzes allerdings eingeschränkten – Auskunftsanspruch. Bei Datenübermittlungen ist das Redaktionsgeheimnis zu beachten, das zu einer strengen Zweckbindung führt.

Der neu gebildete **Beschwerdeausschuss** für den Redaktionsdatenschutz wird (anders als die Datenschutzbeauftragten) erst dann tätig, wenn jemand sich in seinem Recht auf informationelle Selbstbestimmung beeinträchtigt sieht. Der Beschwerdeausschuss kann dabei vier verschiedene Maßnahmen verhängen:

- redaktioneller Hinweis,
- Missbilligung,
- nichtöffentliche Rüge,
- öffentliche Rüge.

Der Deutsche Presserat hat einen Fragebogen entwickelt, mit dem sämtliche Verlage Auskunft zur Datensicherheit geben sollen. Auf Grundlage der Antworten soll in Zusammenarbeit mit den betrieblichen Datenschutzbeauftragten der Verlage ein Kriterienkatalog zur Datensicherheit entwickelt werden. Schließlich sollen Beauftragte des Deutschen Presserats auch anlassunabhängig so genannte Konsultationsgespräche zum Redaktionsdatenschutz mit den Verlagen führen.

Da nicht alle Verlage den Trägervereinen des Deutschen Presserats angehören, stellt sich die Frage, welches Regulativ im Redaktionsdatenschutz für die übrigen Verlage gelten soll. Dabei ist fraglich, ob diese Verlage über § 38a BDSG durch den Deutschen Presserat verpflichtet werden können.

Wie die übrigen Landesbeauftragten für den Datenschutz vertreten wir die Auffassung, dass die Länder nach dem Wortlaut von § 41 BDSG verpflichtet sind, entsprechende Regelungen für die Presse im Landesrecht zu treffen. Dies gilt schon deshalb, weil nicht alle Verlage durch die Selbstregulierung des Deutschen Presserats erreicht werden. Eine bloß dynamische Verweisung im Landesrecht auf § 41 BDSG wäre nicht ausreichend, denn damit würde der Datenschutz bei den nicht im Deutschen Presserat repräsentierten Verlagen nicht in ausreichendem Maße gewährleistet. Auf jeden Fall sollte die Gewährleistung des Datenschutzes bei den Medien bei der zweiten Stufe der Novellierung des BDSG erneut erörtert werden (siehe 2.1.2).

2.2.4 Behördliche Datenschutzbeauftragte

Die Behörden sollten verstärkt von der neu eingeführten Möglichkeit zur Einsetzung behördlicher Datenschutzbeauftragter Gebrauch machen.

Bei der Anpassung des Hamburgischen Datenschutzgesetzes an die Europäische Datenschutzrichtlinie wurde in § 10a HmbDSG die Möglichkeit neu eingefügt, dass die Hamburger öffentlichen Stellen behördliche Datenschutzbeauftragte bestellen.

Aufgaben und Stellung der bzw. des behördlichen Datenschutzbeauftragten

Die behördlichen Datenschutzbeauftragten haben die Aufgabe, die Daten verarbeitenden Stellen und deren Personalvertretungen in der Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz zu unterstützen. Sie sind bei ihrer Tätigkeit weisungsfrei und dürfen wegen der Erfüllung ihrer Aufgaben nicht benachteiligt werden. Sie sind in erforderlichem Umfang von der Erfüllung anderer Aufgaben freizustellen und bei der Erfüllung ihrer Aufgaben zu unterstützen.

Mit der Einführung behördlicher Datenschutzbeauftragter wird das im nicht öffentlichen Bereich bewährte Modell der betrieblichen Datenschutzbeauftragten auch auf den öffentlichen Bereich übertragen und damit die Eigenverantwortlichkeit der Daten verarbeitenden Stellen gestärkt.

Für Daten verarbeitende Stellen, die behördliche Datenschutzbeauftragte bestellen, gelten gegenüber den anderen Daten verarbeitenden Stellen die folgenden Besonderheiten bzw. Erleichterungen:

- Stellen mit behördlichen Datenschutzbeauftragten führen ihre Verfahrensbeschreibungen selbst und müssen diese – anders als Stellen ohne behördliche Datenschutzbeauftragte – nicht an den Hamburgischen Datenschutzbeauftragten übersenden, um ihm mögliche Kontrollbedarfe anzuzeigen.
- Die Vorabkontrolle von Datenverarbeitungsverfahren, von denen besondere Gefährdungen für die Rechte Betroffener ausgehen, obliegt den behördlichen Datenschutzbeauftragten. Wenn behördliche Datenschutzbeauftragte nicht bestellt werden, ist die Vorabkontrolle durch den Hamburgischen Datenschutzbeauftragten durchzuführen.
- Vor pauschalen Entscheidungen über das Absehen von Benachrichtigungen der Betroffenen nach § 12a Abs. 3 Satz 2 HmbDSG sind die behördlichen Datenschutzbeauftragten zu hören. Sind solche nicht bestellt, ist der Hamburgische Datenschutzbeauftragte einzuschalten.

Trotz dieser Vorteile haben bislang nur wenige Behörden einen behördlichen Datenschutzbeauftragten benannt. Aus unserer Sicht wäre es zu begrüßen, wenn die Hamburger Behörden von dieser neuen Möglichkeit verstärkt Gebrauch machen würden.

3. Informations- und Kommunikationstechnik

3.1 E-Government

3.1.1 Allgemeine Vorgaben für das E-Government

Die Finanzbehörde hat im Sommer 2001 den Entwurf eines „E-Government-Fahrplans" vorgelegt, in dem die verschiedenen Aktivitäten und Planungen der Behörden zur Bereitstellung elektronischer Verwaltungsdienstleistungen zusammengefasst werden. Wir haben angeregt, dem Datenschutz bei den Planungen ein angemessenes Gewicht beizumessen.

Bürgerfreundliches E-Government setzt einen wirksamen Datenschutz und die Gewährleistung der Datensicherheit voraus, damit die Betroffenen das notwendige Vertrauen in die elektronischen Abläufe bekommen. Die Datenschutzbeauftragten des Bundes und der Länder haben deshalb Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung erarbeitet, die auch aus unserem Internet-Angebot abgerufen werden können (http://www.hamburg.de/fhh/behoerden/datenschutzbeauftragter/material/buerger1.html).

Aus unserer Sicht sollten beim E-Government die folgenden Rahmenbedingungen beachtet werden:

– Bei der Auswahl und Gestaltung von E-Government-Verfahren sollte entsprechend der Vorgabe von § 5 Abs. 4 HmbDSG vorab geprüft werden, ob die Erhebung personenbezogener Daten überhaupt erforderlich ist oder ob eine anonyme oder pseudonyme Nutzungsmöglichkeit ausreicht (Datenvermeidung bzw. Datensparsamkeit – vgl. Kasten). Dies gilt auch bei Bezahlverfahren für Verwaltungsdienstleistungen (vgl. 3.1.2).

> § 5 Abs. 4 HmbDSG (Datenvermeidung und Datensparsamkeit)
>
> „Die Verarbeitung personenbezogener Daten und die Auswahl und Gestaltung technischer Einrichtungen haben sich auch an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben und weiter zu verarbeiten. Dabei ist jeweils zu prüfen, inwieweit es möglich ist, personenbezogene Daten anonym oder pseudonym zu verarbeiten. Erforderlich sind Maßnahmen zur anonymen oder pseudonymen Datenverarbeitung nur, wenn ihr Aufwand in einem angemessenen Verhältnis zur Schutzwürdigkeit der Daten steht."

– Bei allen E-Government-Angeboten sollten klare, verständliche Bürgerinformationen darüber erfolgen, welche Auswirkungen die Verfahren haben und mit welchen Vorteilen und Risiken sie verbunden sind.

- Für die Bürgerinnen und Bürger darf kein „Anschluss- und Benutzungszwang“ für elektronische Verwaltungsleistungen bestehen, jedenfalls so weit die Verfahren mit der Verarbeitung zusätzlicher personenbezogener Daten verbunden sind. Den Betroffenen sollte zumindest in diesen Fällen nach eigener Entscheidung weiterhin ein konventionelles Verfahren zur Verfügung stehen. Dabei dürfen diejenigen, die das konventionelle Verfahren wählen, weder rechtlich noch faktisch benachteiligt werden. Dies bedeutet insbesondere, dass für die Bürgerinnen und Bürger wesentliche Hinweise und Informationen auch außerhalb elektronischer Verfahren in hinreichendem Umfang und ohne zusätzliche Kosten verfügbar sein müssen.
- Auch bei kundenorientierter Gestaltung von Arbeitsabläufen ist darauf zu achten, dass jeweils nur die erforderlichen Daten erhoben werden und dass die Zweckbindung gewahrt bleibt.
- E-Government-Verfahren müssen durch geeignete technisch-organisatorische Maßnahmen so gestaltet werden, dass nur Befugte die personenbezogenen Daten zur Kenntnis nehmen können (Vertraulichkeit). Die Kommunikation ist deshalb durch kryptografische Verschlüsselung zu schützen. Es ist sicherzustellen, dass die Daten während der Verarbeitung unverfälscht, vollständig und widerspruchsfrei bleiben (Integrität) und ihrem Ursprung zugeordnet werden können (Authentizität). Ferner muss dokumentiert werden, welche Verwaltungsmitarbeiter zu welchem Zeitpunkt welche personenbezogenen Daten in welcher Weise verarbeitet haben (Revisionsfähigkeit).
- Bürger bzw. externe Kunden dürfen aus Sicherheitsgründen keinen direkten Zugriff auf die Verwaltungsrechner erhalten. Stattdessen sind diese Informationen auf einem abgesetzten Server vorzuhalten (vgl. 3.1.4).
- Bei Verfahren, bei denen personenbezogene Daten verarbeitet werden, muss eine Risikoanalyse und ggf. eine Vorabkontrolle durchgeführt werden. Dabei dürfen den Bürgerinnen und Bürgern keine unverantwortbaren Risiken abverlangt werden. Bei besonders sensiblen Daten (insbesondere Gesundheits-, Personal- und Sozialdaten) ist zu prüfen, ob ein elektronisches Verfahren überhaupt vertretbar ist. In jedem Fall müssen bei derartigen Daten über einen Grundschutz hinausgehende Sicherungsmaßnahmen getroffen werden (vgl. 14. TB, 6.1.2).
- Bei der Vorbereitung neuer Verfahren ist der Hamburgische Datenschutzbeauftragte rechtzeitig zu beteiligen.

Der Hamburgische Datenschutzbeauftragte unterstützt ausdrücklich die Bemühungen zur Verbesserung der **Transparenz des Verwaltungshandelns.** Hierzu gehört die Möglichkeit der Betroffenen, elektronisch von datenschutz-

rechtlichen Auskunftsansprüchen Gebrauch zu machen. Auch die Einführung eines allgemeinen Informationszugangsrechts unter Wahrung der datenschutzrechtlichen Belange wird von uns unterstützt.

Beim E-Government kommt einer einwandfreien und sicheren **Authentifizierung** große Bedeutung zu. Im Hinblick auf die gesetzlich gebotene Datensparsamkeit (s. Kasten) sollte jedoch darauf hingewiesen werden, dass nicht für jede Verwaltungshandlung eine Identifikation des „Kunden" erforderlich ist. Dies gilt insbesondere für solche Verfahren, die jedermann ohne Einschränkung und ohne persönliche Betroffenheit zugänglich sind, insbesondere bloße Informationsangebote. Angebote, die zwar eine direkte Kommunikation zwischen den Bürgern und der Verwaltung voraussetzen, etwa hinsichtlich der Zuordnung zu einer bestimmten Gruppe, bei denen jedoch eine namentliche Kenntnis der Betroffenen nicht erforderlich ist, sollten von den Bürgern auch unter Pseudonym genutzt werden können. Ein Anwendungsfall könnte z.B. die Bereitstellung eines erweiterten Vorlesungsverzeichnisses sein, zu dem allein die Mitglieder einer Hochschule Zugang haben sollen.

Hinsichtlich derjenigen Verfahren, bei denen eine namentliche Identifizierung unabdingbar ist, ist eine eindeutige Authentifizierung des Bürgers oder der Bürgerin sicherzustellen. Im Hinblick auf die Gewährleistung des Datenschutzes kommt es insbesondere bei Verfahren, die zur Verarbeitung und Offenbarung sensibler personenbezogener Daten gegenüber einem Bürger oder einer Bürgerin führen, auf eine sehr sichere Authentifizierung an. So weit gesetzlich die Schriftform bei der Kommunikation zwischen Bürger und Verwaltung und bei der Archivierung von Dokumenten (vgl. 3.1.5) vorgesehen ist, muss die Authentizität elektronischer Dokumente durch qualifizierte **elektronische Signaturen** nach dem Signaturgesetz („elektronische Form") Gewähr leistet werden (vgl. 3.6).

Ein wichtiger Aspekt ist auch die Authentifizierung der Behörden gegenüber den Bürgerinnen und Bürgern. Die „Kunden" müssen sicher sein, dass ihre persönlichen Angaben nur von befugten Stellen gelesen werden und dass die von einer Behörde zugesandten elektronischen Dokumente, wie Bescheide oder Verfügungen, rechtswirksam sind **(elektronisches Dienstsiegel)**.

Die Notwendigkeit der Authentifizierung im Rahmen von E-Government-Anwendungen darf nicht zur Bildung unzulässiger allgemeiner Personenkennzeichen führen. Es deshalb ist sicher zu stellen, dass über den zentralen Server keine Bewegungs- bzw. Nutzungsprofile einzelner Bürger erstellt und unterschiedliche Verwaltungsvorgänge nicht unbefugt zusammengeführt werden können.

3.1.2 Datensparsamkeit durch anonymes Bezahlen von Verwaltungsleistungen

Als Gegenleistung für Verwaltungsleistungen müssen Bürgerinnen und Bürger Gebühren zahlen bzw. Auslagen erstatten. Die Notwendigkeit der Bezahlung von Verwaltungsleistungen darf nicht dazu führen, dass sich die „Kunden" allein aus diesem Grund gegenüber der Verwaltung identifizieren müssen.

Bereits weiter oben (vgl. 3.1.1) ist darauf hingewiesen worden, dass auch im elektronischen Verkehr der Bürgerinnen und Bürger mit der Verwaltung keine bzw. möglichst wenig personenbezogene Daten verarbeitet werden sollten (Datenvermeidung bzw. -sparsamkeit). Deshalb sollten Bezahlfunktionen nach Möglichkeit so gestaltet werden, dass sie nicht zu einer Identifikation der Betroffenen in Verfahren führen, in denen ihre Identität nicht ohnehin bekannt ist.

Bei Verwaltungsdienstleistungen, die über das Internet erbracht werden, handelt es sich häufig um Teledienste. Gemäß § 4 Abs. 1 Teledienstedatenschutzgesetz sollen die Diensteanbieter dem Nutzer die Inanspruchnahme und Bezahlung von Telediensten anonym oder unter Pseudonym ermöglichen, soweit dies technisch möglich und zumutbar ist. Ein Anwendungsbeispiel ist die Bereitstellung kostenpflichtiger Informationen.

Im Übrigen ist darauf zu achten, dass durch die Bezahlfunktion keine unzulässige Zusammenführung von personenbezogenen Daten aus verschiedenen Verwaltungsbereichen stattfindet. Für das Internet stehen inzwischen funktionsfähige Verfahren zur Verfügung, über die sich die Bezahlung elektronischer Dienstleistungen anonym und sicher abwickeln lassen. Besondere Bedeutung kommt dabei der Verwendung von anonymen bzw. pseudonymen Prepaid-Verfahren zu (vgl. hierzu 25.1).

3.1.3 Wahlscheinanträge über das Internet

Bei dem neuen Verfahren zur Bestellung von Briefwahlunterlagen über das Internet waren besondere datenschutzrechtliche Bedingungen einzuhalten. Diese betrafen vor allem die Auftragsdatenverarbeitung und die Authentifizierung der antragstellenden Bürgerinnen und Bürger.

Die hamburgische Verwaltung räumt den Bürgerinnen und Bürgern zunehmend die Möglichkeit ein, Dienstleistungen auch über das Internet in Anspruch zu nehmen (siehe 3.1.1). Demgemäß konnten zur Bürgerschafts- und Bezirksversammlungswahl 2001 erstmals – neben dem bislang üblichen schriftlichen Antragsverfahren – die Briefwahlunterlagen auch elektronisch geordert werden.

Bei der Umsetzung dieses Projekts arbeiteten das Senatsamt für Bezirksangelegenheiten (SfB) -Zentralstelle IuK-, das Landeswahlamt, das Landesamt für Informationstechnik (LIT), hamburg.de und das Hamburger Informatik Technologie-Center (HiTeC e.V.) zusammen. Alle beteiligten Stellen verpflichteten sich auf ein gemeinsames Datenschutzkonzept.

Der Antrag auf Zusendung der Briefwahlunterlagen konnte interaktiv über das Internetportal www.hamburg.de (siehe 3.5.5) der hamburgischen Verwaltung gestellt werden. Für die Authentifizierung der Wahlberechtigten mussten neben Namen und Anschrift auch das Geburtsdatum und die auf der Wahlbenachrichtigungskarte enthaltene Nummer des Wählerverzeichnisses im Bestellformular eingegeben werden. Im Wege der Auftragsdatenverarbeitung hat hamburg.de die Informationen entgegengenommen und in verbindlich definierte XML-Datenstrukturen konvertiert. Diese wurden vom LIT in regelmäßigen Abständen in das dortige Rechenzentrum übertragen.

Die Zentralstelle IuK im SfB sorgte dafür, dass die Antragsdaten mit dem IuK-Verfahren DIWA abgeglichen wurden, so dass die bezirklichen Wahldienststellen die beantragten Unterlagen ausstellen und versenden konnten. Antragstellerinnen und Antragsteller wurden elektronisch über die Bearbeitung ihres Antrags informiert. Das der elektronischen Datenverarbeitung zugrundeliegende Serviceflow-Konzept wurde von HiTeC e.V. entwickelt. Zur Schaffung der rechtlichen Voraussetzungen war auch eine Anpassung der Wahlordnung erforderlich, die bis dahin allein die schriftliche Antragstellung vorsah.

Mehr als 10.000 der insgesamt 216.000 Briefwahlanträge wurden online über das Internet gestellt. Aufgrund der elektronischen Anträge wurden ca. 9.300 Wahlscheine tatsächlich ausgestellt. Die übrigen Bestellformulare waren unvollständig oder fehlerhaft ausgefüllt. Es kann davon ausgegangen werden, dass dieses Verfahren fortentwickelt und bei der Bundestagswahl 2002 wieder angeboten wird.

An diesem Projekt wurden wir schriftlich durch Übersendung der Datenschutzkonzeption und auch in mehreren gemeinsamen Gesprächsterminen beteiligt. Als nicht überschaubar stellte sich dabei die Gestaltung der Unterauftragsverhältnisse bei hamburg.de heraus. Erst auf beharrliches Nachfragen konnte letztendlich nachvollzogen werden, welche Institutionen tatsächlich alle mit der Verarbeitung der personenbezogenen Daten der Antragstellerinnen und Antragsteller betraut worden sind.

3.1.4 DV-Verfahren Integrierte Erfassung und Bearbeitung von Zuwendungen (INEZ)

Ein sicheres Authentifizierungsverfahren für diese E-Government-Anwendung soll jetzt spätestens bis zum Ende der Pilotierung eingeführt werden.

Im Rahmen des E-Government werden nicht nur Informationen bereitgestellt, sondern auch zwischen der Verwaltung, externen Organisationen und Bürgern Daten ausgetauscht. Das Projekt „Integrierte Erfassung und Bearbeitung von Zuwendungen (INEZ)“ ist ein erster Anwendungsfall.

Das automatisierte Verfahren INEZ wird seit Anfang 2000 in der Behörde für Arbeit, Gesundheit und Soziales (BAGS) genutzt, um die Zuwendungsbearbeitung zu unterstützen. Ziel des Verfahrens ist es, einerseits die Effizienz in der Bearbeitung einzelner Zuwendungsfälle zu steigern. Andererseits soll das gesamte Zuwendungsgeschehen transparenter werden, ohne dass umfangreiche Einzelrecherchen notwendig sind.

Die Zuwendungsempfänger haben die für das Zuwendungs-Controlling erforderlichen Informationen regelmäßig zu aktualisieren. Um Medienbrüche und Doppelarbeit bei der Aktualisierung zu vermeiden, soll einer definierten Benutzergruppe ein lesender und schreibender Zugriff auf INEZ-Daten über das Internet ermöglicht werden, wobei zunächst die Einbindung von ca. 35 Zuwendungsempfängern geplant ist. Die Zahl der beteiligten Zuwendungsempfänger soll schrittweise erhöht werden. Voraussetzung für die Teilnahme an dem Verfahren ist, dass die BAGS nach erfolgtem Zuwendungsbescheid eine entsprechende Zugriffsberechtigung für INEZ einrichtet. Eine Öffnung des Verfahrens über die geschlossene Benutzergruppe hinaus ist zu einem späteren Zeitpunkt beabsichtigt.

Der Schutzbedarf der mit INEZ verarbeiteten Daten wurde von der BAGS auf unsere Veranlassung hin in einer Risikoanalyse nach §8 Abs. 4 HmbDSG aufgearbeitet. Für die einzelnen Zuwendungsvorhaben werden eine Vielzahl von Daten über Personen verarbeitet, die von dem jeweiligen Zuwendungsempfänger betreut werden, darunter auch Sozial- und Gesundheitsdaten. Nach eingehender Erörterung mit den beteiligten Stellen wird nunmehr unsere Auffassung geteilt, dass es sich um z.T. sehr sensible Daten handelt und daher besondere Schutzmaßnahmen notwendig sind.

Die Architektur der E-Government-Anwendung von INEZ sieht vor, dass die Daten nicht unmittelbar mit dem Verwaltungsverfahren ausgetauscht werden, sondern über gesonderte Server im Landesamt für Informationstechnik (LIT), die durch Firewalls in einem getrennten Bereich geschützt stehen.

Wir haben gefordert, dass neben einer starken Verschlüsselung der übertragenen Daten auch eine sichere Authentifizierung der externen Nutzerinnen und Nutzer erfolgen muss. Die alleinige Überprüfung eines Passwortes reicht nicht aus, da mit einem erspähten Passwort der Zugriff auf die sensiblen Daten von jedem Rechner aus möglich wäre, der an das Internet angeschlossen ist. Die in Frage kommenden Lösungsmöglichkeiten sollen von der Projektgruppe bewertet werden. Die technische Umsetzung soll bis zum Abschluss der laufenden Pilotierung erfolgen. Darüber hinaus haben wir erreicht, dass bis zur Realisierung dieser zusätzlichen Schutzmaßnahme besonders kritische Datenfelder nicht über das Internet gepflegt werden und der Passwortschutz umgehend erhöht wurde.

Der Pilotbetrieb hat gezeigt, dass mit der redundanten Datenhaltung, bei der die Daten nicht nur in dem Verfahren selbst, sondern zusätzlich in einem besonders geschützten Bereich vorgehalten werden, und mit der Synchronisierung der verschiedenen Datenbestände gravierende Nachteile verbunden sind. Für weitere E-Government-Anwendungen wird daher eine Software-Architektur angestrebt, bei der auf eine redundante Datenhaltung verzichtet wird. Wir werden im weiteren Verlauf von INEZ und folgenden E-Government-Projekten darauf achten, dass insbesondere die Vertraulichkeit, Integrität und Authentizität der Daten sichergestellt wird.

3.2. IuK-Infrastruktur

3.2.1 FHHinfoNET

Das Mailing-System der hamburgischen Verwaltung entwickelt sich beständig technisch und organisatorisch weiter. Für die Verschlüsselung sensibler Nachrichteninhalte zeichnet sich eine neue Lösung ab; erste allgemein verbindliche Benutzerregeln wurden vereinbart.

Das vom Landesamt für Informationstechnik (LIT) betriebene elektronische Mailing-System der hamburgischen Verwaltung („FHHinfoNET“, siehe auch 17. TB, 3.1) haben wir im Jahr 2000 einer datenschutzrechtlichen Prüfung unterzogen. Die dabei von uns getroffenen Feststellungen führten zu einer Reihe von Anregungen und Forderungen, deren Umsetzung inzwischen bereits erfolgt oder zumindest verbindlich zugesagt worden ist.

Im Mittelpunkt unserer Erörterungen mit der Finanzbehörde und dem LIT standen dabei die Verschlüsselung von Nachrichten mit sensiblen personenbezogenen Daten und die Erstellung grundlegender Regeln für die Nutzung der Bürokommunikation, vor allem verbindlicher Vorgaben für die Einsichtnahme persönlicher Posteingangsfächer und Terminkalender im Vertretungsfall.

Nach den bestehenden Durchführungsbestimmungen zur Telekommunikationsrichtlinie (MittVw 1994, Seite 35) dürfen sensible personenbezogene Daten nur dann per E-Mail übertragen werden, wenn sie zuvor verschlüsselt worden sind. Bislang verfügt jedoch nur eine sehr kleine Anzahl von Teilnehmern des FHHinfoNET über die Möglichkeit der sogenannten „erweiterten Sicherheit“ (Verschlüsselung des E-Mail-Verkehrs innerhalb der hamburgischen Verwaltung). Insbesondere in solchen Bereichen, die regelmäßig personenbezogene Daten untereinander austauschen, können noch nicht alle Kommunikationspartner verschlüsselt senden und empfangen. Dazu gehören etwa die Personalabteilungen der Behörden und Ämter.

Aus eigenen Prüfungen vor Ort, Anfragen Betroffener an unsere Dienststelle und sogar aus Nachrichten, die in den Postfächern unserer Mitarbeiterinnen und Mitarbeiter eingehen, wissen wir, dass auch weiterhin nachweislich sensible personenbezogene Daten unverschlüsselt per E-Mail verschickt werden. Wir haben dies dann jeweils konkret mit den betreffenden Behörden und Ämtern erörtert und darauf gedrängt, die Einhaltung für die hamburgische Verwaltung verbindlicher organisatorischer Vorgaben konsequent sicher zu stellen.

Die „erweiterte Sicherheit“ konnte noch auf einige weitere Postfächer ausgedehnt werden. Eine flächendeckende Einführung für jedes eingerichtete Postfach im FHHinfoNET kann aber erst im Laufe des Jahres 2002 erfolgen. Die zum Jahreswechsel im LIT vorgesehene Umstellung auf Exchange 2000 lässt es nicht zu, die bereits erteilten Zertifikate weiter zu verwenden. Es müssten für alle Benutzer neue erstellt werden. Der Zugriff auf Nachrichten, die mit den bisherigen Zertifikaten verschlüsselt worden sind, wäre nicht mehr möglich.

Zudem ist geplant, in der hamburgischen Verwaltung eine eigene, die Anforderungen des Bundesamtes für Sicherheit in der Informationstechnik erfüllende Public Key-Infrastruktur einzurichten. Diese soll es zu einem späteren Zeitpunkt erlauben, die an die Mitarbeiter ausgegebenen Zertifikate nicht nur netzintern untereinander zu verwenden, sondern auch für die Kommunikation mit Dritten wie anderen Verwaltungsstellen in Bund und Ländern, aber vor allem auch Bürgern und Institutionen der Freien und Hansestadt Hamburg (siehe hierzu 3.1.1). Es soll damit vermieden werden, dass für die Kommunikation mit verschiedenen Partnern unterschiedliche Schlüssel zum Einsatz kommen müssen.

Dieses Vorhaben ist nicht kurzfristig umsetzbar. Der innerhalb absehbarer Zeiträume wiederholt notwendige Aufwand für die Einrichtung von Zertifikaten soll aber weitgehend vermieden werden. Wir haben uns deshalb unter diesen Voraussetzungen mit der Finanzbehörde und dem LIT darauf verständigt, dass

für einen begrenzten Zeitraum von wenigen Monaten nur noch in zwingend erforderlichen Einzelfällen weitere Zertifikate nach dem bisherigen Verfahren ausgestellt werden. Dazu zählen der Nachrichtenaustausch zwischen Personalabteilungen und dem Personalärztlichen Dienst oder zwischen Staatsanwaltschaft und Gerichten.

Der flächendeckende Einsatz der „erweiterten Sicherheit" für alle bestehenden Postfächer beginnt dann ab April 2002 nach erfolgter Umstellung der Exchange Server auf die neue Version und der Einrichtung der neuen Public Key-Infrastruktur im LIT. Ziel ist es, in einem geordneten Roll-Out-Verfahren alle bereits bestehenden und neu einzurichtenden Postfächer mit der Möglichkeit der Verschlüsselung und Signatur von Nachrichten auszustatten.

Seit dem 11. Oktober 2001 gibt es nunmehr auch eine Vereinbarung nach § 94 HmbPersVG über den Prozess zur Einführung und Nutzung der Bürokommunikation und zur Entwicklung von E-Government (siehe 3.3.2 und 11.1). Sie enthält u. a. erste allgemeinverbindliche Regeln für eine einheitliche Anwendung von elektronischer Kommunikation in der hamburgischen Verwaltung, die entsprechend den damit gewonnenen Erfahrungen fortgeschrieben werden sollen. Insbesondere sind darin auch aus Datenschutzsicht erforderliche und vertretbare Vorgaben für den Umgang mit Postfächern und Terminkalendern in Abwesenheits- und Vertretungsfällen getroffen worden. Dazu gehören vor allem Hinweise zur Kennzeichnung vertraulicher oder privater Inhalte, um deren Kenntnisnahme durch Dritte weitgehend einschränken zu können.

3.2.2 Einsatz von Windows 2000 in der hamburgischen Verwaltung

Der Umfang der Zugriffsrechte zentraler Administratoren wird durch den Einsatz von Windows 2000 erweitert. Erste organisatorische Regelungen sollen durch ein Sicherheitskonzept ergänzt werden.

Die IuK-Infrastruktur der hamburgischen Verwaltung soll flächendeckend von Windows NT (17. TB, 3.3) auf das Betriebssystem Windows 2000 umgestellt werden. Mit der Migration auf Windows 2000 sind hinsichtlich der Sicherheit wesentliche Veränderungen verbunden. Die Rahmenbedingungen hat das Landesamt für Informationstechnik (LIT) in einem Betriebskonzept festgelegt. Eine konzeptionelle Aufarbeitung von Sicherheitsaspekten wird das LIT in einem Sicherheitskonzept vornehmen, das Ende 2001 vorliegen soll.

Dem Verzeichnisdienst „Active Directory" von Windows 2000 liegt standardmäßig ein hierarchisches Domänenkonzept zugrunde. Nach dem Betriebskonzept werden die Behörden als administrativ getrennte Bereiche in eine Gesamtdomäne für die hamburgische Verwaltung integriert. Damit ist das Risiko verbunden, dass sich die Administratoren dieser Domäne (d.h. Mitarbeiter des LIT) Zugriffsrechte auf alle Bereiche und Objekte der Domäne verschaffen können. Es ist festgelegt, dass die Domänen-Administratoren

keinen Zugriff auf die behördlichen Ressourcen-Server nehmen. Eine organisatorische Regelung steht noch aus, wann und durch wen veranlasst die Domänen-Administratoren des LIT in die administrativen Bereiche der Behörden eingreifen dürfen und wie dies überwacht wird. Dabei ist anzustreben, dass die Aktivitäten der Administration revisionssicher registriert werden.

Mit dem „Active Directory“ wird ein Verzeichnisdienst in Windows 2000 integriert, in dem alle in einer Domäne verwalteten Objekte wie Benutzerkonten, Computer etc. mit den spezifischen Informationen enthalten sind. Auf der Grundlage von „Vererbungen“ können Sicherheitsstandards für alle darunter liegenden Bereiche definiert werden. Dies wird auf zentraler Ebene u.a. für die technische Umsetzung der Passwortrichtlinie genutzt, so dass hier ein einheitlicher Standard für alle angeschlossenen Benutzerkonten erreicht wird. Wir haben in Hinblick auf die gesteigerte Bedeutung der Anmeldung für die Systemsicherheit darauf hingewirkt, dass mit einer Mindest-Passwortlänge von acht Zeichen und einer technisch erzwungenen Mischung von Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen die Passwortsicherheit erhöht wird. Weitere Sicherheitseinstellungen sind während des Migrationsprozesses von den Behörden vorzunehmen.

Mit „Kerberos“ wird ein seit längerem genutztes, herstellerunabhängiges Standardprotokoll zur Netzwerkauthentifizierung zur Verfügung gestellt. Der wesentliche Vorteil liegt in der gegenseitigen Authentifizierung von Client und Server, die unter Windows NT nicht realisiert ist. Zudem wird eine Grundlage für eine einheitliche Authentifizierung und Rechteüberprüfung im gesamten Netzwerk geschaffen.

Mit der Netzwerksicherheitsarchitektur „IPSec“ kann die Vertraulichkeit, Authentizität und Integrität der Datenübertragung sichergestellt werden. Über Sicherheitsrichtlinien kann festgelegt werden, in welchen Fällen dieses Protokoll genutzt wird. Mit Windows 2000 kann daher die Forderung des Hamburgischen Datenschutzbeauftragten ohne wesentlichen Mehraufwand umgesetzt werden, eine verschlüsselte Übertragung personenbezogener Daten innerhalb des Netzes der hamburgischen Verwaltung zu gewährleisten. Ein Konzept zur Nutzung von IPSec steht noch aus.

Eine Migration auf das Betriebssystem Windows 2000 ist für die Anwender der Sozialhilfesachbearbeitung bereits flächendeckend erfolgt. Darüber hinaus nutzen einzelne weitere Organisationseinheiten Windows 2000. Der Umstieg weiterer Bereiche der hamburgischen Verwaltung wird voraussichtlich im Jahr 2002 erfolgen. Wir werden diesen Prozess begleiten und auf die Nutzung der damit verbundenen Chancen für den Datenschutz drängen. Eine Broschüre „Datenschutz bei Windows 2000“ stellt der Hamburgische Datenschutzbeauftragte Anfang 2002 zur Verfügung.

3.2.3 Ressourcensteuerung mit SAP R/3

Das zentrale IuK-Verfahren „sap für hamburg“ stellt hohe technische und organisatorische Anforderungen an die Verfügbarkeit und Belastbarkeit sowohl der eingesetzten Hard- und Software als auch des Netzes der FHH. Auch datenschutzrechtliche Aspekte dürfen nicht zu kurz kommen.

In der hamburgischen Verwaltung wird mit der Standardsoftware SAP R/3 ein zentrales IuK-Verfahren für die integrierte Ressourcensteuerung entwickelt („sap für hamburg“). Hierunter fallen folgende Aufgaben: Aufstellung, Bewirtschaftung und Abrechnung des Haushalts, Erstellung von Kassenanordnungen, Abwicklung des Zahlungsverkehrs, Buchhaltung der Landeshauptkasse sowie die Kosten- und Leistungsrechnung. Die bislang für diese Zwecke genutzten Anwendungsprogramme, insbesondere die Mittelbewirtschaftung MBV, laufen mit unterschiedlichen Betriebssystemen und Softwareprodukten. Sie sollen abgelöst und auf eine einheitliche Basis (Windows 2000, SQL 2000 Server) gestellt werden. Zum Einsatz kommen die Module IS/PS, FI, CO und CATS. Die Einführung erfolgt schrittweise. In einigen ausgewählten Verwaltungsbereichen sind Teile, insbesondere IS/PS, bereits in der Produktion. Die Roll Out-Planung sieht Zug um Zug eine flächendeckende Nutzung in allen Behörden und Ämtern spätestens ab 1. April 2003 vor.

Die Verantwortlichkeiten für das Verfahren „sap für hamburg“ sind verteilt. Die Anwendung selbst wird im Rechenzentrum des Landesamtes für Informationstechnik (LIT) betrieben (Rechenstelle). Der Anschluss der dezentral in den Behörden und Ämtern von den Anwendern genutzten PC erfolgt über das ebenfalls vom LIT betriebene Netz der FHH. Für den haushaltsmäßig korrekten Budgetverbrauch ist die fachliche Leitstelle des Haushalts zuständig, für die Kassenanordnungen und deren buchungstechnisch richtige Behandlung die fachliche Leitstelle der Landeshauptkasse. Sachlich zuständige Stellen für die Einrichtung der Buchungskreise und die ordnungsgemäße sichere Anwendung des Verfahrens sind die Beauftragten für den Haushalt der Behörden und Ämter. Programmierende Stelle ist das eigens für das Projekt im LIT eingerichtete Customer Competence Center (CCC). Den hier tätigen Mitarbeiterinnen und Mitarbeitern obliegen die Programmeinstellungen, die Entwicklung von User-Exits und die Pflege der Verfahrensdokumentation.

Die Umsetzung dieses Projekts ist mit erheblichem technischen und organisatorischem Aufwand verbunden. Es ist mit etwa 4.500 Anwendern zu rechnen, die „sap für hamburg“ für die Erfüllung ihrer Aufgaben benötigen. Dies stellt hohe Anforderungen an die Verfügbarkeit der eingesetzten Hard- und Software sowie die Funktionsfähigkeit und Belastbarkeit des Netzes. Es sind umfangreiche Schulungsmaßnahmen notwendig. Einmal festgelegte Rahmenbedingungen können sich jederzeit durch Releasewechsel ändern. Die Verteilung der graphischen Benutzeroberfläche (SAP-GUI) und der regelmäßigen Updates an die Arbeitsplätze setzt zwingend die Nutzung der System Mana-

gement Server (SMS)-Infrastruktur der FHH voraus. Jeder SAP-Client in den Behörden und Ämtern muss unter Windows 2000 laufen und an die vom Landesamt für Informationstechnik (LIT) betriebene Central Site angeschlossen sein.

Im Rahmen der Mittelbewirtschaftung in „sap für hamburg“ werden personenbezogene Daten verarbeitet. Es handelt sich um Namen, Anschriften und Bankverbindungen von Zahlungsempfängern und Schuldnern der FHH. Hinzu kommen Betrag und Grund der Zahlung bzw. der Forderung. Zwar werden große sensible Anwendungsbereiche wie Sozialhilfe, Bußgelder für Ordnungswidrigkeiten im Straßenverkehr, Steuerangelegenheiten und auch die Personaldatenverarbeitung nicht über das Modul IS/PS erfasst. Hier gibt es eigens für diesen Zweck programmierte Schnittstellen aus den jeweiligen Automationsverfahren zur Finanzbuchhaltung in der Kasse. Es verbleiben jedoch auch so noch eine Vielzahl personenbezogener Informationen im Mittelbewirtschaftungsteil, die insbesondere in Verbindung mit dem Grund der Zahlung bzw. Forderung (Verwendungszweck auf dem Überweisungsträger) durchaus sehr sensibel sein können. Davon sind auch die Mitarbeiter der FHH betroffen, soweit ihnen beispielsweise Kosten für Dienstreisen oder die Teilnahme an Fortbildungsveranstaltungen erstattet werden.

Aufgrund der Tatsache, dass in „sap für hamburg“ das Anlegen eines Personenstammdatensatzes für jeden Zahlungsempfänger bzw. -pflichtigen erforderlich ist – Einmalzahler bzw. -empfänger wie bisher wird es nicht mehr geben – und dass alle zahlungsbegründenden Unterlagen gesetzlichen Aufbewahrungsfristen unterliegen, sind auch personenbezogene Auswertungen über längere Zeiträume möglich. Letzteres gilt ebenso für den Bereich der Kosten- und Leistungsrechnung. Hier sind aus datenschutzrechtlicher Sicht organisatorische und technische Maßnahmen erforderlich, die gewährleisten, dass jeder Anwender des SAP-Systems nur auf die personenbezogenen Daten zugreifen kann, die er für die Erfüllung seiner Aufgaben tatsächlich benötigt. Personenbeziehbare Auswertungen dürfen nur im zulässigen, von Rechtsvorschriften vorgegebenen Umfang erfolgen.

Der Vergabe der Zugriffsrechte auf die unter SAP R/3 gespeicherten personenbezogenen Daten kommt daher erhebliche Bedeutung zu. Verbindliche Grundsätze und Verfahrensregelungen sind bereits in einem Berechtigungskonzept festgelegt worden (siehe Senatsdrucksache 2001/0727 vom 26. Juni 2001). Darüber hinaus wird voraussichtlich in Kürze eine weitere Vereinbarung nach § 94 HmbPersVG abgeschlossen, die die Vergabe von Zugriffsrechten zum Schutz der Mitarbeiterinnen und Mitarbeiter bzw. ihrer Daten vor unzulässigen Leistungs- und Verhaltenskontrollen und unberechtigter Einsichtnahme konkretisiert. Danach darf niemand in der Lage sein, allein einen neuen SAP-User einzurichten, zu aktivieren und zu nutzen. Änderungen im Berechtigungssystem sind dauerhaft zu protokollieren.

In den Beschreibungen der standardisierten, auf Fachaufgaben bezogenen Rollen in SAP R/3 ist jeweils darzustellen, ob und in welchem Umfang diese auch Zugriffsrechte auf personenbezogene Daten von Mitarbeiterinnen und Mitarbeitern beinhalten. Es soll technisch so weit wie möglich ausgeschlossen werden, dass eine einzelne Person die vollständige Kontrolle über das SAP R/3-System erlangt. Berechtigungen zur Programmierung, zur Änderung von Systemeinstellungen oder andere weitreichende Rechte sollen in der Produktionsumgebung grundsätzlich nicht vergeben werden.

Ein umfassendes, die einzuhaltenden technischen und organisatorischen Sicherungsmaßnahmen beschreibendes Datenschutzkonzept wird zur Zeit erarbeitet. Ein Entwurf wurde bereits mit uns abgestimmt. Wir werden das Projekt weiter intensiv begleiten.

3.2.4 Zugangskontrolle zum PC mittels Fingerabdruck

Die Nutzung biometrischer Daten zur Authentifizierung ist vor dem Hintergrund der geplanten Speicherung solcher Daten in Ausweisdokumenten aus grundsätzlichen datenschutzrechtlichen Erwägungen bedenklich. Darüber hinaus sind zahlreiche Detailfragen noch nicht geklärt.

Die Finanzbehörde prüft zur Zeit, ob das bestehende Authentifizierungsverfahren für den Zugang zu Arbeitsplatzcomputern in der hamburgischen Verwaltung durch ein biometrisches Verfahren ersetzt werden kann. Dadurch soll sowohl eine erhöhte Sicherheit als auch gleichzeitig eine größere Benutzerfreundlichkeit erzielt werden.

Das derzeitige Verfahren basiert auf einer Benutzerkennung und einem geheimen Passwort. Dabei besteht das Risiko, dass Passworte weitergegeben werden oder dass nicht berechtigte Personen Passworte ausspähen und sich so Zugriff zu sensiblen Daten verschaffen. Dieser Missbrauch soll verhindert werden, indem sich die Nutzer mit einem Fingerabdruck als berechtigt ausweisen. Bei biometrischen Authentifizierungsverfahren werden die biometrischen Merkmale (vgl. 1.3) bzw. ein daraus errechneter komprimierter Datensatz, ein sogenanntes Template, gespeichert und mit den aktuellen Merkmalen des Nutzers verglichen. Nur wenn eine hinreichend große Übereinstimmung besteht, wird der Zugang freigegeben.

Die Überlegungen der Finanzbehörde zum neuen Authentifizierungsverfahren werden von der bundesweiten Planung überlagert, biometrische Merkmale in Ausweisdokumenten zu erfassen. Insbesondere bei einer zentralen Speicherung der biometrischen Daten besteht die Gefahr, dass diese als einheitliches Personenkennzeichen genutzt werden könnten. Ein solches Personenkennzeichen ist jedoch nach dem Bundesverfassungsgerichtsurteil zur Volkszählung nicht zulässig (vgl. 6.1). Vor allem aus diesem Grund halten wir die Nutzung von Fingerabdrücken zur Authentifizierung und eine zentrale

Speicherung der Templates für datenschutzrechtlich bedenklich. Es muss gewährleistet sein, dass die biometrischen Daten für die Zugangskontrolle zu den Arbeitsplatzcomputern nicht mit den Merkmalen in den Ausweisdokumenten abgeglichen werden können.

Neben diesen grundsätzlichen Erwägungen sind für die Planung weitere Datenschutzaspekte zu berücksichtigen. Die Finanzbehörde hat uns daher frühzeitig einbezogen. So haben wir darauf hingewiesen, dass eine zentrale Speicherung von biometrischen Merkmalen auch unabhängig von einer eventuellen Speicherung in Ausweisdokumenten wesentlich problematischer ist als eine Speicherung der Referenzdaten auf einer Chipkarte, die im Besitz des Nutzers verbleibt. Ein missbräuchlicher zentraler Zugriff auf eine sehr große Zahl von biometrischen Daten ist dann nicht möglich. Für die konkret ins Auge gefassten Systeme sind noch zahlreiche technische Fragen offen. Es muss insbesondere geklärt werden,

- wie und wie lange die Originaldaten der Fingerabdrücke gespeichert werden,
- wie und wo die Templates verschlüsselt und gespeichert werden,
- unter welchen Bedingungen diese Verschlüsselung rückgängig gemacht werden kann,
- wie ein missbräuchliches Einspielen von Templates verhindert wird,
- welche weiteren personenbezogenen Daten zur Überprüfung der Echtheit eines Fingerabdrucks verarbeitet werden und
- mit welchen Fehlerwahrscheinlichkeiten die Entscheidungen über den Zugang zum Arbeitsplatzrechner verbunden sind.

Mit der Finanzbehörde haben wir einen engen Informationsaustausch über die Datenschutzaspekte vereinbart.

3.3 Internet E-Mail am Arbeitsplatz

3.3.1 Sichere Nutzung des Internet

Durch die Verlagerung der Internet-Nutzung auf spezielle Server im Rahmen der Terminal-Dienste oder vergleichbare Techniken wird ein wirksamer Schutz vor den Risiken aus dem Internet realisiert.

In den neuen Microsoft-Betriebssystemen (Windows 2000 und in gewissem Rahmen auch Windows XP) stehen standardmäßig Techniken zur Verfügung, die es ermöglichen, über das Netzwerk Sitzungen auf anderen Rechnern zu eröffnen. Diese sog. Terminal-Dienste, die in ähnlicher Form von anderen Betriebssystemen und Herstellern bereits bekannt sind, machen es möglich, die Nutzung des Internet von anderen Anwendungen zu trennen und damit die Risiken, die die Internet-Nutzung mit sich bringt, vom Arbeitsplatz fernzuhalten.

Der Browser, der eine Verbindung ins Internet aufbaut, muss dann nicht mehr auf dem Arbeitsplatz-Rechner selbst ablaufen, sondern kann auf den weniger gefährdeten Terminal-Server verlagert werden. Sicherheitsprobleme, die in diesem Zusammenhang auftreten, wirken sich daher nur auf diese Maschine aus, nicht jedoch auf den Arbeitsplatz selbst. Sie können sich daher auf die dort gespeicherten oder zugreifbaren schützenswerten Daten nicht auswirken.

Die im 17.TB (3.3) vorgeschlagene Trennung der Benutzerumgebungen kann damit in der Form umgesetzt werden, dass die Umgebungen auf verschiedenen Servern realisiert werden; dies erhöht die damit erreichbare Sicherheit weiter.

Mit einer solchen Lösung ist ein gewisser Zusatzaufwand verbunden, da ein zusätzlicher Server in Betrieb genommen werden muss. Allerdings können sich mehrere Benutzer einen Server teilen; je nach Ausstattung (vor allem Hauptspeicher und Prozessorleistung) und Nutzung kann ein Server 50 und mehr Nutzer bedienen. Denkbar wäre auch ein entsprechendes Dienstleistungsangebot z.B. des Landesamts für Informationstechnik (LIT), das auf zentral betriebenen Servern für die Kunden bereitgehalten wird. Der Zugriff von dezentralen Arbeitsplätzen ist im Rahmen der verfügbaren Leitungskapazitäten über das FHH-Netz möglich.

In unserer Dienststelle haben wir durchweg positive Erfahrungen mit dieser Technik gemacht und werden sämtliche Benutzer bei uns entsprechend ausstatten. Auch das Landesamt für Verfassungsschutz wird Anfang kommenden Jahres einer größeren Zahl von Mitarbeitern über einen Terminal-Server den Zugang in das Internet direkt von ihren Arbeitsplatz-Rechnern ermöglichen.

3.3.2 Vereinbarung nach § 94 HmbPersVG

Die Rahmenvereinbarung über den Prozess zur Einführung und Nutzung allgemeiner automatisierter Bürofunktionen und multimedialer Technik (Bürokommunikation) und zur Entwicklung von E-Government zwischen dem Senat und den Spitzenorganisationen der Gewerkschaften berücksichtigt die datenschutzrechtlichen Anforderungen.

Die Rahmenvereinbarung vom 11. Oktober 2001 (MittVw 2001, Seite 210) wurde mit unserer Beteiligung erarbeitet. Sie beschreibt u.a. die Ziele bei der Einführung und dem Ausbau von allgemeinen Bürokommunikationsfunktionen. Geregelt wird auch die Nutzung von E-Mail. Dazu wird auf unsere datenschutzrechtlichen Hinweise verwiesen (11.1).

3.3.3 Checkliste

Vor Beginn der Nutzung von Internet und E-Mail am Arbeitsplatz sollte der Arbeitgeber bestimmte Vorgaben verbindlich festlegen.

Verwaltung und Privatwirtschaft nutzen das Internet und E-Mails als hilfreiche Mittel zur Informationsbeschaffung und zur schnellen Kommunikation. Dabei treten immer wieder Probleme auf, die bis zur fristlosen Kündigung eines Arbeitsverhältnisses führen können. Die wesentlichen Aspekte der Internet- und E-Mail-Nutzung sollten – schon zur Vermeidung von Missverständnissen – durch Betriebs- bzw. Dienstvereinbarungen verbindlich festgelegt werden. Die Mitarbeiter sind über den Rahmen des Einsatzes dieser Techniken umfassend zu unterrichten.

Die nachfolgende Checkliste soll bei der Lösung der wichtigsten Probleme helfen, die auch die schwierige Rechtslage berücksichtigt (siehe 27.1):

- Schulung der Arbeitnehmer über Risiken beim Einsatz von Kommunikationstechnologie
  - Weiß jeder Mitarbeiter, was die Nutzung von E-Mail und Internet bedeutet?
  - Werden die Mitarbeiter regelmäßig über die Bedingungen der Nutzung von E-Mail und Internet unterrichtet?
- Einrichtung technischer Schutzmaßnahmen wie Backup, Anti-Virusprogramme, Verschlüsselung, Firewall mit Sperr- bzw. Positivliste
  - Ist gewährleistet, dass diese Schutzmaßnahmen regelmäßig dem neuesten Stand der Technik angepasst werden?
  - Wer ist für die Gewährleistung der technisch-organisatorischen Maßnahmen verantwortlich?
- Maßnahmen zur Kontrolle der Internet-/E-Mail-Nutzung
  - Was wird routinemäßig protokolliert?
  - Welche Aktionen werden wie aufgezeichnet?
  - Wie lange bleiben die Daten gespeichert?
  - Wer hat Zugriff auf die Auswertungsdateien?
  - Wann liegt eine missbräuchliche Nutzung vor?
  - Welche Maßnahmen werden ergriffen, um eine missbräuchliche Inanspruchnahme zu erkennen?
  - Welche Maßnahmen werden bei Verdacht auf missbräuchliche Nutzung ergriffen?
  - Welche arbeitsrechtlichen Sanktionen sind möglich?
  - Welche Konsequenzen werden ggf. bei strafbaren Handlungen ergriffen?
  - Wie erfährt der Mitarbeiter von der Tatsache, dass seine Daten (ggf. zur Aufklärung missbräuchlicher Inanspruchnahme) ausgewertet wurden?

– Regelung mit klaren Grenzen zwischen dienstlicher und privater Nutzung von Internet und E-Mail
  - Steht jedem Mitarbeiter ein Exemplar dieser Regelungen zur Verfügung (Papier, Intranet)?
  - Werden Postfächer mit Zugriffsbeschränkungen ausschließlich auf den Eigentümer eingerichtet?
  - Ist die Vertretung geregelt – getrennt nach geplantem (z.B. Urlaub) und ungeplantem (z.B. Krankheit) Vertretungsfall?
  - Wer darf – außer dem Eigentümer und dem Vertreter – wann auf das Postfach zugreifen?
  - Wie wird mit Posteingang/-ausgang verfahren?
  - Können E-Mails als privat gekennzeichnet werden?
  - Bestehen besondere Regelungen über den Umgang mit privaten E-Mails?
– Unterrichtung bzw. Mitwirkung von Betriebs- bzw. Personalräten
– Information der Mitarbeiter über Betriebs- bzw. Dienstvereinbarungen und ggf. sonstige Regelungen zur Nutzung des Internet und von E-Mail
– Einbeziehung des betrieblichen Datenschutzbeauftragten

3.4 Dokumentenverwaltung

Die Ablösung einer herkömmlichen Papieraktenverwaltung durch ein elektronisches Dokumentenverwaltungssystem stellt nicht nur hohe Anforderungen an die (Ausfall-) Sicherheit des Systems und die langfristige und damit systemunabhängige Verfügbarkeit der Daten. Bei dem Einsatz elektronischer Dokumentenverwaltungssysteme muss auch den Anforderungen der informationellen Selbstbestimmung Rechnung getragen werden.

Für jede größere Organisation stellt eine effiziente Schriftgutverwaltung eine wesentliche Voraussetzung für einen reibungslosen Arbeitsablauf dar. In einem Arbeitsalltag, in welchem Informationen „blitzschnell“ aus dem Internet abrufbar sind oder zeitnah an die Mailbox diverser Empfänger übermittelt werden können, wird die herkömmliche Papieraktenverwaltung vielfach als Behinderung im täglichen Arbeitsablauf empfunden.

Abhilfe verspricht der Einsatz eines elektronischen Dokumentenverwaltungssystems. Sind die Schriftstücke einmal gescannt, indiziert und elektronisch abgelegt, ermöglichen elektronische Dokumentenverwaltungssysteme den schnellen, ungehinderten Online-Zugriff auf die Inhalte jedes einzelnen Dokumentes – jederzeit, an jedem angeschlossenen Arbeitsplatz. Dabei kann das Wiederauffinden von Dokumenten durch vielfältige Suchfunktionen unterstützt werden.

Der Aufbau einer elektronischen Dokumentenverwaltung setzt die digitalisierte Speicherung von Akteninhalten voraus. Im Gegensatz zu der Speicherung in Papierakten, für welche einige datenschutzrechtliche Sonderregelungen gelten, handelt es sich hierbei um Sammlungen personenbezogener Daten, welche durch automatisierte Verfahren verarbeitet werden können und damit unter den in § 4 Abs. 6 HmbDSG definierten Begriff der automatisierten Datei fallen.

Bei der Einführung eines entsprechenden, automatisierten Verfahrens, mit dem personenbezogene Daten verarbeitet werden sollen, sind daher die datenschutzrechtlichen Bestimmungen und Grundsätze zu beachten. So hat sich die Gestaltung von technischen Einrichtungen für die Verarbeitung personenbezogener Daten z.B. auch an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben und zu verarbeiten (Grundsatz der Datensparsamkeit – § 5 Abs. 4 HmbDSG , siehe 3.1.1). Personenbezogene Daten dürfen grundsätzlich nur für die Zwecke verarbeitet werden, für welche diese ursprünglich erhoben wurden (Zweckbindungsgebot) und das Zugriffskonzept muss gewährleisten, dass die Daten nur dem Personenkreis zugänglich sind, welche diese für die Erfüllung ihrer Aufgaben benötigen („need to know“).

Die im Projekt DOKUMENTA der Behörde für Inneres -Amt A- eingesetzte und erprobte Software (Registraturmodul und Rechercheclient) sowie entsprechende Unterstützung (Schulungen, Projekt- und Anwenderunterstützung) wird inzwischen vom Landesamt für Informationstechnik (LIT) im Wege der Auftragsdatenverarbeitung als Dienstleistung für die Behörden angeboten. Mit der Bereitstellung des notwendigen technischen Verfahrens übernimmt das LIT die Gewährleistung technischer und organisatorischer Maßnahmen zur Datensicherung gemäß LIT-Datensicherungsstandard bei der Auftragsdatenverarbeitung. Die inhaltliche, datenschutzgerechte Ausgestaltung des Verfahrens muss durch die auftraggebenden Behörden erfolgen.

In diversen Behörden (z.B. Justizbehörde, Senatskanzlei, Umweltbehörde, Kulturbehörde, Finanzbehörde) wurden zwischenzeitlich Projekte mit dem Ziel des Einsatzes einer elektronischen Dokumentenverwaltung eingesetzt, an welchen der Hamburgische Datenschutzbeauftragte zunächst nicht beteiligt wurde. In ersten Gesprächsrunden mit den Projekten mussten wir feststellen, dass eine umfassende Auseinandersetzung mit den datenschutzrechtlichen Problemen, welche mit der Einrichtung eines elektronischen Dokumentenverwaltungssystems verbunden sind, vielfach noch nicht in ausreichendem Maß erfolgt ist.

3.4.1 Digitalisierte Schriftstücke /Akteninhalte

In Abhängigkeit von der Aufgabenstellung der jeweiligen Dienststellen können die bisher in Papierakten zu verwaltenden Schriftstücke Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer Personen (personenbezogene Daten) unterschiedlicher Sensibilität beinhalten.

Die Verarbeitung personenbezogener Daten ist gemäß § 5 Abs. 1 HmbDSG grundsätzlich nur zulässig , soweit das Hamburgische Datenschutzgesetz oder eine besondere Rechtsvorschrift über den Datenschutz dies erlaubt oder die Betroffenen eingewilligt haben. Für die manuelle Datenverarbeitung in und aus nicht weiter strukturierten konventionellen Akten bzw. die nicht-automatisierte Verarbeitung außerhalb von Dateien gelten dabei einige datenschutzrechtliche Sonderregelungen, welche u.a. in den Besonderheiten der Papieraktenverwaltung hinsichtlich der eingeschränkten Möglichkeiten der Datenzugänglichkeit und Datenauswertung begründet sind.

Da im Gegensatz zu der Speicherung in Papierakten durch eine digitalisierte Speicherung personenbezogene Datensammlungen entstehen, welche durch automatisierte Verfahren verarbeitet werden können und damit als automatisierte Datei anzusehen sind, kann dieses Aktenprivileg bei „elektronischen Akten“ keine Anwendung finden.

Vor dem Einsatz eines automatisierten Datendokumentations- und Archivierungsverfahrens muss daher zunächst geprüft werden, ob und welche personenbezogenen Daten in den vorhandenen Akten enthalten sind und für die Nutzung des Verfahrens ggf. zusätzlich erfasst werden müssen. Vor der Digitalisierung von Daten muss geklärt werden, in welchem Umfang eine automatisierte Verarbeitung der betroffenen personenbezogenen Daten erforderlich und rechtlich zulässig ist. Vor der Entscheidung über die Übernahme personenbezogener Daten in ein elektronisches Dokumentenverwaltungssystem, haben die Daten verarbeitenden Stellen zu untersuchen, ob und in welchem Umfang mit der Nutzung des Verfahrens Rechte der Betroffenen verbunden sind. Die Übernahme ist nur zulässig, soweit derartige Gefahren durch technische und organisatorische Maßnahmen wirksam beherrscht werden können (§ 8 Abs. 4 HmbDSG).

3.4.2 Ablagestruktur /Zweckbindungsgebot

Das Zweckbindungsgebot verlangt bei der Bearbeitung und Nutzung personenbezogener Daten die Trennung funktional unterschiedlicher Verwaltungsbereiche und die Unterbindung unautorisierter Datenflüsse zwischen Stellen mit unterschiedlichen Aufgaben und Funktionen (informationelle Gewaltenteilung). Dies setzt voraus, dass digitalisierte Dokumente und elektronische Akten verschiedener Verwaltungsbereiche mit unterschiedlichen Aufgabenstellungen und Funktionen in getrennten Datenbeständen ge-

speichert bzw. so gegeneinander „abgeschottet“ werden, dass zugriffsberechtigte Mitarbeiterinnen und Mitarbeiter ausschließlich die Daten angezeigt bekommen, die sie für die Erfüllung der Aufgaben benötigt und welche für diese Zwecke erhoben und gespeichert wurden.

Dies muss bereits bei der Online-Bereitstellung von Übersichten, Listen, Verzeichnissen, sowie „Aktenplänen“ beachtet werden, da beispielsweise aufgrund der aufgabenbezogenen Strukturierung des elektronischen „Aktenplans“ bereits aus der Zuordnung personenbezogener „Aktentitel“ im Dokumentenverzeichnis Rückschlüsse auf persönliche oder sachliche Verhältnisse einzelner Personen möglich sein können.

3.4.3 Zugriffsmanagement

Mit der Übertragung von Zugriffsrechten wird dem Nutzer eines elektronischen Dokumentenverwaltungssystems ein durch diverse Suchfunktionen unterstützter, permanenter, schneller und ungehinderter Aktenzugriff ermöglicht. Die im herkömmlichen Verfahren zumeist gegebene Zutrittskontrolle beim Einzelzugriff durch eine weitere Person (Vier-Augen-Prinzip) entfällt. Es gibt in der Regel keine Einzelanforderungen bei der Registratur, keine Kontrolle durch den sachlich zuständigen Sachbearbeiter, denn es besteht keine Notwendigkeit, die Akte physisch zu entnehmen oder zu transportieren.

Im Hinblick auf personenbezogene Inhalte elektronischer „Akten“ sind daher an die Datenspeicherung und das Zugriffsmanagement (Zugriffshierarchie, Rechtematrix) besondere Anforderungen zu stellen.

Die Aufgabenverteilung aller Beteiligten muss vor der Einführung des Systems klar definiert und gegeneinander abgrenzt werden. Die für die Daten verantwortliche Stelle muss die zugriffsberechtigten Personen (Sachbearbeiter, Vorgesetzte, Registratur, Administratoren, Vertreter, ...) für die elektronischen „Akten“ ermitteln, festlegen und dokumentieren. Dabei sind gesetzlich vorgeschriebene Verarbeitungs-, Übermittlungs- und Zugriffsbeschränkungen ebenso zu beachten wie das Zweckbindungsgebot und Geheimhaltungsvorschriften. Die individuellen, aufgabenbezogen festzulegenden Zugriffsprofile müssen revisionssicher dokumentiert und organisatorischen Veränderungen zeitnah angepasst werden.

Neben der Festlegung des regelmäßig zugriffsberechtigten Personenkreises müssen Regelungen getroffen werden, wie Einsichtsrechte und die bisherige Bereitstellung/Übersendung von Akten (beispielsweise für am Verfahren Beteiligte, parlamentarische Untersuchungsausschüsse, Kontrollinstanzen, Gerichte oder auch eine Aktenabgabe wegen Zuständigkeitswechsels) künftig organisiert und Anonymisierungspflichten technisch umgesetzt werden sollen.

Der Einrichtung von dauerhaften Zugriffsrechten (Online-Anschlüssen) zur automatisierten Direktabfrage durch Dritte kommt bei personenbezogenen Datenbeständen eine besondere Bedeutung zu, weil die abrufende Stelle nach Einrichtung eines solchen Anschlusses (unabhängig von der dienstlichen Notwendigkeit im Einzelfall) über den gesamten Bestand der bereitgehaltenen Daten verfügen kann. Diese mögliche Übermittlung einer sehr umfangreichen Anzahl personenbezogener Daten an Dritte birgt erhebliche Gefahren für das Recht auf informationelle Selbstbestimmung in sich und ist daher nur zulässig, wenn eine Rechtsvorschrift dies ausdrücklich zulässt (automatisiertes Abrufverfahren – § 11 HmbDSG).

3.4.4 Such-/Recherchefunktionen

Der Zugriff auf Papierdokumente ist bisher in der Regel nur über die vordefinierten Ordnungskriterien möglich, nach welchen ihre Ablage erfolgt ist bzw. welche bei ihrer Ablage definiert wurden (Aktenplan, Aktenverzeichnis, Aktentitel, Stichwortverzeichnis).

Die Struktur der Aktenpläne und -verzeichnisse und Akten ist in der Regel sach- und aufgabenbezogen. Da ein Zugriff und eine Auswertung nach anderen Kriterien (insbesondere nach Einzelinhalten von Schriftstücken) grundsätzlich nicht möglich ist, ist eine Zweckbindung der Daten systembedingt gewährleistet.

Elektronische Dokumentenverwaltungssysteme können diverse Suchfunktionen beinhalten. Sofern die Dokumente personenbezogene Daten umfassen, sollten die möglichen Suchkriterien so genau definiert und festgelegt werden können, dass freie Abfragen nach unbestimmten Zusammenhängen nicht möglich sind.

Durch den Einsatz einer OCR-Texterkennungssoftware und der Möglichkeit einer Volltextrecherche ist grundsätzlich auch eine Auswertung von Dokumenteninhalten möglich. Insbesondere die Volltextrecherche kann die Rechte der Betroffenen gefährden, da hierdurch freie Zugriffs- und Auswertungsmöglichkeiten entstehen, welche nicht aufgabenbezogen eingrenzbar sind. Eine weitere Gefahr besteht darin, dass aufgrund der Auswahl fehlerhafter Suchkriterien die für die Bearbeitung erforderlichen Unterlagen ggf. nicht vollständig – dafür aber für die Bearbeitung völlig unerhebliche Unterlagen – in der Trefferliste enthalten sein können.

Der Zugriffsschutz muss auch im Rahmen der Such-/Recherchefunktionen gewährleisten, dass die jeweiligen Nutzer in und über Trefferlisten nur die Akten und Dokumente angezeigt bekommen und einsehen können, für welche ihnen eine aufgabenbezogene Zugriffsberechtigung erteilt worden ist.

In Abhängigkeit von der Sensibilität der enthaltenen Daten kann die Notwendigkeit bestehen, weitreichende Suchfunktionen nur einem beschränkten Personenkreis (z.B. der Registratur) zur Verfügung zu stellen und eine Protokollierung der Datenzugriffe vorzunehmen.

3.4.5 Dokumentenbeschreibung

Zu jedem (gescannten) Dokument wird ein aus mehreren, beschreibenden Datenfeldern bestehender Datenbankeintrag (Deskriptor) erstellt, über welche die Dokumente beschrieben und später gesucht werden können.

Eine erfolgreiche Suche über den Deskriptor setzt voraus, dass die beschreibenden Daten für die Dokumente nach feststehenden Regeln einheitlich erfasst werden. Bei der Festlegung dieser Indizierungsregeln ist die datenschutzrechtliche Zulässigkeit der Datenbankeinträge zu prüfen. Durch die Erfassung personenbezogener Daten für die Indizierung von Dokumenten (z.B. Name der Ersteller/Mitarbeiter) können sich unzulässige Auswertungsmöglichkeiten (z.B. Möglichkeiten der Leistungskontrolle von Mitarbeitern) ergeben.

3.4.6 Netzsicherheit/Verschlüsselung

Die Versendung sensibler Schriftstücke über die Behördenpost ist gemäß den dafür geltenden Bestimmungen nur in verschlossenen Umschlägen zulässig. Eine entsprechende Vertraulichkeit kann bei einer elektronischen Übertragung sensibler Daten und Schriftstücke nur durch Verschlüsselungsverfahren gewährleistet werden.

Bei der Nutzung elektronischer Akten werden die jeweiligen Dokumente über das Netz übertragen. Die Aufnahme vertraulicher, sensibler Daten in das Dokumentenverwaltungssystem setzt daher die Gewährleistung einer verschlüsselten Übertragung zwischen dem LIT und den Behörden voraus.

Auf der Grundlage der bisher in den Projekten geführten Gespräche gehen wir davon aus, dass eine Übernahme von Personalakten in das elektronische Dokumentenverwaltungssystem nicht erfolgen wird.

3.4.7 Speichermedien

Gegenstand der Aussonderung herkömmlicher Schriftgutverwaltung waren bisher abgeschlossene, vollständige Akten. In automatisierten Dateien gespeicherte Daten sind hingegen regelmäßig alle vier Jahre auf ihre Erforderlichkeit hin zu überprüfen und die Datenbestände zu bereinigen (§ 19 Abs. 6 HmbDSG).

Ein System zur Dokumentenaufbewahrung muss daher Löschfunktionen bieten, mit deren Hilfe alle Vorgänge unverzüglich gelöscht werden können, deren Aufbewahrungsfristen erreicht sind. Unter Löschen ist im Sinne der Datenschutzgesetze stets das unwiderrufliche Unkenntlichmachen der Daten

zu verstehen. Diese Anforderung schränkt die Möglichkeit des Einsatzes nur einmal beschreibbarer Datenträger (z.B. CD-ROM) ein, da auf diesen Datenträgern gespeicherte Dokumente nicht mehr verändert und somit auch nicht unkenntlich gemacht werden können. Da das Dokument auch bei der Löschung des rekonstruierbaren Verweises auf dieses Dokument weiterhin gespeichert bleibt, kann eine Löschung bei einem Einsatz nur einmal beschreibbarer Datenträger letztlich nur dadurch realisiert werden, dass ein neuer Datenträger angelegt wird, auf welchen ausschließlich die noch weiterhin zu speichernden Datensätze des Ursprungsdatenträgers kopiert werden. Der alte Datenträger ist anschließend physisch zu vernichten. Diese Variante bietet sich allerdings nur dann an, wenn die Löschläufe nur relativ selten durchgeführt werden müssen.

Neben Löschverpflichtungen sind bei der Speicherung von personenbezogenen Daten Korrekturansprüche Betroffener zu berücksichtigen. Das Verfahren ist so zu gestalten, das Berichtigungen der gespeicherten Daten, die Speicherung ergänzender Angaben und die Sperrung von Daten unter bestimmten Voraussetzungen umsetzbar bleiben (§ 19 HmbDSG).

Elektronische „Akten“ können ohne die physische Begrenzung von Papierbänden tendenziell unendlich groß werden. Regeln für die Aussonderung und Archivierung und Löschung sollten daher auch die Bildung zeitlicher Aktenschnitte sowie die Herausnahme abgeschlossener Vorgänge aus dem Online-Zugriff vorsehen.

3.4.8 Authentizität/Integrität der Daten

Die Aufbewahrung von Dokumenten dient u.a. dem Ziel, den genauen Ablauf und die Rechtmäßigkeit einzelner Vorgänge nachvollziehen zu können. Wird der Akteninhalt (anstelle der Urschrift) auf Bild- oder Datenträgern aufbewahrt, muss die Dokumentenverwaltung daher technisch und organisatorisch so gestaltet sein, dass kein Verlust der Dokumente und keine unerkannte Veränderung ihrer spezifischen Inhalte auftreten kann. Während der Dauer der spezifischen Aufbewahrungsfristen müssen die Dokumente verfügbar sein und jederzeit innerhalb einer angemessenen Frist so lesbar gemacht werden können, dass sie dem Original entsprechen und ein Gericht sie in einem Verfahren als Beweisstück akzeptiert.

Durch das Scannen von Papierdokumenten wird eine digitale Kopie einer Vorlage erstellt. In Abhängigkeit davon, ob das Schriftstück als farbiges oder schwarz/weiß Bild oder unter Einsatz einer OCR-Texterkennung als Text gescannt wird, können bereits bei der Erstellung des digitalen Dokumentes Informationen verloren gehen oder manipuliert werden. Da nach einer Vernichtung der Papierdokumente weder feststellbar sein wird, ob ein Originaldokument (Originalabdruck eines Dienstsiegels, Originalunterschrift etc.) oder eine Kopie als Vorlage verwendet wurde und sämtliche Zeichen und Merkmale

eines Schriftstückes fehlerfrei digital umgesetzt wurden, muss durch technische und organisatorische Maßnahmen sichergestellt werden, dass die Dokumente beim Scannen zweifelsfrei unverändert und vollständig vom Original übernommen wurden.

Digitalisierte, digital erstellte bzw. elektronisch übermittelte Dokumente müssen für die Dauer der Aufbewahrungszeiten dem jeweiligen Urheber zweifelsfrei zugeordnet werden können und gegen unzulässige, unerkannte Veränderungen geschützt sein. Technisch lässt sich dies beispielsweise dadurch gewährleisten, dass die Dokumente digital signiert werden (siehe 3.6). Dann lässt sich beim Aufruf eines Dokumentes feststellen, ob unberechtigte Änderungen daran vorgenommen wurden. Die Verwendung digitaler Signaturen als Sicherheitsinstrument für die Daten, setzt für die Gewährleistung eines dauerhaft sicheren Nachweises ihrer Authentizität jedoch voraus, dass die Zertifikate zum Prüfungszeitpunkt noch vorhanden sind und ihr Sicherheitswert auch in Anbetracht wachsender Rechnerkapazität und der Weiterentwicklung der technischen Möglichkeiten Bestand hat.

Wir werden uns an den Projekten in den einzelnen Behörden und Ämtern weiter aktiv beteiligen und für die Berücksichtigung der datenschutzrechtlichen Belange eintreten.

3.5 Internet

3.5.1 Neuer Rechtsrahmen für Tele- und Mediendienste

Mit der Verabschiedung des Gesetzes über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (Elektronischer Geschäftsverkehr-Gesetz – EGG) wurde auch der Rechtsrahmen für die Verarbeitung personenbezogener Daten im Internet (16. TB, 3.5) weiterentwickelt.

Das EGG enthält in Art. 1 Änderungen des Teledienstegesetzes (TDG), Art. 3 Änderungen des Teledienstedatenschutzgesetzes (TDDSG). Die Länder beabsichtigen eine Anpassung der Datenschutzvorschriften des Mediendienste-Staatsvertrages (MDStV) an die neuen Bestimmungen des TDDSG in der ersten Jahreshälfte 2002.

Durch §§6,7 TDG werden die Informations- und Kennzeichnungspflichten für Diensteanbieter ausgeweitet. Gemäß §6 TDG sind für geschäftsmäßige Teledienste nicht nur Namen und Anschriften der Verantwortlichen anzugeben, sondern darüber hinaus auch Angaben, die eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation mit ihnen ermöglichen, einschließlich der E-Mail-Adresse. Ferner müssen Registernummern des Handels-, Vereins- oder Genossenschaftsregisters, bei freien Berufen Kammerzugehörigkeiten und Berufsbezeichnungen, ferner ggf. Umsatzsteueridentifikationsnummern angegeben werden. Gemäß §7 TDG bestehen bei „kommerziellen Kommunikationen“ zusätzliche Informationspflichten. Insbesondere müssen kommerzielle Angebote eindeutig als solche zu erkennen

sein; dies bedeutet, dass z. B. Werbe-E-Mails und sog. Werbebanner ausdrücklich zu kennzeichnen sind.

In §§ 8 bis 11 TDG werden die Verantwortlichkeiten für die angebotenen Informationen neu geregelt. Dabei wird die bisherige Unterscheidung zwischen dem Angebot eigener und fremder Inhalte und der bloßen Zugangsvermittlung (§ 5 TDG 1997) grundsätzlich beibehalten, jedoch weiter differenziert. Ausgehend von dem Grundsatz, dass Diensteanbieter für eigene Informationen, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich sind (§ 8 TDG), wird zwischen der Durchleitung (§ 9 TDG), der Zwischenspeicherung zur beschleunigten Übermittlung (§ 10 TDG) und der Speicherung von Informationen (§ 11 TDG) unterschieden.

In § 1 Abs. 1 TDDSG erfolgt die Klarstellung, dass das Gesetz ausschließlich für die Verarbeitung personenbezogener Daten gilt, also nicht für Daten juristischer Personen. Ferner wird der Anwendungsbereich der Vorschriften dahingehend präzisiert, dass das Gesetz nicht anzuwenden ist auf die Datenverarbeitung in Dienst- und Arbeitsverhältnissen, soweit die Nutzung der Teledienste zu ausschließlich beruflichen oder dienstlichen Zwecken erfolgt. Ferner ist das TDDSG nicht anwendbar auf die Kommunikation von oder zwischen Unternehmen oder öffentlichen Stellen, soweit die Nutzung der Teledienste ausschließlich zur Steuerung von Arbeits- oder Geschäftsprozessen erfolgt.

Im Hinblick auf die im Mai 2001 in Kraft getretene Novelle des BDSG (vgl. 2.1.2) wurden einige Bestimmungen im TDDSG gestrichen, die in das BDSG Eingang gefunden haben, insb. die Bestimmungen zur Datenvermeidung und Datensparsamkeit. Diese Vorschriften sind weiterhin auch von den Anbietern von Telediensten zu beachten, denn die Schutzvorschriften des BDSG kommen ergänzend zum TDDSG zur Anwendung.

In der Gesetzesbegründung wurde klargestellt, dass die Erlaubnistatbestände für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch Anbieter von Telediensten im TDDSG abschließend geregelt sind und dass deshalb nicht auf allgemeine Erlaubnistatbestände des BDSG zurückgegriffen werden kann. Dem entsprechend ist eine Zweckänderung von Bestandsdaten für Zwecke der Werbung, Markt- und Meinungsforschung weiterhin nur dann zulässig, wenn der Betroffene hierin ausdrücklich eingewilligt hat.

Bedeutsam ist auch die Einführung eines ausdrücklichen Widerspruchsrechts des Betroffenen, wenn Nutzungsdaten zur Erstellung von Nutzungsprofilen unter Pseudonym verwendet werden. Der Diensteanbieter hat die Nutzer auf ihr Widerspruchsrecht hinzuweisen (§ 6 Abs. 3 TDDSG).

Dem Diensteanbieter ist es nunmehr gestattet, Abrechnungsdaten auch für die Aufklärung der missbräuchlichen Inanspruchnahme seiner Dienste zu nutzen, wenn ihm tatsächliche Anhaltspunkte für einen entsprechenden Missbrauchsfall vorliegen (§ 6 Abs. 8 TDDSG).

Schließlich wurden in § 9 TDDSG Bußgeldvorschriften eingeführt. Verstöße gegen das TDDSG können mit einer Geldbuße bis zu 100.000 DM geahndet werden.

Eine fortgeschriebene Orientierungshilfe zum Datenschutz für die Anbieter von Tele- und Mediendiensten (vgl. 17. TB, 3.7) ist aus unserem Internet-Angebot (www.hamburg.datenschutz.de) abrufbar.

3.5.2 Verarbeitung personenbezogener Daten durch Internet-Provider

Bei der Inanspruchnahme des Internet entstehen vielfältige personenbezogene Daten, die Auskunft über das „Surfverhalten" der Internet-Nutzer geben. Die Daten dürfen von den Diensteanbietern nur unter den im Multimediarecht genannten Voraussetzungen erhoben, verarbeitet und genutzt werden.

Während im „real life" eine personenbezogene Registrierung des Verhaltens des Einzelnen bisher nur in Ausnahmefällen stattfindet, ist die Protokollierung des Nutzungsverhaltens im Internet die Regel. Jeder Mausklick im Internet lässt an verschiedenen Stellen Nutzungsdaten entstehen. Dies ist zum einen technisch bedingt, da die bei der Kommunikation über das Internet beteiligten Rechner durch IP-Adressen identifiziert werden. Zum anderen haben manche Diensteanbieter im Internet starke wirtschaftliche Interessen daran, direkt mit den Nutzern zu kommunizieren und ihnen personalisierte Dienstleistungen zu verkaufen.

Die Rechtsgrundlagen zur Erhebung und Verarbeitung personenbezogener Daten ergeben sich für Tele- und Mediendienste aus dem Teledienstedatenschutzgesetz beziehungsweise aus dem Mediendienste-Staatsvertrag (vgl. 3.5.1). Die Zulässigkeit der Verarbeitung von Bestands- und Verbindungsdaten bei E-Mail richtet sich nach dem Telekommunikationsgesetz (TKG) und der Telekommunikations-Datenschutzverordnung (TDSV), da es sich bei E-Mail um einen Telekommunikationsdienst handelt. Die Diensteanbieter dürfen über die in diesen Vorschriften enthaltenen gesetzlichen Befugnisse hinaus keine Daten speichern, es sei denn, eine andere gesetzliche Regelung sieht dies vor.

Bestandsdaten sind Daten, die für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses erforderlich sind. Dies können sein: Name, Anschrift, E-Mail-Adresse, Telefon- oder Telefaxnummer, Geburtsdatum, Bankverbindung, Kreditkartennummer, User-ID und ähnliche Angaben. Bestandsdaten werden bei Zugangs-Providern und bei solchen Telediensteanbietern erhoben, die eine Vertragsbeziehung zwischen dem Anbieter und dem Nutzer voraussetzen, also im wesentlichen bei kostenpflichtigen Diensten.

Die Diensteanbieter dürfen nur die Bestandsdaten speichern, die für die Vertragsgestaltung und -abwicklung erforderlich sind. Die Nutzung der Daten für andere Zwecke außerhalb der gesetzlichen Erlaubnisse – also auch für Werbung und zur Marktforschung – bedarf grundsätzlich einer Einwilligung des Betroffenen. Ein Rückgriff auf die allgemeinen Erlaubnisnormen des BDSG ist nicht möglich.

Verbindungsdaten bei E-Mail-Diensten sind diejenigen Daten, die beim Senden bzw. beim Empfangen von elektronischen Postsendungen anfallen, insbesondere die E-Mail-Adressen von Absender und Empfänger, Zeitpunkte der Sendung bzw. Zustellung und Routing-Informationen (Angaben über diejenigen Rechner, die eine E-Mail durchgeleitet haben). Nicht zu den Verbindungsdaten gehören Angaben mit Bezug zum Inhalt, also auch Bezeichnungen von Datei-Anlagen und über den Betreff.

Die zulässige Speicherung der Verbindungsdaten durch E-Mail-Anbieter ist auf Telekommunikationszwecke beschränkt (Erbringung des Dienstes, Abrechnung und Missbrauchsaufklärung). Daten, die für diese Zwecke nicht mehr erforderlich sind, müssen gelöscht werden.

Nutzungsdaten sind Daten, die erforderlich sind, um die Inanspruchnahme von Tele- und Mediendiensten zu ermöglichen und abzurechnen. Zu den Nutzungsdaten gehören Merkmale zur Identifikation des Nutzers, Angaben über Beginn und Ende sowie Umfang der jeweiligen Nutzung und Angaben über die von den Nutzenden in Anspruch genommenen Tele- bzw. Mediendienste.

Diensteanbieter dürfen Nutzungsdaten erheben und verarbeiten, soweit dies zur Erbringung und Abrechnung eines Tele- oder Mediendienstes erforderlich ist. Die für diese Zwecke gespeicherten Daten dürfen bei Vorliegen zu belegender konkreter Anhaltspunkte auch zur Missbrauchsaufklärung verwendet werden.

3.5.3 Befugnisse von Strafverfolgungsbehörden zur Internet-Überwachung

Verbindungs- und Nutzungsdaten unterliegen dem Fernmeldegeheimnis. Polizei, Strafverfolgungsbehörden und Geheimdienste dürfen auf diese Daten nur auf Grund einer ausdrücklichen gesetzlichen Befugnis zugreifen. Eine generelle Verpflichtung der Diensteanbieter zur Speicherung dieser Daten und von Bestandsdaten für eine mögliche spätere Strafverfolgung würde zu einer unzulässigen Vorratsdatenspeicherung führen.

Soweit eine staatliche Stelle die Herausgabe personenbezogener Daten bzw. die Überwachung eines E-Mail-Anschlusses verlangt, muss sie gegenüber dem Diensteanbieter die Rechtsgrundlage ihrer Forderung darlegen und ggf. notwendige richterliche Anordnungen beibringen. Der Diensteanbieter hat sich von der Einhaltung der formalen Anforderungen an eine entsprechende Maßnahme zu vergewissern, einer Verpflichtung zur inhaltlichen Prüfung der entsprechenden Anordnungen unterliegt er jedoch grundsätzlich nicht. Bei Zweifeln in Bezug auf polizeiliche bzw. staatsanwaltschaftliche Anforderungen insb. hinsichtlich der Übereinstimmung einer Anforderung mit dem Text von richterlichen Anordnungen kann sich der Provider an den Hamburgischen Datenschutzbeauftragten wenden.

Da die Bestandsdaten nicht dem Fernmeldegeheimnis unterliegen, dürfen Strafverfolgungsbehörden auf diese Daten im Rahmen ihrer allgemeinen strafprozessualen Befugnisse (insb. Zeugenbefragung, Durchsuchung und Beschlagnahme) zugreifen. Hinsichtlich der Bestandsdaten der Telekommunikation (also auch bei E-Mail-Diensten) bestehen zusätzliche Auskunftsverpflichtungen gemäß § 89 Abs. 6 TKG.

Fernmeldegeheimnis

Das Fernmeldegeheimnis (Art. 10 GG) schützt die persönliche Geheimsphäre und den Kommunikationsvorgang gegen unberechtigte Eingriffe staatlicher Stellen und gewährleistet die Möglichkeit für die Einzelnen, untereinander nicht für die Öffentlichkeit bestimmte Nachrichten auszutauschen. Das einfachgesetzliche Fernmeldegeheimnis (§ 85 TKG) verpflichtet private Anbieter von Telekommunikationsdienstleistungen. Das Fernmeldegeheimnis umfasst neben den Kommunikationsinhalten auch die „näheren Umstände“ der Telekommunikation, d. h. insbesondere die Angaben über Zeitpunkte, Standort der Kommunikationseinrichtung und Kommunikationspartner.

Das Fernmeldegeheimnis schützt auch Verbindungsdaten. Für ihre Weitergabe an Strafverfolgungsbehörden ist bisher § 12 Fernmeldeanlagengesetz (FAG) einschlägig. Die nur befristet bis Ende 2001 geltende Regelung des § 12 FAG soll nach dem aktuellen Regierungsentwurf eines Gesetzes zu Änderung der Strafprozessordnung durch die §§ 100g, h StPO abgelöst werden. Danach soll einerseits der Zugriff auf Verbindungsdaten nicht mehr beim Verdacht jeglicher Straftat, sondern nur noch beim Verdacht schwerer Straftaten oder von Straftaten mittels einer Endeinrichtung nach § 3 Nr. 3 TKG statthaft sein. Andererseits würde die Neuregelung im Gegensatz zu § 12 FAG auch den Zugriff auf erst künftig anfallende Verbindungsdaten ermöglichen. Aus unserer Sicht muss auch der Zugriff auf Verbindungsdaten einer Evaluation unter-

worfen werden, d. h. es muss – wie bei der Überwachung von Inhaltsdaten – seitens der Strafverfolgungsbehörden nachgeprüft werden, ob und inwieweit es sich bei den Eingriffsbefugnissen in das Fernmeldegeheimnis um geeignete und dem Grundsatz der Verhältnismäßigkeit entsprechende Mittel handelt.

Daten mit Inhaltsbezug (neben dem eigentlichen Inhalt der Mail auch der Betreff, Dateianlagen und deren Bezeichnungen) dürfen auf Grund dieser Regelungen nicht an Strafverfolgungsbehörden übermittelt werden, da es sich nicht um Verbindungsdaten handelt.

Rechtsgrundlage für die Überwachung von Inhalten sind §§ 100a ff. StPO, § 39 Außenwirtschaftsgesetz (AWG) und das Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G10). Die Anordnung nach §§ 100 a, b StPO darf nur durch den Richter oder bei Gefahr im Verzuge – für die ersten drei Tage – auch durch die Staatsanwaltschaft, nicht aber durch deren Hilfsbeamte, getroffen werden. Die angeordneten Maßnahmen berechtigen die Überwachung zukünftiger Telekommunikationsvorgänge und enthalten auch die Verpflichtung für den Diensteanbieter, die entsprechenden E-Mails einschließlich der Verbindungsdaten zu speichern bzw. an die zuständige Strafverfolgungsbehörde herauszugeben.

Nach der Rechtsprechung des BGH stellt ein Zugriff von Strafverfolgungsbehörden auf Inhalte von E-Mail-Postfächern ebenfalls eine Telekommunikationsüberwachung dar. Das Eindringen in E-Mail-Systeme kann nicht auf die strafprozessualen Befugnisse zur Beschlagnahme von Gegenständen oder zur Durchsuchung von Räumen gestützt werden, insbesondere weil der Zugriff anders als bei den vorgenannten Maßnahmen im Regelfall geheim ist und auch die zukünftige Kommunikation umfasst.

Die am 24. Oktober 2001 beschlossene Telekommunikations-Überwachungsverordnung (TKÜV) verpflichtet auch die Anbieter von E-Mail-Diensten (nicht jedoch sonstige Internet Service Provider und Access Provider) zur Bereitstellung technischer Möglichkeiten zur Überwachung der E-Mail-Kommunikation, die über die Kennungen abgewickelt wird, auf die sich die Überwachungsanordnung bezieht.

Nutzungsdaten und die über das Internet kommunizierten Inhalte werden ebenfalls durch das Fernmeldegeheimnis (Art. 10 GG) geschützt, weil Tele- und Mediendienste auf Basis von Telekommunikationsdiensten abgewickelt werden und es sich deshalb um Inhalte der Telekommunikation handelt. Diese Daten dürfen grundsätzlich nur gemäß 100a,b StPO herausgegeben werden (s. oben).

Im Zusammenhang mit der Bekämpfung der Datennetzkriminalität wird von Sicherheitsbehörden gefordert, eine generelle Verpflichtung zur vorsorglichen Speicherung von Verbindungs- und Nutzungsdaten einzuführen. Nach unse-

rer Auffassung wäre eine solche Vorschrift verfassungswidrig. Das Bundesverfassungsgericht hat wiederholt festgestellt, dass die Speicherung personenbezogener Daten nicht zu einer Rundumbeobachtung der Bürger führen darf. Das wäre aber im Bereich der Internetnutzung mit der angestrebten Regelung der Fall. Dieses Verfahren würde den mit den Vorschriften über Tele- und Mediendienste gewährleisteten Datenschutz in unvertretbarer Weise abbauen. Es widerspräche auch dem sowohl in § 3a BDSG als auch in § 5 Abs. 4 HmbDSG (vgl. 3.1.1) enthaltenen Gebot, die Entwicklung und den Einsatz von technischen Verfahren daran auszurichten, keine bzw. so wenig wie möglich personenbezogene Daten zu verarbeiten (Datenvermeidung bzw. -sparsamkeit).

Die Forderung nach einer Vorratsdatenspeicherung von Nutzungs- und Verbindungsdaten lässt sich vergleichen mit einer Verpflichtung der Post, sämtliche Absender- und Empfängerangaben im Briefverkehr für Zwecke einer möglichen späteren Strafverfolgung zu speichern und für den Zugriff der Sicherheitsbehörden bereitzuhalten. Die Datenschutzbeauftragten halten den Versuch, das Internet für Zwecke der Strafverfolgung in ein Fahndungsnetz zu verwandeln, für ungeeignet und unangemessen.

Die bestehenden Befugnisse der Strafverfolgungsbehörden gewährleisten schon jetzt eine effektive Strafverfolgung im Internet. Es ist den Providern ohne weiteres technisch möglich, IP-Nummern ab dem Zeitpunkt eines entsprechenden richterlichen Beschlusses, oder bei Gefahr in Verzug einer staatsanwaltlichen Anordnung, vorzuhalten. Eine ständige Internet-Überwachung wäre zudem zur Verfolgung von schweren Straftaten untauglich, weil Straftäter ohne größere technische Schwierigkeiten auf Provider in anderen Ländern ausweichen könnten, für die derartige Verpflichtungen nicht bestehen.

Wir lehnen Forderungen nach einer solchen Protokollierungs- und Aufbewahrungspflicht bei der Internetnutzung ab. Allen Bürgerinnen und Bürgern muss auch zukünftig eine unbeobachtete Nutzung des Internet möglich sein.

3.5.4 Automatische Prüfung von Internetangeboten

Durch ein Programm-Tool wird die datenschutzrechtliche Prüfung von Internetangeboten deutlich erleichtert. Dies wird in Zukunft zu einer Ausweitung dieser Prüfungen führen.

Der Hamburgische Datenschutzbeauftragte hat in Zusammenarbeit mit dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein ein Programm entwickelt, mit dem sich Internetangebote privater oder öffentlicher Stellen automatisiert überprüfen lassen. Dazu werden in einem ersten Schritt sämtliche Seiten der Angebote auf datenschutzrechtlich relevante Aspekte untersucht und diese dem Prüfer im weiteren Verlauf übersichtlich präsentiert. Gerade bei großen und weit verzweigten Angeboten ist eine manuelle Unter-

suchung eines Angebots auf Cookies, automatische Weitervermittlungen, Anbieterkennzeichnung usw. sehr zeitaufwändig und im Ergebnis unvollständig. Die Automatisierung hilft dem Prüfer daher, den Überblick zu behalten und sich auf die datenschutzrechtlich wesentlichen Aspekte zu konzentrieren.

In Abhängigkeit der gefundenen Sachverhalte und ihrer Bewertung durch den Prüfer wird im zweiten Schritt aus vorgefertigten Textbausteinen ein Prüfbericht erstellt, der anschließend ausgedruckt und wie andere Prüfberichte behandelt werden kann. Dem Prüfer wird dabei also auch die Arbeit der konkreten Formulierung erleichtert, so dass der Zeitaufwand zur Durchführung einer einzelnen Prüfung insgesamt deutlich reduziert ist. Da die verschiedenen Sachverhalte und Bewertungen im Zusammenhang mit den zu Grunde liegenden Rechtsvorschriften (Teledienstedatenschutzgesetz und Mediendienstestaatsvertrag) insgesamt überschaubar sind, kann mit weitgehend vorformulierten Textstücken gearbeitet werden. Dem Prüfer bleibt dabei jedoch immer die Möglichkeit, auf den Einzelfall bezogene Formulierungen zu ergänzen.

Das Prüfwerkzeug ist in seinen Kernfunktionen einsatzfähig. Momentan werden folgende Aspekte berücksichtigt:

- Ausgestaltung und Zugänglichkeit der Anbieterkennzeichnung,
- Verwendung von Cookies und Unterrichtung des Nutzers darüber,
- Automatische Weitervermittlungen auf Angebote Dritter und Realisierung entsprechender Anzeigepflichten,
- Web-Bugs.

Weitere Auswertungen werden in Zukunft ergänzt und das Prüfwerkzeug auf Grundlage konkreter Prüferfahrungen weiterentwickelt. Dies wird unter Einbindung weiterer Datenschutzbeauftragter und Aufsichtsbehörden geschehen.

3.5.5 Datenschutz bei hamburg.de

Bei dem offiziellen Hamburger Internet-Angebot müssen die Anforderungen an den Datenschutz gewährleistet werden.

Der offizielle Internet-Auftritt Hamburgs wurde Anfang 2000 an eine Betreiber-Gesellschaft übertragen, an der Hamburg maßgeblich beteiligt ist. Die Hamburger Internet-Präsenz wird auf einer gemeinsamen technischen Basis mit dem Angebot von schleswig-holstein.de abgewickelt, das die Internet-Aktivitäten der schleswig-holsteinischen Verwaltung und mehrerer Kommunen zusammenführt. Wir begleiten dieses Projekt in enger Kooperation mit dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein.

Bei hamburg.de handelt es sich um einen Tele- bzw. Mediendienst, für den die Vorschriften des Multimediarechts zu beachten sind (vgl. 3.5.1).

Die Betreibergesellschaft hat eine schleswig-holsteinische Firma mit der technischen Abwicklung des Angebots beauftragt. Der Server, auf dem die Angebote bereit gehalten werden, befindet sich in einem Rechenzentrum in Hannover, der von einer dritten Firma betrieben wird. Wir haben die Betreibergesellschaft bereits im Jahr 2000 darauf hingewiesen, dass die datenschutzrechtlichen Verantwortlichkeiten zwischen den beteiligten Unternehmen vertraglich geregelt werden müssen. Nach unserer Auffassung liegt rechtlich eine Form der Datenverarbeitung im Auftrag (vgl. Kasten) vor, die nach § 11 BDSG zu bewerten ist.

Datenverarbeitung im Auftrag liegt vor, wenn eine verantwortliche Stelle (Auftraggeber) die Durchführung bestimmter Hilfs- und Unterstützungsarbeiten bei der Verarbeitung personenbezogener Daten ganz oder teilweise einem Dritten (Auftragnehmer) überträgt, der die Daten entsprechend den Weisungen des Auftraggebers verarbeitet. Dabei bleibt der Auftraggeber für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich. Er ist weiterhin Ansprechpartner für den Betroffenen hinsichtlich der Rechte auf Auskunft, Sperrung und Löschung seiner Daten. Für die Datenverarbeitung im Auftrag durch nicht-öffentliche Stellen ist § 11 BDSG einschlägig. Wenn die Datenverarbeitung im Auftrag durch öffentliche Stellen Hamburgs erfolgt, muss § 3 HmbDSG beachtet werden.

Die Betreibergesellschaft von hamburg.de hat unsere Rechtsauffassung, dass eine Auftragsdatenverarbeitung vorliegt, zwar akzeptiert. Eine verbindliche Vorgabe, die die vom Auftragnehmer zu treffenden technischen und organisatorischen Maßnahmen konkret festlegt, ist jedoch bislang noch nicht in ausreichendem Maße erfolgt.

Dagegen ist hamburg.de unserer Anregung, die Nutzer in einer aus dem Angebot jederzeit abrufbaren „Datenschutzpolitik“ über Umfang und Zwecke der Verarbeitung ihrer persönlichen Daten zu informieren, in vollem Umfang gefolgt.

Das über das Web-Portal www.hamburg.de abrufbare Angebot besteht aus drei „Säulen“:

- Die „Verwaltungs-Säule“ fasst die Angebote der Behörden und sonstigen öffentlichen Stellen zusammen;
- die „Wirtschafts-Säule“ enthält Angebote von Unternehmen;
- die „Bürger-Säule“ soll den Bürgerinnen und Bürgern und Non-Profit-Organisationen Kommunikationsmöglichkeiten über das Internet geben.

Kern des neuen Konzepts ist ein sog. „Lebenslagen-Modell“, das technisch noch nicht voll umgesetzt wurde (s. Kasten).

Lebenslagen-Modell: Die Nutzerinnen und Nutzer sollen nicht nur mit denjenigen Informationen versorgt werden, die sie direkt ansteuern, sondern sie sollen darüber hinaus auch Angebote erhalten, die in einem örtlichen oder sachlichen Zusammenhang mit der nachgefragten Leistung stehen. So sollen Heiratswillige, die sich einen Termin beim Standesamt reservieren, Angebote über Brautausstattung und Räumlichkeiten für die Hochzeitsfeier erhalten.

Technische Basis der Angebote in hamburg.de ist ein „Content-Managementsystem", in dem alle für das Web bestimmten Inhalte vorgehalten und aus dem die angeforderten Web-Seiten dynamisch generiert werden. Dieses System soll Anfang 2002 in Betrieb genommen werden.

Die Neugestaltung des offiziellen Hamburger Internet-Angebots bietet die Chance, nicht nur beim Bürgerservice neue Wege zu beschreiten, sondern auch beispielhafte Lösungen für datenschutzfreundliche Technologien bereitzustellen. Aus Datenschutzsicht stehen dabei folgende Aspekte im Vordergrund:

– Das gesamte Angebot muss so gestaltet sein, dass dabei so wenig wie möglich personenbezogene Daten verarbeitet werden (Datensparsamkeit – vgl. 3.1.1). Insbesondere muss sichergestellt werden, dass der bloße Informationsabruf (z.B. die Anfrage nach Öffnungszeiten, der Abruf von Theater-Programmen oder das „Blättern" in elektronischen Verzeichnissen) nicht zu dauerhaften Datenspuren der Nutzerinnen und Nutzer führt.

– Werden über hamburg.de Bestellungen, Buchungen und andere Rechtsgeschäfte abgewickelt, darf dies nicht dazu führen, dass das Surf-Verhalten der Nutzer ohne deren Einwilligung registriert wird. Ferner ist dafür Sorge zu tragen, dass Verknüpfungen zwischen elektronischen „Behördengängen" und kommerziellen Angeboten nur dann erfolgen, wenn die Nutzer dies im Einzelfall wünschen. Nutzungsprofile sind gemäß den Vorgaben des Multimediarechts nur unter Pseudonym zulässig, sofern der Nutzer die Möglichkeit hat, der Verwendung seiner Daten für die Bildung des Profils zu widersprechen. Es ist selbstverständlich, dass die Unternehmen und Organisationen, die Angebote über die Plattform hamburg.de bereitstellen, die Einhaltung der Datenschutzbestimmungen zu garantieren haben.

– Bei der Bezahlung von Internet-Leistungen öffentlicher und nicht-öffentlicher Stellen sollten die Betroffenen die Möglichkeit haben, die Zahlungen ohne personenbezogene Identifizierung abzuwickeln. Entsprechende Internet-Zahlungsverfahren stehen bereits zur Verfügung (vgl. 3.1.2 und 25.1).

– Seit Frühjahr 2000 ist bei hamburg.de ein kostenloser E-Mail-Dienst realisiert. Nachdem deutlich wurde, dass es Nutzern zunächst ohne größere Schwierigkeiten möglich war, beliebige Absender-Adressen zu verwenden, wurde diese Schwachstelle vom Betreiber abgestellt. Im Hinblick auf die mangelnde Vertraulichkeit der über das Internet abgewickelten Kommunikation haben wir auf die Notwendigkeit hingewiesen, den Zugang der Nutzer zum Mailserver (insb. Übertragung von Passwörtern und Nutzerkennungen) durch kryptografische Verschlüsselung zu sichern.

3.5.6 Anwendbarkeit des deutschen Datenschutzrechts auf das Internet

Aus dem Bundesdatenschutzgesetz, das an die Vorgaben der EG-Datenschutzrichtlinie angepasst wurde, ergibt sich jeweils, wann das deutsche Datenschutzrecht auf das Internet anzuwenden ist.

§ 1 Abs. 5 des novellierten BDSG enthält Regelungen über die Anwendbarkeit des Gesetzes für Erhebungen, Verarbeitungen und Nutzungen personenbezogener Daten durch verantwortliche Stellen, die nicht im Inland ihren Sitz haben. Dabei ist zu unterscheiden, ob sich diese Stelle in einem anderen Mitgliedstaat der Europäischen Union bzw. in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum – EWR – (Norwegen, Island und Liechtenstein) oder in einem Drittland befindet.

Innerhalb des EWR kommt es für die Anwendbarkeit deutschen Datenschutzrechts grundsätzlich nicht mehr – wie bisher – auf den Ort der Verarbeitung (Territorialprinzip), sondern auf den Sitz der verantwortlichen Stelle an (Sitzlandprinzip). Daraus ergibt sich, dass die Vorschriften des BDSG nicht anzuwenden sind, wenn die für die Datenverarbeitung verantwortliche Stelle zwar Daten im Inland verarbeitet, aber in einem anderen Mitgliedsstaat des EWR belegen ist. Als Ausnahme hiervon gilt weiterhin das Territorialprinzip und damit die Anwendung des BDSG, wenn die verantwortliche Stelle eine Niederlassung im Inland unterhält. So ist französisches Datenschutzrecht anwendbar, wenn ein französischer Internet-Anbieter personenbezogene Daten deutscher Nutzer ohne eigene Niederlassung in Deutschland erhebt, verarbeitet oder nutzt.

Die Datenschutzaufsicht wird dann durch die deutschen Datenschutzaufsichtsbehörden ausgeübt, wenn der ausländische Internet-Anbieter eine Niederlassung im Inland hat. Das ergibt sich aus § 38 Abs. 1 Satz 1 BDSG. Dabei haben die deutschen Datenschutzaufsichtsbehörden das Recht des jeweiligen EWR-Mitgliedsstaats anzuwenden. Ein Provider mit Niederlassungen in mehreren EWR-Staaten muss gewährleisten, dass jede dieser Niederlassungen die im jeweils einzelstaatlichen Recht festgelegten Verpflichtungen einhält.

In einem **Drittland** belegene verantwortliche Stellen, die in Deutschland personenbezogene Daten erheben, verarbeiten oder nutzen, haben das deutsche Datenschutzrecht zu beachten. Das deutsche Datenschutzrecht kommt demnach zur Anwendung, wenn ein Internet-Anbieter aus einem Drittland in Deutschland eine Niederlassung betreibt, über die er seine hiesigen Kundenkontakte abwickelt. Danach hat ein Online-Dienst mit Hauptsitz in den USA und Niederlassung in Deutschland das BDSG zu beachten.

Aber auch ohne inländische Niederlassung kommen die deutschen Datenschutzbestimmungen zur Anwendung, wenn die verantwortliche Stelle auf automatisierte oder nicht automatisierte Mittel zurückgreift, die in Deutschland belegen sind. Ein solches automatisiertes Mittel ist z. B. ein inländisches EDV-System, durch das Warenbestellungen auf elektronischem Wege entgegengenommen werden. Entscheidend ist, dass über technische Mittel Einfluss auf die Datenerhebung ausgeübt wird oder ausgeübt werden kann. So ist das BDSG anzuwenden, wenn eine verantwortliche Stelle mit Sitz im Ausland in Deutschland Hardware betreibt (Einwahlknoten, Server, Modems, Leitungen).

Das BDSG ist ferner stets anwendbar, wenn das Angebot in Deutschland gehostet wird, unabhängig davon, ob dabei eine direkte Sachherrschaft über die verwendeten Computersysteme ausgeübt wird. Problematischer ist die Bestimmung des anwendbaren Rechts in den Fällen, in denen die ausländische Stelle ausschließlich nur partiell über Software die Kontrolle auf dem deutschen Computer ausübt. So ist das deutsche Recht in den Fällen anwendbar, in denen sich aus den Drittstaaten erbrachte Internet-Angebote erkennbar an deutsche Nutzer richten, wenn dabei personenbezogene Daten erhoben werden, die durch ein von dem Anbieter gesteuertes automatisiertes Verfahren auf dem Rechner des Nutzers an den Anbieter übermittelt werden. Dabei kann es sich z.B. um spezielle Software handeln, die für die Nutzung eines Dienstes verwendet wird. Auch die Übermittlung von Informationen durch auf dem Rechner des Nutzers installierte aktive Programmkomponenten (z.B. Java-Applets, Active-X-Controls) an einen Empfänger in einem Drittland führt zur Anwendbarkeit deutschen Rechts. Gleiches gilt für Cookies, die zum Wiedererkennen des Nutzers auf seinem Rechner gespeichert werden.

Gemäß § 1 Abs. 5 Satz 3 BDSG hat eine verantwortliche in einem Drittstaat belegene Stelle ohne inländische Niederlassung, die personenbezogene Daten im Inland erhebt, Angaben über im Inland ansässige Vertreter zu machen. Der Vertreter soll sowohl Ansprechpartner des Betroffenen als auch der Aufsichtsbehörde sein. Die Benennung soll die Transparenz der Datenverarbeitung für die Betroffenen verbessern. Die Information über den inländischen Vertreter sollte im Internet zusammen mit den im Teledienstegesetz (TDG) und im Mediendienste-Staatsvertrag (MDStV) vorgesehenen Kennzeichnungspflichten erfolgen.

Nicht anwendbar ist das deutsche Recht gemäß § 1 Abs. 5 Satz 4 BDSG allerdings, „sofern Datenträger nur zum Zwecke des Transits durch das Inland eingesetzt werden," also weder eine Erhebung noch eine sonstige Verarbeitung oder Nutzung der Daten im Inland stattfindet. Letzteres ist im Internet dann der Fall, wenn die Daten lediglich über einen Rechner in einem Mitgliedstaat geroutet werden, jedoch weder der ursprüngliche Sender noch der Empfänger ihren Sitz im EWR haben.

3.6 Neue Regelungen zur Signatur

Die neuen Rechtsvorschriften zur elektronischen Signatur schaffen insgesamt bessere Voraussetzungen für die Nutzung dieser Technik zur Wahrung von Integrität und Zurechenbarkeit von Daten.

Auf Grundlage der EG-Signaturrichtlinie (Richtlinie 1999/93/EG über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen) hat der Bundesgesetzgeber dem Signaturgesetz (Gesetz über Rahmenbedingungen für elektronische Signaturen) im Mai 2001 eine neue Fassung gegeben. Als wesentliche Änderungen gegenüber dem Signaturgesetz von 1997 sind zu nennen:

– der Begriff der „digitalen Signatur" ist durch den der „elektronischen Signatur" ersetzt worden,

– es werden drei Stufen elektronischer Signaturen definiert (s. Kasten), wie in der EG-Richtlinie vorgegeben, sowie als zusätzliche Qualitätsstufe eine freiwillige Akkreditierung von Zertifizierungsdiensteanbietern (sog. Trust Centern) ermöglicht,

– die Erbringung von Zertifizierungsdiensten erfordert keine formale Genehmigung mehr, ist jedoch anzeigepflichtig und wird von der zuständigen Behörde (Regulierungsbehörde für Telekommunikation und Post – RegTP) beaufsichtigt,

– eine Haftungsregelung schützt die Kunden vor Schäden, die durch schuldhaftes Handeln von Zertifizierungsdiensteanbietern entstehen können; eine entsprechende Deckungsvorsorge ist Voraussetzung für die ordnungsgemäße Erbringung von Zertifizierungsdiensten,

– ausländische Signaturen auf Grundlage der EG-Richlinie sind Signaturen nach deutschem Recht im Wesentlichen gleichgestellt, so dass im Europäischen Wirtschaftsraum eine grenzüberschreitende Signierung möglich ist.

Stufen elektronischer Signaturen nach dem Signaturgesetz:

1. Elektronische Signatur: „Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen."
2. Fortgeschrittene elektronische Signatur: „Elektronische Signatur, die ausschließlich dem Signaturschlüssel-Inhaber zugeordnet ist, die Identifizierung des Signaturschlüssel-Inhabers ermöglicht, mit Mitteln erzeugt wird, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und mit den Daten, auf die sie sich bezieht, so verknüpft ist, dass eine nachträgliche Veränderung der Daten erkannt werden kann."
3. Qualifizierte elektronische Signatur: „Fortgeschrittene elektronische Signatur, die auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruht und mit einer sicheren Signaturerstellungseinheit erzeugt wird."

Ergänzend trat im August 2001 das Formanpassungsgesetz (Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr) in Kraft. Bedeutsam ist insbesondere die Einführung einer „elektronischen Form". Danach werden Dokumente, die mit einer qualifizierten elektronischen Signatur versehen sind, weitgehend mit der gesetzlichen Schriftform (§ 126 BGB) gleichstellt. Dadurch werden die Formvorschriften des Zivilrechts an die neue Technologie angepasst und in der Zivilprozessordnung Beweiserleichterungen beim Einsatz qualifizierter elektronischer Signaturen geschaffen. Im Laufe des Jahrs 2002 sollen entsprechende Änderungen im Verwaltungsverfahrensrecht erfolgen, das die Kommunikation zwischen Bürgern und öffentlichen Stellen regelt.

Im Ergebnis bedeutet dies, dass die Voraussetzungen zur Erbringung von Signatur-Dienstleistungen deutlich gesenkt und zugleich Rechtssicherheit für die Anwendbarkeit von Signaturen geschaffen wurde. Dies ist in Anbetracht der sehr hohen Hürden nach dem Signaturgesetz alter Fassung (bzw. der freiwilligen Akkreditierung nach der neuen Fassung) zunächst zu begrüßen, da diese einer Verbreitung der elektronischen Signatur im Wege standen. Allerdings ist der Begriff der „elektronischen Signatur" an sehr geringe Voraussetzungen geknüpft, so dass womöglich ein falscher Eindruck über die mit einer entsprechenden Maßnahme verbundene Integrität und Zurechenbarkeit entstehen könnte. Nur die qualifizierte elektronische Signatur erfüllt die Anforderungen, die in der Regel aus Datenschutzsicht an eine Sicherung in diesem Bereich zu stellen sind.

3.7 Belästigungen durch SMS-Werbung

Die Nutzung von Handynummern zur Übersendung von SMS-Werbung ist unzulässig.

Der Austausch von Kurznachrichten, sogenannter SMS (Short Message Service) erfreut sich immer größerer Beliebtheit. Da liegt es nahe, auch dieses Medium für Werbezwecke zu nutzen. Speziell für SMS-Werbung hat sich noch keine höchstrichterliche Rechtsprechung entwickelt. Allerdings können die für unverlangte Faxwerbung und E-Mail-Werbung entwickelten Rechtsprechungs-Grundsätze herangezogen werden. Danach ist die Zusendung von SMS-Werbung ohne Einwilligung des Empfängers wettbewerbswidrig und daher unzulässig.

Das Problem liegt jedoch in den meisten Fällen in der Rechtsverfolgung. Zuständig für Wettbewerbsverstöße sind die Verbraucherzentralen. Sie besitzen eine Verbandsklagebefugnis für Abmahnungen bei Wettbewerbsverstößen. Informationen der Verbraucher-Zentrale Hamburg zu diesem Thema können im Internet unter www.vzhh.de eingesehen werden.

Aus datenschutzrechtlicher Sicht kommt hier die Möglichkeit für den Betroffenen in Betracht, nach § 28 Abs. 4 BDSG der Nutzung der Handy-Nummer zu Werbezwecken zu widersprechen, wenn der Absender bekannt ist. Die Schwierigkeit für Betroffene und Aufsichtsbehörden besteht zunächst darin herauszufinden, wer der Anbieter des jeweiligen Tele- oder Mediendienstes ist. Dabei ist wie folgt vorzugehen:

- **Anfrage bei der RegTP:** 0190-Rufnummern werden in Blöcken zu je tausend Anschlüssen durch die Regulierungsbehörde für Telekommunikation und Post (RegTP) an Unternehmen (z. B. die Deutsche Telekom AG) vergeben. Die Liste der Inhaber der Rufnummern-Blöcke (RNB) wird von der RegTP im Internet unter http://www.regtp.de/imperia/md/content/reg_tele/rufnummern/mwd/0190_RNB_Betreiber.pdf veröffentlicht.

- **Anfrage bei dem Inhaber des Rufnummern-Blocks** hinsichtlich des Betreibers der konkret nachgefragten 0190-Rufnummer, denn die Inhaber der Rufnummern-Blöcke sind zumeist nur Vermittler, die die Rufnummern anderen Unternehmen (z. B. Anbietern von Hotlines) vermieten. Letztere sind für die Angebote zumeist verantwortlich. Die **Deutsche Telekom** gibt über die Inhaber der 0190-Rufnummern, die von ihr verwaltet werden, in einem automatisierten Verfahren unter der kostenlosen Rufnummer 0800 3301 900 Auskunft. Fraglich ist, ob die Inhaber der Rufnummernblöcke zu derartigen Auskünften verpflichtet sind.

- **Erkundigung** bei dem Inhaber **der 0190-Nummer**.

In vielen Fällen werden die Rufnummern von den Unternehmen an Dritte zur Nutzung weitergegeben. In diesem Fall müssen weitere Ermittlungen erfolgen, um den tatsächlich verantwortlichen Anbieter herauszufinden.

So weit die Daten einem öffentlichen Kunden- oder Teilnehmerverzeichnis entnommen wurden, hat der Betroffene ferner das Recht, bei seinem TK-Diensteanbieter die Löschung der Angaben aus dem Verzeichnis zu verlangen (§ 89 Abs. 9 TKG bzw. § 29 Abs. 3 BDSG). Die Ausübung des Widerspruchsrechts kann jedoch unmittelbare Wirkung nur auf die elektronisch angebotenen Teilnehmerverzeichnisse entfalten, die interaktiv zum Abruf aus dem Internet bereitgestellt werden. Für die in konventioneller Form oder als CD-ROM in Umlauf gebrachten Teilnehmerverzeichnisse wirkt sich der Widerspruch naturgemäß erst mit der nächsten Auflage aus.

Im Übrigen ist es aufgrund der technischen Möglichkeiten kein Problem, an Handy-Nummern Werbe-SMS zu senden. Mobilfunk-Betreiber verkaufen zwar nach unseren Erfahrungen keine Handy-Nummern für Werbezwecke. Gleichwohl bedarf es wegen der einfachen und allseits bekannten Nummernstruktur nur eines kleinen Programms, um Werbe-SMS zu verschicken.

3.8 Straßenbenutzungsgebühren

Durch neue gesetzliche Grundlagen ist die baldige Einführung elektronischer Mautbezahlungssysteme zu erwarten. An diese Systeme sind hohe datenschutzrechtliche Anforderungen zu stellen.

Die Bundesregierung hat im August 2001 einen Gesetzentwurf zur Einführung einer LKW-Maut ab 2003 (Gesetzentwurf zur Einführung von streckenbezogenen Gebühren für die Benutzung von Bundesautobahnen mit schweren Nutzfahrzeugen) beschlossen. Außerdem soll im Rahmen des privaten Fernstraßenbaus die Möglichkeit der Erhebung von Mautgebühren von allen Verkehrsteilnehmern an Brücken, Tunneln und Gebirgspässen geschaffen werden. Die Maut soll auch auf elektronische Weise abgerechnet werden können.

Damit wird in veränderter Form ein Vorhaben aus dem Jahre 1995 wieder aufgegriffen, das seinerzeit intensiv durch die Datenschutzbeauftragten begleitet wurde (siehe 16. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz, 28.1). Zwar haben sich die technischen Voraussetzungen weiterentwickelt, so dass für die automatische Erhebung von Mautgebühren andere Realisierungsmöglichkeiten bestehen als noch vor einigen Jahren. Insbesondere die Einbeziehung der GSM- und GPS-Technik, d.h. Handys in Verbindung mit Satellitennavigation (vgl. 1.1.1), erscheint heute als meistversprechende Technik. Eine konkrete Festlegung auf bestimmte Techniken ist jedoch noch nicht erfolgt.

Allerdings haben sich die datenschutzrechtlichen Probleme in diesem Zusammenhang nicht wesentlich verändert. Die Gefahren, die mit einer Erfassung von Daten im geplanten Umfang verbunden sind, liegen auf der Hand. So könnte z.B. der Systembetreiber über einen längeren Zeitraum Bewegungsprofile der Fahrzeuge – und damit der Fahrer oder der Halter – erstellen.

Um auf eine **datenschutzgerechte Ausgestaltung der Mauterfassung** hinzuwirken, hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 24.-26. Oktober 2001 eine Entschließung mit folgenden Eckpunkten gefasst:

- Die Überwachung der Gebührenzahlung darf nur stichprobenweise erfolgen. Die Identität der Mautpflichtigen darf nur dann aufgedeckt werden, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Gebühren nicht entrichtet worden sind.
- Die Verfahren der Gebührenerhebung und -kontrolle müssen für die Mautpflichtigen durchschaubar sein. Sie müssen sich jederzeit über den Abrechnungsvorgang informieren sowie den eventuellen Kontrollvorgang erkennen können.
- Alle datenschutzrelevanten Systemkomponenten sind so auszugestalten, dass sie weder vom Betreiber noch von anderer Seite beeinträchtigt oder zurückgenommen werden können.
- Es ist sicherzustellen, dass anfallende personenbezogenen Daten von allen beteiligten Stellen vertraulich behandelt werden und einer strikten Zweckbindung unterliegen.
- Das im BDSG festgelegte Prinzip der Datensparsamkeit ist konsequent umzusetzen; dazu gehört auch die Möglichkeit, durch Barzahlung eine Datenverarbeitung komplett zu vermeiden.

3.9 Telearbeit

Aus datenschutzrechtlicher Sicht gibt es keine grundsätzlichen Bedenken gegen den Zugriff von häuslichen Arbeitsplätzen auf besonders sensible personenbezogene Daten in Fachanwendungen der Verwaltung. Die Entscheidung, ob überhaupt und für welche Mitarbeiterinnen und Mitarbeiter dies zugelassen wird, obliegt der jeweiligen Dienststelle.

Der Modellversuch zur Erprobung alternierender Telearbeit in der hamburgischen Verwaltung (17. TB, 7.1) ist erfolgreich abgeschlossen worden. Seit dem 27. Dezember 2000 besteht eine Vereinbarung nach § 94 HmbPersVG zur Einführung im gesamten Verwaltungsbereich, an der wir umfassend beteiligt

worden sind. Mit dem Landesamt für Informationstechnik (LIT) als verantwortlicher Stelle ist ein neues Modell der technischen Anbindung häuslicher Arbeitsplätze an das Netz der FHH erörtert worden, das geeignet ist, die hohen Sicherheitsanforderungen zu gewährleisten. Es wird zukünftig für alle vorhandenen und neu einzurichtenden Telearbeitsplätze verbindlich zum Einsatz kommen.

Unter der Voraussetzung, dass die in der Vereinbarung und ihren Anlagen genannten Rahmenbedingungen eingehalten werden, haben wir grundsätzlich weder datenschutzrechtliche noch datenschutztechnische Bedenken gegen häusliche Arbeitsplätze mit direktem Zugriff auf IuK-Anwendungen der FHH. Falls in Betracht kommende bereichsspezifische Rechtsvorschriften es nicht konkret ausschließen, können auf dieser Basis auch besonders sensible personenbezogene Daten im Rahmen von Telearbeit verarbeitet werden. Aufgrund der bei uns in den vergangenen Monaten eingegangenen Anfragen betrifft dies beispielsweise die Sozialhilfe, die Beihilfe im Personalbereich oder die Verfahrensdaten der Staatsanwaltschaft. Zum Vergleich können hier jeweils auch die bestehenden Vorgehensweisen bei der Heimarbeit – z. B. für die Vergabe von Schreibarbeiten für Gerichte – herangezogen werden.

Von besonderer Bedeutung für den Zugriff auf Fachanwendungen mit sensiblen Daten sind die organisatorisch vor Ort im häuslichen Bereich zu treffenden Maßnahmen. Die betroffenen Dienststellen müssen für sich selbst entscheiden, ob sie ihren Mitarbeiterinnen und Mitarbeitern die Einhaltung der datenschutzrechtlichen Bestimmungen zutrauen und auch die Verantwortung dafür übernehmen wollen. Dazu gehört insbesondere, sich die Einrichtung des Arbeitsplatzes in der häuslichen Umgebung vor Aufnahme der Telearbeit auch tatsächlich anzusehen und in unregelmäßigen Abständen erneut zu überprüfen.

In der Umsetzung dieser Anforderung kann theoretisch ein rechtliches Problem bestehen. Die Telearbeiter könnten unter Berufung auf Art. 13 Grundgesetz den Zutritt zu ihrer Wohnung verwehren. Mit dem Hinweis auf die Unverletzlichkeit der Wohnung können auch weitere Mitbewohner die Kontrolle verhindern. Außerdem handelt es sich hier um eine mitbestimmungspflichtige Leistungs- und Verhaltenskontrolle der Arbeitnehmer durch den Arbeitgeber. Deshalb sieht die Vereinbarung nach § 94 HmbPersVG (siehe Anlage 3/2, Ziffer 5 der Sicherheitsregeln für Telearbeit) ausdrücklich die Regelung vor, dass dem Dienstherrn und dem Hamburgischen Datenschutzbeauftragten Zutritt zur Wohnung für die Überwachung der Einhaltung der datenschutzrechtlichen Vorgaben zu gewähren ist. Diese Regelung ist Bestandteil der schriftlichen Vereinbarung zwischen Telearbeitern und Dienststelle über die mit der Einrichtung des häuslichen Arbeitsplatzes verbundenen gegenseitigen Rechte und Pflichten. Sie ist somit auch wichtige Voraussetzung für die Gewährung von Telearbeit. Deshalb hätte die Verweigerung des Zutritts zur Wohnung für Kontrollzwecke die Beendigung der Telearbeit zur Folge. Die Mitarbeiterinnen

und Mitarbeiter, die das für sie vorteilhafte Angebot der alternierenden Telearbeit nutzen möchten, sollten von vornherein mit ihren Mitbewohnern klären, ob diese die erforderlichen Kontrollen vor Ort im häuslichen Bereich dulden werden.

Im übrigen gehen wir davon aus, dass Telearbeiter an der Fortführung dieser besonderen Arbeitsform so nachhaltig interessiert sind, dass sie den damit verbundenen hohen Datenschutzanforderungen besondere Aufmerksamkeit widmen. Im Gegensatz zur Tätigkeit in den Diensträumen der jeweiligen Behörde, wo sich vielfach jeder auf seine Kolleginnen und Kollegen verlässt oder auch darauf setzen kann, dass individuelle Fehler nicht eindeutig einer bestimmten Person zugeordnet werden können, hätte die Nichteinhaltung von Sicherheitsauflagen unweigerlich spürbare Konsequenzen.

Wenn die Vorgaben aus der Vereinbarung nach § 94 HmbPersVG zur Einführung der alternierenden Telearbeit in der hamburgischen Verwaltung strikt eingehalten werden, obliegt die Entscheidung, ob überhaupt und wenn ja, für welche Mitarbeiterinnen und Mitarbeiter ein Zugriff auf Fachanwendungen mit sensiblen personenbezogenen Daten zugelassen wird, der jeweiligen Dienststelle.

Datenschutz im öffentlichen Bereich

4. Parlamentsspezifischer Datenschutz, Wahlen und Volksabstimmungen

4.1 Wahlen und Volksabstimmungen

4.1.1 Rechenschaftslegung durch die Volksinitiatoren

Für die Vorschriften, die der Senat in der Volksabstimmungsverordnung zum Rechenschaftsbericht der Volksinitiatoren erlassen hat, fehlt es an der erforderlichen gesetzlichen Ermächtigungsgrundlage.

Die Bürgerschaft hat am 6. Juni 2001 das Gesetz zur Änderung des Hamburgischen Gesetzes über Volksinitiative, Volksbegehren und Volksentscheid erlassen. Nach § 30 dieses Gesetzes sind die Volksinitiatoren verpflichtet, innerhalb bestimmter Fristen über die Herkunft und Verwendung der Mittel, die ihnen zur Durchführung der Volksabstimmung zugeflossen sind, gegenüber der Landesabstimmungsleiterin oder dem Landesabstimmungsleiter Rechenschaft zu legen. Die Bürgerschaft hat den Senat in § 31 Satz 2 Nr. 6 des Gesetzes ermächtigt, „das Verfahren der Rechenschaftslegung“ zu regeln.

Durch die Dritte Verordnung zur Änderung der Volksabstimmungsverordnung vom 11. September 2001 hat der Senat eine Bestimmung über den „Inhalt des Rechenschaftsberichts“ (§ 60a) getroffen. Die Vorschrift enthält detaillierte

Aussagen zum Umfang der Einnahme- und Ausgabenrechnung. Insbesondere legt sie fest, dass Spenden, deren Wert in einem Kalenderjahr 2.500 Euro übersteigt, unter Angabe des Namens und der Anschrift der Spenderin oder des Spenders sowie der Gesamthöhe der Spende im Rechenschaftsbericht darzustellen sind.

Bereits im Behördenabstimmungsverfahren zur Änderung der Volksabstimmungsverordnung haben wir unterstrichen, dass die Regelung zum Inhalt des Rechenschaftsberichts durch die gesetzliche Verordnungsermächtigung nicht gedeckt ist. Der in § 31 Satz 2 Nr. 6 des Gesetzes verwendete Begriff „Verfahren" umfasst allein die Art und Weise, nicht dagegen den materiellen Inhalt der Rechenschaftslegung. Entsprechend wird dieser Begriff auch vom Bundesverfassungsgericht ausgelegt (BVerfGE 37, 363, 390; 55, 274, 320 jeweils zu Art. 84 Abs. 1 des Grundgesetzes (GG)). Deutlich wird dies ferner bei einem Vergleich mit § 31 Satz 2 Nr. 1 des Gesetzes, der den Senat ermächtigt, neben der „Form" auch den „Inhalt" der Unterschriften- und Eintragungslisten zu regeln.

Nicht überzeugen kann die Argumentation des Senats, dass der Gesetzgeber bereits die wesentlichen Verfahrensvorschriften erlassen habe, so dass dem Verordnungsgeber die inhaltliche Ausgestaltung der Rechenschaftspflicht vorbehalten bleibe. Das Gesetz enthält z.B. keine Bestimmungen zur Form des Rechenschaftsberichts oder zur Möglichkeit, den Volksinitiatoren eine Nachfrist zur Vervollständigung ihres Berichts bzw. der Belege einzuräumen. Insofern eröffnet die Verordnungsermächtigung dem Senat auch ohne Einbeziehung inhaltlicher Gesichtspunkte einen substanziellen Gestaltungsspielraum.

Die Unterstützung einer Volksinitiative durch Spenden stellt ein sensibles Datum dar. Innerhalb welcher Grenzen dieses Datum aus Gründen demokratischer Transparenz offenbart werden muss, ist eine bedeutsame politische Frage. Ohne einen klaren Anhaltspunkt im Gesetz kann nicht davon ausgegangen werden, dass das Parlament die Abwägung und Bewertung dieser Frage der Regierung überlassen wollte.

Wir empfehlen, baldmöglichst die Reichweite der Verordnungsermächtigung eindeutig zu regeln. Auch den Volksinitiatoren legen wir nahe, von sich aus auf eine Klärung der Rechtslage hinzuwirken.

5. Allgemeine Verwaltungsangelegenheiten

5.1 Datenverarbeitung der Bezirksrechtsämter

Bereits bei der Planung und Entwicklung eines neuen IuK-Verfahrens muss daran gedacht werden, ein Konzept für die Löschung und Archivierung der Daten zu erarbeiten.

Im Berichtszeitraum haben wir das IuK-Verfahren RechtsamtProjekt (RePro) im Bezirksrechtsamt Wandsbek geprüft. RePro ist ein von der Zentralstelle IuK des Senatsamtes für Bezirksangelegenheiten entwickeltes Dialogverfahren für die bezirklichen Rechtsämter der Freien und Hansestadt Hamburg. Sein Zweck ist die computerunterstützte Sachbearbeitung in den Geschäftstellen der Rechtsämter. Die letzte wesentliche Verfahrensumstellung erfolgte im Jahre 1998 mit dem Wechsel vom Betriebssystem UNIX/SINIX mit der Datenbank INFORMIX zugunsten von Windows NT Applikationen.

Das Dialogsystem unterstützt die Erfassung und Verwaltung von sogenannten Stammdaten. Auf Basis dieser Daten wird die Bearbeitung von Vorgängen zu Widersprüchen, Klagen, Eingaben, Beschwerden, Ordnungswidrigkeitenverfahren, Liegenschaftsangelegenheiten und Regressüberprüfungen umfassend unterstützt. Das Verfahren bietet ausführliche Statistiken und Auswertungen an.

Wir haben einige Mängel festgestellt, die überwiegend gering waren und zügig behoben worden sind. Dies trifft allerdings nicht auf einen Mangel zu, auf den wir die beteiligten Stellen schon 1998 hingewiesen haben. Es besteht kein Löschungskonzept für die einzelnen Datensätze, so dass bislang auch keine Daten gelöscht worden sind. Somit sind Datensätze im System vorhanden, bei denen das Datum des Verfahrensabschlusses weit über 5 Jahre – teilweise fast schon 10 Jahre – zurückliegt.

Die älteren Datensätze werden für statistische Auswertungen, z.B. für die Beantwortung von Anfragen aus der Bürgerschaft und der Bezirksversammlung, genutzt. An eine anonymisierte oder pseudonymisierte Speicherung der Datensätze für solche Zwecke wird derzeit nicht gedacht. Eine Trennung in einen Datenbestand der zur Zeit aktiv genutzten Datensätze und in Archiv-Datensätze ist nicht realisiert.

Wir haben das Bezirksamt Wandsbek und das Senatsamt für Bezirksangelegenheiten daran erinnert, dass ein Löschungs- und Archivkonzept bereits 1998 angekündigt wurde und deshalb überfällig ist. Das Konzept muss sich an den fachlichen Anforderungen orientieren und ist technisch zu implementieren. Die Löschung sollte automatisiert umgesetzt werden.

Eine Trennung zwischen Archiv und laufendem Datenbestand wurde ebenfalls bereits 1998 zugesagt. Für ältere Datensätze, die nicht mehr für die Sachbearbeitung benötigt werden, sondern nur noch für statistische Auswertungen und Planungszwecke herangezogen werden, ist eine personenbezogene Speicherung nicht erforderlich. Solche Datensätze sind zu anonymisieren oder zu pseudonymisieren.

Das Senatsamt für Bezirksangelegenheiten hat daraufhin mitgeteilt, die Entwicklung und Implementierung der Lösch- und Archivierungsfunktion sei bislang aus Kapazitätsgründen nicht erfolgt. Diese Funktion sei jedoch jetzt in

die Planungen für das nächste Programm-Update aufgenommen worden und der Beginn der Entwicklungsarbeiten sei für den Jahresanfang 2002 vorgesehen. Wir haben deutlich gemacht, dass wir damit zwar einverstanden sind, eine weitere Verschiebung der Entwicklungsarbeiten aber wegen der Löschungsverpflichtung nach § 19 Abs. 3 Nr. 2 HmbDSG und der Vielzahl der Daten, die unzulässigerweise noch gespeichert sind, nicht hinnehmen werden.

5.2 Behördlicher Aktentransport

Die Entwicklung beim behördlichen Aktentransport gibt Anlass zu vorsichtigem Optimismus, aber keineswegs zur Entwarnung.

Bei Kontrollen des Behörden-Transport-Service (BTS), über den der behördeninterne Post- und Aktenaustausch abgewickelt wird, stellten wir 1999 in großer Anzahl gravierende Verstöße gegen Anforderungen des Datenschutzes fest (vgl. 17. TB, 18.). Unsere Prüfungen beim BTS setzten wir im Berichtszeitraum intensiv fort.

Dabei konnten wir, allerdings mit deutlichen Einschränkungen, eine positive Entwicklung verzeichnen. Das Hanseatische Oberlandesgericht, das Landgericht und das Amtsgericht Hamburg haben im Mai 2001 eine Gemeinsame Verfügung zur Gewährleistung des Datenschutzes erlassen und dabei im Wesentlichen unseren Formulierungsvorschlag vom Dezember 1999 aufgegriffen. In der überarbeiteten Fassung der Geschäftsordnungsbestimmungen zum Postversand vom Oktober 2001 hat die Finanzbehörde erneut unterstrichen, dass für Vorgänge mit schutzbedürftigen personenbezogenen Angaben verschlossene Briefumschläge oder ggf. entsprechend geeignete Versandbehältnisse verwendet werden müssen.

Erhebliche Defizite beim Datenschutz bestehen nach wie vor im Bereich der Sozialämter und des Amtes für Soziales und Rehabilitation. Selbst Unterlagen mit Gesundheitsdaten werden von diesen Stellen in beträchtlicher Anzahl unverschlossen zur Beförderung übergeben. Deshalb haben wir uns im Oktober 2001 erneut an das Senatsamt für Bezirksangelegenheiten (SfB) sowie die Behörde für Arbeit, Gesundheit und Soziales (BAGS) mit der dringenden Bitte um Abhilfe gewandt.

Offen vorgefunden haben wir beim BTS z.B. den Kostenvoranschlag eines Sanitätshauses für die Anfertigung einer Rumpfprothese zur Stabilisierung der Wirbelsäule, die Abrechnung der Kosten für einen Nervenstimulator, die Entlassungsanzeige eines Krankenhauses mit der Diagnose „Angina pectoris, Kardiomyopathie, Niereninsuffizienz“, Rechnungen über die Neulieferung von Fixiergurten mit ärztlicher Verordnung wegen Chora Huntington, einen Kostenverpflichtungsschein des Bernhard-Nocht-Instituts für Tropenmedizin mit der Diagnose „Tuberkulose des Darmes und der Mesenteriallymphknoten“ sowie den Sozialhilfeantrag für einen psychosozial betreuten Heroinabhängigen.

Bei den Gerichten und insbesondere bei der Staatsanwaltschaft Hamburg hat sich, verglichen mit den Verhältnissen zu Beginn unserer Kontrollen im Sommer 1999, eine wesentliche Verbesserung ergeben. Allerdings sahen wir Anlass, die Präsidentin des Landgerichts Hamburg im April 2001 auf gravierende Datenschutzverstöße hinzuweisen. Die vom Landgericht unverschlossen übersandten Unterlagen in Strafsachen enthielten u.a. Angaben über die Homosexualität, die schwere seelische Abartigkeit, die Muskel- und Atemwegserkrankung der Betroffenen sowie über die Unterbringung in einem psychiatrischen Krankenhaus.

Nachdem wir die Anforderungen an einen datenschutzgerechten Post- und Aktenaustausch, auch in Abstimmung mit der Finanzbehörde, wiederholt verdeutlicht haben, wird sich bei künftigen Verstößen eine förmliche Beanstandung nicht mehr vermeiden lassen.

6. Personalausweise und Pässe

6.1 Fingerabdruck und sonstige biometrische Merkmale

Im Bereich der Biometrie ist vor übereilten gesetzgeberischen Maßnahmen dringend zu warnen.

Der Gesetzentwurf der Bundesregierung für ein Terrorismusbekämpfungsgesetz sieht vor, dass Personalausweis und Pass neben dem Lichtbild und der Unterschrift weitere biometrische Merkmale von Fingern oder Händen oder Gesicht des Inhabers, auch in verschlüsselter Form, enthalten dürfen. Die Einzelheiten sollen durch ein besonderes Bundesgesetz geregelt werden. Die biometrischen Merkmale dürfen nur zur Überprüfung der Echtheit des Dokumentes und zur Identitätsprüfung des Inhabers verwendet werden. Eine Nutzung für erkennungsdienstliche Zwecke zur Gefahrenabwehr oder Strafverfolgung ist damit ausgeschlossen. Wesentliche Punkte wie z.B. das datenschutzrechtlich zu fordernde Verbot einer zentralen Referenzdatei lässt der Gesetzentwurf jedoch offen.

Abgesehen von der grundsätzlichen Frage der Geeignetheit und Angemessenheit dieser Maßnahme, sind die verschiedenen Ausprägungen der Biometrie aus Datenschutzsicht sehr unterschiedlich zu bewerten (siehe 1.3). Im Folgenden werden die Risiken aufgezeigt, die im Zusammenhang mit einem flächendeckenden Einsatz biometrischer Merkmale in Ausweisdokumenten zu erkennen sind, und die bekanntesten Verfahren dahingehend bewertet. Hinzu kommt das generelle Problem, dass derartige deutsche Ausweise nur bei gleichartigen Ausweisen anderer Staaten im gesamten Schengenbereich wirkungsvoll sein werden, aber Länder wie England und Frankreich solche Ausweise ablehnen.

6.1.1 Erhebung neuer Daten

Mit dem Foto und der Unterschrift des Inhabers enthalten deutsche Ausweisdokumente bereits biometrische Daten. Vor der Entscheidung, neue Merkmale zu speichern, ist zu prüfen, ob nicht die bereits erfassten Merkmale genügen und damit auf die Erhebung neuer personenbezogener Daten verzichtet werden kann. Möglicherweise können die zurzeit verwendeten biometrischen Daten die Qualitätsanforderungen an eine automatisierte Verarbeitung nicht in vollem Umfang erfüllen; dies ließe sich jedoch mit geringerer Eingriffstiefe in das Recht auf informationelle Selbstbestimmung beheben als die Verwendung eines völlig neuen Merkmals. Mit heute vorhandener Technik ist es z.B. möglich, das Foto auf dem Personalausweis automatisch mit dem Gesicht der Person zu vergleichen, die den Ausweis vorzeigt. Einer Änderung des Ausweisdokuments bedarf es dafür nicht. Weitere Sicherheitsvorkehrungen gegen Fälschungen und missbräuchliche Nutzungen von Ausweisdokumenten wie ein Hologramm des Fotos sind möglich und datenschutzrechtlich vertretbar.

6.1.2 Gefahr der Bildung eines einheitlichen Personenkennzeichens

Es ist zu befürchten, dass sich mit dem neu erfassten biometrischen Merkmal bzw. mit dem daraus generierten Datensatz eine Vielzahl unterschiedlicher Dateien erschließen und verknüpfen lassen. Ein derartiges Merkmal käme deshalb einem einheitlichen Personenkennzeichen gleich, das gemäß dem Volkszählungsurteil des Bundesverfassungsgerichts unzulässig ist (BVerfGE 65,1, -53-).

In Bereichen, in denen Biometrie für andere Zwecke zum Einsatz kommt (z.B. Zugangskontrolle – siehe 3.2.4), wäre eine Verknüpfung der verschiedenen Daten technisch möglich. Dies könnte zum einen durch Verwendung der im Ausweis gespeicherten Daten als Referenzmaterial für solche Zwecke erfolgen. Zum anderen könnten gespeicherte biometrische Daten mit denen abgeglichen werden, die zum Zwecke der Ausweiserstellung verwendet werden. Dies wäre, auch wenn es keine durchgängig verwendeten Standards für die Codierung biometrischer Daten gibt, zumindest mit einigem Aufwand verfahrensübergreifend durchführbar. Biometrische Verfahren, die bereits eine vergleichsweise große wirtschaftliche Bedeutung haben (Fingerabdruck und Gesichtserkennung) sind aus diesem Grund für die Verwendung in Ausweisen weniger geeignet.

6.1.3 Speicherung biometrischer Daten

Zur Erhöhung der Fälschungssicherheit von Ausweisdokumenten ist nur eine biometrische Verifikation erforderlich, d.h. der Abgleich der biometrischen Merkmale einer konkreten Person mit den auf einem Ausweis gespeicherten Daten. Eine Speicherung außerhalb des Ausweises ist dafür nicht erforderlich.

Das zusätzlich angestrebte Ziel der Vermeidung von „Doppelidentitäten“ (biometrische Identifikation) setzt die Speicherung personenbezogener Daten in zentralen Referenzdateien voraus. Aufgrund der geringen Größe der einzelnen Datensätze ist dies aus technischer Sicht durchaus vorstellbar. Aus Sicht des Datenschutzes ist eine solche Datensammlung insbesondere im Hinblick auf die Bildung eines einheitlichen Personenkennzeichens und die unvermeidlichen Missbrauchsmöglichkeiten jedoch abzulehnen.

Für die Ausweise selbst besteht die Möglichkeit, die Referenzdaten als Rohdaten oder als biometrischen Datensatz zu speichern. Während Rohdaten ggf. auch grafisch gespeichert werden können (z.B. das Bild eines Fingerabdrucks), muss für elektronische Biometriedaten ein maschinenlesbarer Datenträger (Barcode, Speicherchip etc.) auf dem Ausweis geschaffen werden. Um einen unkontrollierten Zugriff auf diese Daten zu verhindern, kommt dafür nur eine verschlüsselte Speicherung in Betracht. Während dies gegen einen alltäglichen Zugriff schützen mag, kann bei der Vielzahl von Geräten, in denen der Entschlüsselungsschlüssel vorhanden sein muss (bei Polizei und Grenzkontrollbehörden), jedoch kaum davon ausgegangen werden, dass die verschlüsselt gespeicherten Daten auf Dauer vor interessierten Dritten verborgen bleiben.

6.1.4 Eignung für die Überwachung

Die zentrale Speicherung biometrischer Merkmale würde das Potenzial für eine neue Qualität der Überwachung eröffnen. Gelingt es, biometrische Daten im Alltag zu erfassen und diese mit einer zentralen Datenbank abzugleichen, können weitgehende Bewegungsprofile der Betroffenen erstellt werden. Im Gegensatz zu einer Erfassung eines biometrischen Merkmals unter Mitwirkung des Betroffenen handelt es sich hierbei um nicht-kooperative Vorgänge, die dem Betroffenen womöglich nicht einmal bewusst sind. Dafür sind nur solche Merkmale geeignet, die kontaktlos und über eine gewisse Distanz erfasst werden können. Dies trifft vor allem auf die Gesichtserkennung zu, die bei geeignetem Blickwinkel mittels gewöhnlicher Kameras erfolgen kann.

Demgegenüber ist die flächendeckende Erfassung des Fingerabdrucks oder der Handgeometrie ohne Wissen und Mitwirkung des Betroffenen nicht oder nur unter sehr großem Aufwand möglich. Zwar können Fingerabdrücke auch heimlich von berührten Gegenständen abgenommen werden. Dies eignet sich jedoch – wegen des hierfür erforderlichen Aufwands – nur zur Behandlung von Einzelfällen und ist daher mit einer Überwachung nicht vergleichbar. Handgeometrie, Iris- oder Augenhintergrunderkennung sind weder über Distanz noch im Nachhinein erfassbar.

6.1.5 Überschießende Daten

Einige biometrische Merkmale lassen neben der Nutzung zur Identifizierung auch völlig andere Auswertungen zu. So kann möglicherweise auf bestimmte gesundheitliche Zustände oder Dispositionen, auf Faktoren wie Stress, Betrunkenheit oder Müdigkeit geschlossen werden. Bekannt ist dies von Bildern des Gesichts, der Hand und des Augenhintergrunds sowie von verhaltensbasierten biometrischen Merkmalen (Sprache, Unterschrift) sowie in besonderer Weise von genetischen Daten. Weniger problematisch sind nach aktueller Kenntnis Fingerabdruck und Iris.

In der Regel sind nur aus den biometrischen Rohdaten solche Zusatzinformationen ableitbar, nicht aber aus den daraus gewonnenen sog. Templates. Aus diesem Grund dürfen insbesondere die Rohdaten selbst nicht zentral gespeichert werden. Außerdem sind im Verarbeitungsprozess einer konkreten biometrischen Kontrolle die Rohdaten möglichst früh zu löschen, um die Gefahr einer Zweckentfremdung zu verringern.

6.1.6 Ergebnis

Im Ergebnis zeigt sich, dass keines der Merkmale unproblematisch ist. Vor der Entscheidung für ein bestimmtes biometrisches Merkmal in Ausweisen müssen die verschiedenen Risiken daher sorgfältig gegeneinander abgewogen werden. Hierzu bedarf es einer ausführlichen Diskussion. Die Aufforderung des Bundesrates an die Bundesregierung, unverzüglich das Gesetzgebungsverfahren zur Einführung biometrischer Merkmale in Ausweisdokumenten einzuleiten, ist daher abzulehnen. Vorzuziehen wäre ein Erprobungsgesetz – wie zur Zeit für die datenschutzrechtlich ebenfalls sehr problematische Volkszählung. Dabei wären gleichzeitig in einem praxisnahen Großversuch Ausweise mit zusätzlichen Sicherheitsmerkmalen gemäß den neu herausgegebenen Exemplaren ohne biometrische Merkmale sowie mit biometrischen Merkmalen zu erproben und zu bewerten. Einzubeziehen wäre auch das beträchtliche Restrisiko, dass bei PC-gestützten Merkmalen wegen Gerätedefekten und auch statistisch zu erwartenden Falscherkennungen eine Vielzahl von Bürgern bei der Ausweiskontrolle trotz eines echten eigenen Ausweises aufgehalten und intensiver überprüft werden, als sonst notwendig.

7. Meldewesen

7.1 Novellierung des Melderechtsrahmengesetzes (MRRG)

Gegenwärtig zeichnet sich eine bedenkliche Absenkung des Datenschutzniveaus im Meldewesen ab.

Die Bundesregierung hat am 17. August 2001 den Entwurf eines Gesetzes zur Änderung des Melderechtsrahmengesetzes und anderer Gesetzes vorgelegt. Der Gesetzentwurf sieht u.a. die Erteilung von Melderegisterauskünften im

Wege des automatisierten Abrufs über das Internet, den Verzicht auf die Abmeldung bei innerdeutschen Umzügen bei gleichzeitig erhöhter Effizienz des behördlichen Rückmeldeverfahrens sowie die weitgehende Abschaffung der Mitwirkungspflicht des Wohnungsgebers bei An- oder Abmeldungen vor.

Die nachstehenden Punkte aus dem Gesetzgebungsverfahren betrachten wir als besonders kritisch.

7.1.1 Verringerte Schutzwirkung melderechtlicher Auskunftssperren

Nach der geltenden Fassung des MRRG ist die melderechtliche Auskunftssperre mit einer absoluten und umfassenden Schutzwirkung gegenüber Auskunftsanträgen nicht-öffentlicher Stellen ausgestattet. Jede Melderegisterauskunft an Private ist unzulässig, und zwar unabhängig davon, ob die Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen, die zur Eintragung der Auskunftssperre führte, konkret von der anfragenden Person oder Einrichtung ausgeht. Auf diese Weise soll verhindert werden, dass der für die Gefahr Verantwortliche gegenüber der Meldebehörde einen unverdächtigen Dritten („Strohmann“) vorschiebt und so die Auskunftssperre umgeht.

Nach dem Gesetzentwurf sollen Melderegisterauskünfte trotz Auskunftssperre erteilt werden dürfen, wenn nach Anhörung des Betroffenen eine Gefahr ausgeschlossen werden kann. Hiergegen bestehen erhebliche Bedenken. Häufig dürfte es vom Zufall oder auch vom kriminellen Geschick des Anfragenden abhängen, ob der Betroffene und die Meldebehörde den Zusammenhang zwischen dem Auskunftsantrag und dem der Auskunftssperre zugrunde liegenden Sachverhalt erkennen oder nicht. Um Klarheit zu gewinnen, wären intensive Nachforschungen durch die Meldebehörde erforderlich, die nicht leistbar und mit ihrem gesetzlichen Aufgabenprofil auch nicht vereinbar wären. Bei auffälliger Häufung von Gläubigeranfragen und entsprechendem Missbrauchsverdacht steht es der Meldebehörde frei, die Auskunftssperre nach Ablauf nicht zu verlängern.

7.1.2 Speicherung von Seriennummern im Melderegister

Die Seriennummern des Personalausweises und des Passes dürfen seit dem 1. September 1991 nicht mehr im Melderegister gespeichert werden. Der Bundesrat spricht sich in seiner Stellungnahme zum Gesetzentwurf demgegenüber dafür aus, für die Mitwirkung bei Maßnahmen der Gefahrenabwehr oder Strafverfolgung die Seriennummer im Melderegister zu speichern. Damit soll es den Sicherheitsbehörden ermöglicht werden, schnell und ohne weitergehende Ermittlungen die Echtheit der Ausweispapiere festzustellen.

Die Bundesregierung geht in ihrer Gegenäußerung noch einen Schritt weiter. Sie will auch den Verfassungsschutzbehörden, dem Bundesnachrichtendienst (BND), dem Militärischen Abschirmdienst (MAD) sowie den für Strafvollstreckung und Strafvollzug zuständigen Behörden über das Melderegister den Zugriff auf die Seriennummern erlauben.

Der Vorschlag des Bundesrates weicht ohne zwingenden Grund die bewährte funktionelle Trennung des Melderegisters einerseits sowie des Personalausweis- und Passregisters andererseits auf. Die Echtheit von Ausweispapieren und die Identität der Ausweisinhaber festzustellen, gehört zu den wesentlichen Zweckbestimmungen des Personalausweis- und Passregisters. Aus diesen Registern darf unter den gesetzlich näher umschriebenen Voraussetzungen die Seriennummer auch an Sicherheitsbehörden übermittelt werden. Insofern besteht für die vom Bundesrat befürwortete und von der Bundesregierung noch ausgeweitete Regelung kein sachlicher Bedarf. Im Übrigen soll das Fälschungsrisiko durch die im November 2001 eingeführten Hologramme in Ausweispapieren weiter reduziert werden.

7.1.3 Erweiterung der Auskunftsverweigerungsgründe

Der Bundesrat tritt in seiner Stellungnahme dafür ein, die Tatbestände, die die Meldebehörde zur Auskunftsverweigerung gegenüber den Betroffenen berechtigen, in Angleichung an § 19 des Bundesdatenschutzgesetzes (BDSG) deutlich zu erweitern. Dieser Vorschlag ist abzulehnen. Die bisherige datenschutzfreundliche Regelung, nach der Auskünfte gegenüber Betroffenen nur aus besonderen personenstands- bzw. adoptionsrechtlichen Gründen abgelehnt werden dürfen, hat sich bewährt. Sicherheitsdefizite haben sich bislang nicht ergeben und sind bei Fortbestand der Rechtslage auch künftig nicht zu erwarten.

8. Personenstandswesen

8.1 Umstellung auf die Software AutiSta NT beim Projekt Automation Standesamt (PASTA)

Dem in der Risikoanalyse ermittelten Schutzbedarf muss durch geeignete technische und organisatorische Maßnahmen Rechnung getragen werden.

Nach Mitteilung des Senatsamtes für Bezirksangelegenheiten (SfB) soll die beim Projekt Automation Standesamt (PASTA) für die Vorgangsbearbeitung von Personenstandsfällen eingesetzte Software Autista, ein DOS-basiertes Programm, durch eine neue Windows-basierte Software AutiSta NT abgelöst werden. Der Einsatz des neuen Verfahrens soll voraussichtlich mit zentral im Landesamt für Informationstechnik (LIT) liegenden Datenbanken realisiert werden.

Da mit dem neuen Verfahren Risiken für den Datenschutz verbunden sind, hat das SfB, gemäß der Forderung des § 8 Abs. 4 Hamburgisches Datenschutzgesetz (HmbDSG), hierfür eine Risikoanalyse durchgeführt und dem Hamburgischen Datenschutzbeauftragten zur Stellungnahme zugeleitet. In dieser Risikoanalyse wird der Schutzbedarf für das PASTA-Verfahren mit der Software AutiSta NT auf Grund der Schutzbedürftigkeit der personenbezogenen Verarbeitungsdaten insgesamt als „sehr hoch“ eingestuft.

Dieser hohe Schutzbedarf wurde zwar auf den geplanten Serverbetrieb im LIT übertragen; für die Clients sowie für die notwendigen Kommunikationsverbindungen wurde dagegen nur ein mittlerer Schutzbedarf ermittelt. Besondere technische und organisatorische Maßnahmen sind weder für die Kommunikationsverbindungen, Büro- und Technikräume noch für die Clients vorgesehen. Der Datentransfer des Verfahrens zwischen dem LIT und den Standesämtern in den Bezirken soll zudem unverschlüsselt erfolgen.

Sofern der Schutzbedarf des Dialogverfahrens aufgrund besonders schutzwürdiger personenbezogener Daten tatsächlich als „sehr hoch“ einzustufen ist, muss sich dieser hohe Schutzbedarf nach unserer Auffassung insbesondere auch in der Betrachtung der Clients und der Kommunikationsverbindungen sowie ggf. vorgesehener Schnittstellen zu anderen Anwendungen wiederfinden.

Wie uns das SfB mitteilte, sollen die von uns aufgezeigten Problempunkte erneut einer intensiven Prüfung hinsichtlich der Möglichkeit des Einsatzes von Sicherheitsmaßnahmen unterzogen werden. Die daraus resultierenden Ergebnisse sollen dann in die in Arbeit befindliche Datenschutzkonzeption einfließen. Der Entwurf der Datenschutzkonzeption soll uns dann zur abschließenden Bewertung zugeleitet werden.

9. Umwelt

9.1 Hamburgisches Bodenschutzgesetz

In Hamburg wurde ein Landes-Bodenschutzgesetz weitgehend datenschutzkonform geschaffen.

Das im Jahre 1998 eingeleitete behördliche Abstimmungsverfahren über den Entwurf eines Hamburgischen Bodenschutzgesetzes konnte endlich zum Abschluss gebracht werden. Mit dem am 20. Februar 2001 beschlossenen Hamburgischen Gesetz zur Ausführung und Ergänzung des Bundes-Bodenschutzgesetzes (Hamburgisches Bodenschutzgesetz – HmbBodSchG) sind auch unsere langjährigen Forderungen, gesetzliche Grundlagen für die Nutzung eines Bodeninformationssystems und die Verarbeitung der in ihm gespeicherten personenbezogenen Daten zu schaffen (vgl. zuletzt 17. TB, 5.1), erfüllt worden. Die entsprechenden datenschutzrechtlichen Bestimmungen wurden im Zweiten Teil des Gesetzes geregelt.

In den §§ 5 und 6 sind im Wesentlichen der Inhalt und die Führung des Bodeninformationssystems festgelegt worden. Danach darf die zuständige Behörde die zum Zwecke der Aufgabenerfüllung nach dem Bundes-Bodenschutzgesetz, dem HmbBodSchG und nach den auf Grund dieser Gesetze erlassenen Rechtsverordnungen, insbesondere zur Führung des Bodeninformationssystems, erforderlichen personenbezogenen Daten erheben und verarbeiten. Weiterhin ist geregelt, dass auf das Bodeninformationssystem und die mit ihm verbundene Verarbeitung personenbezogener Daten grundsätzlich das Hamburgische Datenschutzgesetz Anwendung findet.

Regelungen für die Übermittlung von Daten aus dem Bodeninformationssystem an andere Behörden und öffentliche Stellen sowie die Unterrichtung der Öffentlichkeit über Art und Ausmaß schädlicher Bodenveränderungen, die von einem Grundstück ausgehen, sind in den §§ 7 und 8 festgeschrieben worden.

Weitere Regelungen über Auskünfte aus dem Bodeninformationssystem wurden nicht getroffen, da nach § 4 Umweltinformationsgesetz (UIG) jeder Anspruch auf freien Zugang zu Informationen über die Umwelt hat, soweit nicht schutzwürdige öffentliche Belange oder Interessen der Betroffenen entgegenstehen (§§ 7, 8 UIG).

9.2 Sonstiges

Die im 17. TB (5.2) angekündigten Novellierungen von Umweltschutzgesetzen konnten zwischenzeitlich ebenfalls abgeschlossen werden, so dass auch in dem Hamburgischen Wassergesetz vom 11. April 2000 (HmbGVBl. S. 78), dem Hamburgischen Naturschutzgesetz vom 2. Mai 2001 (HmbGVBl. S. 75) und dem Hamburgischen Abwassergesetz vom 24. Juli 2001 angemessene bereichsspezifische datenschutzrechtliche Regelungen enthalten sind. Über die Notwendigkeit von bereichsspezifischen datenschutzrechtlichen Regelungen im Hamburgischen Abwassergesetzes hatten wir bereits 1992 berichtet (vgl. 11.TB, 5.3).

10. Sozialdaten

10.1 Anforderung ärztlicher Unterlagen durch Krankenkassen bei Krankenhäusern

Immer wieder schießen Krankenkassen über das Ziel hinaus, wenn es darum geht, die Krankenhausbehandlung von Versicherten zu überprüfen.

Bereits seit mehreren Jahren beschäftigen wir uns mit der Praxis einiger Krankenkassen, pauschal ärztliche Unterlagen bei den Krankenhäusern abzufordern (vgl. 13. TB, 21.8.2). Nachdem das seinerzeit mit der AOK Hamburg verabredete Verfahren weitgehend keine Probleme bereitet, hat sich im Berichtszeitraum bei der Betriebskrankenkasse Hamburg (BKK Hamburg) eine

Praxis entwickelt, die wir nach § 25 HmbDSG datenschutzrechtlich beanstanden mussten. Die BKK Hamburg verlangt von den Krankenhäusern, dass ihr sämtliche von ihr angeforderten Krankenberichte, Entlassungsberichte und Krankenakten direkt – und nicht dem Medizinischen Dienst der Krankenversicherung (MDK) – zugeleitet werden. Dies verstößt gegen datenschutzrechtliche Bestimmungen.

Die gesetzlichen Krankenkassen dürfen medizinische Daten nur für die Erfüllung der in § 284 Abs. 1 Fünfter Teil Sozialgesetzbuch (SGB V) aufgezählten Aufgaben erheben und speichern. Die medizinischen Daten der Patienten, die in einem Krankenhaus behandelt werden, unterliegen der ärztlichen Schweigepflicht im Sinne von § 203 Strafgesetzbuch (StGB). Sie dürfen nur „befugt" von den Krankenhäusern an Dritte übermittelt werden. Eine Befugnis zur Übermittlung der Daten an eine Krankenkasse kann sich aus einer Rechtsvorschrift oder aus einer Einwilligung des Patienten ergeben. Im SGB V sind in einer Reihe von Vorschriften detailliert die Befugnisse bzw. die Verpflichtungen der Leistungserbringer zur Übermittlung personenbezogener Patientendaten an die Krankenkassen festgelegt. Die Vorschriften stellen eine abschließende Regelung dar.

Für die Krankenhäuser ist in § 301 SGB V festgelegt, welche Daten von den Krankenhäusern zu Abrechnungszwecken an die Krankenkassen zu übermitteln sind. Der Datenkatalog des § 301 SGB V stellt nicht nur eine Regelung für die Fälle der maschinenlesbaren Übermittlung von Leistungsdaten dar, sondern eine abschließende Regelung zulässiger Datenübermittlungen zu Abrechnungszwecken von Krankenhäusern an Krankenkassen.

§ 301 Abs. 1 Satz 1 Nr. 3 SGB V legt fest, dass auf Verlangen der Krankenkasse die medizinische Begründung für die Überschreitung der Dauer der Krankenhausbehandlung zu übermitteln ist. Die Vorschrift eröffnet nicht die Befugnis der Krankenkasse zur umfassenden Erhebung von Krankenhausentlassungsberichten, Arztbriefen, Befundberichten, ärztlichen Gutachten etc. Diese Unterlagen enthalten wesentlich mehr Informationen als die in der genannten Vorschrift erwähnte „medizinische Begründung". Zulässig ist die Übermittlung von Informationen auf bestimmte Fragen im erforderlichen Umfang.

Darüber hinaus kann die Krankenkasse nach § 275 Abs. 1 in Verbindung mit § 284 Abs. 1 Nr. 7 SGB V Unterlagen anfordern zur Prüfung, ob der MDK eingeschaltet wird. § 275 SGB V regelt abschließend, wann die Krankenkassen den MDK einschalten müssen. Im übrigen besteht danach ein Beurteilungsspielraum der Krankenkassen hinsichtlich der Einschaltung des MDK. Zur Durchführung dieser Prüfung dürfen in Ausnahmefällen, die zu begründen sind, von den Krankenkassen für die Prüfung im jeweiligen Einzelfall über § 301 SGB V hinaus erforderliche Daten von den Krankenhäusern angefordert werden. Da das Sozialgesetzbuch hierfür keine Übermittlungsbefugnis vorsieht, bedarf eine solche Übermittlung der Einwilligung des Versicherten.

Wird der MDK von der Krankenkasse mit der Erstellung eines Gutachtens beauftragt, so kann er hierfür erforderliche zusätzliche Daten bei den Leistungserbringern – u.a. den Krankenhäusern – unter Hinweis auf die Rechtslage (bei Rechnungsprüfungen § 275 Abs. 1 Nr. 1 in Verbindung mit § 276 Abs. 2 Satz 1 2. Halbsatz SGB V, bei der Überprüfung der Notwendigkeit und Dauer der stationären Behandlung § 276 Abs. 4 in Verbindung mit § 276 Abs. 2 Satz 1 2. Halbsatz SGB V) anfordern. Dies kann auch beispielsweise Operations- oder Entlassungsberichte umfassen.

§ 276 Abs. 2 SGB V erlegt den Krankenhäusern Verpflichtungen zur Übermittlung von Daten unmittelbar an den MDK auf. Die medizinische Bewertung von Einzelfällen wird in § 275 SGB V dem MDK übertragen. Die im Sozialgesetzbuch insoweit festgelegte Aufgabenverteilung zwischen Krankenkassen und MDK darf nicht durch abweichende Verfahren unterlaufen werden. Eine Versendung der nach diesen Vorschriften angeforderten Unterlagen an die Krankenkassen ist daher allenfalls dann hinnehmbar, wenn die medizinischen Unterlagen in einem besonderen verschlossenen Umschlag übersandt werden, der mit der Anschrift des MDK sowie mit einem Vermerk „Ärztliche Unterlagen – Nur vom MDK zu öffnen“ versehen ist. Damit wird sichergestellt, dass die im SGB V festgelegte Aufgabenteilung zwischen MDK und Krankenkassen eingehalten wird und eine unzulässige Einsichtnahme durch die Krankenkassen nicht erfolgt.

Die Praxis der BKK Hamburg genügt diesen rechtlichen Vorgaben nicht. In Fällen, in denen sie auf Grund der ihr nach § 301 SGB V übermittelten Daten Zweifel an der Notwendigkeit oder Dauer der stationären Krankenhausbehandlung erhebt, verlangt die BKK Hamburg von den Krankenhäusern die Übersendung von Arztberichten, Entlassungsberichten oder Krankenakten. Die BKK Hamburg legt diese Unterlagen den bei ihr beschäftigten Ärzten zur Beurteilung vor, ob die medizinische Notwendigkeit der stationären Krankenhausbehandlung gegeben war. Die Prüfung der Unterlagen durch die bei der BKK Hamburg beschäftigten Ärzte umfasst auch die Fragestellung, ob die Unterlagen dem MDK zur weiteren Stellungnahme übergeben werden sollen. Von dem Versicherten wird für dieses Verfahren keine Einwilligungserklärung eingeholt.

Diese Praxis wurde auch im Kreis der Datenschutzbeauftragten des Bundes und der Länder erörtert. Dabei bestand Einvernehmen über die Unzulässigkeit des Verfahrens. Der Bundesbeauftragte hat die Problematik bereits an das Bundesversicherungsamt (BVA) herangetragen mit dem Ergebnis, dass die Auffassung der Datenschutzbeauftragten grundsätzlich vom BVA geteilt wird.

Trotz dieser Rechtslage weigerte sich die BKK Hamburg bislang, das Verfahren den rechtlichen Erfordernissen anzupassen. Auch die seit Jahren bei der AOK Hamburg praktizierte Einwilligungslösung, die mit uns abgestimmt wurde, will

die BKK Hamburg nicht übernehmen. Das Verfahren der AOK ist im Einzelnen wie folgt ausgestaltet:

Die Versicherten werden schriftlich gebeten, in eine zeitweise Überlassung von bestimmten Patientendaten durch das Krankenhaus oder den Arzt einzuwilligen. In diesem Schreiben werden Anlass, Zweck und Verfahren der Prüfung beschrieben; außerdem wird darauf hingewiesen, dass bei einer Verweigerung der Schweigepflichtentbindung mit einer direkten Anforderung der Unterlagen durch den MDK zu rechnen ist. Ob die Prüfung durch eigene Ärzte der Krankenkasse oder durch Dritte erfolgt, ist dabei rechtlich unerheblich.

Willigt der Versicherte in die Übermittlung der ärztlichen Unterlagen an die Krankenkasse ein, darf die Krankenkasse die Materialien nur für die Prüfung verwenden, ob der MDK eingeschaltet werden soll oder nicht. Eine Verwendung für weitere Zwecke oder eine Auswertung nach unterschiedlichen Gesichtspunkten hat zu unterbleiben. Unzulässig ist es auch, die Unterlagen zur Versichertenakte zu nehmen oder die Angaben elektronisch bei der Krankenkasse zu speichern.

Kommt die Krankenkasse zu dem Ergebnis, dass eine Begutachtung durch den MDK erforderlich ist, sind diesem die Unterlagen ausnahmslos zu übergeben. Soll der MDK nicht eingeschaltet werden, hat die Krankenkasse die Unterlagen entweder ordnungsgemäß zu vernichten oder dem Absender zurück zu geben.

Dieses Verfahren darf sich ausdrücklich allenfalls auf begründete Einzelfälle beschränken, d.h. ein regelhafter Einsatz wäre unzulässig.

Da der Mangel von der BKK Hamburg weder fristgerecht behoben wurde noch die Behebung des Mangels durch die Krankenkasse erkennbar war, haben wir nach § 25 Abs. 1 Satz 2 HmbDSG eine weitere Beanstandung an die für das Sozialversicherungswesen zuständige Aufsichtsbehörde vorbereitet. Bis zum Redaktionsschluss war noch offen, ob die weitere Beanstandung auch ausgesprochen werden muss, weil wir vorher der Aufsichtsbehörde im Rahmen unserer ständigen Praxis die Gelegenheit gegeben haben, doch noch für eine Mängelbeseitigung zu sorgen.

10.2 Zusammenarbeit zwischen Sozialämtern und Arbeitsämtern

Auch wenn neue gesetzliche Bestimmungen eine verstärkte Zusammenarbeit zwischen Sozialämtern und Arbeitsämtern zulassen, dürfen datenschutzrechtliche Grundsätze dabei nicht außer Acht bleiben.

Am 1. Januar 2001 trat das „Gesetz zur Verbesserung der Zusammenarbeit von Arbeitsämtern und Trägern der Sozialhilfe“ in Kraft. Es enthält praktisch zwei gleichlautende Einfügungen in das Dritte Buch Sozialgesetzbuch (SGB III) und in das Bundessozialhilfegesetz (BSHG), nämlich einer Verpflich-

tung zur Zusammenarbeit und einer Regelung zu Modellvorhaben. Im Berichtszeitraum haben wir uns eingehender mit der praktischen Durchführung des Modellvorhabens JobPlan in Hamburg auseinandergesetzt.

Die rechtlichen Rahmenbedingungen für Modellvorhaben sind durch die Einfügungen eines § 421d SGB III und eines § 18a BSHG geschaffen worden. Danach fördert das Bundesministerium für Arbeit und Sozialordnung (BMA) auf Antrag regionale gemeinsame Modellvorhaben zur Verbesserung der Zusammenarbeit des Arbeitsamtes und der örtlich zuständigen Träger der Sozialhilfe für Arbeitslosenhilfebezieher und für arbeitslose Empfänger von Hilfe zum Lebensunterhalt nach dem BSHG. Übergreifendes Ziel ist es dabei, für den genannten Personenkreis die Hilfebedürftigkeit zu überwinden und die Bedingungen zu ihrer beruflichen Eingliederung in den regulären Arbeitsmarkt zu verbessern. Hierfür sollen die Arbeitsämter und die Träger der Sozialhilfe Kooperationsvereinbarungen nach § 371a SGB III und § 18 Abs. 2 BSHG abschließen.

Die diesbezüglichen Hamburger Kooperationsvereinbarungen basieren auf dem bundesweiten Modellvorhaben MoZArT (Modellprojekt zur Verbesserung der Zusammenarbeit von Arbeitsämtern und Trägern der Sozialhilfe) des BMA. JobPlan ist eines der Projekte, die bundesweit durch MoZArT gefördert werden.

Ziel von JobPlan ist es, durch eine enge Zusammenarbeit zwischen Sozialhilfeträger und Arbeitsamt, bei gleichzeitiger Verzahnung von Instrumenten und Fachwissen, eine möglichst hohe Zahl von Langzeitarbeitslosen in den allgemeinen Arbeitsmarkt zu integrieren. Für Hamburg stehen nicht die Hilfen aus den gesetzlichen Leistungsansprüchen der jeweiligen Zielgruppen des Arbeitsamtes oder des Sozialhilfeträgers im Vordergrund, sondern vielmehr die Frage der individuellen Geeignetheit einer Maßnahme auf Grund eines vorliegenden Hilfeplans. Die hierfür notwendigen Schritte sehen wie folgt aus:

- In einem Assessmentverfahren werden für Personen mit unklarer Eingliederungsperspektive individuelle Eingliederungspläne erstellt. Die Durchführung der Assessmentverfahren wurde an Dritte vergeben, damit sowohl die Arbeitsämter als auch die Sozialämter durch eine professionelle und möglichst objektive Analyse der Persönlichkeit und der Fähigkeiten eines Bewerbers zuverlässige Aussagen über geeignete Beschäftigungsfelder erhalten. Sie sind Voraussetzung für das anschließende Clearing-Verfahren.

- In einer Clearingstelle entscheiden Mitarbeiterinnen und Mitarbeiter beider Ämter auf der Basis der Ergebnisse des Assessmentverfahrens gemeinsam und verbindlich sowohl für das Klientel des Arbeitsamtes als auch für das des Trägers der Sozialhilfe, welche konkreten Maßnahmen zur Überwindung der Hilfebedürftigkeit und der beruflichen Eingliederung in den regulären Arbeitsmarkt getroffen werden sollen.

Gegen die Einschaltung eines privaten Anbieters hatten wir zunächst datenschutzrechtliche Bedenken erhoben, obwohl der Datenaustausch zwischen Sozialamt, Arbeitsamt und beauftragter Stelle – hier also dem Anbieter – durch die Bestimmungen des § 421d Abs. 3 Satz 1 SGB III bzw. § 18a Abs. 3 Satz 1 BSHG grundsätzlich zulässig ist. Im Rahmen dieses zugelassenen Eingriffs in das informationelle Selbstbestimmungsrecht kommt es jedoch darauf an, dass den allgemeinen datenschutzrechtlichen Erfordernissen entsprochen wird. Dies heißt insbesondere:

– Nur das erforderliche Minimum an Daten darf verlangt werden.

– Die Daten dürfen grundsätzlich nur für den Zweck verwendet werden, für den sie erhoben oder erfasst wurden.

– Es muss durch ergänzende Vorkehrungen dafür gesorgt werden, dass bei der Organisation und beim Verfahren des Umgangs mit personenbezogenen Daten auf die Rechte des einzelnen Rücksicht genommen wird (z.B. durch Mitwirkungs- und Kontrollrechte).

Da diese Grundsätze nicht durchgängig verwirklicht waren, haben wir die Behörde für Arbeit, Gesundheit und Soziales auf die datenschutzrechtlichen Defizite hingewiesen und erreichen können, dass einige Änderungen vorgenommen worden sind. Insbesondere ging es uns darum, den „Vertrag zur Durchführung von Assessmentverfahren für Beziehende von Arbeitslosenhilfe und Sozialhilfe“ zu konkretisieren und den datenschutzrechtlichen Erfordernissen anzupassen. Hierbei handelte es sich im einzelnen um folgende Punkte:

– Der Anbieter wird verpflichtet, die Bestimmungen des Sozialdatenschutzes einzuhalten. Das heißt u.a., dass der Anbieter die übermittelten Daten nach § 78 SGB X ausschließlich für Zwecke der Durchführung von Assessmentverfahren und der Erstellung von Fähigkeitsprofilen verwenden darf. Er hat die Sozialdaten im selben Umfang geheim zu halten wie der Sozialleistungsträger selbst. Nach Abschluss der Assessmentverfahren und Abrechnung der Vergütungen aus dem Vertrag hat der Anbieter die Daten physisch zu löschen. Eine nur logische Vernichtung der Daten reicht nicht aus.

– Der Anbieter hat alle im Zusammenhang mit der Ausführung des Vertrags bekannt gewordenen Daten – auch nach Beendigung des Auftrags – geheim zu halten und nicht an Dritte weiter zu geben. Diese Verpflichtung erstreckt sich auch auf die Mitarbeiterinnen und Mitarbeiter des Anbieters. Außerdem ist er verpflichtet, alle Personen, die er zur Durchführung des Auftrags einsetzt, auf die Einhaltung der Datenschutzvorschriften hinzuweisen.

– Die auftraggebenden Sozialleistungsträger haben das Recht, bei dem Anbieter jederzeit Auskünfte über die Einhaltung des Sozialdatenschutzes einzuholen, während der üblichen Geschäftszeit die Geschäftsräume zu betreten, um dort die Einhaltung des Sozialdatenschutzes zu überprüfen, und die Auftragsunterlagen sowie die gespeicherten Sozialdaten und Datenverarbeitungsprogramme einzusehen.

– Die Vergabe von Unteraufträgen durch den Anbieter ist nur mit schriftlicher Zustimmung beider auftraggebenden Sozialleistungsträger zulässig.

Außerdem wurden auf unsere Anregung die eingesetzten Formulare in einigen Punkten überarbeitet, damit nur die erforderlichen Daten erhoben werden.

Mit dem erreichten Ergebnis können wir insgesamt zufrieden sein. Wir werden aber den weiteren Verlauf des Projektes verfolgen und unter Umständen auf neu auftretende datenschutzrechtliche Probleme hinweisen. Beispielsweise sind die genannten gesetzlichen Regelungen zur Verbesserung der Zusammenarbeit von Sozialämtern und Arbeitsämtern ausdrücklich auf Modellvorhaben, nicht auf eine grundlegende Umstellung der Sozialhilfe zugeschnitten. Auch geht der Gesetzgeber davon aus, dass eine getrennte Datenverarbeitung von den Arbeitsämtern und den beteiligten örtlichen Trägern der Sozialhilfe zu führen ist. Die Ermächtigung des § 421a Abs. 3 SGB III kann für Formen der Kooperation nach § 371a SGB III nicht in Anspruch genommen werden.

Schließlich könnten auch die unterschiedlichen Zuständigkeiten für den Datenschutz bedeutsam werden. Für die Arbeitsämter ist der Bundesbeauftragte für den Datenschutz zuständig, für die Sozialämter die Landesbeauftragten. Für mögliche gemeinsame Anlaufstellen müssten daher neue datenschutzrechtliche Zuständigkeiten geregelt werden.

10.3 Krankenhilfe nach dem Bundessozialhilfegesetz (BSHG)

Das Sozialamt darf für die Gewährung von Krankenhilfe grundsätzlich nur solche Angaben erheben, die auch eine Krankenkasse zulässigerweise erfahren würde.

Nach § 37 Bundessozialhilfegesetz (BSHG) ist Personen, die keinen ausreichenden Krankenschutz allgemein oder bei einer einzelnen Krankheit haben, eine wirksame Krankenhilfe durch den Sozialleistungsträger zu gewähren. Die Krankenhilfe richtet sich in Art und Umfang weitgehend nach den Leistungen der gesetzlichen Krankenversicherung, sofern dem die Besonderheiten der Sozialhilfe nicht entgegenstehen. Grundsätzlich umfasst die Krankenhilfe alle Maßnahmen zur Behandlung von Krankheiten, soweit sie notwendig und wirtschaftlich sind, d.h. die Leistungen der Krankenhilfe sollen in der Regel den Leistungen der gesetzlichen Krankenversicherung entsprechen. Neben der ärztlichen und zahnärztlichen Behandlung sowie der

Krankenhausbehandlung gehören dazu auch die sonstigen zur Genesung, zur Verbesserung oder zur Linderung der Krankheitsfolgen erforderlichen Leistungen, wie z.B. Heil- und Genesungskuren.

Um die zur Gewährung von Krankenhilfe erforderlichen Prüfungen anstellen zu können, benötigt der Sozialleistungsträger grundsätzlich auch die Angaben, die ansonsten zulässigerweise die gesetzliche Krankenversicherung erhalten würde. Die hierfür maßgeblichen Übermittlungsregelungen ergeben sich aus den §§ 294 ff. Fünfter Teil Sozialgesetzbuch (SGB V).

§ 301 SGB V regelt abschließend die Pflichten der Krankenhäuser und Vorsorge- oder Rehabilitationseinrichtungen zur Übermittlung der Angaben, die zur Abrechnung der erbrachten ärztlichen Leistungen erforderlich sind. Dabei werden die zu übermittelnden Angaben aus datenschutzrechtlichen Gründen in Absatz 1 und 4 enumerativ aufgeführt.

Die zulässigerweise übermittelten Angaben sind nach § 304 SGB V bei der gesetzlichen Krankenversicherung – und damit auch beim Sozialleistungsträger – ordnungsgemäß aufzubewahren. Die Vorschrift ergänzt und modifiziert die Regelung des § 84 Zehnter Teil Sozialgesetzbuch (SGB X), wonach eine Pflicht zur Löschung von Sozialdaten besteht, wenn ihre Kenntnis für die speichernde Stelle zur Aufgabenwahrnehmung nicht mehr erforderlich ist und durch die Löschung schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden.

Um diesen und anderen datenschutzrechtlichen Anforderungen entsprechen zu können, sind die Sozialdienststellen nach der Gemeinsamen Dienstvorschrift der Behörde für Arbeit, Gesundheit und Soziales und des Senatsamtes für Bezirksangelegenheiten über die Anlage, Führung und Vernichtung von Sozialhilfe-, Blindengeld- und Kriegsopferfürsorgerakten verpflichtet, in einer gesonderten zweiten Heftung der Akte besonders schutzwürdige Unterlagen abzulegen. Hierbei handelt es sich im wesentlichen um Unterlagen, die von einer der in § 203 Abs. 1 oder 3 Strafgesetzbuch (StGB) genannten geheimnisverpflichteten Personen erstellt worden sind, also insbesondere von Ärzten, Apothekern, Sozialarbeitern, Angehörigen privater Versicherungen sowie deren Gehilfen (z.B. Arzthelfer). Die in der zweiten Heftung abgelegten Unterlagen müssen bei Aktenversand grundsätzlich aus der Sozialhilfeakte entfernt und zum Retent genommen werden.

Die im Gesetz genannten Befugnisse rechtfertigen nicht die Weitergabe von Angaben, ohne dass vorher die Erforderlichkeit der Übermittlung geprüft und festgestellt wurde. Beispielsweise werden Angaben über Dritte, die sich aus der Familienanamnese ergeben, sowie Labor-, EKG- und Röntgenbefunde in der überwiegenden Zahl der Fälle von der gesetzlichen Übermittlungsbefugnis nicht gedeckt sein.

Datenschutzrechtlich vorrangig verantwortlich für die Einhaltung der Übermittlungsregelungen sind allerdings die Krankenhäuser bzw. die Vorsorge- oder Rehabilitationseinrichtungen, nicht jedoch die Krankenkassen oder sonstigen Kostenträger. Die Sozialleistungsträger können insoweit lediglich verpflichtet werden, nur die nach § 301 SGB V zugelassenen Angaben anzufordern. Hinsichtlich der nicht zugelassenen, aber „aufgedrängten" Angaben besteht entweder die Möglichkeit, sie der übermittelnden Stelle zurück zu senden oder nach § 84 Abs. 2 SGB X zu vernichten.

Das Senatsamt für Bezirksangelegenheiten ist von uns auf diese Rechtslage hingewiesen worden und hat dies zum Anlass genommen, die bezirklichen Sozialdienststellen bei der Gewährung von Krankenhilfe für Krankenhaus- und Kurbehandlungen auf die Verpflichtung aufmerksam zu machen, nur die in § 301 SGB V zugelassenen und für die Aufgabenerfüllung erforderlichen Angaben in der zweiten Heftung der Sozialhilfeakte aufzubewahren. Da die Problematik in ähnlicher Weise auch in den Durchführungsbereichen der Behörde für Arbeit, Gesundheit und Soziales und der Behörde für Schule, Jugend und Berufsbildung auftreten kann, haben wir veranlasst, dass diese Stellen ebenfalls entsprechend verfahren.

10.4 Befreiung von der Rundfunkgebührenpflicht

Datenschutzrechtliche Mängel beim Verfahren zur Befreiung von der Rundfunkgebührenpflicht sind weitgehend beseitigt worden.

Wir haben im Berichtszeitraum gemeinsam mit unseren Kollegen aus den anderen NDR-Vertragsländern (Mecklenburg-Vorpommern, Niedersachsen und Schleswig-Holstein) das Verfahren zur Befreiung von der Rundfunkgebührenpflicht näher untersucht. Ausgelöst wurde dies durch zahlreiche Eingaben, die wir insbesondere von Studierenden erhalten hatten.

Personen mit geringem Einkommen können auf Antrag regelmäßig von der Rundfunkgebührenpflicht befreit werden, wenn das Einkommen den eineinhalbfachen Sozialhilferegelsatz plus Kaltmiete nicht überschreitet. Die Anträge sind in den Sozialämtern zu stellen, wo sie geprüft und unter bestimmten Voraussetzungen beschieden werden. Der Norddeutsche Rundfunk (NDR) hatte zunächst von Studierenden zusätzliche Daten durch einen gesonderten Fragebogen erhoben. Sonstige Antragsteller mussten den Fragebogen nicht ausfüllen. Bei den Daten ging es u.a. um Angaben über Heiz- und Stromkosten, Versicherungsbeiträge verschiedenster Art, Sparprämien, Telefon- und Handygebühren, Kabel- und Internetgebühren, Fahrtkosten, Studiengebühren und -material sowie Kosten für die Unterhaltung eines PKW. Mit dem Fragebogen sollte geprüft werden, inwieweit die Angaben der Studierenden glaubwürdig sind.

Aus unserer Sicht war dieses Verfahren aus zwei Gründen datenschutzrechtlich problematisch. Zum einen bestand der Eindruck, dass die Glaubwürdigkeit der Studierenden pauschal in Zweifel gezogen wurde, weil nur sie den Fragebogen auszufüllen hatten. Zum anderen erhielt das Sozialamt einen tiefen Einblick in die Haushaltskasse der Studierenden, obwohl die Notwendigkeit einer rechtlichen Befugnis zur Datenerhebung in diesem Umfang nicht gegeben war. Die Befreiungsverordnung definiert abschließend, welche Rundfunkteilnehmer unter welchen Voraussetzungen von der Rundfunkgebührenpflicht befreit werden können. Sie fordert von den Antragstellern grundsätzlich lediglich den Nachweis der Unterkunftskosten (ohne Strom- und Heizkosten). Eine Sonderbehandlung für Studierende ist nicht vorgesehen.

In zahlreichen Gesprächsrunden mit Vertretern des NDR konnten wir erreichen, dass der Umfang reduziert und der Datenverarbeitungsprozess datenschutzfreundlicher gestaltet wird. So ist jetzt vorgesehen, dass vom Sozialamt nur dann auf bereits vorliegende Angaben zum Bezug von Sozialhilfe und Wohngeld zurück gegriffen werden darf, soweit dies für die Prüfung des Antrages auf Rundfunkgebührenbefreiung erforderlich ist und der Antragsteller eine entsprechende Einwilligungserklärung auf dem Antragsformular unterzeichnet hat. Daneben wurde vereinbart, dass die Speicherung der einmal erhobenen Plausibilitätsdaten zukünftig nur dann erfolgen wird, wenn eine weitere Prüfung des Antrages durch den NDR erforderlich ist. Falls eine Befreiung von der Rundfunkgebührenpflicht aus finanziellen Gründen ohne weitere Beteiligung des NDR bereits vom Sozialamt ausgesprochen werden kann, werden diese Daten nicht an den NDR oder die Gebühreneinzugszentrale (GEZ) weiter geleitet.

Neben dieser inhaltlichen Veränderung sollen in Kürze auch Änderungen im Verfahrensablauf eintreten. Hierzu hat der NDR ein automatisiertes Verfahren entwickelt, das zur Online-Bearbeitung von Anträgen auf Befreiung von der Rundfunkgebührenpflicht in Sozialbehörden dienen soll. Das Datenschutz- und Datensicherheitskonzept wurde mit uns abgestimmt, so dass aus unserer Sicht keine Bedenken gegen erste Pilotanwendungen bestehen. Nach Ablauf eines Jahres will der NDR einen Erfahrungsbericht über den Einsatz des neuen Systems anfertigen. Andere Landesrundfunkanstalten beobachten diese Entwicklung mit großem Interesse und wollen bei einem positiven Pilotierungsergebnis das Verfahren ebenfalls einsetzen.

In den Gesprächsrunden zwischen den Datenschutzbeauftragten der Länder und den Vertretern des NDR bestand im übrigen Einvernehmen darüber, dass für die datenschutzrechtliche Kontrolle des Verfahrens der Rundfunkgebührenbefreiung in den Sozialdienststellen allein die Landesbeauftragten für den Datenschutz zuständig sind. Die Einhaltung der Datenschutzbestimmungen bei der Rundfunkanstalt wird vom Datenschutzbeauftragten des NDR überwacht.

10.5 Projekt PILOT

Neue Formen der Unterstützung hilfebedürftiger Kinder und deren Eltern dürfen nicht dazu führen, dass dauerhaft ohne eine rechtlich einwandfreie Grundlage Daten übermittelt werden.

Mit dem Projekt PILOT sollen verbesserte Handlungsmöglichkeiten der Jugendhilfe im Hinblick auf das Phänomen der Delinquenz strafunmündiger Kinder erprobt werden. PILOT fungiert als regionaler Ansprechpartner für Eltern, Kinder, Opfer, Beratungsdienste, Polizei und die Vormundschaftsgerichte. Es gibt vornehmlich den Eltern im Zusammenhang mit Normenverletzungen ihrer Kinder Rat und Unterstützung, vermittelt im Bedarfsfall weitere Hilfen und ermutigt und unterstützt gegebenenfalls eine Konfliktschlichtung analog dem Täter-Opfer-Ausgleich. PILOT nimmt auch Meldungen der Polizei über Normenverletzungen von Kindern entgegen und schaltet wenn nötig das Familiengericht ein.

PILOT hat seine Arbeit im Januar 2000 aufgenommen und sollte zunächst für zwei Jahre in einer ausgewählten Region unter der Regie der Behörde für Schule, Jugend und Berufsbildung durchgeführt werden. Seine Laufzeit wurde inzwischen um ein Jahr verlängert und endet am 31. Dezember 2002. Wir hatten Gelegenheit, von Beginn an das Projekt zu begleiten. Im Mittelpunkt unserer Diskussion stand dabei die Datenübermittlung von der Polizei an PILOT, weil es hierfür keine einwandfreie rechtliche Grundlage gibt.

Nach eingehenden Erörterungen hat die Polizei eine Verfahrensweise für die Datenübermittlung entwickelt, die dem besonderen Modellcharakter des Projektes Rechnung tragen soll. Wir haben allerdings Zweifel, ob die vorgesehene Datenübermittlung von der Polizei an das Projekt PILOT grundsätzlich von § 20 des Gesetzes über die Datenverarbeitung bei der Polizei (PolDVG) getragen wird. Die allenfalls in Betracht kommenden Bestimmungen des § 20 Abs. 1 Nr. 5 PolDVG und des § 20 Abs. 2 PolDVG rechtfertigen ebenfalls keine generelle Weitergabe der Daten.

Auch wenn im Einzelfall das Kindeswohl nachhaltig gefährdet sein kann, muss dies nicht in jedem Fall gleichbedeutend sein mit den in § 20 Abs. 1 Nr. 5 PolDVG genannten schwerwiegenden Beeinträchtigungen von gewichtigen Rechtspositionen einzelner. Daraus folgt, dass lediglich im begründeten Einzelfall die Polizei die ihr bekannt gewordenen Erkenntnisse an PILOT weitergeben darf, nicht jedoch generell. Im Ergebnis kommt es also darauf an, wie die Einzelfallabwägung auf Seiten der Polizei ausgefallen ist.

§ 20 Abs. 2 PolDVG lässt eine Datenübermittlung durch die Polizei nur an eine andere für die Gefahrenabwehr zuständige öffentliche Stelle zu. Außerdem muss die Kenntnis der Daten zur Aufgabenerfüllung der empfangenen Stelle erforderlich erscheinen. Aus den uns vorliegenden Unterlagen zur Aufgabenbeschreibung von PILOT, insbesondere dem vom Senat gestellten Auftrag zur

Projekteinrichtung, ergibt sich nicht explizit, dass PILOT auch Aufgaben der Gefahrenabwehr wahrzunehmen hat. Schon deshalb scheidet § 20 Abs. 2 PolDVG als Befugnisnorm aus.

Dennoch haben wir es letztendlich datenschutzrechtlich für hinnehmbar gehalten, angesichts des Modellcharakters von PILOT, seiner zeitlichen und örtlichen Begrenzung sowie seiner Zielsetzung die Datenübermittlung in der von der Polizei vorgeschlagenen Weise vorzunehmen. Bei dieser Entscheidung haben wir uns ganz wesentlich davon leiten lassen, dass PILOT zugesichert hat, die nach § 8 Hamburgisches Datenschutzgesetz erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherung einzuhalten und die Daten zum frühestmöglichen Zeitpunkt, spätestens jedoch nach drei Jahren von Beginn des Projektes an zu löschen. Über die Einhaltung dieser Zusicherung werden wir uns bei Gelegenheit im Verlauf des Projektes überzeugen.

Nach Ablauf der Pilotphase sollen die im Rahmen des Projektes gewonnenen Erfahrungen ausgewertet und über die Fortführung bzw. Ausweitung der Konzeption entschieden werden. Zu diesem Zeitpunkt muss unter den dann geltenden Rahmenbedingungen erneut beurteilt werden, ob das Verfahren den datenschutzrechtlichen Anforderungen genügt. Eine Fortführung ohne eine entsprechende gesetzliche Klarstellung der Übermittlungsbefugnisse ist allerdings bereits jetzt datenschutzrechtlich nicht tragbar.

10.6 Projekt Kindertagesbetreuung (KITA-Card)

Die dezentralen Bescheide für die Kindertagesbetreuung werden bisher ohne KITA-Card weitgehend datenschutzkonform bearbeitet.

Im Berichtszeitraum hat die Behörde für Schule, Jugend und Berufsbildung (BSJB) das Projekt Kindertagesbetreuung mit dem Ziel eingerichtet, ein integriertes Verfahren zur Bewilligung, Abrechnung und zum Controlling der Kindertagesbetreuung in Hamburg einzuführen. Das Projekt ist in zwei Phasen gegliedert. Mit der Realisierung der ersten Phase wird die Sachbearbeitung auf der Grundlage des bisherigen Bewilligungsverfahrens unterstützt und eine Vernetzung mit der zentralen Abrechnungsstelle vorgenommen. Dieser Projektteil ist seit Mai 2001 in Betrieb genommen worden.

Für die dezentrale Nutzung wurde das bisher zentral genutzte Verfahren, das auf SAP R/3 basiert, ergänzt. Die Dateneingabe erfolgt jetzt direkt in den sieben Bezirken. Dafür wurden die erforderlichen Module überwiegend in Eigenentwicklung programmiert und bedienen die im Hintergrund laufenden SAP-Standard-Programme. Die Datenhaltung erfolgt nach wie vor in einer zentralen Datenbank.

Es wurde ein rollenbasiertes Berechtigungskonzept aufgebaut, mit dem die datenschutzrechtlichen Anforderungen umgesetzt werden. Die Profile und Rechte orientieren sich dabei an den fachlichen Vorgaben, wobei eine Flexibilität hinsichtlich unterschiedlicher Aufgabenwahrnehmungen möglich ist, etwa durch die Kombination von Profilen in den Bezirken. Nur die Sachbearbeitung des zuständigen Bezirks hat Vollzugriff auf die Daten. Um eine Doppelfallprüfung zu ermöglichen, haben jedoch Sachbearbeiter anderer Bezirke den Zugriff auf die Anschrift und das Geburtsdatum des Kindes. Der Berechtigungsumfang der zentralen Stelle im Amt für Jugend wurde nicht ausgeweitet.

Mit der erfolgten Vergrößerung des Funktionsumfangs des Verfahrens ist auch das Löschungs- und Archivierungskonzept fortzuschreiben, um sicherzustellen, dass nicht mehr erforderliche Daten so früh wie möglich gelöscht werden. Die Löschungsfristen für einzelne Daten können sich entsprechend den fachlichen Anforderungen unterscheiden. Auf die noch ausstehende Umsetzung haben wir hingewiesen.

An einzelnen Arbeitsplätzen, an denen die Kindertagesbetreuung bearbeitet wird, ist auch ein Internetzugang eingerichtet. Aufgrund der Sensibilität der verarbeiteten Daten wurden zusätzliche Sicherungsmaßnahmen umgesetzt, um die Gefahr durch unwissentlich installierte Schadenssoftware zu reduzieren. Entweder ist der Internetzugang nur über separate Benutzerkennungen am Arbeitsplatz verfügbar oder es sind nur vorab freigegebene Internetadressen aufrufbar.

In einer zweiten Phase des Projekts soll nach der Umstellung auf den Euro bis 2003 der heutige Bescheid durch die sogenannte KITA-Card ersetzt und ein Controllingsystem implementiert werden. Gegenstand der zweiten Phase soll auch die Unterstützung der Budgetaufstellung, die Vermittlung von Tagespflegepersonen sowie ggf. die Nutzung eines Data-Warehouses sein. Dabei ist nicht geplant, Daten auf einer Chipkarte zu speichern, sondern Papierausdrucke für die Gutscheine zu verwenden.

In dieser Projektphase soll der Datenumfang der gespeicherten Daten über das bisherige Maß ausgeweitet werden. Hierzu haben wir bereits in der Planungsphase an den datenschutzrechtlichen Grundsatz erinnert, dass sich der Datenumfang streng nach der Maßgabe der Erforderlichkeit richten muss.

Für die Unterstützung der Controllingaufgaben, die mit der KITA-Card und der Budget-Aufstellung verbunden sind, werden die fachlichen Abforderungen noch spezifiziert. Die Aufbereitung der Daten soll in aggregierter Form erfolgen. Wir haben darauf hingewiesen, dass beim Aufbau eines Data-Warehouses die einzelnen Datensätze in anonymisierter Form gespeichert werden sollten, um dem gesetzlich vorgegebenen Ziel der Datensparsamkeit Rechnung zu tragen. Dies soll im weiteren Projektverlauf realisiert werden.

10.7 Videoüberwachung in Heimen

Da die Bewohnerinnen und Bewohner von Heimen ein Anrecht darauf haben, sich grundsätzlich unbeobachtet in den Räumen bewegen zu können, ist vor dem Einsatz einer Videoüberwachungsanlage eine sorgfältige Güterabwägung vorzunehmen.

Wie in vielen Lebensbereichen, werden zunehmend auch in Heimen Videokameras eingesetzt (vgl. 1.2.1). Hierfür gibt es die unterschiedlichsten Gründe. Beispielsweise steht nicht ständig für die Eingangskontrolle ein Pförtner zur Verfügung, die Wahrnehmung des Hausrechts soll unterstützt werden oder es liegen sogar tatsächliche Anhaltspunkte dafür vor, dass eine konkrete Gefahr abgewehrt werden muss. Um sicher zu gehen, dass die Videoüberwachungsanlagen den datenschutzrechtlichen Erfordernissen entsprechen, machen die Heimaufsichtsbehörden den Heimen seit geraumer Zeit zur Auflage, von uns eine gutachtliche Stellungnahme einzuholen. Dies begrüßen wir ausdrücklich, weil wir dadurch die Möglichkeit haben, die Heimleitungen auf die mit einer Videoüberwachung verbundenen Risiken für das Recht auf informationelle Selbstbestimmung hinzuweisen und für einen datenschutzgerechten Einsatz der Überwachungseinrichtungen zu sorgen. Im einzelnen geht es dabei um folgende Punkte:

– Unterstützung bzw. Ersatz der Pförtnertätigkeit

Häufig wird der Eingangsbereich innerhalb des Gebäudes von einer deutlich sichtbaren Videokamera überwacht, die weder ferngesteuert werden kann noch über eine Zoomeinrichtung verfügt. Weitere Kameras sind nicht installiert. Außen an der Eingangstür ist ein deutlicher Hinweis auf die Videoüberwachung angebracht. Ein zweiter Hinweis befindet sich im Flur. Die Bilder werden ständig auf einen Monitor übertragen, der im Dienstzimmer des Pförtners oder des Pflegepersonals aufgestellt ist. Zugang zu dem jeweiligen Raum hat nur autorisiertes Personal. Eine Möglichkeit zur Bildaufzeichnung besteht nicht.

Nach einer Güter- und Interessenabwägung sind wir in solchen Fällen regelmäßig zu dem Ergebnis gekommen, dass der Grund für die Installation der Videoüberwachungsanlage nachvollziehbar ist und die gesetzlichen Zulässigkeitsvoraussetzungen des § 6b BDSG vorliegen.

– Wahrnehmung des Hausrechts

Oft waren die Gründe für die Installation von Kameras vor allen Dingen Sicherheitsaspekte. So hatte es in einigen Fällen bereits Einbrüche in Geschäftsräume des Heimes gegeben, die vom Personal nicht rechtzeitig bemerkt werden konnten. Aber auch Straftaten gegenüber Bewohnerinnen und Bewohnern und Sachbeschädigungen durch externe Personen waren der Anlass, zur verbesserten Wahrnehmung des Hausrechts und für Beweissicherungs-

zwecke eine Videoanlage zu installieren. Gleichzeitig versprach man sich davon eine abschreckende Wirkung für die Zukunft.

Soweit solche tatsächlichen Anhaltspunkte dafür vorlagen, dass eine konkrete Gefahr abgewehrt werden musste, haben wir gegen die Videoüberwachung keine Einwände erhoben. Allerdings haben wir in einigen Fällen angeregt, die Entwicklung der Straftaten zu beobachten. Bei einer zurückgehenden Zahl könnte die Präventionswirkung der Videoanlage auch aufrecht erhalten werden, indem zwar die Kameras an ihren Standorten belassen und die Hinweise auf die Videoüberwachung nicht entfernt werden, aber die Übertragung auf die Bildschirme sowie die Bildaufzeichnung für eine befristete Zeit ausgesetzt wird. Im Ergebnis würde es sich bei den Kameras also um Attrappen handeln. Nach Ablauf der Frist könnte geprüft werden, wie sich diese Maßnahme bewährt hat.

– Bildaufzeichnungen

Die auflaufenden Bilder werden vielfach ständig analog oder digital aufgezeichnet. Nach jeweils festgelegten Zeiträumen werden die Bilder durch das Überschreiben mit neuen Bildern gelöscht, sofern keine besonderen Vorkommnisse während der Speicherdauer eingetreten sind. Falls Bilder für Zwecke der Beweissicherung benötigt werden, erfolgt eine Übernahme der Bildinformationen auf ein gesondertes Speichermedium.

Im Falle von Bildaufzeichnungen verlangen wir regelmäßig, dass die Heimleitung in einer Dienstanweisung o.ä. schriftlich den Umgang mit der Videoüberwachungsanlage regelt. Wesentliche Regelungsinhalte sollten sein:

– Beschreibung von Umfang und Zweck der Anlage,

– Festlegung des zulässigen Gebrauchs,

– Festlegung einer kurzen Aufbewahrungszeit von Aufnahmen, soweit sie nicht für ein strafrechtliches Ermittlungsverfahren benötigt werden,

– Zulässigkeit und Verfahren der Anfertigung und Auswertung von Videoaufnahmen,

– Bestimmung des Mitarbeiterkreises, der zur Kontrolle des Videosystems zugelassen ist,

– Vernichtung von Datenträgern, auf denen noch Bildmaterial gespeichert ist.

In jedem Fall empfehlen wir, die Bewohnerinnen und Bewohner vor der Installation der Videoanlage schriftlich über Art und Umfang der Überwachungstechnik zumindest zu unterrichten, damit die Betroffenen auf eigene schutzwürdige Interessen hinweisen können. Beim Einzug neuer Bewohnerinnen und Bewohner bietet es sich an, bei der Unterzeichung des Heimvertrages entsprechend über die Videoüberwachung aufzuklären.

10.8 Bekanntgabe von Aktenverlusten

Es ist für das Auffinden verloren gegangener Jugendamts- und Sozialamtsakten nicht erforderlich, in die Verlustanzeige personenbezogene Sozialdaten aufzunehmen.

Mehrfach haben wir festgestellt, dass in den Mitteilungen für die hamburgische Verwaltung der Verlust von Jugendamts- und Sozialamtsakten von den Bezirksämtern unter Angabe personenbezogener Daten des Betroffenen angezeigt wird. Dabei handelt es sich um den Vor- und Familiennamen und das Geburtsdatum als Teil des Aktenzeichens.

Nach § 35 Abs. 1 SGB I hat jeder Hilfeempfänger Anspruch darauf, dass die ihn betreffenden Sozialdaten nicht unbefugt weitergegeben werden. Eine Durchbrechung dieses Sozialgeheimnisses ist nur unter den Voraussetzungen der §§ 67 ff SGB X zulässig. Da für die Offenbarung personenbezogener Sozialdaten im Zusammenhang mit der Anzeige einer verloren gegangenen Akte nicht auf eine gesetzliche Erlaubnis zurück gegriffen werden kann, kommt allenfalls das Vorliegen einer Einwilligung des Betroffenen in Betracht. Wie wir von den Jugend- und Sozialämtern erfahren haben, wird regelmäßig eine solche Einwilligung nicht eingeholt.

Aus welchen Gründen überhaupt eine Veröffentlichung des Aktenverlustes erforderlich ist, konnte uns bislang nicht schlüssig erläutert werden. Auch ist uns noch nicht beantwortet worden, welche zusätzlichen Erfolgsaussichten für das Auffinden der Akte mit einer solchen Veröffentlichung verbunden sind und ob es Erkenntnisse gibt, in wie vielen Fällen die Veröffentlichung zu einem Erfolg geführt hat. Wir meinen, ein Finder würde sich wohl auch ohne einen Hinweis in den Mitteilungen für die hamburgische Verwaltung mit der aktenführenden Dienststelle in Verbindung setzen und das Auftauchen der Akte melden, sofern die Akte als Irrläufer bei einer nicht zuständigen Dienststelle eingehen sollte.

Falls aus zwingenden Gründen jedoch die Verlustanzeige unverzichtbar sein sollte, wäre es aus unserer Sicht zunächst ausreichend, lediglich das Aktenzeichen ohne den Namen des Betroffenen anzugeben. Im Zusammenhang mit der Tatsache, dass es sich um eine Akte des jeweiligen Jugend- oder Sozialamtes handelt, wäre die Akte hinreichend deutlich benannt. Ein Finder könnte dann mit der Dienststelle Kontakt aufnehmen, um die Aktenidentität zu prüfen. Dadurch würde vermieden, dass sonstigen Personen die Identität der Hilfeempfängerin oder des Hilfeempfängers offenbart wird.

Einige Dienststellen haben uns bereits zugesichert, künftig entsprechend zu verfahren. Um hierfür eine einheitliche Regelung zu erreichen, haben wir vorsorglich das Senatsamt für Bezirksangelegenheiten auf die Problematik aufmerksam gemacht. Dort ist eine Überprüfung mit dem Ziel veranlasst worden, in Abstimmung mit den Bezirksämtern und den beteiligten Fachbehörden eine Neuregelung der Verfahrens herbeizuführen.

Die Überprüfung hat dazu geführt, dass in die „Dienstvorschrift über die Aktenführung, Ablieferung, Vernichtung und Fristen für die Aufbewahrung des Schriftgutes im Jugendamt der Bezirksämter“ eine ausdrückliche Regelung aufgenommen wurde, wonach bei einer Anzeige des Verlustes von Jugendamtsakten nur noch das Aktenzeichen anzugeben ist. Die Bekanntgabe des Namens der oder des Betroffenen ist nicht mehr statthaft. Ein entsprechendes Ergebnis lag bis zum Redaktionsschluss für den Sozialamtsbereich noch nicht vor.

11. Personaldaten

11.1 Bürokommunikation mit Internet und E-Mail

Die Anlage zur Rahmenvereinbarung über die Bürokommunikation soll eine erste Grundorientierung für alle mit Werkzeugen der Bürokommunikation arbeitenden Beschäftigten der Verwaltung schaffen.

Für die E-Mail-Nutzung sind aus datenschutzrechtlicher Sicht (siehe 27.1) folgende in der Rahmendienstvereinbarung (siehe 3.3.2) getroffene allgemeine Regeln von Bedeutung. Sie sind für alle Beschäftigten in der hamburgischen Verwaltung verbindlich:

1. Bei einer absehbaren Abwesenheit vom Arbeitsplatz, die länger als einen Arbeitstag (z.B. Urlaub, Dienstreise oder Dienstgang, Fortbildung, Abwesenheit auf Grund entsprechender Arbeitszeitverteilung) dauert, ist der elektronisch verfügbare Abwesenheits- und Vertretungsassistent zu nutzen und in geeigneter Weise einzustellen. Mit seiner Hilfe soll die Absenderin bzw. der Absender einer E-Mail über die zu erwartende Dauer der Abwesenheit und die getroffene Vertretungsregelung unterrichtet werden oder darüber, an wen die E-Mail weitergeleitet wurde.
2. Bei unvorhersehbarer Abwesenheit vom Arbeitsplatz, die länger als drei Tage dauert (z.B. bei Erkrankung), kann der zuständige Amtsleiter oder eine von ihm beauftragte Person die Einschaltung des Abwesenheits- und Vertretungsassistenten veranlassen oder, falls dies im Einzelfall nicht ausreicht, um die Bearbeitung elektronischer Posteingänge sicherzustellen, weitere Maßnahmen treffen (insbesondere Öffnung des Postfaches). Als „privat“ gekennzeichnete oder als solche erkennbare Nachrichten dürfen von der Vertretung nicht geöffnet werden. Wird ein solcher Eingang versehentlich geöffnet oder ergibt sich erst bei versehentlicher Lektüre, dass die Nachricht privater Natur ist, ist die Nachricht unverzüglich zu schließen und der Inhalt vertraulich zu behandeln.

   Dies gilt auch, falls es vergessen wurde, die notwendigen Vorkehrungen bei einer länger als drei Tage andauernden Abwesenheit zu treffen.

   Über die getroffenen Maßnahmen wird der Besitzer bzw. die Besitzerin des Postfachs unverzüglich nach Rückkehr informiert.

3. Sensible personenbezogene Daten dürfen elektronisch nur verschlüsselt übermittelt werden. Innerhalb des FHHinfoNET ist dies durch die Nutzung der Funktion „erweiterte Sicherheit“ grundsätzlich möglich.

4. Die Arbeitsplatzausstattung ist grundsätzlich für dienstliche Zwecke bestimmt. Gelegentliche Nutzungen, auch des Internetzugangs, für private Zwecke sind zulässig, wenn hierdurch dienstliche Belange nicht beeinträchtigt werden. Insbesondere im Fall ungeplanter Abwesenheit kann nicht mit Sicherheit verhindert werden, dass der Inhalt privater Nutzung Dritten bekannt wird. Dieses kann vermieden werden, wenn für die private Kommunikation ein Postfach bei einem externen Provider genutzt wird („Webmail“).

5. Generelle Regelungen zum Datenschutz und zur Datensicherheit (insbesondere Verwendung sicherer Passworte, Schutz des PC vor der Benutzung durch Unbefugte) und zum Virenschutz sind strikt zu beachten.

11.2 Projekt Personalwesen (PROPERS)

Im Projekt Personalwesen hat es im Jahr 2001 zwei wesentliche technische Veränderungen gegeben.

Seit Ende Mai 2001 können alle Behörden und Ämter die neue vom Personalamt freigegebene Version der Emulationssoftware für den Zugriff auf PAISY einsetzen. Hiermit werden alle Anwendungsdaten, Benutzerkennungen und Passworte, die zwischen dem Rechenzentrum im Landesamt für Informationstechnik (LIT) und den PAISY-Arbeitsplätzen in den Personalabteilungen und lohnanschreibenden Stellen ausgetauscht werden, verschlüsselt übertragen. Ohne diese Verschlüsselungsmöglichkeit war bis dahin gemäß dem Datenschutzkonzept für PAISY eine physikalische Trennung der PC der Personalabteilungen von denen der übrigen Arbeitsplätze im Netz der jeweiligen Behörde erforderlich. Diese Teilnetzbildung kann bei Umstellung auf die neue Version der Emulationssoftware aufgehoben werden.

Im 17. TB, 7.4 hatten wir die technische Konfiguration für den Abruf personenbezogener Budgetdaten (Personalcontrolling) beschrieben. Der ursprünglich unter UNIX betriebene HTTP-Server, auf dem das Personalamt für den Abruf durch die Behörden und Ämter Daten aus PAISY für dezentrale Auswertungen und Personalberichte bereitstellt, ist durch einen HTTP-Server unter Windows 2000 ersetzt worden. Dies führt zu datenschutztechnischen Verbesserungen und erleichtert die Administration der Zugriffsberechtigungen. Darüber hinaus wird es durch den Wechsel des Betriebssystems auch möglich, den Behörden und Ämtern die Ergebnisse programmierter Auswertungen (INFO), die bisher nur zentral über das LIT ausgedruckt und verteilt werden konnten, als Textdatei zur weiteren Verarbeitung anzubieten. Das Umstellungskonzept ist vom Personalamt mit uns abgestimmt worden.

11.3 Einsicht in Personalakten

Im Rahmen eines Bewerbungsverfahrens dürfen der Personalrat, die Frauenbeauftragte und die Schwerbehindertenvertretung auch bei Vorliegen einer Einwilligung der Bewerber nicht in die Personalakte einsehen.

Stellenausschreibungen werden üblicherweise mit dem Hinweis versehen, in die Weitergabe und Einsicht der Personalakte einzuwilligen. Dies führte in einzelnen Fällen dazu, dass auch der Personalrat, die Frauenbeauftragte oder die Schwerbehindertenvertretung die Personalakten vorgelegt bekamen. Eine pauschalierte Einwilligung der Bewerber zur Einsicht in ihre Personalakte verstößt jedoch gegen den Erforderlichkeitsgrundsatz.

Möglicherweise liegt der Grund für die pauschalierte Formulierung im Leitfaden zur Gestaltung von Auswahlverfahren (2. Auflage 1997). Ziffer 6 weist darauf hin, dass bei internen Bewerbern nur mit deren Einverständnis die Personalakte beizuziehen sei. Eine Differenzierung nach der Erforderlichkeit und dem einsichtnehmenden Personenkreis wird dabei nicht vorgenommen.

Die absendende und anfordernde Dienststelle haben sich jedoch an dem Erforderlichkeitsgrundsatz zu orientieren (§ 96 e Abs. 3 Hamburgisches Beamtengesetz – HmbBG). Die in § 96 e Abs. 1 HmbBG i.V.m. § 28 Abs. 3 HmbDSG vorgesehene gesetzliche Erlaubnis zur Einsichtnahme in die Personalakte ohne Einwilligung der Betroffenen gilt nicht für den Personalrat, die Frauenbeauftragte oder die Schwerbehindertenvertretung, da dieser Personenkreis nicht zu den dort genannten Organisationseinheiten gehört.

Die gesetzliche Beschränkung auf den erforderlichen Umfang darf auch nicht durch eine pauschalierte Einwilligung unterlaufen werden. Dies widerspricht den vorrangigen Regelungen des § 78 Abs. 2 HmbPersVG und § 95 Abs. 2 Satz 3 SGB IX. Nach § 78 Abs. 2 Satz 3 HmbPersVG dürfen Personalakten nur mit Zustimmung des Angehörigen des öffentlichen Dienstes und nur durch ein von ihm bestimmtes Mitglied des Personalrats eingesehen werden. Die Kommentare zu vergleichbaren Regelungen (beispielsweise § 68 Abs. 2 BPersG, §§ 83 Abs. 1, 99 Abs. 1 BetrVG) gehen davon aus, dass die Erlaubnis zur Einsicht nur in dem dort genannten Rahmen möglich ist und nicht durch eine pauschalierte Einwilligung des Betroffenen umgangen werden kann.

Bewerbungsunterlagen sind nicht mit Personalakten gleichzusetzen. Die Dienststelle hat den Personalrat nach § 78 Abs. 2 HmbPersVG zu unterrichten (Satz 1) und ihm die erforderlichen Unterlagen vorzulegen (Satz 2). Zu diesem Zweck sind ein Auszug aus der Personalakte, soweit notwendig, sowie die für die Bewerbungsentscheidung erforderlichen Angaben zu erstellen. Die Schwerbehindertenvertretung hat nach § 95 Abs. 2 Satz 3 SGB IX bei Bewerbungen schwerbehinderter Menschen das Recht auf Einsicht in die entscheidungsrelevanten Teile der Bewerbungsunterlagen und auf Teilnahme an Vorstellungsgesprächen.

11.4 Sonstiges

Weitere Themen zum Personaldatenschutz waren:

- Automationsvorhaben Personalärztlicher Dienst,
- Dezentralisierung der Personalverwaltung der Justizbehörde,
- Hamburgische Disziplinarordnung,
- Umgang mit erkrankten Mitarbeitern (Rückkehrgespräche),
- Versand von Versorgungsmitteilungen,
- Assessmentcenter in der hamburgischen Verwaltung,
- Privatanschrift auf den Besoldungsmitteilungen.

12. Statistik

12.1 Zensus 2001

Bei der Durchführung der Testerhebungen nach dem Zensustestgesetz sind zur Wahrung des Rechts auf informationelle Selbstbestimmung besondere verfahrentechnische Maßnahmen zu treffen.

Im Jahr 2000 hatten wir uns mit der künftigen europaweiten Volkszählung, den dafür entwickelten Alternativmodellen und dem Entwurf eines Gesetzes zur Vorbereitung eines registergestützten Zensus (Zensusvorbereitungsgesetz) beschäftigt. Dieses Gesetz ist am 3. August 2001 in Kraft getreten. In diesem Gesetz ist bestimmt, dass die im Zusammenhang mit dem Zensustestgesetz (ZensTeG) erforderlichen Erhebungen, Untersuchungen von Registern und statistisch-methodischen Untersuchungen als Bundesstatistik durchgeführt werden.

Für Bundesstatistiken gilt insbesondere, dass die erforderlichen Hilfs- und Erhebungsmerkmale im einzelstatistischen Gesetz genannt sein müssen und dass sämtliche erhobene Daten ausschließlich in den Statistischen Ämtern des Bundes und der Länder verarbeitet werden (Abschottung). Die Daten unterliegen der strikten statistischen Geheimhaltung und dürfen in keiner Form in den Verwaltungsvollzug zurückfließen. Außerdem sind sie zum frühestmöglichen Zeitpunkt zu anonymisieren bzw. zu löschen. Mit der Anordnung als Bundesstatistik sind auch die vom Bundesverfassungsgericht im Volkszählungsurteil von 1983 zur Sicherung des Rechts auf informationelle Selbstbestimmung verlangten besonderen verfahrensrechtlichen Vorkehrungen für die Durchführung und Organisation der Datenerhebung und -verarbeitung bei einer Volkszählung erfüllt worden.

Für einen künftigen registergestützten Zensus ist insbesondere die Statistiktauglichkeit der betroffenen Register zu ermitteln. Hierzu sind umfangreiche Erhebungen und Verfahrenstests und -entwicklungen notwendig. Um

die Qualität und Validität der aus den Registern gewonnenen Daten überprüfen zu können, ist neben den Testerhebungen bei den Melderegistern und der Bundesanstalt für Arbeit auch eine Befragung von Personen in ausgewählten Gebäuden vorgesehen.

Da in Deutschland keine Register über kleinräumige Bestands- und Strukturdaten von Haushalten (z.B. Anzahl, Größe, Zahl der Personen) vorhanden sind, ordnet das ZensTeG auch eine Gebäude- und Wohnungsstichprobe in ausgewählten Gemeinden an.

Weiterhin ist die Zusammenführung von Register- und Wohnungsdaten festgelegt worden, so dass Anhand dieser Daten Zusammenhänge zwischen den unter gleicher Anschrift gemeldeten Personen festgestellt werden können. Sie dienen daher der statistischen Qualitätskontrolle der Melderegister.

Die Vorarbeiten für die zum Stichtag 5. Dezember 2001 vorgesehenen Testerhebungen, Stichproben und Befragungen sind vom Statistischen Landesamt eingeleitet worden und werden von uns begleitet. Aussagen über die Qualität der Register sind erst nach Abschluss sämtlicher Arbeiten – frühestens im 2. Halbjahr 2002 – möglich.

13. Finanzen und Steuern

13.1 Zentrales Kontenregister

Statt eines Zentralen Kontenregisters soll bei der Bundesanstalt für Finanzdienstleistungsaufsicht ein datenschutzrechtlich vertretbares Abrufverfahren eingerichtet werden.

Im ersten Gesetzentwurf für ein 4. Finanzmarktförderungsgesetz war in Art. 6 (Gesetz über das Kreditwesen) vorgesehen, alle in Deutschland geführten Bankkonten in einem Zentralen Kontenregister beim Bundesaufsichtsamt für das Kreditwesen (künftig: Bundesanstalt für Finanzdienstleistungsaufsicht) zu erfassen, um auf diese Weise die Voraussetzungen u.a. für eine wirksame Bekämpfung der Geldwäsche, von unerlaubten Bank- und Finanzdienstleistungsgeschäften und der Finanzierung des Terrorismus zu schaffen.

Die Einrichtung des Zentralen Kontenregisters wurde von den Datenschutzbeauftragten als ungeeignet und unverhältnismäßig angesehen. Daher bestand die Absicht, diese Konten-Evidenzzentrale im Rahmen einer gemeinsamen Entschließung der Datenschutzbeauftragten des Bundes und der Länder aus datenschutzrechtlichen Gründen abzulehnen.

Das Bundeskabinett hat aber die Planung eines Zentralen Kontenregisters nicht weiterverfolgt. Statt dessen wurde am 14. November 2001 ein neuer Gesetzentwurf zum 4. Finanzmarktförderungsgesetz beschlossen. Er sieht in Art. 6 vor, dass die Kreditinstitute verpflichtet werden, selbst eine Datei über alle bei ihnen geführten Bankkonten anzulegen.

Diese einzelnen Konteninformationen dürfen in einem automatisierten Verfahren durch die geplante Bundesanstalt abgerufen werden, soweit dies zur Erfüllung ihrer aufsichtlichen Aufgaben nach dem Gesetz über das Kreditwesen und nach dem Geldwäschegesetz – insbesondere im Hinblick auf unerlaubte Bankgeschäfte oder Finanzdienstleistungen oder den Missbrauch der Institute durch Geldwäsche oder betrügerische Handlungen zu Lasten der Institute – erforderlich ist und besondere Eilbedürftigkeit im Einzelfall vorliegt.

Durch den automatisierten Abruf von Konteninformationen besteht für die Bundesanstalt die Möglichkeit, einen aktuellen und zutreffenden Überblick über sämtliche Kontoverbindungen einer Person oder eines Unternehmens zu erhalten. Dies ist zwar bereits nach geltendem Recht möglich, setzt aber ein entsprechendes zeitraubendes Auskunftsersuchen der Bundesanstalt an alle Kreditinstitute in Deutschland voraus.

Über diese Daten erteilt die Bundesanstalt den für die Leistung der internationalen Rechtshilfe sowie im Übrigen den zur Verfolgung von Straftaten mit Ausnahme von Steuerstraftaten zuständigen Strafverfolgungsbehörden oder Gerichten auf Ersuchen Auskunft, soweit dies zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist. Zur Datenschutzkontrolle sollen diese Datenabrufe bei der Bundesanstalt protokolliert werden.

Soweit nicht im weiteren Gesetzgebungsverfahren neuer datenschutzrechtlicher Handlungsbedarf entsteht, sind die im vorliegenden Gesetzentwurf getroffenen Regelungen datenschutzrechtlich vertretbar.

13.2 Zugriff der Finanzverwaltung auf DV-gestützte Buchungssysteme

Die Finanzämter können – auch wegen datenschutzrechtlicher Bedenken – erst ab 2002 bei Außenprüfungen auf die in DV-Systemen gespeicherten Buchhaltungsunterlagen eines Steuerpflichtigen zugreifen.

Durch das Steuersenkungsgesetz (StSenkG) vom 23. Oktober 2001 ist u.a. § 147 Abgabenordnung (AO) um einen Absatz 6 ergänzt worden, der den Finanzämtern ab 1. Januar 2002 das Recht einräumt, bei Außenprüfungen die im DV-System eines Steuerpflichtigen gespeicherten Buchhaltungsunterlagen einzusehen und das DV-System für die Prüfung dieser Unterlagen zu nutzen.

Gemäß § 147 Abs. 6 AO kann die Finanzverwaltung im Rahmen einer Außenprüfung nach pflichtgemäßem Ermessen zwischen drei Zugriffsmöglichkeiten wählen:

- **Nur-Lese-Zugriff**

Sie hat das Recht, Einsicht in die gespeicherten Daten zu nehmen und das Datenverarbeitungssystem zur Prüfung der Unterlagen zu nutzen. Bei diesem nur lesenden Zugriff nutzt sie vor Ort beim Steuerpflichtigen dessen Hard- und Software, wobei der Datenbestand nicht verändert werden darf. Dieser Zugriff

umfasst das Lesen, Filtern und Sortieren der Daten ggf. unter Nutzung der im Datenverarbeitungssystem vorhandenen Auswertungsmöglichkeiten.

- **Mittelbarer Datenzugriff**

Sie kann vom Steuerpflichtigen verlangen, dass er die gespeicherten Daten nach ihren Vorgaben maschinell ausgewertet oder von einem beauftragten Dritten auswerten lässt. Dabei fordert sie den Steuerpflichtigen oder sein (sachkundiges) Personal vor Ort auf, gespeicherte Daten mit Hilfe seiner Hard- und Software nach konkreten Vorgaben zu verarbeiten.

- **Überlassung von Daten auf Datenträgern**

Sie kann außerdem verlangen, dass ihr die gespeicherten Daten auf einem maschinell verwertbaren Datenträger zur Auswertung überlassen werden. Dieser Datenträger ist spätestens nach Bestandskraft der aufgrund der Außenprüfung ergangenen Bescheide an den Steuerpflichtigen zurückzugeben oder zu löschen.

Die Einzelheiten sind in dem Schreiben des Bundesministeriums der Finanzen über die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) vom 16. Juli 2001 (BStBl. I S. 415) geregelt.

Diese Zugriffrechte sollten ursprünglich bereits ab 1. Januar 2001 zur Anwendung kommen und haben nachhaltige Kritik bei Wirtschaftsverbänden und den Datenschutzbeauftragten hervorgerufen. Grund war insbesondere, dass die in den DV-Systemen von Unternehmen gespeicherten und zu prüfenden steuerlich relevanten Daten (z.B. Finanzbuchhaltung, Lohnbuchhaltung) in vielen Fällen nicht von den ebenfalls dort gespeicherten Personaldaten abgeschottet sind.

Nach § 9 Bundesdatenschutzgesetz (BDSG) und den vom Bundesministerium der Finanzen erlassenen „Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme“ sind die Unternehmen zwar gehalten, ihre Daten gegen unberechtigte Kenntnisnahme und Zugriffe zu schützen (Speicher- und Zugriffskontrolle). Es hat sich aber herausgestellt, dass dies bei vielen Unternehmen nicht in ausreichendem Maße geschehen ist. Um den Unternehmen Gelegenheit zu geben, ihre Datenverarbeitungssysteme programmtechnisch so auszustatten, dass eine Beschränkung des Zugriffs auf die steuerlich relevanten Daten möglich ist, wurde im Einführungsgesetz zur Abgabenordnung geregelt, dass diese Vorschrift erst ab 1. Januar 2002 zur Anwendung kommt.

Bei einer Außenprüfung darf sich die Einsichtnahme nur auf die Daten erstrecken, soweit dies durch die Prüfungsanordnung gemäß § 196 AO hinreichend bestimmt ist. Aus diesem Grund wurde die Forderung erhoben, in die Abgabenordnung u.a. zur Datenschutzkontrolle eine Verpflichtung aufzunehmen, die Datenzugriffe zur protokollieren. Der Finanzausschuss des Deutschen Bundestages hat eine gesetzliche Regelung in der AO für nicht erforderlich gehalten, so dass diese Forderung nicht durchgesetzt werden konnte.

13.3 Auskunftspflicht von Firmen gegenüber dem Finanzamt

Firmen sind verpflichtet, den Finanzämtern Auskünfte über Konten und Bankverbindungen ihrer Kunden mitzuteilen, wenn diese mit ihrer Steuerschuld in Verzug sind.

In einem Rechtsstreit zwischen einem hamburgischen Finanzamt und einem Energieversorgungsunternehmen hat der Bundesfinanzhof (BFH) entschieden, dass Versorgungsunternehmen verpflichtet sind, den Finanzämtern Auskünfte über Konten und Bankverbindungen ihrer Kunden zu erteilen, um Steuerschulden eintreiben zu können.

Diese Auskunftspflicht beruht auf der Grundlage des § 93 Abs. 1 Abgabenordnung (AO) und dient dem Ziel, durch die Inpflichtnahme Privater die Ermittlung steuerlicher Tatbestände zu fördern und so für eine wirkungsvolle und gleichmäßige Erfüllung von Steuerschulden Sorge zu tragen.

Nach der Entscheidung des BFH reicht es bei Vorliegen der rechtlichen Voraussetzungen des § 93 Abs. 1 AO aus, wenn die Begründungserfordernisse des § 93 Abs. 1 und 2 AO beachtet werden. Danach soll das Finanzamt zunächst versuchen, die zur Aufklärung des Sachverhalts notwendigen Auskünfte von dem Steuerpflichtigen selbst zu erlangen. Ein Auskunftsersuchen an Dritte, d.h. an dem Besteuerungsverfahren nicht beteiligte Personen oder Stellen, soll erst dann gerichtet werden, wenn die Sachverhaltsaufklärung durch die Beteiligten nicht zum Ziel führt oder keinen Erfolg verspricht. Dies muss aus Auskunftsersuchen deutlich hervorgehen. Weiterhin ist in dem Auskunftsersuchen anzugeben, worüber Auskünfte erteilt werden sollen (z.B. ob und für welche Konten die Steuerpflichtigen ggf. Einzugsermächtigungen erteilt haben) und ob die Auskunft für die Besteuerung des Auskunftspflichtigen oder für die Besteuerung anderer Personen angefordert wird.

Diese Auskunftspflicht gilt sinngemäß für sämtliche Adressaten des § 93 Abs. 1 AO (z.B. rechtsfähige Vereinigungen, Behörden, Banken, Betriebe gewerblicher Art).

Gegen diese Entscheidung hat das Energieversorgungsunternehmen Verfassungsbeschwerde eingelegt. Das Bundesverfassungsgericht hat seinem Beschluss vom 15. November 2000 (1 BvR 1213/00) bestätigt, dass die Pflicht eines Energieversorgungsunternehmens, den Finanzämtern im Rahmen der Vollstreckung von Steuerforderungen nach § 93 Abgabenordnung (AO) Auskunft über Kontoverbindungen ihrer Kunden erteilen zu müssen, verfassungsrechtlich gerechtfertigt ist. Denn dieser Eingriff beruhe auf einer hinreichend bestimmten gesetzlichen Grundlage und verletzte den Grundsatz der Verhältnismäßigkeit nicht.

13.4 Projekt ELSTER (Elektronische Steuererklärung)

Das amtliche Programm für die elektronische Steuererklärung (Elsterformular 2000) konnte aufgrund von Sicherheitsproblemen vorübergehend nicht aus dem Internet heruntergeladen oder aktualisiert werden.

Im 17. TB, 8.2 hatten wir die Funktionsweise des Verfahrens zur elektronischen Steuererklärung (ELSTER) beschrieben und festgestellt, dass die getroffenen Sicherheitsmaßnahmen dem Stand der Technik entsprechen. Dabei sind wir noch davon ausgegangen, dass die Nutzung nur möglich ist über im Handel erhältliche Steuerberatungs- und -berechnungsprogramme, die eine Schnittstelle für ELSTER beinhalten. Die Steuerverwaltungen des Bundes und der Länder bieten ihr gemeinsames amtliches Programm zur elektronischen Steuererklärung „Elsterformular 2000“ aber auch kostenlos im Internet unter www.elsterformular.de an. Nach einem von der Stiftung Warentest Ende März 2001 veröffentlichten Bericht über erhebliche Sicherheitsmängel wurde dieses Angebot zum Download bzw. automatischen Update jedoch vorübergehend eingestellt.

Hintergrund dafür war der gegen mögliche missbräuchliche Angriffe aus dem Netz nicht ausreichend geschützte Server. Zu diesem Zeitpunkt wäre es durchaus möglich gewesen, auf dem betreffenden Rechner der Finanzverwaltung – für den betroffenen Steuerzahler nicht erkennbar – die amtliche ELSTER-Software gegen eine modifizierte Version auszutauschen. Durch eine Veränderung der im Programm enthaltenen IP-Adressen hätten die Steuererklärungen nicht an die zuständigen Finanzämter, sondern einen beliebigen anderen Server gesandt werden können. Die persönlichen Daten der betroffenen Steuerzahler wären damit ohne deren Wissen an unbefugte Dritte gelangt. In die „ausgetauschte“ Version hätten aber auch Viren und trojanische Pferde eingebaut werden können. Auf diese Weise wären auch alle anderen auf den PC der Betroffenen gespeicherten Daten einem missbräuchlichen Zugriff ausgesetzt gewesen.

Seit dem 18. Mai 2001 ist die amtliche Steuererklärungssoftware wieder unter www.elsterformular.de abrufbar. Das Sicherheitskonzept wurde erheblich überarbeitet und verbessert. Das Herunterladen und Aktualisieren des jetzt mit einem X.509-Zertikat signierten Programms ist nur noch verschlüsselt über https (SSL, 128 Bit) möglich. Der Benutzer kann also inzwischen die Identität des Anbieters der Software und die Integrität der Anwendung jederzeit überprüfen. Darüber hinaus erfolgt eine permanente Softwareüberwachung durch einen Bytecode Check, der bei einem unberechtigten Änderungsversuch das Programm automatisch deaktiviert.

13.5 Online-Zugriff des Rechnungshofs auf PROSA, PROJUGA und PROPERS

Für die Realisierung eines Online-Zugriffs auf PROPERS ist eine gesetzliche Grundlage erforderlich.

Im 17. TB (6.4) hatten wir über die Online-Zugriffe des Rechnungshofs auf Daten des Projekts Sozialhilfe-Automation (PROSA) und Projekt Jugendamts-Automation (PROJUGA) zur Überwachung der Haushalts- und Wirtschaftsprüfung berichtet. Die hierfür zu treffenden technisch-organisatorischen Sicherheitsmaßnahmen sind zwischenzeitlich mit dem Rechnungshof, dem Senatsamt für Bezirksangelegenheiten und uns einvernehmlich abgestimmt und in einer Anlage zur Vereinbarung über die automatisierten Abrufverfahren zur Übermittlung von Daten aus PROSA und PROJUGA schriftlich festgelegt worden, so dass gegen eine Realisierung dieser Online-Zugriffe keine datenschutzrechtlichen Bedenken mehr bestehen.

Auf der Grundlage des § 95 Abs. 3 Landeshaushaltsordnung (LHO) möchte der Rechnungshof in gleicher Weise auch die Daten des Dialogverfahrens PROPERS (Projekt Personalwesen) prüfen können. Hiergegen bestehen aus unserer Sicht erhebliche datenschutzrechtliche Bedenken.

Der Online-Zugriff des Rechnungshofs auf PROPERS ist rechtlich anders zu bewerten als der auf PROSA oder PROJUGA. Der Zugriff auf Sozialdaten richtet sich nach den bereichsspezifischen Datenschutzvorschriften des SGB (§§ 79, 78a SGB-X). Danach ist die Einrichtung eines automatisierten Abrufverfahrens grundsätzlich zulässig. Eine gesonderte Rechtsverordnung ist nicht erforderlich, es bedarf allein einer Vereinbarung über den Inhalt der Abrufe und der zu treffenden technisch-organisatorischen Sicherheitsmaßnahmen zwischen den beteiligten Stellen. Weder § 95 Abs. 3 LHO (Beteiligung des Rechnungshofs an automatisierten Abrufverfahren) noch § 11 Abs. 2 HmbDSG (Rechtsverordnung des Senats) kommen hier zur Anwendung.

Da das Dialogverfahren PROPERS kein automatisiertes Abrufverfahren ist, würde mit dem vom Rechnungshof gewünschten Online-Zugriff erstmals ein automatisiertes Abrufverfahren entstehen. Dafür gilt aber § 95 Abs. 3 LHO nicht, wonach sich der Rechnungshof an bestehenden automatisierten Abrufverfahren beteiligen kann, ohne dass der Senat nach § 11 Abs. 2 HmbDSG eine entsprechende Rechtsverordnung erlassen bzw. eine bereits vorhandene entsprechend erweitern müsste. Infolgedessen ist der Online-Zugriff für ein neues, erst entstehendes Abrufverfahren nur mit besonderer Rechtsverordnung des Senats zulässig.

Dies wird bei Betrachtung des Wortlauts vergleichbarer Regelungen in anderen Landeshaushaltsordnungen deutlich. Im Saarland wurde die LHO nur dahingehend ergänzt, dass die Auskunftspflicht „auch elektronisch gespeicherte Daten sowie deren automatisierten Abruf“ umfasst. Dies hat man in Hamburg möglicherweise so beabsichtigt, aber nicht so allgemein umgesetzt.

Da sich diese Situation auch bei anderen IuK-Verfahren ähnlich darstellt (z.B. beim Mittelbewirtschaftungsverfahren – DHB-X – oder künftig bei SAP), haben wir dem Rechnungshof zur Vermeidung von ständig neuen Rechtsverordnungen nach § 11 Abs. 2 HmbDSG eine Änderung des § 95 Abs. 3 LHO – analog der Regelung im Saarland – vorgeschlagen. Hierfür haben wir einen entsprechenden Formulierungsvorschlag unterbreitet.

13.6 Bereichsspezifische Regelungen in der Abgabenordnung

Der Fortgang wird durch eine Arbeitsgruppe unterstützt.

Auf Grund der ersten Gespräche zwischen dem Bundesbeauftragten für den Datenschutz (BfD) und dem Bundesministerium für Finanzen (BMF) über die Berücksichtigung datenschutzrechtlicher Belange in der Abgabenordnung hat das BMF eine Arbeitsgruppe „Datenschutz in der Abgabenordnung“ eingesetzt.

Diese Arbeitsgruppe hat unter Beteiligung des BfD im April 2001 ihre Arbeit aufgenommen. Im Rahmen dieser Arbeitsgruppensitzung wurden zunächst einige Grundsätze zur Vorgehensweise einvernehmlich festgelegt. Weiterhin wurde von der Arbeitsgruppe eine Liste sämtlicher Vorschriften der Abgabenordnung erarbeitet, die datenschutzrechtlich relevant sind. Diese Vorschriften sollen in einem weiteren Schritt mit den Regelungen in den Datenschutzgesetzen des Bundes und der Länder verglichen werden. Zu diesem Zweck wurde die von der Arbeitsgruppe erarbeitete Liste den Landesbeauftragten für den Datenschutz zur Stellungnahme zugeleitet. Dabei ging es u.a. auch um die Frage der Bildung von Schwerpunkten. Ein zusammenfassendes Ergebnis lag bei Redaktionsschluss noch nicht vor.

14. Schule und Berufsbildung

14.1 Technikunterstützung im Verwaltungsbereich der allgemeinbildenden Schulen

Vor der Aufnahme des Echtbetriebes müssen für das Verfahren die erforderlichen Grundschutzmaßnahmen getroffen werden.

Im 17. TB (9.1) haben wir erstmals über datenschutzrechtliche Aspekte des Projektes Technikunterstützung im Verwaltungsbereich der allgemeinbildenden Schulen (TUVAS) berichtet. Die vorgesehene IuK-Unterstützung im Bereich der Schulverwaltung umfasst das Schulsekretariat, die Schulleitung sowie die mit Planungsaufgaben beauftragten Lehrerinnen und Lehrer. Inzwischen ist das Projekt so weit vorangeschritten, dass bis zum Redaktionsschluss alle (ca. 380) staatlichen allgemeinbildenden Schulen mit der erforderlichen Hardware ausgestattet waren und bereits im September 2001 mit den Anwenderschulungen für das Schulverwaltungsprogramm „Lehrer- und Schülerdatenbank“ (LUSD) begonnen wurde.

Eine endgültige Entscheidung hinsichtlich des technischen Konzeptes der LUSD stand bis zum Redaktionsschluss noch aus. Zur Zeit wird eine dezentrale Datenhaltung in den Schulen realisiert, es wird jedoch auch die Möglichkeit einer Überführung in eine zentrale Datenhaltung geprüft.

Bei der datenschutzrechtlichen Begleitung des Verfahrens sind wir auf eine Sicherheitslücke des Softwareproduktes aufmerksam geworden, die unter Umständen dazu führen konnte, dass unberechtigte Personen auf die Daten im System zugreifen. Nach unserem entsprechenden Hinweis hat die Behörde für Schule, Jugend und Berufsbildung (BSJB) beim Hersteller des Softwareproduktes für eine Schließung der Sicherheitslücke gesorgt.

Wir haben eine der 20 Pilotschulen im November 2000 geprüft und festgestellt, dass vor Ort Unklarheiten hinsichtlich der Maßnahmen zur Gewährleistung der Datensicherheit und des Datenschutzes bestanden. So erfolgte beispielsweise keine klare Trennung zwischen den Sachbearbeitungskennungen und Kennungen mit Administrationsrechten.

Neben den benötigten Windows-NT-Benutzerkonten waren weitere Konten eingerichtet, die nicht genutzt wurden. Die Konten waren zunächst nicht entsprechend der Paßwortrichtlinie konfiguriert, so dass es z.B. keine Begrenzung der Fehlversuche bei der Passworteingabe gab. Das verfügbare Antivirenprogramm war über einen längeren Zeitraum nicht aktualisiert worden. Die räumliche Absicherung des Zugangs zu den PC stellte sich als nicht ausreichend dar. Der von der Schule für die Erfassung entwickelte und genutzte Erhebungsbogen entsprach nicht den datenschutzrechtlichen Anforderungen.

Die BSJB hat zwischenzeitlich einen einheitlichen Erfassungsbogen entwickelt, welcher u.a. den nach § 1 Abs. 4 Schul-Datenschutzverordnung erforderlichen Hinweis auf die der Datenerhebung zugrunde liegende Rechtsvorschrift bzw. auf die Freiwilligkeit der Angaben enthält. Hinsichtlich der Notwendigkeit einer regelmäßigen Aktualisierung des Antivirenprogramms konnte ebenfalls Übereinstimmung erzielt werden. Die BSJB hat die hierfür erforderlichen Voraussetzungen geschaffen.

Der produktive Einsatz eines automatisierten Verfahrens, mit welchem personenbezogene Daten verarbeitet werden sollen, bedingt gemäß § 8 HmbDSG jedoch die Gewährleistung technischer und organisatorischer Grundschutzmaßnahmen. Sie müssen gemäß dem Ergebnis der nach § 8 Abs. 4 HmbDSG durchzuführenden Risikoanalyse ggf. noch um zusätzliche Schutzmaßnahmen erweitert werden. Die Diskussion über das Ergebnis der inzwischen vorliegenden Risikoanalyse für die LUSD war bis zum Redaktionsschluss noch nicht beendet. Kritisch ist in jedem Fall, dass die Entscheidung über die Einführung des Verfahrens von der BSJB bereits getroffen wurde, ohne sicher zu sein, dass mögliche Gefahren für die Rechte der Betroffenen durch technische

und organisatorische Maßnahmen wirksam beherrscht werden können. Damit wurde der Intention des Gesetzgebers, eine Vorabkontrolle durchzuführen, nicht entsprochen.

Im Rahmen unserer Projektbegleitung haben wir wiederholt darauf hingewiesen, dass die Gewährleistung des Grundschutzes durch entsprechende technische und organisatorische Regelungen eine unabdingbare Zulässigkeitsvoraussetzung für die Verarbeitung personenbezogener Daten mit Hilfe der LUSD in den Schulen darstellt. Die BSJB hatte zunächst hierfür keinen vorrangigen Handlungsbedarf gesehen, inzwischen aber nach unserer eingehenden Intervention die allgemein verbindliche Regelungen bezüglich der Aufgaben der Systemadministration sowie der Mindeststandards der äußeren Datensicherung getroffen. Wir werden die Umsetzung prüfen und die Einführung der LUSD in den allgemeinbildenden Schulen weiter begleiten.

14.2 Fehlzeiten in Abschlusszeugnissen

Durch die Angabe von Fehlzeiten in Abschlusszeugnissen haben hamburgische Schülerinnen und Schüler schlechtere Chancen auf dem Arbeitsmarkt als Schülerinnen und Schüler aus anderen Bundesländern.

Wir haben erst durch eine Eingabe davon erfahren, dass auf Grund von § 13 Abs. 2 des Allgemeinen Teils der neugefassten Ausbildungs- und Prüfungsordnung für berufliche Schulen (APO-AT) vom 25. Juli 2000 die Versäumnisse der Schülerin und des Schülers in den Zeugnissen mit der Unterscheidung „entschuldigt“ oder „unentschuldigt“ anzugeben sind. In der bisher geltenden Fassung der APO-AT fehlte eine entsprechende Regelung.

In Anbetracht der Tatsache, dass durch die Neufassung der APO-AT eine differenzierte Bekanntgabe von Fehlzeiten erfolgt und damit schutzwürdige Belange von Schülerinnen und Schülern berührt sein können, hätten wir nach Ziffer 3.2 der Richtlinie zur Beteiligung des Hamburgischen Datenschutzbeauftragten vom 12. November 1992 an dem Rechtsetzungsvorhaben beteiligt werden müssen. Mit Befremden haben wir festgestellt, dass dies bei der Neufassung der APO-AT unterblieben ist. Die Behörde für Schule, Jugend und Berufsbildung (BSJB) haben wir deshalb aufgefordert, durch geeignete Maßnahmen sicherzustellen, dass bei künftigen Rechtsetzungsverfahren seitens der Behörde die Vorgaben der Richtlinie zur Beteiligung des Hamburgischen Datenschutzbeauftragten beachtet werden.

Da die neugefasste APO-AT jetzt gilt, kommt es vor allen Dingen darauf an, mögliche nachteilige Auswirkungen für die betroffenen Schülerinnen und Schüler im Vollzug zu mindern. Durch die Verwendung der Zeugnisse im außerschulischen Bereich (z.B. bei Bewerbungen) ist nämlich zu befürchten, dass wegen der Fehlzeitenangabe die Entwicklungsmöglichkeiten der Schülerin oder des Schülers in aller Regel beeinträchtigt werden. Außerdem darf nicht verkannt werden, dass ein Abschlusszeugnis den Betroffenen sein ganzes Leben lang begleitet.

Als vergleichsweise kurzfristige Lösung wäre vorstellbar, dass nachteilige Angaben und Bemerkungen, die aus pädagogischen Gründen sinnvoll sein können, in einem gesonderten Beiblatt zum Zeugnis aufgeführt werden. Im eigentlichen Zeugnisvordruck könnten diese Angaben dann entfallen, so dass der Betroffene dieses Zeugnis im außerschulischen Bereich verwenden könnte, ohne dass dem Schüler die wichtigen Informationen zu seinem Arbeitsverhalten verloren gingen. Eine Durchschrift des Zeugnisses und des Beiblattes wäre in der Schule zum Schülerbogen zu nehmen.

Alternativ könnte folgendes Verfahren eingeführt werden: Berufsschüler, die unentschuldigte Schulversäumnisse aufweisen, könnten auf Antrag neben dem nach der APO-AT auszustellenden Zeugnis eine Zweitausfertigung auf einem Zeugnisformular erhalten, auf dem die für entschuldigte und unentschuldigte Versäumnisse vorgesehene Zeile durchgestrichen ist.

Die eigentliche Lösung des Problems muss jedoch darin liegen, dass durch eine Änderung der APO-AT klargestellt wird, dass Vermerke über Fehlzeiten künftig nicht mehr im Abgangs- oder Abschlusszeugnis angegeben werden. Damit würde eine Angleichung an andere Ausbildungsbereiche erfolgen. Beispielsweise wird auf die früher übliche Angabe von Fehlzeiten in Zeugnissen für Rechtsreferendare bereits seit einigen Jahren verzichtet.

Die BSJB hat unsere Hinweise zum Anlass genommen, eine Umfrage in den anderen Bundesländern wegen der dortigen Praxis vorzunehmen. Dabei hat sich gezeigt, dass eine der hamburgischen Regelung in der APO-AT vergleichbare Vorschrift nur in Niedersachsen besteht. Nachdem daraufhin der Landesbeauftragte für den Datenschutz Niedersachsen auf unseren Wunsch hin die Angelegenheit dem niedersächsischen Kultusministerium vorgelegt hat, entwickelte sich auch dort eine grundsätzliche Diskussion, die bis zum Redaktionsschluss noch nicht beendet war.

Unbeschadet der Vorreiterrolle Hamburgs war die BSJB nicht bereit, unseren Argumenten zu folgen und hält daran fest, dass die in der APO-AT getroffene Regelung rechtmäßig ist. Die Angabe von Fehlzeiten, ob entschuldigt oder unentschuldigt, stelle eine sachgerechte ergänzende Information zu den Leistungsbewertungen dar. Wer aus welchem Grunde auch immer nicht anwesend war, könne das Lernangebot der Schule, dessen Leistungsziel mit dem Zeugnis testiert werde, in dieser Zeit nicht genutzt haben. Eine solche Information könne sich sowohl günstig als auch ungünstig für die Schülerin oder den Schüler auswirken. Denn in der Leistungsbewertung werde grundsätzlich ein Bonus beispielsweise wegen krankheitsbedingter Fehlzeiten nicht gewährt. Das entsprechende Testat könne also der Schülerin oder dem Schüler zur Erklärung eines Leistungseinbruches dienen. Im übrigen stelle die ausdrückliche Ausweisung von Fehlzeiten als „unentschuldigt“ eine wichtige Information zum Arbeitsverhalten der Schülerin oder des Schülers dar.

Diese Begründung kann unsere Bedenken nicht entkräften, zumal nicht nachvollziehbar ist, warum die Schülerinnen und Schüler in Hamburg anders behandelt werden sollen als – mit Ausnahme in Niedersachsen – in allen anderen Bundesländern. Die zwangsläufige Folge ist, dass Schülerinnen und Schüler aus Hamburg bei Bewerbungen in Konkurrenz mit Schülerinnen und Schülern aus anderen Bundesländern in einer schlechteren Position und damit nicht chancengleich sind. Wir bezweifeln, ob dies bislang von der BSJB bedacht wurde und auch tatsächlich so gewollt ist.

Derzeit bleibt es nach alledem bei der zwischen uns und der BSJB unterschiedlichen rechtlichen Bewertung. Sobald uns das Ergebnis der grundsätzlichen Erwägungen aus Niedersachsen vorliegt, werden wir jedoch prüfen, ob wir unsere rechtliche Überzeugungsarbeit wieder aufnehmen.

14.3 Schulen ans Netz

Bei der fortschreitenden Nutzung des Internets in den Schulen dürfen die damit verbundenen Risiken nicht vergessen werden.

Die Anbindung der Schulen an das Internet hat sich in den letzten Jahren erheblich verbessert. Nahezu sämtliche weiterführenden Schulen sind mittlerweile an das Netz angeschlossen. Im Mittelpunkt des Interesses stand dabei verständlicherweise die Frage, wie die neuen technischen Möglichkeiten für den Bildungsauftrag der Schulen nutzbar gemacht werden können. Weniger Beachtung fanden Probleme des Datenschutzes, die mit der verstärkten Nutzung neuer interaktiver Medien verbunden sind:

- Jede Aktivität im Internet hinterlässt eine Datenspur. So kann nachvollzogen werden, von welchem Rechner aus welche Angebote im WorldWideWeb aufgerufen wurden.
- Die Kommunikation im Internet ist unsicher, d. h. weder kann man sicher sein, mit wem man es auf der anderen Seite gerade zu tun hat noch ist die Kommunikation vertraulich. Eine E-Mail, die an einen Adressaten im selben Stadtteil gesandt wird, kann durchaus über Netzknoten in Hongkong und in den USA geleitet und dort mitgelesen oder sogar verändert werden.
- Alle Informationen, die auf der Homepage der Schule im Web veröffentlicht werden, sind nicht nur für das schulische Umfeld sondern weltweit abrufbar. Gleiches gilt für Schülerzeitungen und Veröffentlichungen in Newsgroups. Alle im Internet veröffentlichten Informationen können auch noch nach Jahren recherchiert und zum Beispiel bei Personalentscheidungen herangezogen werden.
- Der Anschluss an das Internet gefährdet die Sicherheit der angeschlossenen Rechner und der auf ihnen gespeicherten Daten. Nicht nur Programmviren, sondern auch aktive Inhalte von Web-Angeboten (z. B. ActiveX, Java) bergen vielfach unterschätzte Sicherheitsrisiken.

Aus unserer Sicht sollte die Schule auf diese Probleme auf verschiedenen Ebenen reagieren. So sollten die Schülerinnen und Schüler nicht nur lernen, wie sie möglichst effektiv an bestimmte Informationen im Internet herankommen oder selbst Internet-Angebote gestalten. Ihnen sollte vielmehr auch vermittelt werden, wie sie risikobewusst mit den neuen Möglichkeiten umgehen. Schließlich ist darauf hinzuweisen, dass sich auch die Schulen an die Vorgaben des Multimediarechts halten müssen (vgl. 3.5.1).

14.3.1 Internet-Datenschutz im Unterricht

Während Datenschutz im „Offline-Bereich“ häufig eine recht trockene Materie ist, lassen sich die Datenschutzprobleme im Internet anschaulich vermitteln. Dabei geht es zum einen darum, zu verdeutlichen, welche Daten beim Surfen preisgegeben werden. Kaum ein Internet-Nutzer weiß wirklich, welche Informationen er automatisch an den Anbieter übermittelt, dessen Seite er im Web aufruft. Inzwischen gibt es im Netz eine ganze Reihe von Angeboten, die sich dieser Problematik angenommen haben (siehe unten).

Auch der Cyberspace ist kein rechtsfreier Raum. Deshalb muss den Schülerinnen und Schülern vermittelt werden, dass sie bestimmte Regeln beachten müssen, z. B. wenn sie Informationen über andere Menschen im Internet veröffentlichen wollen. Gleiches gilt für den Zugriff auf Nutzungsdaten (als Nutzungsdaten werden diejenigen Informationen bezeichnet, die beim Surfen anfallen). Auch für den datenschutzgerechten Umgang mit diesen Daten bietet das Internet mittlerweile Hilfestellungen.

Zur Medienkompetenz gehört schließlich auch die Fähigkeit, das eigene Verhalten selbst so zu steuern, dass die Risiken und Gefahren minimiert werden. Hierzu gehört zum Beispiel, dass die Schülerinnen und Schüler alle Möglichkeiten zur anonymen Inanspruchnahme des Internet kennen lernen und auch wissen, dass die Identität ihrer „Chat-Partner“ und E-Mail-Freunde im Regelfall ungesichert ist. Bei einer Person, die sich im Chat-Room als 15-jähriges Mädchen ausgibt, kann es sich in Wirklichkeit durchaus um einen älteren Herrn handeln, der nicht nur edle Motive hat.

Die im Internet verwendete Software, insbesondere die Browserprogramme (Internet-Explorer, Netscape-Navigator), enthalten vielfältige „Stellschrauben“, durch die sich der Datenschutz verbessern lässt (vgl. hierzu unsere Empfehlungen zur Erhöhung der Sicherheit bei Standard-Browsern – http://www.hamburg.de/Behoerden/HmbDSB/material/keycheck.htm). Durch zusätzliche Programme ist es möglich, den Datenmissbrauch durch Dritte zu unterbinden oder zumindest einzuschränken. Derartige „Tools“ stehen häufig kostenlos zur Verfügung. Schließlich könnte sich auch ein „Besuch“ beim virtuellen Datenschutzbüro (http://www.datenschutz.de) lohnen, das von vielen Datenschutzbehörden unterstützt wird und auf datenschutzrechtliche Fragen fundierte und schnelle Antworten liefert.

14.3.2 Datenschutz auch für die Schule

Schülerinnen und Schüler sind Träger von Persönlichkeitsrechten, deren Ausübung allerdings an ihre Einsichtsfähigkeit gebunden ist. Doch auch soweit die Einsichtsfähigkeit nicht gegeben ist, bedeutet dies nicht, dass der Datenschutz keine Rolle spielt, sondern umgekehrt: hier muss die Schule dafür Sorge tragen, dass die Rechte der Schülerinnen und Schüler gewährleistet werden. So definieren §§ 98 bis 100 Hamburgisches Schulgesetz (HmbSG) den rechtlichen Rahmen für die Verarbeitung personenbezogener Daten der Schülerinnen und Schüler.

Die Nutzung des Internet berührt eine Reihe von Datenschutzproblemen im Verhältnis Schule-Schüler. Zugriffe auf das Internet werden sowohl auf den Unterrichtsrechnern (Clients) als auch in Netzkomponenten (Proxy-Server, Firewalls) protokolliert. Dies bedeutet, dass die von einem Schüler aufgerufenen Seiten möglicherweise von anderen Benutzern, die dasselbe Gerät verwenden, nachvollzogen werden können. Findet eine Protokollierung in Firewalls und in Proxy-Servern statt, entstehen umfassende Dateien über sämtliche Surf-Aktivitäten.

Das Datenschutzrecht enthält die Vorgabe zur Datensparsamkeit, d.h. es sollen so wenig personenbezogene Daten wie möglich verarbeitet werden (vgl. hierzu 3.1.1). Deshalb sollten die Einstellungen auf den Unterrichts-PC so gesetzt werden, dass keine Zwischenspeicherungen und Historik-Dateien entstehen. Es ist wesentlich datenschutzfreundlicher, Vorkehrungen zu treffen, die einen Missbrauch (z.B. durch Zugriff auf pornographische oder rechtsradikale Angebote) verhindern als nachträglich den Missbrauch aufzuklären. So sind Filterprogramme der nachträglichen Protokollierung von Surf-Aktivitäten vorzuziehen. Allerdings kann es bei konkretem Missbrauchsverdacht gerechtfertigt sein, Zugriffe auf unzulässige Inhalte aufzuklären und zu unterbinden, indem Protokolldateien zeitweise geführt und ausgewertet werden.

Voraussetzung für derartige Maßnahmen ist es stets, dass die Schülerinnen und Schüler umfassend über die einzuhaltenden Regeln und die Kontrollmaßnahmen informiert werden. Eine heimliche Aufzeichnung und Auswertung der Nutzungsdaten würde den Datenschutz unzulässig einschränken.

Ein vergleichbares Problem besteht bei der Verwendung von E-Mail: auch hier kann es durchaus sinnvoll sein, dass die Lehrerin oder der Lehrer in Inhalte Einsicht nimmt. Wichtig ist dabei, dass den Schülerinnen und Schülern vorher mitgeteilt wird, unter welchen Umständen ihre E-Mails geöffnet werden. Auch hier geht es darum, nicht hinter dem Rücken der Betroffenen zu agieren, sondern mit deren Wissen und möglichst auch mit deren Einsicht und Einverständnis.

Von besonderer datenschutzrechtlicher Brisanz sind Veröffentlichungen in Newsgroups oder im WWW. Da auf derartige Veröffentlichungen weltweit zugegriffen werden kann, müssen sich die Angaben über Schülerinnen und Schüler auf ein Mindestmaß beschränken. Dabei sollten Möglichkeiten zur Anonymisierung beziehungsweise zur Erschwerung der personenbezogenen Zuordnung genutzt werden. So ist es weniger problematisch, wenn Veröffentlichungen nur unter Nennung des Vornamens der Schülerin oder des Schülers erfolgen. Die Veröffentlichung des vollen Namens der Schülerinnen und Schüler ist nur mit deren ausdrücklicher Einwilligung, beziehungsweise (bei Jüngeren) mit Einwilligung der Eltern zulässig. Gleiches gilt auch für die Veröffentlichung von Bildern, bei denen die Gesichter der abgebildeten Personen zu erkennen sind. Auch hierfür ist die Einwilligung der Betroffenen erforderlich. Einwilligungen müssen tatsächlich freiwillig, d.h. ohne Zwang und Nachteile bei Verweigerung, erfolgen. Wirksam sind nur Einwilligungen, bei denen die Betroffenen vorab angemessen informiert wurden.

14.4 Neues BAföG-Dialogverfahren

Die Anforderungen des Datenschutzes werden beim neuen Dialogverfahren vom Hochschulamt und vom Bezirksamt Hamburg-Mitte erfüllt.

Vom Hochschulamt der Behörde für Wissenschaft und Forschung (BWF) wird seit 1996 ein IuK-Verfahren zur Zahlung für Leistungen nach dem Bundesausbildungsförderungsgesetz (BAföG) genutzt. Dieses Verfahren enthält neben eigenen Programmen einen umfangreichen Teil von Entwicklungen aus dem BAföG-Verbund anderer Bundesländer. Im Berichtszeitraum wurde das Abrechnungsverfahren um ein neues Dialogverfahren ergänzt, das aus Nordrhein-Westfalen übernommen wurde, um die Bearbeitung von BAföG-Anträgen zu unterstützen und die Abläufe zu verbessern.

Bedauerlich ist, dass die BWF entgegen ihrer Verpflichtung aus § 23 Abs. 4 HmbDSG in Verbindung mit Ziffer 3.2 der Richtlinie zur Beteiligung des Hamburgischen Datenschutzbeauftragten vom 12. November 1992, uns nicht schon bei der Planung dieser neuen Anwendung unterrichtet hat. Vielmehr haben wir erst von dritter Seite davon erfahren, dass ein neues IuK-Verfahren entwickelt worden ist und der Beginn des Echtbetriebs unmittelbar bevorstehen würde. Die BWF hat zugesagt, durch geeignete Maßnahmen sicherzustellen, dass bei künftigen Planungen neuer IuK-Vorhaben seitens der Behörde die maßgeblichen Vorgaben zur Beteiligung des Hamburgischen Datenschutzbeauftragten beachtet werden.

Die Dialogeingaben in das neue Verfahren erfolgen seit Mitte 2001 sowohl im Studentenwerk Hamburg für die an den Hamburger Hochschulen immatrikulierten Studenten als auch im Bezirksamt Hamburg-Mitte für den Personenkreis, der ansonsten Anspruch auf Ausbildungsförderung hat. Die Daten werden für die beiden Bereiche getrennt auf einem zentralen Server im Hoch-

schulamt gespeichert und monatlich automatisiert an bisherige Abrechungsverfahren übergeben.

Durch die Einführung des Dialogverfahrens hat sich der Umfang der verarbeiteten Daten nicht verändert. Um den Anforderungen nach einer größeren Servicefreundlichkeit gerecht werden zu können, wurden die Zugriffsrechte im Studentenwerk so eingestellt, dass die Sachbearbeiter der beiden Gruppen jeweils lesend auf alle Daten ihres Bereichs zugreifen können.

Das Hochschulamt kommt in der Risikoanalyse nach § 8 Abs. 4 HmbDSG zu dem Ergebnis, dass für die Daten ein hoher Schutzbedarf besteht und hat entsprechende technische und organisatorische Maßnahmen festgelegt. Das Hochschulamt hat die Anforderungen in Policies dokumentiert und hat die von ihm betreuten Clients so konfiguriert, dass die Anwender nur Zugriff auf die erforderlichen Systemressourcen haben und ein hoher Passwortschutz besteht. An den Arbeitsplätzen mit Internetzugang wurden dafür getrennte Benutzerkennungen eingerichtet, von denen aus kein Zugriff auf das Dialogverfahren besteht.

Wir haben das Bezirksamt Hamburg-Mitte aufgefordert, ebenfalls zusätzliche Schutzmaßnahmen zu treffen, damit der von dort betreute Personenkreis nicht schlechter gestellt ist als die Studierenden. Das Bezirksamt hat eine entsprechende datenschutzgerechte Lösung realisiert.

14.5 Chipkarte für Studierende

Jetzt gibt es auch eine Rechtsgrundlage für die Karte.

Die Universität Hamburg hatte zum Wintersemester 1999/2000 damit begonnen, einen chipkartenbasierten Studierendenausweis (UniHamburgCard) einzuführen. Dies musste auf freiwilliger Basis erfolgen, weil eine universitäre Rechtsgrundlage für eine solche Karte fehlte (vgl. 17. TB, 9.2). § 111 des novellierten Hamburgischen Hochschulgesetzes (HmbHG), das am 1. August 2001 in Kraft getreten ist, erlaubt nunmehr ausdrücklich die Einführung eines maschinenlesbaren Studierendenausweises, ohne dass hierfür eine Einwilligung der Betroffenen eingeholt werden muss.

Durch Rechtsverordnung hat der Senat allerdings die Daten und Funktionen eines maschinenlesbaren Studierendenausweises näher zu bestimmen. Darin müssen die in diesem Zusammenhang nötigen Verfahrensregelungen getroffen und die Daten benannt werden, die zur Erteilung des Ausweises erhoben und verarbeitet werden dürfen. Bis eine solche Rechtsverordnung vorliegt, die noch mit uns abzustimmen ist, darf die UniHamburgCard weiterhin nur an die Studierenden ausgegeben werden, die damit auch einverstanden sind.

Bei einer datenschutzrechtlichen Prüfung des gegenwärtigen Verfahrens zur Ausgabe der UniHamburgCard konnten wir nur wenige Mängel feststellen. Im wesentlichen ging es dabei um Defizite im Bereich der Räume, in denen die Daten der Studierenden elektronisch und in Papierform aufbewahrt werden, und um die fehlende Anpassung des IuK-Sicherheitskonzeptes an die durchgeführte Migration von Windows 95 auf Windows NT. Die Migration an sich haben wir begrüßt, weil Windows NT gegenüber dem inhärent unsicheren System Windows 95 deutliche Vorteile hinsichtlich des Datenschutzes und der Datensicherheit bietet. Insoweit hat es sich für die Universität gelohnt, uns von Beginn an bei der Planung und Einführung der UniHamburgCard zu beteiligen. Die wenigen festgestellten Mängel will die Universitätsverwaltung kurzfristig beheben.

14.6 Daten ehemaliger Studierender (Alumnis)

Für die in Zukunft immer wichtiger werdende Kontaktpflege mit ehemaligen Studierenden dürfen die hamburgischen Hochschulen demnächst die entsprechenden Daten verarbeiten.

Ehemalige Studierende (Alumnis) fühlen sich sehr viel mehr als früher mit ihrer Hochschule verbunden und wollen dies durch bestimmte konkrete Maßnahmen zum Ausdruck bringen. Die Aktionen der Universität Hamburg „Neue Stühle für das Audimax“ und „Ex-Libris“ hatten deshalb eine entsprechende Resonanz. So konnte beispielsweise die gesamte Bestuhlung des Auditorium Maximum mit Spenden der Alumnis erneuert werden. Darauf aufbauend sollen als Teil einer umfassenden Hochschulentwicklungsstrategie sogenannte Alumni-Netzwerke entstehen, um die Absolventen mit ihren Erfahrungen in der Berufswelt aktiv in die Entwicklung der Hochschule einzubinden. Alumnis sollen nicht nur Geldgeber, sondern auch Ratgeber „ihrer“ Hochschule werden.

Um dieser Entwicklung Rechnung zu tragen, enthält das am 1. August 2001 in Kraft getretene novellierte Hamburgische Hochschulgesetz (HmbHG) einen Auftrag der Hochschulen zur Betreuung der Alumnis. § 111 HmbHG erlaubt die Verarbeitung entsprechender Daten zur Kontaktpflege mit ehemaligen Hochschulmitgliedern. Der Senat hat allerdings durch Rechtsverordnung zu bestimmen, welche Daten für diese Zwecke erhoben und verarbeitet werden dürfen, welche Aufbewahrungsfristen gelten sollen und wie das Verfahren bei der Ausübung des Auskunfts- und Einsichtsrechts zu gestalten ist. Eine solche Rechtsvorschrift liegt zwar noch nicht vor, sie befand sich aber zum Redaktionsschluss bereits in einer ersten behördeninternen Abstimmung.

Die Universität Hamburg hat zugesagt, uns an der weiteren Vorbereitung der Rechtsverordnung – wie schon bei der datenschutzgerechten Ausgestaltung des bisherigen Verfahrens – rechzeitig zu beteiligen. Bislang durfte die letzte der Universität bekannte Korrespondenzanschrift für Zwecke der Ehemaligen-

betreuung nur mit Einwilligung der Betroffenen verwendet werden. Eine Aktualisierung des Adressenbestandes war rechtlich nicht möglich. Der Universität ist klar, dass ohne Einwilligung der Betroffenen die Aktivitäten zur Kontaktpflege erst aufgenommen werden dürfen, wenn der Senat die Rechtsverordnung in Kraft gesetzt hat.

15. Bauen, Wohnen und Wirtschaftsverwaltung

15.1 Einrichtung einer Videoüberwachungsanlage

Die geplante Videoüberwachung soll datenschutzfreundlich gestaltet werden.

Das Bezirksamt Harburg plant, im öffentlich zugänglichen Bereich der Fußgängertunnel an der S-Bahn-Haltestelle Harburg-Rathaus sechs Videokameras zur Verbesserung der Sicherheit einzusetzen. Die Kameras sollen ausschließlich dazu dienen, die verzweigten, unübersichtlichen Tunnelzugänge und Personenaufzüge mittels Monitor vom zentralen Stützpunkt der S-Bahn Wache überwachen zu können. Damit soll erreicht werden, dass insbesondere Störungen, die von Personen in dem Tunnelbereich ausgehen, möglichst schnell festgestellt und abgewehrt werden können (z.B. bei Belästigungen, Vandalismusschäden).

Nach den Planungen sollen bei dieser Videoüberwachung sog. Übersichtsaufnahmen gemacht werden, die lediglich das tatsächliche Geschehen in dem Tunnelbereich erkennen lassen, so dass bei Feststellung entsprechender Vorkommnisse geeignete Maßnahmen durch die S-Bahnwache ergriffen werden können (z.B. Einschreiten von Mitarbeitern der S-Bahnwache oder Benachrichtigung der Polizei). Eine Personenidentifizierung soll aufgrund der Kameraobjektive und fehlender Zoomeinrichtung nicht möglich sein. Es sollen auch keine Kamerabilder aufgezeichnet werden.

Unter der Voraussetzung, dass keine personenbezogenen oder -beziehbaren Informationen aufgenommen, gespeichert oder übertragen werden, sind Persönlichkeitsrechte nicht beeinträchtigt. Aus diesem Grund bestehen gegen das geplante Vorhaben aus unserer Sicht keine grundsätzlichen datenschutzrechtlichen Bedenken.

Wir haben die verantwortliche Stelle aber darauf hingewiesen, dass für die Bürger und Bürgerinnen erkennbar sein muss, dass im Bereich des Fußgängertunnels eine Videoüberwachung stattfindet und dass an den Ein- und Ausgängen der Fußgängertunnel entsprechende Hinweisschilder anzubringen sind.

Zur Beurteilung der datenschutzrechtlich einschlägigen Frage, ob tatsächlich ein Personenbezug ausgeschlossen ist, werden wir uns vor Inbetriebnahme der Videoüberwachung überzeugen.

15.2 Selbstauskünfte aus dem Gewerbezentralregister

Für Auskünfte aus dem Gewerbezentralregister liegen zwei Gesetzentwürfe vor, von denen der neuere Entwurf vorzuziehen ist.

Im 16. TB (10.3) hatten wir über die datenschutzrechtliche Problematik berichtet, dass öffentliche Auftraggeber bei der Vergabe von Bauleistungen von Bewerbern und Bietern zum Nachweis ihrer Zuverlässigkeit eine Selbstauskunft aus dem Gewerbezentralregister verlangen. Diese Selbstauskünfte sollen nach dem Entwurf eines „Gesetzes zur Bekämpfung illegaler Praktiken im öffentlichen Auftragswesen“ (mit Stand 16. Mai 2000) des Bundesministeriums für Wirtschaft und Technologie (BMWi) gesetzlich geregelt werden. Im § 4 ist vorgesehen, dass Unternehmen, die bei der Vergabe von Bau- und Dienstleistungsaufträgen in die engere Wahl kommen, zum Nachweis ihrer Zuverlässigkeit auf Verlangen des öffentlichen Auftraggebers einen Auszug aus dem Gewerbezentralregister vorzulegen haben, der nicht älter als drei Monate sein darf.

Anfang September 2001 haben wir dann von einem Referentenentwurf über ein „Gesetz zur Erleichterung der Bekämpfung von illegaler Beschäftigung und Schwarzarbeit“ des Bundesministeriums für Arbeit und Sozialordnung (BMA) Kenntnis erhalten, der mit den Bundesressorts noch nicht abgestimmt worden ist. Dieser Entwurf sieht in Art. 11 (Gesetz zur Bekämpfung von Schwarzarbeit), Art. 13 (Gewerbeordnung) und Art. 14 (Arbeitnehmer-Entsendegesetz) Regelungen vor, wonach den öffentlichen Vergabestellen – durch entsprechende Ergänzung des § 150a Gewerbeordnung (Auskunft an Behörden) – ein unmittelbar gegen das Gewerbezentralregister gerichteter Auskunftsanspruch über dort eingetragene rechtskräftige Straf- oder Bußgeldentscheidungen nach dem Gesetz zur Bekämpfung der Schwarzarbeit und dem Arbeitnehmer-Entsendegesetz eingeräumt wird. Nach unserer Auffassung entspricht der Gesetzentwurf des BMA besser dem Gebot der Verhältnismäßigkeit, nur die unbedingt notwendigen Informationen zu erhalten.

16. Ausländerwesen

16.1 Verschärfungen des Ausländerrechts

Die Gesetzentwürfe der Bundesregierung zur Terrorismusbekämpfung sehen eine Vielzahl von Verschärfungen des Ausländerrechts vor, die die informationelle Selbstbestimmung der Betroffenen einschränken.

Auch der überarbeitete Entwurf des Terrorismusbekämpfungsgesetzes enthält eine Reihe von Vorschriften, die die Erhebung zusätzlicher Ausländerdaten und ihre Übermittlung an weitere Empfänger und unter geringeren Voraussetzungen vorsehen. Die Rechtsänderungen betreffen Hamburg vor allem

deshalb, weil ihre Umsetzung weitgehend in den Händen der Landesbehörden liegt. Deshalb beteiligen wir uns an der bundesweiten datenschutzrechtlichen Diskussion um diese Regelungen.

Eine wesentliche Änderung des Ausländergesetzes liegt in der inhaltlichen Erweiterung und Formalisierung der ausländerrechtlichen Dokumente: Aufenthaltsgenehmigungen, Ersatzpapiere und Duldungen sollen in Zukunft hinsichtlich der Grunddaten maschinenlesbar sein und Felder für biometrische Merkmale enthalten (vgl. dazu oben 1.3 und 6.1). Die Daten, zu denen auch „Anmerkungen“ gehören, sollen verschlüsselt werden können, so dass die Betroffenen die Angaben nicht ohne weiteres zur Kenntnis nehmen und auf ihre Richtigkeit überprüfen können. Alle öffentlichen Stellen einschließlich der Sozialversicherungsträger sollen das Recht erhalten, auf die automatisch lesbaren Daten zuzugreifen und sie weiter zu verarbeiten.

Als neuen Grund für die Versagung einer Aufenthaltsgenehmigung bestimmt der Gesetzentwurf nun auch eine „Gefährdung der freiheitlichen demokratischen Grundordnung“ und die Unterstützung einer „Vereinigung, die den internationalen Terrorismus unterstützt“. Dieser Versagungsgrund rechtfertigt zugleich erweiterte Maßnahmen zur Identitätsfeststellung und zur Übermittlung von Visumsdaten an die deutschen Geheimdienste. Ob diese sehr weite Tatbestandsfassung dem rechtsstaatlichen Gebot der Bestimmtheit und Normenklarheit genügt, die bei der gesetzlichen Einschränkung des Grundrechts auf informationelle Selbstbestimmung einzuhalten ist, erscheint zumindest diskussionsbedürftig.

Als neue Maßnahme zur Identitätsfeststellung bei Ausländern schafft der Gesetzentwurf überdies die Möglichkeit, das gesprochene Wort auf Ton- oder Datenträger aufzunehmen, um die Herkunftsregion oder den Herkunftsstaat des Ausländers zu klären. Hier sollte nach einer Testphase geprüft werden, ob die Eingriffs-Maßnahme zur Erreichung des erklärten Ziels wirklich geeignet ist.

Auch im Asylverfahrensgesetz soll die Möglichkeit der Sprachspeicherung aufgenommen werden. Darüber hinaus dehnt der Gesetzentwurf die bislang differenzierten Fristen zur Aufbewahrung der Identifizierungsunterlagen insgesamt auf 10 Jahre aus und gibt damit die Unterscheidungen zwischen Ausländern mit verschiedenem Aufenthaltsstatus auf.

Im Ausländerzentralregister sollen in Zukunft auch „freiwillig gemachte Angaben zur Religionszugehörigkeit“ gespeichert werden. Gruppenauskünfte aus dem Register werden nach dem Gesetzentwurf allgemein „zur Abwehr von Gefahren“ und nicht mehr nur „zur Abwehr einer im Einzelfall bestehenden Gefahr“ z.B. für die freiheitliche demokratische Grundordnung zugelassen. Ausländer mit festem Aufenthaltsrecht sollen von der Datenübermittlung an Dritte nicht mehr ausgenommen werden. Zu den möglichen Empfängern von

Datenübermittlungen gehören nach dem Entwurf in Zukunft auch die Luftfahrtbehörden. Abrufe im automatisierten Verfahren sollen hinsichtlich des Datenumfangs erweitert und an geringere Voraussetzungen geknüpft werden. Bei der Visadatei, die ebenfalls im Ausländerzentralregistergesetz geregelt ist, erweitert der Entwurf ebenfalls den Speicherumfang und den Kreis der möglichen Datenübermittlungs-Empfänger. So sollen die Visadaten nun auch auf Ersuchen der Sozialhilfeträger an diese übermittelt werden.

Insgesamt beschneidet das Gesetzespaket den Datenschutz von Ausländern in vielen Bereichen. Wir räumen ein, dass die Bedrohung durch den internationalen Terrorismus Verschärfungen des Ausländerrechts und auch Einschränkungen des informationellen Selbstbestimmungsrechts der Ausländer rechtfertigen kann. Die vorzusehenden Grundrechtseingriffe erfordern jedoch eine gewissenhafte Prüfung der Geeignetheit, der Erforderlichkeit und der Angemessenheit der Maßnahmen. Da mögliche Auswirkungen einzelner Vorschläge derzeit kaum absehbar sind, sollte vermehrt Gebrauch gemacht werden von einer Befristung und einer obligatorischen Evaluierung der einzuführenden Maßnahmen nach einem ersten Praxistest. Andere Vorschläge zielen auf langfristige Wirkungen. Hier erscheint eine überstürzte Neuregelung ohne fundierte Folgenabschätzungsprüfung kaum angemessen.

16.2 Beanstandung der Ausländerdatenverarbeitung

Aufgrund einer Prüfung beanstandeten wir im Jahr 2000 gegenüber dem Senat, dass die Ausländerbehörden u.a. Datenlöschungs- und Vernichtungsvorschriften des Ausländerrechts nicht beachteten. Eine Dienstanweisung der Behörde für Inneres zur Aktenführung hilft dem ab. Entgegen unserer Beanstandung bestätigte der Senat dagegen die Praxis, dass die Ausländerbehörden Mitteilungen über einzelne geringfügige Rechtsverstöße von Ausländern zunächst zur Kenntnis und zur Akte nehmen.

16.2.1 Prüfungsergebnis

Bei einer im Januar 2000 im Ortsamt Wilhelmsburg durchgeführten Prüfung der Ausländerdienststelle stellten wir eine ganze Reihe von Datenschutzmängeln fest. Von diesen im Prüfbericht vom 3. Mai 2000 niedergelegten Defiziten machten wir nach einer ausführlichen Korrespondenz mit der Behörde für Inneres die folgenden zum Gegenstand einer formellen Beanstandung:

- Ausländerakten enthielten – z.T. viele Jahre alte – Mitteilungen der Polizei über einzelne geringfügige Verstöße, Anzeigen, Personalienfeststellungen.
- Der Ausgang des Verfahrens, also auch das tatsächliche Vorliegen eines Rechtsverstoßes, war der Akte häufig nicht zu entnehmen und wurde auch nicht ermittelt.

– Vorgänge, die dem Ausländer – z.B. aufgrund der Tilgungsbestimmungen des Bundeszentralregistergesetzes – nicht mehr vorgehalten werden dürfen, wurden entgegen dem Ausländerrecht nicht vernichtet.

– Bei ausländerrechtlichen Entscheidungen und Stellungnahmen an den Petitionsausschuss der Bürgerschaft griff die Ausländerbehörde auch auf Vorgänge zurück, die nach dem Ausländerrecht hätten vernichtet werden müssen.

Die weiteren Feststellungen des Prüfungsberichts betrafen folgende Sachverhalte:

– Bei Einbürgerungsanträgen versandte die Ausländerdienststelle die gesamte Ausländerakte ohne Einwilligung der Betroffenen an die Einbürgerungsabteilung.

– Die Sachbearbeiterinnen und Sachbearbeiter der zentralen und aller bezirklichen Ausländerdienststellen haben Lese- und Schreibzugriff auf die im System PAULA gespeicherten Daten von allen in Hamburg lebenden Ausländern. Die Schreib-Zugriffe wurden zwar protokolliert, eine Auswertung / Stichprobenkontrolle der Rechtmäßigkeit der Zugriffe fand jedoch nicht statt. Die Lese-Zugriffe wurden nicht protokolliert.

– Alte Akten der bezirklichen Ausländerdienststellen werden in der zentralen Ausländerbehörde der Behörde für Inneres archiviert und stehen dem Zugriff der Fachbehörde offen.

– Sozial- und Gesundheitsdaten wie Gutachten vom Gesundheitsamt und Krankenhausentlassungsberichte wurden in Ausländerakten unverschlossen aufbewahrt.

16.2.2 Beanstandung mit Teilerfolg

Die formelle Beanstandung vom 3.August 2000 gegenüber dem zuständigen Senator für Inneres beschränkten wir darauf, dass auch nicht mehr verwertbare Erkenntnisse und Mitteilungen über geringfügige Rechtsverstöße von Ausländern unbefristet aufbewahrt und genutzt werden. Wir stützten uns auf § 80 Abs.2 Ausländergesetz (AusLG), der die Vernichtung ausländerrechtlich unerheblicher Vorgänge fordert. Wir vertraten die Rechtsauffassung, dass einzelne geringfügige Rechtsverstöße nach § 46 Abs.2 AusLG keinen Ausweisungsgrund bilden und dass deswegen auch die Polizei oder andere Dienststellen solche Verstöße – jenseits der formellen Einleitung von Straf- und Bußgeldverfahren – nicht an die Ausländerbehörde mitteilen dürfen. Welche Rechtsverstöße „geringfügig“ sind, ist im AuslG und der Verwaltungsvorschrift konkretisiert.

Nach § 46 AuslG können allerdings geringfügige Rechtsverstöße dann einen Ausweisungsgrund bilden, wenn sie nicht vereinzelt vorkommen. Wer wie lange wie viele geringfügige Verstöße sammelt, bis sie zusammen als Ausweisungsgrund erheblich werden, ist nirgendwo geregelt. Wir schlugen vor, dass von einer erheblichen „Häufung" von Rechtsverstößen frühestens dann ausgegangen wird, wenn innerhalb eines Jahres zu einem ersten Verstoß ein zweiter hinzutritt. Wir lehnten jedoch ab, dass die Ausländerbehörde selbst die Jahresfrist beobachtet und jeden geringfügigen Rechtsverstoß erst einmal mitgeteilt bekommt.

Die Stellungnahme des Innensenators wies die Beanstandung im wesentlichen zurück, kündigte aber eine Dienstanweisung an, Teilakten anzulegen für Vorgänge, die später nach § 80 AuslG zu vernichten sind. Angesichts der Zurückweisung war ich nach § 25 HmbDSG gehalten, eine „weitere Beanstandung" an den Senat zu richten. Diese erfolgte mit Schreiben vom 18. September 2000.

Der Senat befasste sich am 19.Dezember 2000 damit. Der Präsident des Senats teilte uns am 18. Januar 2001 die Entscheidung mit, die in einer Reihe von Punkten unserem Anliegen entsprach:

– Soweit es um die weitere Aufbewahrung von Mitteilungen über Rechtsverstöße in Ausländerakten geht, sollen die Sachbearbeiterinnen und Sachbearbeiter anlassbezogen – etwa bei Vorsprache des Ausländers oder Aktenabgabe an eine andere Stelle – prüfen, ob einzelne Vorgänge nach § 80 AuslG zu vernichten sind.

– Mitteilungen über nicht ausländerrechtsrelevante Vorgänge wie Personalienfeststellungen, nicht benötigte Anzeigen oder Freisprüche sollen in Zukunft nicht mehr zu den Akten genommen werden.

– Für Ausweisungsvorgänge nach § 80 AuslG, die Mitteilungen über Rechtsverstöße enthalten, sollen Teilakten angelegt werden, wobei eine rechtzeitige Wiedervorlage vor der gebotenen Vernichtung zu verfügen ist.

Hinsichtlich der Mitteilungen einzelner geringfügiger Rechtsverstöße an die Ausländerbehörde soll es allerdings bei der bisherigen Praxis bleiben. Soweit nicht die vorstehenden Aktenführungsregeln greifen, erhalten und sammeln die Ausländerdienststellen also weiterhin ohne Befristung jede Mitteilung auch über einzelne geringfügige Verstöße.

Die für den Jahreswechsel 2000 / 2001 angekündigte Dienstanweisung wurde am 27. September 2001 erlassen und hatte uns rechtzeitig als Entwurf vorgelegen.

16.2.3 Weitere Folgerungen

Über die weiteren Feststellungen des Prüfberichts konnten wir mit der Behörde für Inneres Lösungen finden:

- Für die Übermittlung der Ausländerakte an die Einbürgerungsabteilung legte die Behörde für Inneres im März 2001 den Vordruck einer Einwilligungserklärung vor, der „ab sofort" verwendet werde. Eine Abstimmung mit uns hätte die Erklärung möglicherweise noch datenschutzfreundlicher und verständlicher gestalten können. Hinsichtlich der Übermittlung der ganzen Ausländerakte stellten wir nach ausführlichen Begründungen der Behörde für Inneres unsere Bedenken zurück.
- Für den umfassenden lesenden Zugriff der Mitarbeiterinnen und Mitarbeiter auf die PAULA-Daten wurde im Juni 2000 die Protokollierung eingeführt.
- Für die Kontrolle des schreibenden und des lesenden Zugriffs wurde im August 2000 ein Verfahren für eine Stichproben-Auswertung der Protokolldaten und deren Dokumentation beschlossen.
- Hinsichtlich der Archivierung von bezirklichen Ausländerakten wird je nach Fallkonstellation der Verbleib im Bezirk oder die Übermittlung an die zentrale Ausländerbehörde differenziert geregelt. Unsere Bedenken gegen die Übermittlung haben wir nach den Ausführungen der Behörde für Inneres nicht aufrecht erhalten.
- Sozial- und Gesundheitsdaten sollen der Ausländerakte in Zukunft nur in verschlossenen Umschlägen beigefügt werden.

16.3 Öffentlichkeitsarbeit der Ausländerbehörde

Die seit November 1999 angekündigte und von der Bürgerschaft geforderte „Medienleitlinie für die Ausländerbehörde" ist bisher über einen Entwurf nicht hinausgekommen. Ein weiterer Fall einer problematischen Veröffentlichung macht sie dringender denn je.

16.3.1 Medienleitlinie der Behörde für Inneres

Im 17. TB (11.1) hatten wir ausführlich über die gesetzlichen Möglichkeiten und Grenzen der Ausländerbehörde berichtet, sich gegenüber nachteiligen oder falschen Presseberichten zu wehren und dabei personenbezogene Informationen über Ausländer zu offenbaren. Das HmbDSG und das Hamburgische Pressegesetz lassen dies derzeit nur in Form einer presserechtlichen Gegendarstellung oder als Auskunft auf eine Presseanfrage zu.

Soweit nicht spezielle Regelungen z.B. für parlamentarische Anfragen oder hinsichtlich Sozialdaten eingreifen, bedarf es bei Auskünften an die Presse jeweils einer Abwägung zwischen den Interessen der Behörde und denen der betroffenen Ausländer. Folgende Abwägungskriterien hatten wir der Behörde

für Inneres nahegelegt: Handelt es sich um eine Tatsachenbehauptung, die in wesentlichen Punkten unwahr ist? (Bloße Meinungsäußerungen von Redakteuren rechtfertigen keine Offenbarung personenbezogener Daten.) Ist die Falschmeldung geeignet, den Ruf der Behörde erheblich zu beeinträchtigen? Ist die Richtigstellung durch die Offenbarung personenbezogener Daten Betroffener geeignet und notwendig, um der Rufschädigung entgegenzuwirken?

Im September 2000 erhielten wir den angekündigten Entwurf für eine „Medienleitlinie der Ausländerbehörde". Neben Ausführungen zur presserechtlichen Auskunft und Gegendarstellung enthielt er einen Abschnitt „Gleichwertige Maßnahmen". Mit diesem Begriff wurden insbesondere spontane Presseerklärungen der Ausländerbehörde als Reaktion auf Presseberichte bezeichnet und jenseits des Presserechts für zulässig erklärt. Die zuvor für Gegendarstellungen beschriebenen Abwägungskriterien werden auf diese „gleichwertigen Maßnahmen" erstreckt. Da auch andere Abschnitte des Entwurfs aus unserer Sicht datenschutzrechtlich verbesserungsbedürftig waren, fiel unsere Stellungnahme vom Oktober 2000 insgesamt kritisch aus. Seitdem haben wir trotz mehrfacher Erinnerungen von der Behörde für Inneres nichts mehr zur Medienleitlinie gehört. Dies überrascht um so mehr, als die Bürgerschaft auf ihrer Sitzung am 4./5. April 2001 folgenden Beschluss fasste:

Die Bürgerschaft begrüßt, dass zu diesem Themenkomplex (Öffentlichkeitsarbeit der Ausländerbehörde) eine Medienleitlinie erarbeitet wird, und bittet, ihre Fertigstellung nun zügig zu realisieren. Dabei sind die Belange des Datenschutzes angemessen zu berücksichtigen. Insbesondere sollten sich klarstellende Äußerungen der Behörden auf das notwendige Maß beschränken.

16.3.2 Ein weiterer Fall

Wie dringend eine Leitlinie für datenschutzgerechte Öffentlichkeitsarbeit der Behörde ist, zeigte ein weiterer Fall: Am 27. Oktober 2000 berichtete die tageszeitung (taz) darüber, dass ein mit Namen genannter Armenier ohne seine Familie von der Ausländerbehörde zur Abschiebung abgeholt und dann im Gefängnis Holstenglacis untergebracht worden sei. Nach dem Text der taz „setzte die Ausländerbehörde sich über die Koalitionsvereinbarung hinweg", die vorsehe, bei Abschiebungen grundsätzlich die Einheit der Familie zu wahren. Als Reaktion auf diesen Artikel veröffentlichte die Behörde am selben Tag eine Pressemitteilung, in der sie mit ergänzenden personenbezogenen Angaben zu der ausländischen Familie begründete, warum die Koalitionsvereinbarung, die auch Ausnahmen vorsehe, eingehalten wurde. Die meisten der von der Ausländerbehörde offenbarten Daten – zweimalige illegale Einreise, Nichterscheinen bei einem Ausreisetermin, Vorlage eines ärztlichen Attests, Geburt des dritten Kindes 1999, eine Weigerung, Deutschland zu verlassen – waren für die Argumentation keineswegs zwingend.

In unserer Stellungnahme machten wir deutlich, dass die Datenoffenbarung selbst dann den Datenschutz verletzte, wenn man den als zu weit kritisierten Entwurf der Medienleitlinie zugrunde legt: Die offenbarten Daten korrigierten keine falschen Tatsachenbehauptungen, sondern stützten nur die eigene rechtliche Bewertung. Erst nach Erinnerung erhielten wird dreieinhalb Monate später die erstaunliche Antwort der Behörde für Inneres: Die Angelegenheit habe zu einer Kleinen Anfrage in der Bürgerschaft geführt, die Offenbarung stütze sich deswegen auf die Befugnisnorm des § 13 Abs.2 Nr. 8 HmbDSG. Damit behauptete die Behörde für Inneres, die Datenoffenbarungen in der Presseerklärung hätten der Bearbeitung einer Kleinen Anfrage „gedient“ und überwiegende schützenswerte Interessen der ausländischen Familie hätten nicht entgegengestanden. Die Kleine Anfrage wurde jedoch erst am 7. November 2000 gestellt (10 Tage nach der Presseerklärung) und war vorher nur angekündigt worden. Eine Abwägung mit den Interessen der Ausländer war weder vorgetragen noch ersichtlich. Wir bedauern den wenig ernsthaften Umgang mit datenschutzrechtlichen Normen in diesem Fall.

16.4 Anfragen beim Sozialamt bei Einbürgerungen

Die Anfragen der Einbürgerungsabteilung der Behörde für Inneres bei den Sozialämtern wurden auf eine neue Grundlage gestellt, die dem Selbstbestimmungsrecht gerecht wird und sich auf die erforderlichen Informationen beschränkt.

Bei der datenschutzrechtlichen Prüfung des interbehördlichen Post- und Aktenaustauschs fiel uns im Januar 2000 ein offen versandtes Formblatt auf, das folgende Erklärung eines Einbürgerungsbewerbers enthielt: „ Ich befreie das Sozialamt von der Pflicht zur Wahrung des Datengeheimnisses gegenüber der Behörde für Inneres – E 5.“ Diese pauschale Einwilligungserklärung genügte den gesetzlichen Anforderungen nicht: § 67 b Abs.2 SGB X fordert eine schriftliche Aufklärung der betroffenen Person über den Zweck der Datenverarbeitung und über die Folgen einer Verweigerung der Einwilligung. § 5 Abs.2 HmbDSG sieht vor, dass Gegenstand, Inhalt und Umfang der erlaubten Datenverarbeitung, die Art der Daten, der Verwendungszweck und die Dauer der Aufbewahrung bezeichnet werden.

Die genaue Bezeichnung der vom Sozialamt abgeforderten Informationen über die Einbürgerungsbewerber ist insbesondere deswegen wichtig, weil Einbürgerungen auf zwei verschiedenen gesetzlichen Grundlagen erfolgen:

– die „Anspruchseinbürgerung“ nach § 85 Ausländergesetz (AuslG), für die nur zu klären ist, ob der Lebensunterhalt „ohne Inanspruchnahme von Sozial- oder Arbeitslosenhilfe“ bestritten wird bzw. ob der Antragsteller den Grund für eine Inanspruchnahme zu vertreten hat,

– die „Ermessenseinbürgerung“ nach § 8 Staatsangehörigkeitsgesetz (StAG), für die zu klären ist, ob der Antragsteller „sich und seine Angehörigen zu ernähren imstande ist“. Bezieht der Bewerber Sozialhilfe, wird die Einbürgerung abgelehnt, auch wenn er die Bedürftigkeit nicht zu vertreten ist. Die Formulierung in § 8 StAG rechtfertigt auch die Nachfrage nach sonstigem Einkommen und anderen staatlichen Leistungen.

Wir schlugen der Behörde für Inneres dementsprechend Formulierungen für zwei neue Einwilligungserklärungen vor. In einem Gespräch im Juni 2000 erläuterten uns Vertreter der Behörde das Einbürgerungsverfahren in der Praxis, insbesondere die persönliche Vorsprache der Bewerber und die dabei zu klärenden Fragen. Wir einigten uns dann auf neue Vordruck-Entwürfe für die Abfrage:

– Die Einwilligungserklärung bezieht sich zunächst auf die vorrangige Mitwirkungspflicht des Antragstellers und erklärt, dass die bisher vorgelegten Unterlagen die für die Einbürgerung notwendigen Klärungen nicht hinreichend deutlich erbracht haben. Dabei wird differenziert zwischen dem Nachweis des Lebensunterhalts ohne Sozial- oder Arbeitslosenhilfe einerseits und der Frage, ob der Einbürgerungsbewerber einen Sozialhilfebezug zu vertreten hat andererseits („Nicht Zutreffendes streichen“). Die betroffene Person willigt dann mit ihrer Unterschrift ein, „dass die Einbürgerungsbehörde bei meinem Finanzamt, Sozialamt und Arbeitsamt (Nicht Zutreffendes streichen) die hierzu erforderlichen Auskünfte einholt.“ Welche Auskünfte erforderlich sind, richtet sich nach der Art des Einbürgerungsantrags.

– In einem eigenen Formblatt werden die für die Einbürgerung nach § 85 AuslG zulässigen Fragen an das Sozial- oder Arbeitsamt festgelegt. Sie beziehen sich z.B. auf das Vetretenmüssen eines Sozialhilfebezuges.

– In einem weiteren Formblatt werden die für die Einbürgerung nach §§ 8 und 9 StAG erheblichen Fragen umschrieben. Sie beziehen sich in erster Linie auf den gegenwärtigen, vergangenen oder zukünftigen Sozialhilfebezug und auf Unterhaltsverpflichtungen.

Nach dieser Einigung erstaunte uns die Zuschrift eines Sozialamts im August 2001, nach der die Einbürgerungsbehörde immer noch die alten Erklärungen benutzte und erklärte, einer Einwilligungserklärung bedürfe es gar nicht, wenn das Sozialamt keine Akte über den Antragsteller habe. Dem widersprachen wir und konnten insofern Konsens mit dem Leiter des Einwohner-Zentralamts herstellen, zu dem die Einbürgerungsabteilung gehört. In Zukunft sollen ausschließlich die verabredeten neuen Formblätter verwendet werden.

17. Verfassungsschutz

17.1 Auskunftsbefugnisse des Bundesamtes für Verfassungsschutz

Die Auskunftsbefugnisse des Verfassungsschutzes müssen rechtsstaatlich strikt begrenzt werden.

Der Gesetzentwurf der Bundesregierung für ein Terrorismusbekämpfungsgesetz sieht vor, dass das Bundesamt für Verfassungsschutz (BfV) bei Kreditinstituten, Finanzdienstleistungsinstituten und Finanzunternehmen unentgeltlich Auskünfte zu Konten, Konteninhabern, Geldbewegungen und Geldanlagen einholen darf. Auskunftsrechte des BfV bestehen nach dem Gesetzentwurf auch gegenüber Luftfahrtunternehmen sowie gegenüber solchen Unternehmen, die geschäftsmäßig Postdienstleistungen, Telekommunikationsdienste und Teledienste erbringen oder daran mitwirken.

Das BfV soll auf diese Weise zur Abwehr schwerwiegender Gefahren in den Bereichen Terrorismus, gewaltbereiter Ausländerextremismus und Spionage in die Lage versetzt werden, Finanzströme nachzuvollziehen sowie Bewegungs- und Kommunikationsprofile zu erstellen. Für die Durchsetzung der Auskunftsersuchen stehen dem Verfassungsschutz gemäß der amtlichen Begründung keine Zwangsbefugnisse zu; das Verwaltungsvollstreckungsgesetz findet keine Anwendung. Eine Befugnis oder Verpflichtung für die Unternehmen, personenbezogene Daten für Auskünfte an das BfV auf Vorrat zu speichern, sieht der Gesetzentwurf nicht vor.

Die Auskunftsregelungen zugunsten des BfV sind datenschutzrechtlich nur dann vertretbar, wenn sie befristet und einer effizienten Erfolgskontrolle (Evaluierung) auf der Grundlage aussagefähiger Berichte unterzogen werden. Auch in den Einzelheiten sind Verbesserungen gegenüber dem Gesetzentwurf notwendig. So sollte die Anordnung eines Auskunftsersuchens nur zulässig sein, wenn die Erforschung des Sachverhalts auf andere Weise (z.B. durch Auswertung allgemein zugänglicher Publikationen) aussichtslos oder wesentlich erschwert wäre (Subsidiaritätsklausel). Auch sollte die Anordnung von Auskunftsersuchen, die sich auf zukünftige Telekommunikation und zukünftige Nutzung von Telediensten beziehen, auf höchstens drei Monate befristet werden (mit der Möglichkeit der Verlängerung bei Fortbestehen der Anordnungsvoraussetzungen). Insoweit empfiehlt sich die am 30. November 2001 beschlossene Nachfolgeregelung zu § 12 des Fernmeldeanlagengesetzes (FAG) als Vorbild. Schließlich sollte das Gesetz vorsehen, dass den zuständigen parlamentarischen Gremien regelmäßig über Mitteilungen an Betroffene oder über die Gründe, die einer Mitteilung entgegenstehen, zu berichten ist.

17.2 Anfrage in Einbürgerungsverfahren

Bei Datenübermittlungen zwischen Einbürgerungsbehörde und Verfassungsschutz ist besondere Sensibilität geboten.

Nach den terroristischen Anschlägen in den USA am 11. September 2001 wird auch in Hamburg die Regelanfrage in Einbürgerungsverfahren praktiziert. Das Einwohner-Zentralamt (EZA) fragt beim Landesamt für Verfassungsschutz (LfV) generell wegen etwaiger Erkenntnisse über Einbürgerungsbewerberinnen und -bewerber an, unabhängig davon, ob hierzu nach den Unterlagen des EZA im Einzelfall Anlass besteht oder nicht.

Die Regelanfrage in Einbürgerungsverfahren ist nach den ausländerrechtlichen Vorschriften zwar zulässig, aber nicht zwingend vorgeschrieben. Ob sie einen wirksamen Beitrag zur Bekämpfung des internationalen Terrorismus leisten kann, erscheint zweifelhaft. Terroristische „Schläfer“ sind weniger an dauerhafter Integration im Gastland als vielmehr an hoher Mobilität interessiert und vermeiden Handlungen, die eine intensive staatliche Überprüfung ihrer persönlichen Verhältnisse zur Folge haben. Von ihnen sind daher keine Einbürgerungsanträge zu erwarten.

Wir regen an, dass der Senat der Bürgerschaft nach Ablauf von zwei Jahren seit Einführung der Regelanfrage einen detaillierten Erfahrungsbericht vorlegt, der im Einzelnen in nicht personenbezogener Form darstellt, ob und inwieweit aufgrund der Regelanfrage verwertbare und für die Einbürgerungsentscheidung erhebliche Erkenntnisse gewonnen wurden, die das EZA bei einer Beschränkung auf Einzelfallanfragen nicht erfahren hätte.

Auch die bis Oktober 2001 durchgeführten Einzelfallanfragen des EZA begegnen datenschutzrechtlichen Bedenken. Bei einer Kontrolle stellten wir fest, dass das EZA seinen Auskunftsersuchen an das LfV in einer Reihe von Fällen umfangreiche Ablichtungen aus den Einbürgerungsakten beigefügt hat. Insbesondere Urteile, Anklageschriften, anwaltliche Schriftsätze in Asylverfahren sowie Bescheide und Anhörungsprotokolle des Bundesamtes für die Anerkennung ausländischer Flüchtlinge (BAFl) wurden dem LfV übermittelt. Daten von Mitbeschuldigten, Zeugen und sonstigen Dritten hatte das EZA vor der Übermittlung nicht anonymisiert. In einzelnen Fällen machte das EZA dem LfV auch Unterlagen über strafrechtliche Verurteilungen zugänglich, die nach dem Bundeszentralregistergesetz (BZRG) im Einbürgerungsverfahren nicht mehr verwertet werden durften.

Wir haben dem EZA im November 2001 mitgeteilt, dass diese Praxis insbesondere unter dem Gesichtspunkt der Erforderlichkeit dringend überprüft werden muss. Das EZA darf dem LfV personenbezogene Daten nur insoweit übermitteln, als sie für eine aktuelle und fundierte fachliche Einschätzung der verwertbaren Erkenntnisse über die Einbürgerungsbewerberin oder den Einbürgerungsbewerber benötigt werden.

18. Verkehr

18.1 Übermittlung von Kfz-Halterdaten an Bezirksämter

Eine Weiterübermittlung von Kfz-Halterdaten, welche die Polizei im zentralen Fahrzeugregister durch Abruf im automatisierten Verfahren erhoben hat, an die Bezirksämter ist als gesetzlich nicht zugelassene Durchbrechung der Zweckbindung rechtswidrig.

Für Übermittlungen aus dem außerordentlich großen und teilweise hoch sensiblen Datenbestand des Zentrales Verkehrsinformationssystems (ZEVIS) an staatliche und andere Stellen gelten differenzierte Datenverarbeitungsregelungen, welche die Zulässigkeit der Übermittlung namentlich von der Art der Daten, den Aufgaben der empfangenden Stelle und insbesondere dem mit der Übermittlung verfolgten Zweck abhängig machen. Nach § 36 Abs. 2 Satz 1 Nr. 1a Straßenverkehrsgesetz (StVG) dürfen Daten aus dem zentralen Fahrzeugregister an Bezirksämter als Verwaltungsbehörden im Rahmen ihrer Zuständigkeit zur Verfolgung straßenverkehrsrechtlicher Ordnungswidrigkeiten durch Abruf im automatisierten Verfahren übermittelt werden. Nach § 36 Abs. 2 Satz 1 Nr. 1 StVG dürfen Datenübermittlungen aus dem zentralen Fahrzeugregister an die Polizei im automatisierten Verfahren dagegen nicht nur im Rahmen ihrer Zuständigkeit zur Verfolgung von straßenverkehrsrechtlichen Ordnungswidrigkeiten, sondern u.a. auch zum Zwecke der Abwehr von Gefahren für die öffentliche Sicherheit erfolgen.

Wird ein Kraftfahrzeug unbefugt abgestellt, so ist damit auch dann, wenn kein Verkehrshindernis entsteht, wegen Verstoßes gegen die wegerechtlichen Sondernutzungsvorschriften eine Gefahr für die öffentliche Sicherheit verbunden, für deren Abwehr die Bezirksämter zuständig sind. Für diesen Zweck der Gefahrenabwehr gestattet § 36 Abs. 2 Satz 1 Nr. 1a StVG den Bezirksämtern jedoch nicht den automatisierten Abruf der Kfz-Halterdaten aus dem zentralen Fahrzeugregister.

Ein Bezirksamt versuchte, dieses gesetzliche System von Abrufbefugnis und Zweckbindung wie folgt zu unterlaufen: Es bat die Polizei darum, im Rahmen ihrer Befugnis nach § 36 Abs. 2 Satz 1 Nr. 1 StVG die unbekannten Daten der Halter von unbefugt abgestellten Kraftfahrzeugen automatisiert beim zentralen Fahrzeugregister abzurufen und diese Daten dann an das Bezirksamt zu übermitteln, damit dieses – und nicht etwa die Polizei – im Rahmen seiner Zuständigkeit für die Gefahrenabwehr die notwendigen Schritte zur Beendigung der unerlaubten Sondernutzung ergreifen könnte.

Im Einvernehmen mit der Polizei haben wir das Bezirksamt auf folgendes hingewiesen: Zwar darf die Polizei nach § 36 Abs. 2 Satz 1 Nr. 1 StVG Halterdaten automatisiert aus dem zentralen Fahrzeugregister abrufen, wenn sie sie für

ihre eigenen Maßnahmen der Gefahrenabwehr nutzen will. Würde die Polizei dagegen Halterdaten aus dem zentralen Fahrzeugregister abrufen, obwohl sie gar nicht zum Zwecke der polizeilichen Gefahrenabwehr oder einem anderen in § 36 Abs. 2 Nr. 1 StVG genannten Zwecke tätig werden will, sondern ihr Abruf nur zwecks Übermittlung dieser Daten an ein Bezirksamt für dessen Aufgabe der ordnungsbehördlichen Gefahrenabwehr erfolgen soll, so verstieße sie damit gegen die in dieser Vorschrift enthaltene Zweckbindung. Auf diese Weise würde zugleich die Differenzierung zwischen § 36 Abs. 2 Satz 1 Nr. 1 einerseits und Nr. 1a StVG andererseits unterlaufen.

In Fällen des unbefugten Abstellens von Kraftfahrzeugen stehen dem Bezirksamt für die Ermittlung der Halterdaten als Möglichkeiten generell Anfragen bei der jeweils örtlich zuständigen Kfz-Zulassungsstelle und beim Kraftfahrtbundesamt zur Verfügung, zum Zwecke der Gefahrenabwehr jedoch nicht der „kurze Dienstweg“ der Halterdaten-Anfrage bei der Polizei.

19. Polizei

19.1 Terrorismusbekämpfungsgesetze

Trotz Verbesserungen gegenüber einem ersten Entwurf räumt der Regierungsentwurf des Terrorismusbekämpfungsgesetzes auch Polizeibehörden weitreichende Datenverarbeitungsbefugnisse ein. Dadurch wird die informationelle Selbstbestimmung in einem Maße eingeschränkt, das zu einem großen Teil durch die Belange der Terrorismusbekämpfung weder veranlasst noch gerechtfertigt ist.

Die terroristischen Anschläge in den USA vom 11. September 2001 führten rasch zu weitreichenden Aktivitäten des Bundesgesetzgebers. Nach der zügigen Verabschiedung des sog. ersten Sicherheitspakets mit Neuregelungen im materiellen Strafrecht und Vereinsrecht befindet sich bei Redaktionsschluss nunmehr das wesentlich umfassendere und mit massiven Eingriffen in die informationelle Selbstbestimmung der Bürger verbundene Gesetz zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz) im Gesetzgebungsverfahren.

In der Absicht, terroristische Gewalt effektiv und erfolgreich verhindern und bewältigen zu können, will die Bundesregierung neben den Nachrichtendiensten sowie den Ausländer- und Asylbehörden vor allem auch der Polizei erhebliche zusätzliche Eingriffs- und Datenverarbeitungsbefugnisse einräumen. Sie verfolgt mit dem Entwurf die Absicht, einen intensiveren polizeiinternen Informationsaustausch und eine enge Zusammenarbeit der Polizei mit allen übrigen Sicherheitsbehörden einschließlich der Ausländerbehörden zu ermöglichen und eine engere Verzahnung der verschiedenen Datenbestände der einzelnen Behörden zu gestatten.

Auf teilweise erfolgreiche Kritik ist die noch im Oktober 2001 im Referentenentwurf des Bundesinnenministeriums vorgesehene neuartige Befugnis für das Bundeskriminalamt (BKA) gestoßen, von sich aus zur Feststellung tatsächlicher Anhaltspunkte für eine Straftat initiativ zu werden. In einer Entschließung vom 25. Oktober 2001 haben die Datenschutzbeauftragten des Bundes und der Länder diese Regelung aus folgenden Gründen massiv kritisiert: Die geplante Befugnis des BKA, Vorermittlungen ohne Anfangsverdacht im Sinne der Strafprozessordnung (StPO) zu ergreifen, führt zu Eingriffen in das Persönlichkeitsrecht, die weit über das verfassungsrechtlich Zulässige hinausreichen und das bewährte System der Strafverfolgung sprengen. Dies würde die bisher klaren Grenzen zwischen BKA und Verfassungsschutz sowie zwischen Gefahrenabwehr und Strafverfolgung verschieben. Damit würden im Prinzip alle Bürgerinnen und Bürger betroffen sein, ohne dass sie sich auf die Schutzmechanismen der StPO verlassen könnten.

Diese Kritik wurde berücksichtigt. Der vom Bundeskabinett am 7. November 2001 beschlossene Entwurf des Terrorismusbekämpfungsgesetzes verzichtet auf diese Regelung und enthält auch eine Reihe von weiteren Verbesserungen gegenüber dem ursprünglichen Referentenentwurf. Aus der Sicht des Datenschutzes enthält der Entwurf im polizeilichen Bereich allerdings noch folgende gravierenden Mängel:

Durch eine Änderung von § 7 BKA-Gesetz soll das BKA bei sämtlichen öffentlichen und nicht-öffentlichen Stellen ohne nähere Begründung „zur Erfüllung seiner Aufgabe als Zentralstelle ... Daten zur Ergänzung vorhandener Sachverhalte oder sonst zu Zwecken der Auswertung“ erheben dürfen. Damit wird eine Grauzone eröffnet, die zu Vorfeldermittlungen des BKA ohne justizielle Aufsicht führt, die deutlich über die vom Grundgesetz zugelassene unterstützende Zentralstellenfunktion hinausgeht, ferner die Zuständigkeiten der Länder zur Gefahrenabwehr beeinträchtigt und damit Rechtsklarheit vermissen lässt. Wie weit dieser Spielraum definiert wird, wird daran deutlich, dass das BKA trotz einer im BKA-Gesetz fehlenden Rechtsgrundlage über die Rasterfahndung auf der Grundlage von § 7 BKA-Gesetz im Herbst 2001 versucht hat, insbesondere bei Firmen umfangreiche Datenbestände zu erheben und im Rasterungswege maschinell abzugleichen – eine Aufgabe, die die Polizeigesetze den Landespolizeien zuweisen (siehe nachfolgend 19.2).

Die Kompetenz des Bundesgrenzschutzes (BGS) nach § 22 BGS-Gesetz zu anlasslosen Personenkontrollen in einem zudem erweiterten Grenzgebiet soll um die Befugnis erweitert werden, sich Ausweispapiere zur Prüfung aushändigen zu lassen. Eine so nachhaltige Datenerhebung ohne jeglichen Anlass erscheint unverhältnismäßig.

Die Möglichkeiten für eine Rasterfahndung nach Bundes- oder Landesrecht (vgl. nachfolgend 19.2) sollen durch eine Änderung von § 68 Sozialgesetzbuch Zehntes Buch auf die Verarbeitung von Sozialdaten im Rahmen einer solchen Fahndung erweitert werden. Zur Durchbrechung des Sozialgeheimnisses im Rahmen einer Rasterfahndung gibt es keinen tragfähigen sachlichen Grund.

Schließlich sollen vor allen Dingen die Möglichkeiten zum Datenaustausch zwischen den Ausländerbehörden, dem beim Bundesverwaltungsamt geführten Ausländer-Zentralregister (AZR) und den Auslandsvertretungen einerseits sowie Polizeidienststellen (insbesondere dem BKA und den Landeskriminalämtern) andererseits erheblich ausgeweitet werden. So soll eine Änderung des § 16 Abs. 4 AZR-Gesetz Polizeivollzugsbehörden einen weitgehenden Zugriff auf das AZR gestatten und damit die Zweckbindung der dortigen Daten deutlich aufweichen.

Vor allem aber soll der neue § 64a Ausländergesetz einen umfassenden Datenaustausch zwischen den Auslandsvertretungen und Ausländerbehörden einerseits und dem BKA und den Landeskriminalämtern andererseits ermöglichen und dabei den letztgenannten Polizeibehörden die Speicherung und Nutzung aller Daten gestatten, die mit Anfragen von Auslandsvertretungen und Ausländerbehörden übermittelt worden sind, wenn das zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist. Auch damit wird die Zweckbindung der von den erstgenannten Dienststellen im Ausländerbereich erhobenen Daten ausgehebelt.

Diese Kritik am Regierungsentwurf gilt in noch stärkerem Maße für die Entschließung des Bundesrates zur Terrorismusbekämpfung vom 9. November 2001, in der dieser noch weiter gehende Einschränkungen des Rechts auf informationelle Selbstbestimmung fordert. Hinzuweisen ist darauf, dass in einer Expertenanhörung im Innenausschuss des Bundestages massive Kritik an Umfang und Ausmaß der Einschränkungen des Datenschutzes, wie sie im Regierungsentwurf vorgesehen sind, geäußert wurde.

Aus der Sicht des Datenschutzes erscheint es daher dringend geboten, den Regierungsentwurf im parlamentarischen Gesetzgebungsverfahren gründlich zu überarbeiten. Dabei sollte auch erwogen werden, die nicht terrorismusbezogenen Vorhaben aus dem Gesetzespaket auszukoppeln und zu einem späteren Termin ohne Zeitdruck erneut in die öffentliche Diskussion und ggf. das Gesetzgebungsverfahren zu bringen. Schließlich erscheint es angezeigt, die Geltung aller neuen Eingriffs- und Datenverarbeitungsbefugnisse zu befristen und nach einigen Jahren zu überprüfen.

19.2 Rasterfahndung in Hamburg

Die nach den Terroranschlägen in den USA vom 11. September 2001 angelaufene Rasterfahndung in Hamburg erfordert eine strikte Beachtung der Belange des Datenschutzes und macht die grundsätzliche Problematik dieses polizeilichen Handlungsinstruments deutlich.

Kurz nach den Terroranschlägen in den USA vom 11. September 2001 entwickelte sich bundesweit die Tendenz, zur Verhütung künftiger Anschläge auf polizeirechtlicher Grundlage Rasterfahndungen durchzuführen. Diese waren bislang in Hamburg allein auf der Grundlage von § 98a Strafprozessordnung (StPO) zur Aufklärung von Verbrechen und Ergreifung der Täter durchgeführt worden (vgl. 15. TB, 15.2). Bei der polizeirechtlichen Rasterfahndung gemäß § 23 des Gesetzes über die Datenverarbeitung der Polizei (PolDVG) geht es dagegen um die Verhütung künftiger Straftaten. Die Vorschrift sieht – anders als andere landesrechtliche Regelungen – eine Information des Hamburgischen Datenschutzbeauftragten erst nach Abschluss der Maßnahme vor.

Am 19. September 2001 ordnete der damalige Innensenator eine Rasterfahndung zur Verhinderung weiterer Anschläge durch islamistische Terroristen an. Dabei geht es – wie auch in den Medien ausführlich berichtet wurde – vorrangig um die rechtzeitige Enttarnung von sog. Schläfern, also Personen, die längere Zeit gänzlich unauffällig leben oder gelebt haben und dann terroristische Gewalttaten begehen. Anhand der Kriterien in der Anordnung hat die Polizei u. a. aus meldebehördlichen Datenbeständen sowie von Hamburger Hochschulen die dortigen Daten über männliche ausländische Studenten einer bestimmten Altersgruppe angefordert. Anschließend rasterte die Polizei in einem maschinellen Abgleich die angelieferten Datenbestände. Dabei wurden allein die Personen herausgefiltert, die sämtliche in der Anordnung genannten Kriterien erfüllten und als Trefferfälle bezeichnet werden.

Bei mehreren im Herbst 2001 – insbesondere bei der Polizei – erfolgten Überprüfungen der Rasterfahndung konnten wir feststellen, dass aufgrund der Anordnung von den Dienststellen die sehr großen betroffenen Datenbestände überwiegend sorgfältig angefordert, angeliefert, aufbereitet und abgeglichen wurden. Von der Polizei sind keine Sozialdaten in den Rasterabgleich einbezogen worden.

Allerdings ist zu beachten, dass die Datenverarbeitung im Rahmen der Rasterfahndung nur auf Grund dieser Anordnung vom 19. September 2001 zulässig war, bis diese durch die weitere Anordnung des Innensenators vom 15. Oktober 2001 geändert und ersetzt wurde. Insbesondere zusätzliche Datenanforderungen und Rasterungskriterien, die nicht durch die zu diesem Zeitpunkt maßgebliche erste Anordnung gedeckt waren, wurden erst ab Wirksamkeit der weiteren Anordnung statthaft. Daten, deren Abgleich erst mit der geänderten Anordnung zugelassen wurde – wie die Staatsangehörigkeit – , durften nur mit in eine Rasterung einbezogen werden, die erst nach der Ände-

rung der Anordnung am 15. Oktober 2001 stattfand. Denn die Schutzfunktion des Behördenleitervorbehalts in § 23 Abs. 4 Satz 1 PolDVG zu Gunsten der Betroffenen gebietet es, dass Änderungen der Anordnung immer erst für die Zukunft wirken. Diese Schutzfunktion würde unterlaufen, wenn man Rasterungen mit noch nicht statthaften Kriterien und damit eine Rückwirkung der Änderungsanordnung zuließe. Zusätzliche Daten, die erst von der Änderungsanordnung erfasst wurden, durften nur als Ergebnis der zweiten Rasterung an andere Stellen übermittelt werden.

Die im Rahmen der ersten Rasterung durchgeführte Datenverarbeitung erweist sich gerade aus dem letzten Grund, teilweise aber auch aus anderen Aspekten als partiell problematisch. Eine Hochschule hat der Polizei ein nicht abgefragtes und von der Anordnung nicht gedecktes personenbezogenes Merkmal geliefert, eine weitere Hochschule ein abgefragtes Kriterium für einen von der Anordnung nur teilweise gedeckten Zeitraum. Dies war nicht korrekt. Die Polizei hat in sachgerechter Weise die insoweit gelieferten „überschüssigen" Daten schon vor Durchführung des ersten Rasterabgleichs aussortiert.

Die Polizei hat andererseits aufgrund der Anordnung vom 19. September 2001 einen Datenbestand, den sie nach der Anordnung bei einer außerhamburgischen Dienststelle anfordern durfte, der aber in gleicher Form bei einer in der Anordnung nicht genannten hamburgischen Dienststelle ebenfalls vorhanden ist, bei letzterer angefordert.

Weiterhin durfte nach der ersten Anordnung bei Personen zwar die Ausländereigenschaft als solche abgefragt und in den Rasterabgleich eingestellt werden, nicht jedoch die Staatsangehörigkeit. Gleichwohl sind der Polizei von Dienststellen Angaben zur Staatsangehörigkeit weitergegeben worden, und die Polizei hat die Staatsangehörigkeit als Rasterungskriterium berücksichtigt.

Diese problematischen Datenverarbeitungen durch die Polizei und insbesondere der erste Rasterabgleich durch sie erfolgten zu einem Zeitpunkt, in dem die Polizei die Änderung der ursprünglichen Anforderungskriterien durch den Innensenator bereits als nötig ansah. Der Innensenator hatte aber die spätere Anordnung vom 15. Oktober 2001 noch nicht getroffen.

Wir haben der Polizei deutlich gemacht, dass § 23 PolDVG nur Datenanforderungen bei den in der Anordnung genannten Dienststellen und mit den in der Anordnung genannten Kriterien sowie deren rasterweise Verarbeitung gestattet, nicht jedoch einen Rasterabgleich, der sich auf Datenbestände und Kriterien erstreckt, die erst in einer künftigen Anordnung des Innensenators enthalten sind.

Wir haben in diesem Zusammenhang auch festgestellt, dass die unter Mitwirkung der Polizei seinerzeit erarbeitete Verfahrensrichtlinie zum Ablauf von Rasterfahndungen nach § 98a StPO (vgl. 15. TB, 15.2), die auch für Rasterfahndungen nach § 23 PolDVG weitgehend sehr hilfreich ist, nicht entsprechend herangezogen worden ist.

Allerdings hat die frühe Berücksichtigung des zusätzlichen, in der ersten Anordnung noch nicht enthaltenen, aber den Personenkreis einschränkenden Merkmals der Staatsangehörigkeit – wie auch von der Polizei beabsichtigt – dazu geführt, dass die Zahl der ohne dieses Kriterium zu erwartenden Trefferfälle sehr deutlich vom vierstelligen in den dreistelligen Bereich reduziert wurde. Vor diesem Hintergrund und angesichts der Tatsache, dass die Hamburger Polizei unter einem erheblichen Erwartungsdruck steht und insbesondere in der Zeit zwischen der ersten und zweiten Anordnung organisatorisch und personell außerordentlich belastet war, haben wir von einer Beanstandung abgesehen. Die Polizei sollte allerdings effektive Verfahren entwickeln, um den Zeitraum zwischen der polizeilichen Erkenntnis, dass die Anforderung aus anderen Datenbeständen und die Aufnahme zusätzlicher Kriterien in die Anordnung sachgerecht sind, und der Änderung der Anordnung durch den Innensenator nachhaltig zu verkürzen.

Die für die erste Rasterung von den Dienststellen an die Polizei gelieferten Daten über Tausende ausländische Studenten, die nicht sämtliche Kriterien für Trefferfälle erfüllten, werden von der Polizei sicher verwahrt und nicht mehr verwendet. Die baldige Vernichtung dieser Daten war bei Redaktionsschluss sicher gestellt.

Im Zuge der bundesweiten polizeilichen Tätigkeit wurde unter der Koordination des BKA eine einheitliche Kriterienliste für die Rasterfahndungen entwickelt. In der weiteren Anordnung vom 15. Oktober 2001 hat daraufhin der damalige Innensenator – wie oben erwähnt – eine Rasterfahndung mit veränderten Kriterien angeordnet. Die daraufhin durchgeführte zweite Rasterung war bei Redaktionsschluss noch nicht abgeschlossen.

Die Trefferfälle werden bei einer Sonderkommission im Landeskriminalamt (LKA) gesondert in einer eigenen Arbeitsdatei verarbeitet. Die Abarbeitung der Trefferfälle erfolgt mit den üblichen polizeilichen Ermittlungsmethoden (z.B. Befragung von Betroffenen). Angesichts der Zahl der Trefferfälle und der Ermittlungskapazität der Sonderkommission wird diese Abarbeitung einen erheblichen Zeitraum in Anspruch nehmen. § 23 Abs. 5 PolDVG schreibt die Benachrichtigung der von weiteren polizeilichen Maßnahmen betroffenen Personen vor, soweit dadurch nicht z.B. die Erfüllung polizeilicher Aufgaben vereitelt oder erheblich gefährdet würde. Wir werden darauf hinwirken, dass die vorgeschriebenen Benachrichtigungen sobald wie möglich erfolgen.

Die Rasterfahndung in Hamburg macht deutlich, dass sie entsprechend den Vorgaben in § 23 Abs. 2 Satz 2 PolDVG ohne die Einbeziehung von besonders sensiblen Daten wie Sozialdaten in den Abgleich durchgeführt werden kann. Deshalb erscheint die im Entwurf des Terrorismusbekämpfungsgesetzes (s.o. 19.1) vorgesehene Änderung von § 68 Sozialgesetzbuch Zehntes Buch (SGB X) nicht notwendig, nach der eine Übermittlung von Sozialdaten künftig zulässig sein soll, wenn sie zur Durchführung einer nach Bundes- oder

Landesrecht zulässigen Rasterfahndung erforderlich ist. Hinzu kommt, das uns keine Anhaltspunkte dafür vorliegen, wonach die bisherige Regelung des § 68 SGB X einer effektiven Aufgabenerledigung der in der Vorschrift genannten Stellen im Wege stand.

Gegen die Einbeziehung landesrechtlich erlaubter Rasterfahndungen in die Vorschrift des § 68 SGB X spricht auch, dass das SGB X bislang ein in sich geschlossenes System von Datenverarbeitungsregelungen enthält. Eine voreilige Öffnung des SGB X kann jedenfalls wegen der hohen Eingriffsintensität der Rasterfahndung nicht die Lösung sein.

Vor allem aber zeigt die aktuelle Rasterfahndung die grundsätzlichen Probleme dieses polizeilichen Instruments (vgl. 15. TB, 15.2) sehr deutlich auf: Der maschinelle Abgleich großer Datenbestände nach bestimmten Rasterungskriterien mit dem Ziel, Trefferfälle herauszufiltern, ist nur dann erfolgversprechend, wenn der jeweilige Persönlichkeitstypus (z.B. Schläfer) sich von den weitaus meisten Menschen durch eine Kombination von Eigenschaften oder Verhaltensweisen abhebt. Nur dann ist die Einbeziehung von Tausenden von gänzlich unverdächtigen Personen, bei denen es sich ja polizeirechtlich um Nichtstörer im Sinne von § 10 des Gesetzes über die Sicherheit und Ordnung handelt, in den Datenabgleich unter Datenschutzaspekten vertretbar.

Für Personen, deren Daten in den Abgleich einbezogen werden, ohne sämtliche Rasterungskriterien zu erfüllen, und von denen die Sonderkommission deshalb keine Kenntnis erhält, dauert dieser Eingriff in ihre informationelle Selbstbestimmung typischerweise bis zur Vernichtung der angelieferten Daten nach Abschluss der jeweiligen Rasterung. Für Personen, die sämtliche Abgleichskriterien erfüllen (Trefferfälle), dauert der Eingriff in die informationelle Selbstbestimmung wesentlich länger, nämlich zumindest bis zu ihrer Befragung oder schriftlichen Benachrichtigung über die getroffenen Maßnahmen nach § 23 Abs. 5 PolDVG. Gerade dann, wenn wie hier diese Benachrichtigung zeitlich weit hinausgeschoben wird, ist der Grundrechtseingriff besonders intensiv.

19.3 Neue Infrastruktur zur polizeilichen Datenverarbeitung

Der Ausbau der Systeme POLAS-neu und COMVOR ist planmäßig vorangekommen, während die Einführung des System INPOL-neu um Jahre zurückgeworfen worden ist.

Beim Ausbau der polizeilichen Informationssysteme konnte das bislang ausstehende Detailkonzept zur Protokollierung verwirklicht werden (vgl. 17. TB, 13.1). Die Polizei hat im Einvernehmen mit uns geregelt, wo die Protokolldateien gespeichert werden und nach welchen Kriterien und bei welchen Anlässen eine Protokollauswertung möglich ist. Bei der Frage, wer die Aus-

wertung vornimmt, konnten wir uns mit dem Vorschlag des Vier-Augen-Prinzips nicht durchsetzen, da für den zweiten Auswerter eigens neue Zugriffsberechtigungen hätte realisiert werden müssen. Den gefundenen Kompromiss, dass nur Personen die Auswertungen vornehmen dürfen, deren besondere Zuverlässigkeit erwiesen ist, halten wir für akzeptabel.

19.3.1 POLAS-neu

Beim polizeilichen Auskunftssystem der Hamburger Polizei POLAS-neu hat die Polizei im Herbst 2000 im Einvernehmen mit uns die Errichtungsanordnung für die Personendatei POLAS-neu in Kraft gesetzt. Zu deren zentralen Elementen gehört das neue Berechtigungskonzept mit erweiterten Zugriffsrechten, das die informationstechnische Konsequenz aus der organisatorisch weitgehend vollzogenen Verschmelzung von bisherigen Polizeirevieren und Kriminalkommissariaten zu Polizeikommissariaten und dem damit einher gehenden immer stärker spartenübergreifenden Einsatz von Polizeivollzugsbeamten (insbes. Schutz- oder Kriminalpolizisten) zieht (vgl. 17. TB, 13.1.1). Mit der Errichtungsanordnung ist in POLAS-neu erstmals eine abruffähige Lichtbildkomponente eingeführt worden (vgl. nachfolgend 19.4).

19.3.2 COMVOR

Im Rahmen des Verfahrens zur computergestützten Vorgangsbearbeitung COMVOR sind die Vorgangsbearbeitung mit Formularen und insbesondere die Indexdatei flächendeckend eingeführt (vgl. 17. TB, 13.1.2). Auf Büroarbeitsplätzen der Hamburger Polizei (vor allem in den Polizeikommissariaten und im Landeskriminalamt) ist polizeiliche Sachbearbeitung und Informationsverarbeitung inzwischen ohne COMVOR nicht mehr möglich. Im Frühjahr 2000 hat die Polizei die Errichtungsanordnung für die Indexdatei COMVOR-F in Kraft gesetzt, die die mit uns vereinbarten Vorkehrungen zum Datenschutz und zur Datensicherheit (vgl. 17. TB, 13.1.2) enthält. In der bis zuletzt strittigen Frage der Dauer der Speicherung von Kindern in COMVOR-Index konnten wir uns mit dem Bestreben, die Speicherungsdauer bei beschuldigten Kindern generell auf zwei Jahre zu begrenzen, nicht durchsetzen. Als vermittelnde Lösung hat die Polizei vorgeschlagen, den Zugriff auf die für fünf Jahre gespeicherten Daten von beschuldigten Kindern nur Ermittlern und Sachbearbeitern (z. B. in den Kommissariaten) einzuräumen. Damit bleibt der großen Mehrzahl der hamburgischen Polizeivollzugsbeamten der Zugriff auf diese sensiblen Kinderdaten verwehrt. Wir halten diesen erzielten Kompromiss für vertretbar.

In Zukunft wird die mit uns abzustimmende Inbetriebnahme von Schnittstellen zwischen dem polizeilichen Verfahren COMVOR und den automatisierten Verfahren anderer Dienststellen im Mittelpunkt stehen. Von besonderer Bedeutung ist dabei die stufenweise Inbetriebnahme der Schnittstelle zwischen COMVOR und dem staatsanwaltschaftlichen Verfahren MESTA (vgl. nachfolgend 20.2).

19.3.3 INPOL-neu

Die sehr ambitionierten Pläne des vom Bundeskriminalamt betriebenen Projektes zur Ersetzung des derzeitigen bundesweiten Informationssystems der Polizei (INPOL-aktuell) durch INPOL-neu wurden im Berichtszeitraum zunächst weiter verfolgt (vgl. 17. TB, 13.1.3). Noch Anfang 2001 war eine Inbetriebnahme zentraler Komponenten von INPOL-neu und insbesondere die Migration (Übernahme) von Verbunddateien zwischen dem BKA und den Landespolizeien von INPOL-aktuell nach INPOL-neu im Jahre 2001 vorgesehen. Ein Absturz des Systems im Rahmen des Probebetriebes im April 2001 machte jedoch diverse gravierende Fehler deutlich, die den ganzen technischen Ansatz in Frage stellen und eine externe Überprüfung erforderlich machen.

Angesichts der aufgetretenen großen technischen Probleme und der sich daraus ergebenden Ungewissheit, ob das System überhaupt bis Ende 2003 starten könne, ist von Seiten der Innenministerkonferenz dem Hersteller eine Frist bis Ende 2001 gesetzt worden, die Schwierigkeiten zu beheben. Sollte das System auch dann nicht korrekt arbeiten, wird die Innenministerkonferenz die schwerwiegende Frage erörtern, ob trotz der Investitionen in Höhe eines dreistelligen DM-Millionenbetrages die bisherigen Planungen aufgegeben und durch einen völlig neuen technischen Ansatz ersetzt werden sollen.

Die Probleme mit INPOL-neu machen beispielhaft deutlich, dass die effektive polizeiliche Nutzung von Informationen gerade durch technische Probleme und durch möglicherweise überfrachtete technische Konzepte – allein das Fachkonzept für INPOL-neu war ursprünglich 6.000 Seiten stark – nachhaltig beeinträchtigt werden kann. Dagegen scheitert die für die effektive polizeiliche Aufgabenerfüllung erforderliche Datenverarbeitung nur selten an datenschutzrechtlichen Bedenken. So steht der nach den Anschlägen vom 11. September 2001 geforderten Effektivierung der Fahndung gerade nach Terroristen primär entgegen, dass INPOL-aktuell hierfür unzureichend ausgelegt ist und die Inbetriebnahme von INPOL-neu sich aus den geschilderten technischen Gründen zumindest erheblich verzögern wird.

19.4 Lichtbildkomponente in POLAS

Der dezentrale Zugriff in den Kommissariaten auf die beim Landeskriminalamt (LKA) digital gespeicherten Lichtbilder ist datenschutzrechtlich akzeptabel, weil er eine zuverlässige und rasche Feststellung ermöglicht, ob eine angetroffene Person mit einer in POLAS gespeicherten Person identisch ist.

Wenn über eine Person, die in POLAS aufgenommen ist, eine Kriminalakte existiert, so sind in diesen Fällen die aus erkennungsdienstlichen Maßnahmen herrührenden digitalen Lichtbilder über diese Person in POLAS aufgenommen (vgl. 16. TB, 15.2). Allerdings war im Rahmen von POLAS-Abfragen bis zum Herbst 2000 ein Zugriff auf die in der Kriminalakte der jeweiligen Person vorhandenen digitalisierten Lichtbilder nicht möglich.

Erwies sich bei einer polizeilichen Maßnahme zur Identitätsfeststellung die Beiziehung von Lichtbildern als erforderlich, so musste das örtliche Kommissariat die mutmaßlichen Personalien der angetroffenen Person an die zuständige Fachdienststelle des LKA mitteilen, die dann – sofern vorhanden – ein Foto aus der Kriminalakte der Person per Telefax an das Kommissariat übermittelte. Die Beiziehung der Lichtbilder und vor allem die teilweise mäßige Qualität der auf dem Telefax befindlichen Personenabbildungen dehnten den Zeitbedarf für eine zweifelsfreie Personenidentifizierung und die damit verbundene Freiheitsentziehung des Betroffenen häufig erheblich aus.

Deshalb verfolgte die Polizei seit längerem Tendenzen, Lichtbilder aus erkennungsdienstlichen Maßnahmen in POLAS abruffähig zu speichern und den bislang auf eine Fachdienststelle im LKA begrenzten Zugriff auf diese Lichtbilder hamburgweit auf die örtlichen Kommissariate auszudehnen. Dies ist allerdings datenschutzrechtlich problematisch. Das Erstellen von Lichtbildern ist eine erkennungsdienstliche Behandlung, deren besondere Eingriffstiefe sich z.B. aus den speziellen Regelungen in § 81b Strafprozessordnung (StPO) und § 7 des Gesetzes über die Datenverarbeitung der Polizei ergibt. Indem der Zugriff auf Bilder im zentralen digitalen Lichtbildbestand des LKA auf Beamte in den lokalen Kommissariaten erweitert wird, wird die Eingriffsintensität gegenüber der konventionellen Maßnahme deutlich erhöht. Vor dem Hintergrund dieses intensiven Eingriffs in das Recht auf informationelle Selbstbestimmung ist der Verhältnismäßigkeitsgrundsatz strikt zu beachten.

Bei der Integration der Lichtbildkomponente in den örtlich abfragbaren POLAS-Bestand sind unter unserer Mitwirkung folgende Vorkehrungen zur Gewährleistung des Datenschutzes getroffen worden: Abfragbar sind allein Bilder, die nach § 81b Fall 2 StPO für erkennungsdienstliche Zwecke aufgenommen worden sind. Die Einführung der Lichtbildkomponente ist erst mit unserer Billigung der Errichtungsanordnung für die POLAS-Personendatei eingeführt worden. Dabei gewährleistet die Kombination aus der Zuweisung einer Berechtigung gemäß dem umfangreichen Berechtigungskonzept, der Vergabe einer zugleich personen- und dienstpostenbezogenen Chipkarte und der Verwendung eines individuellen Passwortes ein hohes Datenschutzniveau (vgl. 17. TB, 13.1). Der Zugriff auf digitale Lichtbilder der U-Gruppe (Kriminalaktenunterlagen) von POLAS ist nur über die Eingabe der Personalien der betreffenden Person möglich. Zugleich ist durch Dienstanweisung sichergestellt worden, dass keine Lichtbilder außerhalb von POLAS gespeichert werden, und die Vernichtung von außerhalb von POLAS vorhandenen Bildern geregelt worden.

Bei einer Vorführung im Polizeipräsidium konnten wir uns davon überzeugen, dass die Qualität der bei POLAS-Abrufen angezeigten Bilder aus der Kriminalakte exzellent ist. Sie ermöglichen regelmäßig die zweifelsfreie Feststellung, ob eine angetroffene Person mit einer unter bestimmten Identitätsangaben in

POLAS gespeicherten Person identisch ist, durch die berechtigten Vollzugsbeamten des örtlichen Kommissariats. Damit wird der für die Betreffenden mit dem schweren Grundrechtseingriff einer Freiheitsentziehung verbundene Zeitbedarf für die Identifizierung deutlich reduziert.

19.5 Online-Zugriff des Bundesgrenzschutzes auf Dateien der Hamburger Polizei

Der mit der Verordnung zur Einführung automatisierter Abrufverfahren für den Bundesgrenzschutz (BGS) ermöglichte Online-Zugriff des BGS auf Dateien der Hamburger Polizei ist gesetzeswidrig, soweit dieser Zugriff in seinem eigenen bundespolizeilichen Aufgabenbereich (z.B. als Bahnpolizei) stattfindet.

Im Sommer 2001 unterbreitete uns die Behörde für Inneres den Entwurf einer Verordnung zur Einführung automatisierter Abrufverfahren für den BGS. Durch diese Verordnung – in der letztlich beschlossenen Fassung – wird den in Hamburg tätigen BGS-Beamten ein lesender Zugriff (ohne Änderungsberechtigung) auf drei zentrale Dateien der Hamburger Polizei eingeräumt, nämlich auf die POLAS-Personendatei (vgl. oben 19.3.1 und 17. TB, 13.1.1), die Vorgangsverwaltungsdatei COMVOR-F (vgl. oben 19.3.2 und 17. TB, 13.1.2) und die Gefahrenabwehrdatei Offene Drogenszene (vgl. 14. TB, 15.1.1). Letztere, die ursprünglich nur die Drogenszene in St. Georg betraf, ist seit dem Jahr 2000 hamburgweit eingerichtet.

Soweit die BGS-Beamten in Hamburg zur Unterstützung der Hamburger Polizei bei deren Aufgaben tätig werden, haben wir gegen diesen Online-Zugriff keine Bedenken, da die BGS-Bediensteten hier gemäß den Vorschriften im Bundes- und Landesrecht den Weisungen der Hamburger Polizei unterliegen und eine Kontrolle des Abrufverhaltens durch den Hamburgischen Datenschutzbeauftragten wie gegenüber einer Hamburger Behörde gesetzlich gesichert ist.

Bei der Abstimmung des Verordnungsentwurfs haben wir mehrfach deutlich gemacht, dass es demgegenüber gesetzeswidrig ist, BGS-Bediensteten auch dann den automatisierten Zugriff auf diese drei Dateien der Hamburger Polizei zu gestatten, wenn sie im Rahmen ihrer eigenen bundespolizeilichen Aufgaben, z.B. als Bahnpolizei, tätig werden.

In den drei umfangreichen Dateien ist jeweils ein sehr großer Bestand von Bürgerdaten gespeichert. § 27 Abs. 3 des Gesetzes über die Datenverarbeitung der Polizei (PolDVG) schließt nach unserer Auffassung den umfassenden Zugriff des BGS auf die drei genannten Dateien aus. Nach dieser Vorschrift darf die zuständige Behörde (nur) „zur Erfüllung von Aufgaben, die nicht nur örtliche Bedeutung haben, mit anderen Ländern und mit dem Bund einen Datenverbund vereinbaren, der eine automatisierte Datenübermittlung ermöglicht."

Die drei Dateien enthalten personenbezogene Daten mit zumeist auf Hamburg begrenzter und damit lediglich örtlicher Bedeutung – bis hin zu Angaben über Geschädigte und Zeugen bei Bagatelldelikten. Eine gesetzliche Grundlage dafür, dass diese Daten durch automatischen Abruf aus der Verfügungsgewalt der Hamburger Polizei hinausgelangen, gibt es nicht.

Mit § 11 Abs. 2 Hamburgisches Datenschutzgesetz (HmbDSG) unvereinbar ist die verordnungsweise Zulassung von Online-Zugriffen, die nicht der Kontrolle durch den Hamburgischen Datenschutzbeauftragten unterliegen. Denn nach der amtlichen Begründung sichert § 11 Abs. 2 Satz 2 HmbDSG dessen Unterrichtung, damit sogleich oder auch später eine datenschutzrechtliche Kontrolle durchgeführt werden kann. Zu den Stellen, die gemäß § 23 HmbDSG der Kontrolle durch den Hamburgischen Datenschutzbeauftragten unterliegen, gehört der BGS nicht.

Der Bundesbeauftragte für den Datenschutz (BfD) kann nach seiner und unserer Auffassung das Abrufverhalten des BGS etwa als Bahnpolizei nicht auf die Vereinbarkeit mit dem Landesrecht (z. B. dem PolDVG) überprüfen. Zudem ist die Prüfung des BfD, ob die Abrufpraxis des BGS hier mit dem Bundesrecht vereinbar ist, dadurch erschwert, dass die Abrufe nicht beim BGS, sondern bei der Hamburger Polizei protokolliert werden.

Trotz unserer eindringlichen Kritik hat der damalige Senat am 18. September 2001 die Verordnung insoweit unverändert beschlossen. Daraufhin haben wir am 18. Oktober 2001 die Anwendung der Verordnung förmlich beanstandet, soweit diese für den BGS einen automatisierten Abruf der dort genannten Dateien der Polizei Hamburg auch im Bereich der originären bundespolizeilichen Aufgaben des BGD zulässt. Nach der Zurückweisung unserer Kritik durch den damaligen Innensenator am 29. Oktober 2001 werden wir uns weiter um eine datenschutzkonforme Anwendung der Verordnung bemühen.

19.6 DNA-Datei

Molekulargenetische Untersuchungen zur Identitätsfeststellung in künftigen Strafverfahren sind ohne richterliche Anordnungen auf der Grundlage von Einwilligungen der Betroffenen allenfalls dann hinnehmbar, wenn schon vor der Einwilligung unter staatsanwaltschaftlicher Mitwirkung eine eingehend begründete Negativprognose getroffen worden ist.

§ 81f Strafprozessordnung (StPO) schreibt für molekulargenetische Untersuchungen zur Identitätsfeststellung in künftigen Strafverfahren sowohl bei aktuell Beschuldigten als auch bei verurteilten Personen stets eine richterliche Anordnung vor. Einwilligungen der Betroffenen sind als rechtliche Grundlage für solche molekulargenetischen Untersuchungen, die zur Einstellung der DNA-Profile der Betroffenen in die bundesweite DNA-Datei führen, ungeeignet.

Abweichend hiervon hatte im Oktober 1999 erstmals eine Große Strafkammer des Landgerichts richterliche Anordnungen als entbehrlich bezeichnet, wenn die Betroffenen zuvor in die molekulargenetische Untersuchung eingewilligt hatten (vgl. 17. TB, 13.3). Dieser Auffassung von der Anwendbarkeit der Einwilligungsregelung haben sich in der Folgezeit alle Großen Strafkammern des Landgerichts Hamburg, die über diese Frage zu entscheiden hatten, angeschlossen.

Wir halten diese gefestigte Rechtsprechung des Landgerichts Hamburg, die im Ergebnis auch von einigen außerhamburgischen Landgerichten vertreten wird, auch im Hinblick auf die klare Regelung in § 5 Abs. 2 Hamburgisches Datenschutzgesetz (HmbDSG) für verfehlt, nach der die vorherige umfassende Aufklärung des Betroffenen und die Freiwilligkeit der Einwilligung für die Wirksamkeit der Einwilligungserklärung unabdingbar sind. Betroffene können die Komplexität einer molekulargenetischen Untersuchung und ihre Auswirkungen selbst nach vorheriger Aufklärung kaum überschauen. Gegen die Freiwilligkeit der Einwilligung gerade von Inhaftierten spricht nicht zuletzt, dass diese typischerweise den Eindruck haben werden, ihr Verhalten in der Einwilligungsfrage werde sich positiv oder negativ auf mögliche Vollzugslockerungen für sie auswirken (vgl. 17. TB, 13.3).

Gleichwohl bleibt die von uns für nicht sachgerecht gehaltene landgerichtliche Rechtsprechung zur Einwilligungsfrage in Hamburg maßgeblich. In intensiven Verhandlungen mit der Justizbehörde, der Behörde für Inneres, der Staatsanwaltschaft Hamburg und der Polizei haben wir uns deshalb nachdrücklich für einen auch ohne richterliche Anordnungen effektiven Datenschutz eingesetzt.

Zum einen sind die Anschreiben an die betroffenen Beschuldigten nach § 81g StPO und Verurteilten bzw. Gleichgestellten nach § 2 DNA-Identitätsfeststellungsgesetz (DNA-IFG) und die Einwilligungsformulare für die Betroffenen so ausgestaltet worden, dass sie namentlich den Gang des Verfahrens, die Auswirkungen der Einwilligung und den Kreis der auf die Daten in der DNA-Datei zugriffsberechtigten Stellen so nachvollziehbar wie möglich darstellen. Vor allem wird das Verbot nachteiliger Folgen aus der Verweigerung einer Einwilligung sowie die Möglichkeit zum Widerruf der Einwilligung hervorgehoben. Zum anderen haben wir den Behörden deutlich gemacht, dass die Einwilligung der Betroffenen erst dann eingeholt werden darf, wenn zuvor die Negativprognose gestellt worden ist, gegen sie würden auch künftig Strafverfahren zu führen sein und hierfür sei die Speicherung des DNA-Profils erforderlich.

Wir haben deutlich gemacht, dass diese Negativprognose angesichts der sehr komplexen Gesetzes- und Rechtsprechungslage eine juristische Beurteilung erfordert, die sachgerechterweise von der Staatsanwaltschaft vorzunehmen ist. Die mehrköpfige ständige „Ermittlungsgruppe (EG) DNA“, die bei der Polizei zur Abarbeitung der mehr als 20.000 Altfälle nach § 2 DNA-IFG ein-

gerichtet worden ist und die Ende 2000 ihre Arbeit aufgenommen hat, steht entsprechend unserem Vorschlag unter der Leitung eines turnusmäßig wechselnden Staatsanwalts. Richtschnur für die Arbeit der EG ist die im Sommer 2000 unter Berücksichtigung der Einwilligungslösung geänderte Fachanweisung des Landeskriminalamtes (LKA).

Dass eine frühzeitige vollprofessionelle juristische Negativprognose vor Durchführung der molekulargenetischen Untersuchung unerlässlich ist, haben inzwischen die Entscheidungen des Bundesverfassungsgerichtes vom 14. Dezember 2000 und vom 15. März 2001 deutlich gemacht. Das Bundesverfassungsgericht hat in diesen Entscheidungen materiell hohe Ansprüche an die Negativprognose gemäß § 81g StPO und § 2 DNA-IFG gestellt, gegen die Betroffenen würden auch künftig Strafverfahren zu führen sein. Das Gericht hat außerdem betont, frühere Verurteilungen seien als Grundlage einer Negativprognose um so weniger geeignet, je länger sie zurücklägen. Das Bundesverfassungsgericht hat in jenen Verfahren die Ausgangsentscheidungen, in denen zumeist pauschal und undifferenziert begründete richterliche Anordnungen die molekulargenetische Untersuchung gestattet hatten, durchweg aufgehoben.

19.7 Dateien im IuK-Verfahren CRIME

Die neue Anwendung CRIME bietet technisch die Möglichkeit, Daten einzelner Betroffener in einer Art und einem Umfang zu verarbeiten, die weitreichende Schlüsse auf Persönlichkeit und Lebenswandel zulassen. Deshalb ist eine sorgfältige Risikoanalyse erforderlich.

Ende Juli 2001 trat die Polizei mit dem Vorhaben an uns heran, die neue Anwendung CRIME (Criminal Research Investigation Management SoftwarE) als Grundlage für den Betrieb von Dateien einzuführen. Dateien unter der Anwendung CRIME ermöglichen die Erstellung von Lage- und Gefährdungsbeurteilungen auch weit im Vorfeld möglicher Straftaten, das Erkennen von relevanten Personen, Institutionen, Objekten, Sachen und namentlich Zusammenhängen bei Gefährdungssachverhalten, die Fertigung von Lagebildern und Führungsinformationen sowie die Speicherung und den Nachweis von Bild- und Textmaterial.

Dateien unter CRIME haben also weniger den Zweck, vorhandene Erkenntnisse über eine einzelne Person abfragefähig zur Verfügung zu stellen. Als Analyseinstrumente neuer Art (vgl. 17. TB, 13.2) sollen die Dateien unter CRIME es vielmehr primär ermöglichen, mit Hilfe der dort gespeicherten Angaben durch Recherchen und automatisierte Auswertungen neue Erkenntnisse zu gewinnen. Datenverarbeitung unter CRIME zielt daher vorrangig auf Verdachtsgewinnung und Verdachtsverdichtung ab. Zu diesem Zweck sollen Daten über Sachverhalte und Personen gerade auch in Rollen, die für die bisherige polizeiliche Datenverarbeitung nicht typisch sind (z.B. gefährdete

Personen, potentielle Täter, Gefährder), mit teilweise sehr tiefgehenden und höchst sensiblen Angaben verknüpft werden.

Ein zentrales Element für die mit Dateien unter CRIME intendierten Strukturermittlungen ist dabei das Erkennen und die (auch graphische) Aufzeigung von Verknüpfungen zwischen möglichst vielen Datenobjekten, wobei die Speicherungszwecke angesichts des Vorfeldcharakters der Speicherungen regelmäßig nicht klar definiert sind. Dies führt zwingend zu einem Konflikt zwischen CRIME und zentralen datenschutzrechtlichen Forderungen wie der nach Begrenzung auf überprüfte („harte“) Daten und Datensparsamkeit.

§ 8 Abs. 4 Satz 1 Hamburgisches Datenschutzgesetz fordert u. a. vor der Einführung eines Verfahrens, mit dem personenbezogene Daten verarbeitet werden sollen, eine Risikoanalyse durch die Daten verarbeitende Stelle. Dabei ist im einzelnen aufzuzeigen, welche Risiken für den Datenschutz mit diesem Verfahren verbunden sind und wie diese beherrscht werden können (zur Risikoanalyse beim standesamtlichen Verfahren PASTA s. o., 8.1). Mit den Dateien unter CRIME sind nach Einschätzung der Polizei und nach unserer Auffassung wegen der Vielzahl und Sensibilität der zu verarbeitenden Daten und vor allem wegen der Fülle der möglichen Verknüpfungen erhebliche Gefahren für die Rechte der Betroffenen verbunden.

Bei Redaktionsschluss dauerten die Bemühungen um die einvernehmliche Ausgestaltung einer Risikoanalyse noch an. Dazu gehört insbesondere die Diskussion, ob und ggf. welche spezifischen Schutzmaßnahmen das Risiko eines Schadens, der bei der unrechtmäßigen Datenverarbeitung mit CRIME sehr hoch sein kann, beherrschbar machen oder als tragbar erscheinen lassen können. Das Ergebnis wird Bedeutung für die Arbeit des Landeskriminalamtes (LKA) gerade im Bereich der Strukturermittlungen auf den Gebieten der Rauschgiftdelikte, der organisierten Kriminalität, des polizeilichen Staatsschutzes und der Kapitalverbrechen haben.

Eine komplexe Anwendung wie CRIME erfordert vor der Aufnahme des Echtbetriebs umfangreiche Tests. Die mit uns abgestimmte Fachanweisung der Polizei für die Nutzung von Echtdaten im Testbetrieb schließt sowohl den Testbetrieb mit unverfremdeten personenbezogenen Daten als auch insbesondere durchgängig die Übernahme personenbezogener Daten aus dem sog. Probewirkbetrieb in den späteren Produktionsbetrieb (Echtbetrieb) aus. In Abweichung von diesen Vorgaben möchte die Polizei bei einer CRIME-Datei Tests mit unverfremdeten Personendaten durchführen und bei einer anderen CRIME-Datei die Daten aus dem Probewirkbetrieb nach dessen Abschluss nicht löschen, sondern in den Produktionsbetrieb übernehmen. Wir haben dies als bedenklich bezeichnet.

20. Staatsanwaltschaft

20.1 EUROJUST

Für die Rechtsstellung von EUROJUST als möglicher Vorläufer einer künftigen europäischen Staatsanwaltschaft sind umfassende Datenschutzvorschriften erforderlich.

Der Europäische Rat hat im Herbst 1999 in Tampere die Einrichtung einer gemeinsamen Stelle EUROJUST zur justiziellen Zusammenarbeit beschlossen. EUROJUST soll zur Bekämpfung der schweren organisierten Kriminalität eine sachgerechte Koordinierung der nationalen Staatsanwaltschaften erleichtern und die strafrechtlichen Ermittlungen unterstützen sowie die Erledigung von Rechtshilfeersuchen vereinfachen. Zusätzlich beschloss der Rat im Dezember 2000 die Einrichtung einer vorläufigen Stelle zur justiziellen Zusammenarbeit, PRO-EUROJUST genannt, die am 1. März 2001 ihre Arbeit aufgenommen hat. Diese Stelle soll bis zur Einrichtung von EUROJUST die Zusammenarbeit der Ermittlungsbehörden zur Bekämpfung der schweren grenzüberschreitenden Kriminalität verbessern und die Koordinierung von Ermittlungen anregen und verstärken. Ein Beschluss des Rates über die Einrichtung von EUROJUST soll bis Ende des Jahres 2001 verabschiedet werden.

Die Aufgabenstellung von EUROJUST führt möglicherweise dazu, dass eine europäische Großbehörde heranwächst, die Daten nicht nur über verdächtige Personen, sondern auch über Opfer und Zeugen sammeln soll, und damit zwangsläufig tiefgreifende Eingriffe in Bürgerrechte vornehmen würde. In diesem Falle käme als europarechtliche Grundlage für EUROJUST nur eine Konvention in Betracht, da für Grundrechtseingriffe eine demokratische Legitimation notwendig wäre.

Mit Blick auf die sensiblen personenbezogenen Daten, die von EUROJUST erhoben, verarbeitet und genutzt werden sollen, und unter Berücksichtigung der eigenen Rechtspersönlichkeit von EUROJUST sind umfassende Datenschutzvorschriften erforderlich. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat im Oktober 2001 in einer Entschließung deutlich gemacht, dass die notwendigen Datenschutzvorschriften sowohl Regelungen zur Verarbeitung, Speicherung, Nutzung, Berichtigung und Löschung personenbezogener Daten als auch zum Auskunftsanspruch der Betroffenen sowie zur einer Kontrollinstanz von EUROJUST enthalten müssen. Dabei sind folgende Punkte von besonderer Bedeutung:

Der Informationsaustausch mit Partnern sollte EUROJUST dann erlaubt sein, wenn er zur Erfüllung seiner Aufgaben erforderlich ist. Bei Weiterleitung dieser Daten an Drittstaaten und -stellen ist die Zustimmung des Mitgliedstaates einzuholen, von dem diese Daten geliefert wurden. Sind personenbezogene Daten betroffen, so muss grundsätzlich eine Übereinkunft zwischen EURO-

JUST und der Partnerstelle über den Datenschutzstandard getroffen werden. Der Katalog der personenbezogenen Daten, die automatisiert verarbeitet werden dürfen, ist streng am Maßstab der Erforderlichkeit und an den Aufgaben von EUROJUST zu orientieren. Der geplante Ermittlungsindex sollte so ausgestaltet sein, dass es sich um eine reine Vorgangsverwaltung handelt.

Neben den Vorschriften über die Änderung und Berichtigung von Daten erscheint auch eine Sperrungsregelung erforderlich, die dazu führt, dass Daten unter bestimmten Voraussetzungen nicht gelöscht, sondern lediglich gesperrt werden. Sofern Daten nach Ablauf bestimmter sonstiger Fristen zu löschen sind, z.B. nach Ablauf der Verjährungsfrist einzelner Mitgliedstaaten, sollte sich die Sperrungsfrist bei EUROJUST nach der Frist des Mitgliedstaates richten, in dem sie am kürzesten ist, um eine mögliche Umgehung nationaler Löschungsfristen zu vermeiden. Von hoher Bedeutung sind ferner konkrete Vorschriften zur Datensicherheit.

Wenn EUROJUST Daten verarbeitet, die ursprünglich von einem Mitgliedstaat geliefert wurden, handelt es sich im Ergebnis um Daten von EUROJUST. Insofern ist ein prinzipieller Auskunftsanspruch von Betroffenen gegenüber EUROJUST unverzichtbar. Dieser darf lediglich im Strafverfolgungsinteresse oder aus Gründen des Gemeinwohls nach einer Abwägung mit den Interessen der Betroffenen an einer Auskunftserteilung relativiert werden. Unabdingbar ist eine gemeinsame, unabhängige Kontrollinstanz, deren Entscheidungen bindenden Charakter haben müssen. Den Betroffenen ist ein angemessener Rechtsschutz gegenüber EUROJUST durch eine noch festzulegende nationale oder supranationale Gerichtsbarkeit zu gewähren.

Zur Erfüllung seiner Aufgaben muss EUROJUST Auskünfte über strafrechtliche Ermittlungsverfahren einholen. § 474 Strafprozessordnung in der geltenden Fassung ermöglicht den Ermittlungsbehörden der Bundesrepublik Deutschland keine Beantwortung derartiger Ersuchen. Ferner ist für den Zugriff des deutschen EUROJUST-Mitglieds auf das Bundeszentralregister und auf das Zentrale Staatsanwaltschaftliche Verfahrensregister eine eindeutige gesetzliche Grundlage erforderlich.

20.2 Automation bei der Staatsanwaltschaft

Der weitere Ausbau des automatisierten Verfahrens der Staatsanwaltschaft und insbesondere die Inbetriebnahme der Schnittstellen zu anderen automatisierten Verfahren erfordern eine frühzeitige und umfassende Beteiligung des Hamburgischen Datenschutzbeauftragten.

Im März 2000 ist die Staatsanwaltschaft Hamburg räumlich und sachlich grundlegend neu organisiert worden. Während sie zuvor auf 7 Standorte im Stadtgebiet verteilt war, ist sie nun auf den Bereich Gorch-Fock-Wall/Johannes-Brahms-Platz/Kaiser-Wilhelm-Straße konzentriert. Sie ist nunmehr in einen zentralen Verwaltungsbereich und 7 Hauptabteilungen gegliedert. Die bisher

in den Verfahrensablauf eingebundenen unterschiedlichen Organisationseinheiten (Zentralkartei, Geschäftsstelle, Kanzlei, Kostenbeamte, Strafnachrichtenstelle) sind in Serviceteams zusammengefasst, deren Mitglieder als Einheitssachbearbeiter möglichst viele Aufgaben durchführen.

Das gemeinsam mit den Ländern Schleswig-Holstein, Brandenburg und Hessen entwickelte Verfahren „Mehrländer-Staatsanwaltschafts-Automation" (MESTA) (vgl. 17. TB, 14.1), an dem sich inzwischen auch Nordrhein-Westfalen beteiligt, konnte erst nach der vollständigen räumlichen Konzentration der Staatsanwaltschaft flächendeckend auf den weit mehr als 500 Arbeitsplätzen eingeführt werden. Alle Staats- und Amtsanwälte, Rechtspfleger und Serviceteam-Angehörige verfügen jetzt über einen MESTA-Anschluss und können damit im Rahmen der für sie maßgeblichen Zugriffsrechte (vgl. 17. TB, 14.1) auf einen zentralen Bestand von Personen- und Verfahrensdaten zugreifen. Insbesondere die Vorgangsverwaltung mit dem Zugriff auf das örtliche staatsanwaltschaftliche Verfahrensregister und die in großen Teilen durch die Verwendung von Formularen gekennzeichnete Erstellung von Schriftstücken erfolgen jetzt durchgängig mit MESTA.

Die durch das am 1. November 2000 in Kraft getretene Strafverfahrensänderungsgesetz neu in die Strafprozessordnung (StPO) eingeführten §§ 474 ff. StPO enthalten die seit langem überfälligen bereichsspezifischen Datenverarbeitungs- und Datenschutzregelungen für Strafverfolgungsbehörden und Strafgerichte. In diesem Rahmen fordert § 490 StPO für die Errichtung von Dateien grundsätzlich eine Errichtungsanordnung. Die umfangreiche Errichtungsanordnung für das MESTA-Verfahrensregister der Staatsanwaltschaft enthält in sehr detaillierter Form insbesondere Regelungen über den Umfang der zu speichernden Daten, Speicherungszwecke, Weiterübermittlungen und Datenlöschungen. Sie ist im Herbst 2001 mit uns abgestimmt worden.

Die mit den Umzügen und der Neuorganisation verbundenen erheblichen Mehrbelastungen mögen mit ursächlich dafür gewesen sein, dass seitens der Staatsanwaltschaft im Jahre 2000 die erforderlichen frühzeitigen und umfassenden Informationen an uns über bevorstehende Automationsschritte nicht erfolgten. Im Januar 2001 haben wir bei der Staatsanwaltschaft die Zusicherung erreichen können, dass sie uns in der schon durch die Richtlinie zur Beteiligung des Hamburgischen Datenschutzbeauftragten gebotenen Weise informieren wird, bevor im Rahmen von MESTA weitere Schritte der Automatisierung des staatsanwaltschaftlichen Verfahrens in Betrieb gehen. Gleichzeitig konnte Konsens darüber erzielt werden, dass lesende Zugriffe im Rahmen von MESTA (vgl. 17.TB, 14.1) stichprobenweise protokolliert werden. Wir begrüßen die Bereitschaft der Staatsanwaltschaft hierzu. Im Dezember 2000 ist das Intranet der Staatsanwaltschaft eingeführt worden, das den dort Beschäftigten in einer datenschutzgerechten Weise Zugänge zum Internet ermöglicht.

Im Mittelpunkt der Fortentwicklung von MESTA steht nunmehr die Inbetriebnahme und der Ausbau von Schnittstellen zu anderen automatisierten Verfahren (vgl. 17.TB, 14.1). Nachdem bereits im Vorberichtszeitraum namentlich die Schnittstellen zum Bundeszentralregister und zum Verkehrszentralregister genutzt werden konnten, geht es um die Schnittstellen von MESTA zum polizeilichen Verfahren COMVOR (s.o. 19.3) und zum Zentralen staatsanwaltschaftlichen Verfahrensregister (ZStV).

Nach umfangreichen Erprobungen ist im Herbst 2000 die erste mit uns abgestimmte Komponente der Schnittstelle zwischen MESTA und COMVOR (vgl. 17.TB, 14.1) in Betrieb gegangen. In Verfahren gegen bekannte Beschuldigte (sog. Js-Sachen) werden zwischen Staatsanwaltschaft und Polizei wechselseitig das jeweilige Aktenzeichen sowie Tatzeit, Tatort, Delikt und Beschuldigtendaten ausgetauscht. Ferner übermittelt die Staatsanwaltschaft den Verfahrensausgang an POLAS (s.o., 19.3). Als nächster Schritt ist auch der Austausch der Personendaten von Geschädigten, Anzeigenden und Zeugen geplant. Anschließend soll die Schnittstelle auch für Verfahren gegen unbekannte Beschuldigte (sog. UJs-Sachen) genutzt werden können.

Die Funktionstüchtigkeit der Schnittstelle zwischen MESTA und dem ZStV wurde zunächst von Schleswig-Holstein stellvertretend für die anderen MESTA-Partnerländer getestet (vgl. 17.TB, 14.1). Dabei gestaltete sich die Bewältigung und Reduzierung der zunächst anfallenden Datenflut langwierig. Nachdem der Echtbetrieb der Schnittstelle zwischen MESTA und dem ZStV in einigen anderen Partnerländern bereits begonnen hatte, ist in Hamburg die Betriebsaufnahme der Schnittstelle im Herbst 2001 erfolgt.

Der Datenaustausch erfolgt entgegen unseren Forderungen vorerst unverschlüsselt. In der Frage der datenschutzrechtlichen Anforderungen zum Einsatz automatisierter staatsanwaltschaftlicher Informationssysteme konnte bislang kein Kompromiss im Konflikt zwischen der Justizministerkonferenz und den Datenschutzbeauftragten des Bundes und der Länder in der Frage erzielt werden, ob der Datenaustausch zwischen den Staatsanwaltschaften und dem ZStV verschlüsselt zu erfolgen hat (vgl. 17. TB, 14.1) Ein gewisser, nach unserer Auffassung jedoch nicht hinreichender Sicherheitsstandard wird dadurch erreicht, dass der Datenaustausch mit dem ZStV über eine gesonderte Leitung erfolgt.

Die Justizbehörde ist an uns mit dem Wunsch herangetreten, auch die Einrichtung einer Schnittstelle zwischen der dortigen Gnadenabteilung und MESTA datenschutzrechtlich zu bewerten. Wir haben darauf hingewiesen, dass § 488 Abs. 1 in Verbindung mit § 483 Abs. 1 StPO die Einrichtung einer solchen Schnittstelle nicht zulässt.

20.3 Berichtspflichten bei wohnraumbezogenen Abhörmaßnahmen

Die vorgesehene Berichterstattung durch den Senat an die Bürgerschaft macht das Ausmaß der Grundrechtsbeeinträchtigungen bei wohnraumbezogenen Abhörmaßnahmen (sog. Lauschangriffen) nicht hinreichend deutlich.

Das Gesetz zur Umsetzung von Art. 13 Abs. 6 des Grundgesetzes (GG) vom 18. Juli 2000 (vgl. oben, 2.2.1) verpflichtet zu einer umfassenden Berichterstattung und parlamentarischen Kontrolle über verdeckte Datenerhebungsmaßnahmen aus Wohnungen in Hamburg sowohl bei der Strafverfolgung als auch im präventiv-polizeilichem Bereich (vgl. 17. TB, 14.2). Hinsichtlich der Ausgestaltung der Berichte gerade im Hinblick auf unverdächtige Gesprächsteilnehmer in Wohnungen hat sich der Senat jedoch unserer Rechtsauffassung (vgl. 17. TB, 14.2) nicht angeschlossen. Er wird einen Erhebungsbogen verwenden, der gerade keinen Aufschluss über den von den Überwachungsmaßnahmen nur zufällig betroffenen Personenkreis erlaubt.

Der Senat begründet dies zum einen damit, dass von einer Überwachungsmaßnahme im Rechtssinne nur diejenigen Personen betroffen seien, gegen die sich die Maßnahme richte, nicht jedoch zufällig anwesende Personen, bei denen lediglich eine hinzunehmende Beeinträchtigung vorliege. Zum anderen beruft sich der Senat darauf, unter den zu überwachenden Objekten würden sich voraussichtlich auch solche befinden, die typischerweise von einer Vielzahl wechselnder Personen frequentiert würden, so dass die in diesem Teilbereich allein möglichen Schätzungen zu Verzerrungen und damit zur Unbrauchbarkeit der in den Berichten enthaltenen statistischen Angaben führen würden.

Wir halten beide Argumente für unzutreffend. Das Vorliegen eines Grundrechtseingriffs zu Lasten zufällig anwesender Personen hängt nicht davon ab, dass sich die staatliche Überwachungsmaßnahme gezielt gegen diese Personen richtet. Vielmehr ist der Eingriff deshalb zu bejahen, weil das gesprochene Wort auch dieser Personen ohne ihr Wissen und typischerweise gegen ihren Willen von staatlichen Stellen abgehört wird.

Schwierigkeiten bei der statistischen Zuordnung dürften lediglich bei der Überwachung von Hotel- und Sammelunterkünften mit häufig wechselnden Personen auftreten. Hier halten wir es für ausreichend, wenn diese besonderen Fälle zur Vermeidung statistischer Verzerrungen gesondert ausgewiesen werden und insoweit lediglich die Zahl der überwachten Hotels und Sammelunterkünfte mitgeteilt wird.

Voraussichtlich führt es nur zu geringer Mehrarbeit, wenn neben dem ohnehin anzufertigenden Protokoll eine einfache Strichliste über die Zahl abgehörter zufällig anwesender Personen geführt wird, um den Abgeordneten im Kontrollgremium einen Überblick über die Größenordnung auch im Sinne einer Rechtstatsachenabschätzung zu verschaffen. Die im jeweiligen Bericht an das

parlamentarische Kontrollgremium enthaltene Statistik ist auch deshalb Bestandteil der gesetzlichen Regelung geworden, damit die Abgeordneten einen Eindruck über den tatsächlichen Umfang und die Wirkung akustischer Wohnraumüberwachungsmaßnahmen erhalten.

In unserem Sinne haben die Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung vom 26. Juni 2000 gefordert, dass die effektive parlamentarische Kontrolle von Lauschangriffen durch aussagekräftige jährliche Berichte gewährleistet sein muss. Diese Forderung gilt sowohl gegenüber der Bundesregierung als auch gegenüber dem Senat. Gleichwohl beruhen nunmehr auch die Berichte der Bundesregierung gemäß Artikel 13 Abs. 6 Satz 1 GG für 1999 (Bundestags-Drucksache 14/3998) und 2000 (Bundestags-Drucksache 14/6778) wie zuvor schon derjenige für 1998 (Bundestags-Drucksache 14/2452) auch für Hamburg auf der Verwendung des oben kritisierten Erhebungsbogens. Sie lassen deshalb keine aussagekräftigen Feststellungen über die Zahl der bisher bei Lauschangriffen im Rahmen der Strafverfolgung tatsächlich betroffenen Personen zu.

Der Vorsitzende des Gremiums nach Art. 13 Abs. 6 GG des Deutschen Bundestages hat am 5. Februar 2001 gegenüber dem Bundesbeauftragten für den Datenschutz ausgeführt, dass die Mitglieder dieses Gremiums wie die Konferenz der Datenschutzbeauftragten zu der Auffassung gekommen sind, dass der erste Bericht der Bundesregierung keine effektive parlamentarische Kontrolle ermöglicht. Die Mitglieder des Gremiums haben daher die Bundesregierung zur Mitteilung von gegenüber der bisherigen Berichtspraxis angereicherten Erkenntnissen gebeten. Im Hinblick auf die Bitte des Gremiums hat die Justizministerkonferenz im April 2001 ihren Strafrechtsausschuss mit der Prüfung der erhobenen Forderungen betraut. Die Prüfungen der zuständigen Arbeitsgruppe des Strafrechtsausschusses sind noch nicht abgeschlossen.

Die ohne personenbezogene Daten zu erstellenden Berichte auf den Gebieten der Strafverfolgung und der Gefahrenabwehr sind nach dem Gesetz vom 18. Juli 2000 jeweils gegenüber einem von der Bürgerschaft zu wählenden Gremium zu erstellen. Insoweit wird unseren Vorstellungen entsprochen. In der 16. Wahlperiode sind der Bürgerschaft derartige Berichte noch nicht vorgelegt worden. Zu Beginn der 17. Wahlperiode hat die Bürgerschaft im Herbst 2001 beschlossen, die parlamentarische Kontrolle von akustischen Maßnahmen der Wohnraumüberwachung auf den beiden genannten Rechtsgebieten durch ein einheitliches Gremium ausüben zu lassen.

Das vom Bundesministerium der Justiz initiierte Forschungsvorhaben zur Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation (vgl. 17. TB, 14.2) ist an das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg vergeben worden. Die durch das Strafverfahrensänderungsgesetz 1999 im wesentlichen mit Wirkung vom

1. November 2000 grundlegend novellierte Strafprozessordnung (StPO) enthält für dieses Forschungsvorhaben in § 476 Abs. 2 Satz 2 und Abs. 3 i.V.m. § 477 StPO eine hinreichende bereichsspezifische Datenverarbeitungsregelung.

20.4 Mitteilungen in Strafsachen

Die Übersendung von Anklageschriften an Stellen außerhalb der Strafjustiz wurde für Verfahren, in denen Überwachungen der Telekommunikation oder vergleichbare Maßnahmen durchgeführt wurden, von der Staatsanwaltschaft Hamburg in datenschutzrechtlich vorbildlicher Weise geregelt.

Die von den Landesjustizverwaltungen erlassene Anordnung über Mitteilungen in Strafsachen (MiStra) sieht in Abs. 6 Nr. 4 vor, dass bei Übermittlungen für andere Zwecke als die des Strafverfahrens (z.B. an Ausländerbehörden oder an Dienstvorgesetzte der Angeschuldigten) die Anklageschrift mit dem wesentlichen Ergebnis der Ermittlungen zu übersenden ist, falls nicht eine abweichende staatsanwaltschaftliche Anordnung im Einzelfall ergeht.

Das wesentliche Ergebnis der Ermittlungen soll die Angeschuldigten, die Verteidiger, das Gericht und die Sitzungsvertreter der Staatsanwaltschaft über den Sachstand und die Beweislage, die sich bis zum Abschluss der Ermittlungen ergeben haben, unterrichten und dient damit der Vorbereitung auf die Hauptverhandlung. Je nach Sachverhalt und angeklagter Straftat kann die Darstellung des Ermittlungsergebnisses auch detaillierte Angaben zu den Teilnehmern und Inhalten überwachter Telefonate oder Gespräche in Wohnungen, Einzelheiten zu Rasterfahndungen, Verdeckten Ermittlungen, längerfristigen Observationen usw. enthalten.

Diese datenschutzrechtlich besonders sensiblen Informationen sind zwar im Rahmen des Strafverfahrens bedeutsam, für die Übermittlungsempfänger nach der MiStra hingegen in der Regel nicht von Interesse. Für die Empfänger kommt es vielmehr grundsätzlich allein auf die tatsächliche und rechtliche Würdigung der Staatsanwaltschaft an, die im Anklagesatz Ausdruck findet.

Deshalb haben wir der Staatsanwaltschaft Hamburg empfohlen, abweichend von der MiStra das wesentliche Ergebnis der Ermittlungen nur dann zu übersenden, wenn dies im Einzelfall zur Aufgabenerfüllung des Empfängers erforderlich ist. Die für diese Einschätzung maßgebenden Gründe sollten aktenkundig gemacht werden. Um den Verwaltungsaufwand für die Staatsanwaltschaft in vertretbaren Grenzen zu halten, haben wir unseren Vorschlag auf solche Verfahren beschränkt, in denen Strafverfolgungsmaßnahmen von besonderer Eingriffsintensität durchgeführt wurden. Praktische Bedeutung hat dies insbesondere für Überwachungen der Telekommunikation nach § 100a der Strafprozessordnung (StPO).

Der Leitende Oberstaatsanwalt hat unsere Anregung aufgegriffen und im Mai 2001 eine entsprechende Verfügung erlassen. Die Staatsanwaltschaft hat zur Unterstützung künftiger Datenschutzkontrollen dafür Sorge getragen, dass die von der Verfügung betroffenen Verfahren besonders erfasst werden. Die Staatsanwaltschaft Hamburg hat damit bundesweit Maßstäbe für eine datenschutzfreundliche Mitteilungspraxis in Strafsachen gesetzt.

21 Gesundheitswesen

21.1 Prüfung des Gesundheitsamts Hamburg-Mitte

Die Prüfung ergab u.a. Defizite bei der Verarbeitung von Daten psychisch Kranker; sie führte zu Änderungen von Kommunikationsverfahren und zu zusätzlichen Sicherungsmaßnahmen.

Im Juni 2000 prüften wir ausgewählte Abteilungen des Gesundheitsamts Hamburg-Mitte: die Geschäfts- und Poststelle, den Sozialpsychiatrischen Dienst und die Gutachtenabteilung. Festgestellt wurden Mängel in den folgenden Bereichen:

- Zugangsschutz: Das Reinigungspersonal hatte Zugang zu Klientenakten; Telefaxe mit sensiblen personenbezogenen Daten für die Seuchenbekämpfung oder die Gutachterabteilung kamen in der Poststelle an; Schreiben des Sozialpsychiatrischen Dienstes lagen offen in der Poststelle zum Versand.

- Organisation des Datenschutzes: Es fehlte eine mit dem Datenschutz vertraute, verantwortliche Person und eine aktualisierte Sammlung von Datenschutz-Unterlagen. Die Aktenführung erschwerte eine Umsetzung des Auskunfts- und Akteneinsichtsrechts.

- Erhebung und Nutzung sensibler Daten: Der Sozialpsychiatrische Dienst erfragte beim Klinikum Nord Daten auch von solchen Patienten, die nicht (mehr) zwangsweise untergebracht, sondern freiwillig (weiter) behandelt wurden. Die Daten wurden ohne Einwilligung der Betroffenen für Zwecke der nachgehenden Hilfe genutzt.

- Speicherung sensibler Daten: Es wurden von anderen Dienststellen zugesandte Informationen zu psychisch Kranken entgegengenommen und aufbewahrt, ohne dass dafür eine Zuständigkeit bestand. Das „Eingangsbuch“ in der Gutachtenabteilung mit klientenbezogenen Daten wurde ohne durchgreifenden Grund 10 Jahre aufbewahrt.

- Schweigepflicht: Auskünfte an Polizei und Staatsanwaltschaften erfolgten ohne Prüfung der Anrufer-Identität und gingen z.T. über den rechtlich zulässigen Umfang hinaus.

– Akteneinsichtsrecht: Entgegen der Rechtslage wurde den Patienten eine eigene Einsichtnahme in die Akten des Sozialpsychiatrischen Dienstes grundsätzlich verwehrt.

Die Bemühungen um Mängelbeseitigung nahmen viel Zeit in Anspruch, führten aber zuletzt weitgehend zum Erfolg. Insbesondere wurden folgende Maßnahmen zur Verbesserung des Datenschutzes erreicht:

– Die Aktenschränke wurden den Sicherheitsbedürfnissen angepasst. Es wurden neue abteilungsspezifische Faxgeräte angeschafft.
– Für den Datenschutz wurde ein verantwortlicher Ansprechpartner benannt und der Unterlagenordner überarbeitet und aktualisiert.
– Die Kommunikation mit dem Klinikum Nord zur Nachsorge der psychisch kranken Patienten wurde auf die untergebrachten Patienten beschränkt.
– Die gesammelten Meldungen zu psychisch Kranken, mit denen das Bezirksamt gar nicht in Kontakt stand oder tritt, wurden vernichtet.
– Das „Eingangsbuch“ wird nur noch 2 Jahre aufbewahrt.
– Eine Dienstanweisung verpflichtet die Mitarbeiterinnen und Mitarbeiter,
  – personenbezogene Akten nach Dienstschluss wegzuschließen,
  – ausgehende Post mit personenbezogenen Daten in verschlossenen Umschlägen an die Poststelle zu geben,
  – zugesandte Mitteilungen über Klienten nicht aufzubewahren, wenn keine Zuständigkeit besteht,
  – die Akten in einer bestimmten Weise zu strukturieren und zu paginieren,
  – Patientendaten nicht per Fax oder unverschlüsselt über E-Mail zu übermitteln.

In unserem abschließenden Schreiben an das Gesundheitsamt wiesen wir noch einmal darauf hin, dass die Mitarbeiterinnen und Mitarbeiter der psychiatrischen Dienste bei Anfragen von Polizei und Staatsanwaltschaft sich der Identität der anrufenden Person vergewissern müssen und nur dann Auskunft geben dürfen, wenn die gesetzliche Voraussetzung vorliegt oder begründet behauptet wird. Diese fordert, dass von der betroffenen Person eine erhebliche Gefahr für sich selbst oder andere oder für bedeutende Sachwerte ausgeht.

Auch zum Akteneinsichtsrecht nach § 32 des Hamburgischen Gesetzes über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten mussten wir noch einmal klarstellen, dass (aktuell oder früher) psychisch kranke Personen selbst Einsicht in die Vorgänge des psychiatrischen Dienstes nehmen können, wenn eine „Verständigung mit ihnen möglich“ ist und es sich nicht um Mitteilungen Dritter oder die persönlichen Gesprächsaufzeichnungen der Therapeuten handelt.

21.2 Prüfung des Patientenabrechnungssystems AKTIVA des LBK

Die Prüfung des zentralen Patientenabrechnungssystems AKTIVA des Landesbetriebs Krankenhäuser (LBK) zeigte vor allem Probleme des Zugriffsberechtigungs-Konzepts. Sie führte zu Änderungen technischer und organisatorischer Datensicherungsmaßnahmen.

In Zusammenarbeit mit der betrieblichen Datenschutzbeauftragten des LBK prüften wir im Mai 2001 den LBK-Servicebetrieb Finanzdienstleistungen mit dem Projekt AKTIVA. Dies organisiert zentral das Forderungs- und Rechnungswesen für alle Häuser des Landesbetriebs.

Die Datenverarbeitung von AKTIVA geht aus von der in den einzelnen Krankenhäusern durchgeführten Patientenaufnahme nach SAP IS-H und überträgt die Aufnahme-Stammdaten der Patienten in eine zentrale Datenbank. Auf diese Daten haben die Mitarbeiterinnen und Mitarbeiter des Servicebetriebes Zugriff. In den dezentralen Aufnahmestellen werden zusätzlich abrechnungsrelevante Daten auf einem Papierbogen erhoben und der AKTIVA-Zentrale übersandt.

Auf den Stationen erheben die behandelnden Ärzte die Diagnosedaten und übermitteln sie auf einer „Patientenverlaufskarte“ an das krankenhausinterne AKTIVA-“Doku-team“. Dieses überträgt sie wiederum in die zentrale Datenbank. Die Erfassungsbögen sollen entsprechend unseren Forderungen in Zukunft nur noch 3 Monate nach der Erfassung aufbewahrt werden.

Im Servicebetrieb hatten bei unserer Prüfung zunächst alle ca.15 Mitarbeiterinnen und Mitarbeiter Zugriff auf alle Stamm-, Abrechnungs- und Diagnosedaten aller gegenwärtigen und bereits entlassenen LBK-Patienten. Auf unsere Bedenken hin wurden Gruppen von einzelnen Mitarbeiterinnen und Mitarbeitern gebildet, denen jeweils ein Krankenhaus zugeordnet wurde. Dies wurde in der Zugriffsberechtigung abgebildet. So konnte die jeweilige Zugriffsberechtigung auf einen Bruchteil der bislang zugriffsfähigen Datenmenge begrenzt werden. Die AKTIVA-Mitarbeiterinnen und -Mitarbeiter können darüber hinaus bestimmte Daten wie z.B. die Diagnosen, die der Abrechnung als feststehend vorgegeben bleiben, nur lesen und nicht ändern.

In der Diskussion ist noch, wie lange auf die Patientendaten in AKTIVA zugegriffen werden darf. Einerseits sieht § 14 des Hamburgischen Krankenhausgesetzes vor, dass der Direktzugriff auf die Datenbank nach Abschluss der Behandlung gesperrt wird. Andererseits muss gewährleistet werden, dass bei einer späteren Wiederaufnahme desselben Patienten ein Zugriff auf die früheren Daten wieder möglich wird. Hier ist der LBK auch auf die von SAP IS-H angebotenen bzw. noch zu entwickelnden Funktionalitäten angewiesen.

Während die Einbindung des Verfahrens in das Netzwerk des LBK und der Rechenzentrums-Betrieb keinen Anlass zur Kritik gaben, zeigten sich in der Konfiguration des SAP-Systems einige Schwächen. Der Landesbetrieb hat auf diese Probleme reagiert und eine Reihe von Sofortmaßnahmen ergriffen. Einer umfassenden Revision wird auch das Berechtigungskonzept unterzogen, das im geprüften Zustand den Anforderungen an Rechteminimierung, Transparenz und Administrierbarkeit nicht genügt. Die Abarbeitung dieser Thematik, die vom LBK bereits unabhängig von unserer Prüfung aufgegriffen wurde, wird sich aufgrund ihrer Komplexität noch hinziehen. Wir werden auf eine fristgerechte Umsetzung nach dem vom LBK vorgelegten Zeitplan achten.

21.3 Genomanalyse und Datenschutz

Eine von Hamburg geleitete Arbeitsgruppe der Datenschutzbeauftragten entwickelte einen konkreten Vorschlag zur gesetzlichen Regelung genetischer Untersuchungen. Die Konferenz der Datenschutzbeauftragten beteiligt sich damit an der Diskussion um anstehende Gesetzesinitiativen.

Im Jahre 2000 wurde die Struktur der menschlichen DNA weitgehend entschlüsselt. Dies nahm die Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Oktober 2000 zum Anlass, schon 1989 beschlossene Grundsätze für den Schutz der informationellen Selbstbestimmung bei genetischen Untersuchungen zu bekräftigen und eine gesetzliche Regelung zu fordern. Ferner setzte die Datenschutzkonferenz eine Arbeitsgruppe unter unserem Vorsitz ein, die die datenschutzrechtlichen Konsequenzen der Genomentschlüsselung erörtern und mögliche Schutz-Maßnahmen entwickeln sollte.

Im Dezember 2000 erreichte uns ein ausführlicher Fragenkatalog der Enquete-Kommission „Recht und Ethik der modernen Medizin“ des Deutschen Bundestages zu den Themen Speicherung von Gendaten, Umgang mit Proben für genetische Untersuchungen, Möglichkeiten der Datenschutzkontrolle im Bereich der Gentechnik und anderes – insgesamt 21 zum Teil komplexe Fragen. In Abstimmung mit den anderen Datenschutzbeauftragten übernahmen wir die bundesweite Koordination der Antworten, legten einen ersten Entwurf vor und integrierten die Beiträge aus den anderen Bundesländern zu einer ausführlichen gemeinsamen Stellungnahme. Sie wurde der Enquete-Kommission im Februar 2001 übersandt.

Die ebenfalls im Februar 2001 erstmals tagende Arbeitsgruppe hatte die damalige Vorsitzende des Ethik-Beirats im Bundesgesundheitsministerium, Frau Prof. Dr. Kollek, eingeladen und erfuhr Neues über technische Entwicklungen in der Genforschung. Die Arbeitgruppe beschloss dann, die mehrfach geäußerten datenschutzrechtlichen Forderungen einerseits zu konkretisieren und andererseits auf alle gegenwärtig diskutierten Anwendungsfelder auszu-

dehnen. Anhand der Vorbilder des Gentechnikgesetzes von Österreich und eines entsprechenden Entwurfs aus der Schweiz erarbeitete die Gruppe einen 14-seitigen Regelungsvorschlag, der Grundlage für ein Gesetz sein könnte. In vier ganztägigen Treffen wurden insbesondere die Bereiche „genetische Forschung“ und „heimliche Abstammungstests“, aber auch Probleme der Anonymisierung und der datenschutzrechtlichen Sicht pränataler Diagnostik vertieft erörtert.

Neben allgemeinen Zulässigkeitsbedingungen enthält der Vorschlag besondere Regelungen für genetische Untersuchungen zu medizinischen Zwecken, zur Klärung von Identität und Abstammung, zu Forschungszwecken sowie im Zusammenhang mit Arbeits- und Versicherungsverhältnissen. Außer dem „genetischen Fingerabdruck“ für Zwecke der Strafverfolgung, der bereits in der Strafprozessordnung gesetzlich normiert ist, deckt der Vorschlag die bekannten Anwendungsfelder für genetische Untersuchungen ab. Er betont das Informations- und Entscheidungsrecht der betroffenen Personen und setzt es in Beziehung zu den Erfordernissen in den verschiedenen Fachgebieten.

Die Kernanliegen und Lösungsansätze der Vorschläge sind:

- Stärkung des Selbstbestimmungsrechts durch einen grundsätzlichen Einwilligungsvorbehalt für die Durchführung genetischer Untersuchungen;
- Information und Transparenz für die betroffene Person durch Umschreibung des notwendigen Aufklärungsumfangs;
- Qualität und Sicherheit genetischer Tests durch Arzt- und Zulassungsvorbehalte;
- Schutz von Ungeborenen, Minderjährigen und nicht einsichtsfähigen Personen durch abgestufte Beschränkung zugelassener Untersuchungsziele;
- Gewährleistung des Rechts auf Nichtwissen durch differenzierte Entscheidungs- und Offenbarungsoptionen;
- Verhinderung heimlicher Gentests durch das Gebot der Probennahme direkt durch Arzt oder Labor;
- Verhinderung von missbräuchlicher Nutzung genetischer Erkenntnisse im Arbeitsleben und im Versicherungsverhältnis durch ein grundsätzliches Verbot, von Bewerbern Gentests oder Testergebnisse zu fordern oder entgegen zu nehmen;
- Selbstbestimmung der Betroffenen auch im Forschungsbereich durch einen grundsätzlichen Einwilligungsvorbehalt bei einzelnen Forschungsprojekten und Proben- und Gendatenbanken;
- Sicherung zuverlässiger Pseudonymisierungsverfahren bei Proben- und Gendatenbanken durch externe Datentreuhänder;

– Hilfe für die Betroffenen durch die Pflicht des Forschers, individuell bedeutsame Untersuchungsergebnisse mitzuteilen;

– Absicherung der Regelungen durch die Einführung von Straftatbeständen.

Neben diesen bereichsspezifischen Bestimmungen zu den verschiedenen Zwecken genetischer Untersuchungen wird eine grundlegende Strafnorm im Strafgesetzbuch angeregt, um heimliche Gentests ohne gesetzliche Ermächtigung oder ohne die Einwilligung der betroffenen Person zu unterbinden.

Auf unseren Vorschlag fasste die Datenschutzkonferenz im Oktober 2001 eine weitere Entschließung zum Thema Genomanalyse und übernahm die Regelungsvorschläge der Arbeitsgruppe als Beitrag der Datenschutzbeauftragten für die öffentliche Diskussion und anstehende Gesetzesinitiativen. Wir haben die Vorschläge sowohl den Fraktionen des Bundestags als auch dem Ethikrat, der Enquete-Kommission „Recht und Ethik der modernen Medizin", der Bundesgesundheitsministerin und der Bundesärztekammer zur Berücksichtigung bei ihren zukünftigen Überlegungen zugeleitet und ihre Veröffentlichung im Internet (auch www.hamburg.datenschutz.de) veranlasst. Ein Beitrag in einer Fachzeitschrift zu den Vorschlägen ist verabredet und soll im ersten Quartal 2002 erscheinen.

21.4 Recht auf Einsichtnahme in Patientenunterlagen

Das grundsätzliche Recht der Patienten, die Behandlungsdokumentation ihres Arztes oder Therapeuten einzusehen, wird insbesondere im psychotherapeutischen Bereich nicht durchgehend beachtet.

Eine Reihe von Eingaben betraf auch im Berichtszeitraum wieder das Recht von Patienten, in ihre Behandlungsunterlagen Einsicht zu nehmen. Einzelne Ärzte waren erst nach wiederholter Darstellung von Gesetzeslage und Rechtsprechung bereit, Kopien von Patientenunterlagen auszuhändigen oder Einsicht in die Akten nehmen zu lassen.

In Gesprächen mit Ärzten und Therapeuten zeigte sich, dass vor allem Psychiater zu der Auffassung neigen, therapeutische Unterlagen seien für den Patienten grundsätzlich tabu bzw. eine Einsichtnahme in sie sei in das Ermessen des Therapeuten gestellt. Die Bitte um Akteneinsicht wurde selbst als Symptom für die Fortdauer der psychischen Krankheit gewertet, deren Überwindung durch die Einsichtnahme gefährdet würde. Das gelte auch hinsichtlich bereits abgeschlossener Behandlungen.

Die Rechtslage ist jedoch eine ganz andere: Vorrangig sind die *gesetzlichen* Regelungen des Akteneinsichtsrechts von Patienten zu beachten:

Für den öffentlichen Gesundheitsdienst, also in erster Linie für die Gesundheitsämter, gilt §29 Abs.1 des Gesetzes über den öffentlichen Gesundheitsdienst in Hamburg: „Den Betroffenen ist unentgeltlich Auskunft über die zu ihrer Person gespeicherten Daten zu erteilen und, soweit dies ohne Verletzung schutzwürdiger Interessen Dritter möglich ist, Einsicht in die sie betreffenden Unterlagen zu gewähren."

Für die psychiatrischen Dienste der Bezirke und die psychiatrischen Krankenhäuser gilt speziell §32 des Hamburgischen Gesetzes über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten, der wörtlich dieselbe Regelung enthält, und danach ergänzt: „Der psychisch kranken Person können Auskunft und Einsicht versagt werden, wenn eine Verständigung mit ihr wegen ihres Gesundheitszustands nicht möglich ist." Neben dieser Einschränkung ist kein Platz für eine Verweigerung der Akteneinsicht aus subjektiven fürsorgerischen oder therapeutischen Erwägungen des Arztes oder Psychologen.

Für die in Hamburg niedergelassenen Ärzte gilt zum einen die Berufsordnung, die in §10 Abs.2 ebenfalls vorschreibt: „Der Arzt hat dem Patienten auf dessen Verlangen grundsätzlich in die ihn betreffenden Krankenunterlagen Einsicht zu gewähren. Auf Verlangen sind dem Patienten Kopien der Unterlagen gegen Erstattung der Kosten herauszugeben."

Soweit Patientendaten in Dateien (Praxiscomputer, Karteikartensystem) betroffen sind, gilt daneben das Auskunftsrecht des §34 Bundesdatenschutzgesetz: „Der Betroffene kann Auskunft verlangen über ... die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen ... Die Auskunft ist unentgeltlich ..."

Nur soweit keine gesetzlichen Normen eingreifen oder diese interpretationsbedürftig sind, ist auf die Rechtsprechung zum Behandlungsvertrag und das vertragliche Einsichtsrecht zurückzugreifen. Während das Bundesverwaltungsgericht einer zwangsweise untergebrachten Person ein sehr weitgehendes Einsichtsrecht zugestand, differenziert der Bundesgerichtshof: Der Einsicht unterliegen danach die objektiven physischen Befunde und Berichte über Behandlungsmaßnahmen wie Medikation und Operationen, nicht aber subjektive Wertungen des Arztes. In einem Beschluss vom 16.September 1998 bestätigte das Bundesverfassungsgericht diese Judikatur grundsätzlich. Es forderte aber in jedem Einzelfall eine besondere Abwägung zwischen den betroffenen Interessen. Dies könne durchaus dazu führen, dass sich das Einsichtsrecht auch einmal auf „den sensiblen Bereich nicht objektivierter Befunde" erstreckt.

Diese allgemeinen Rechtssprechungshinweise wurden vom „Bremer Diskussionsforum ‚Charta der Patientenrechte'" im Jahr 2000 konkretisiert. Wir halten dieses von allen wichtigen Akteuren im Bremer Gesundheitswesen getragene Diskussionsergebnis für hilfreich und verallgemeinerbar. Wir haben es der Hamburger Ärztekammer auch als unsere Auffassung empfohlen. Es enthält folgende Feststellungen:

- Behandlungsdokumentationen in Krankenhäusern sind objektiviert und grundsätzlich voll einsichtsfähig.
- Nur bei Gefahr für Leben und Gesundheit des Patienten kommt eine Einsichtsverweigerung in Betracht. Vor einer Verweigerung ist jedoch eine ärztliche Vermittlung des Inhalts der Dokumentation zu versuchen.
- Bei psychotherapeutischen und psychiatrischen Behandlungen hat der Patient einen Anspruch auf Einsichtnahme in folgende Daten und Dokumente:
  - an Dritte versandte Arztbriefe, Gutachten zur Einleitung der Behandlung u. ä.;
  - vor der Behandlung erstellte Befunde, Prognosen und Behandlungsempfehlungen, z.B. gutachtliche Überprüfungen vor Kostenübernahme;
  - Behandlungsdokumentationen nach Abschluss oder Abbruch einer Therapie; hier soll der Therapeut den Patienten vor Einsichtnahme darüber informieren, dass die Einsichtnahme negative Konsequenzen für eine Folgebehandlung haben kann.
- Während einer Psychotherapie ist eine Einsichtnahme in die subjektiven Daten der Dokumentation problematisch, weil sie die Behandlungsstrategie des Therapeuten offenbart und damit gefährdet. Hier kommt eine Vereinbarung zwischen Therapeut und Patient in Betracht, eine neutrale dritte Person Einsicht nehmen zu lassen.
- In jedem Falle sollte der Therapeut mit dem Patienten über das Interesse an der Einsicht und über mögliche Folgen einer Einsichtnahme ein Gespräch führen.

21.5 Forschungsprojekte

Bei verschiedenen medizinischen Forschungsprojekten war entweder die Anonymisierung der Patientendaten bzw. ihre sichere Pseudonymisierung zu gewährleisten oder eine ausreichende Aufklärung der Betroffenen für eine wirksame Einwilligung sicherzustellen.

Im Berichtszeitraum wurden uns folgende Forschungsprojekte bzw. Einzelfragen zur datenschutzrechtlichen Prüfung vorgelegt:

- UKE-Untersuchungen

  - zur Langzeitversorgung bei ambulant betreuten Schlaganfallpatienten,
  - zu Venenleiden,
  - zu „Beziehungsbiographien im sozialen Wandel“,
  - zur Entwicklung der Todesursachen bei Drogenabhängigen,
- die bundesweite, im UKE federführend betreute Heroinstudie,
- Studie des Bernhard-Nocht-Institutes zu genetischen Untersuchungen bei periodischen Fiebersyndromen,
- Studie des Hygiene-Instituts zu Infektionen nach Entlassung aus dem Krankenhaus nach Operationen,
- Folgestudie der Behörde für Arbeit, Gesundheit und Soziales zur epidemiologischen Untersuchung der Bille-Siedlungs-Bewohner,
- mehrere Projekte, für die Daten aus dem Hamburger Krebsregister angefordert wurden,
- Datenbank des Instituts für interdisziplinäre Infektiologie GmbH beim AK St. Georg zur Verminderung des Therapieversagens bei AIDS,
- Serumbank und elektronische Patientenakte beim Institut für klinische Forschung und Entwicklung des Landesbetriebs Krankenhäuser (LBK),
- Seniorenbefragung Stellingen durch das Gesundheitsamt Eimsbüttel,
- Folgestudie zur norddeutschen Leukämie- und Lymphomstudie des Bremer Instituts für Präventionsforschung und Sozialmedizin,
- eine bundesweite private Datenbank mit medizinischen Patientendaten aus Arztpraxen zur Auswertung zu Forschungszwecken,
- Folgen des Widerrufs einer Probanden-Einwilligung bei einer klinischen Studie,
- Multizentrische Studie zur Qualitätssicherung in der Endoskopie,
- Überregionale Untersuchung zur molekularen Epidemiologie, Resistenzsituation und Behandlung von Tuberkulose in Deutschland,
- Telematikplattform für medizinische Forschungsnetze, insbesondere das Kompetenznetzwerk Morbus Parkinson,
- Studie des Deutschen Krebsforschungszentrums zum Röntgenkontrastmittel „Thorotrast“,
- Studie der FU Berlin mit Hamburger Ärzten und einem privaten Hamburger Institut zur Wirkung von Hormonen auf Haut und Haare bei Frauen nach den Wechseljahren.

Neben jeweils spezifischen Fragestellungen ging es aus datenschutzrechtlicher Sicht meist um die Fragen,

- ob von den betroffenen Probanden eine Einwilligung in die Teilnahme am Forschungsprojekt eingeholt werden muss, oder ob eine Aktenanalyse ohne Kenntnis der Betroffenen möglich ist;

- wie und in welchem Umfang die Betroffenen – im Falle der Einwilligungsbedürftigkeit – über das Forschungsprojekt informiert werden müssen;

- wann, wie lange und in welcher Form die medizinischen Daten von den Identitätsdaten der Probanden getrennt und ggf. wieder zusammengeführt werden können (Pseudonymisierung);

- wie bei der Speicherung und Übermittlung von personenbeziehbaren medizinischen Daten die Datensicherheit z.B. durch Verschlüsselungen, elektronische Signaturen, abgestufte Zugriffsberechtigungen und Firewallsysteme technisch gewährleistet werden kann;

- wann – im Falle einer anonymen Datenverarbeitung – tatsächlich davon ausgegangen werden kann, dass die medizinischen Daten einer bestimmten Person nicht mehr zugeordnet werden können.

Den datenschutzrechtlichen Beurteilungsmaßstab bilden Forschungsklauseln in verschiedenen Gesetzen. So enthalten das Hamburgische Krankenhausgesetz, das Hamburgische Gesundheitsdienstgesetz, das Hamburgische Gesetz über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten, das Hamburgische Krebsregistergesetz bereichsspezifische und das Hamburgische Datenschutzgesetz allgemeine, subsidiär heranzuziehende Bestimmungen über die Datenverarbeitung zu Forschungszwecken. Bundesgesetzlich gibt es Forschungsklauseln z.B. im zehnten Buch Sozialgesetzbuch und im Bundesdatenschutzgesetz.

Ohne auf die eher geringen Unterschiede in den einzelnen Regelungen einzugehen, kann festgestellt werden, dass vorrangig die Einwilligung der Probanden in die Teilnahme an einem Forschungsprojekt eingeholt werden soll. Erst wenn dies unmöglich oder unverhältnismäßig aufwendig oder wissenschaftlich nicht vertretbar ist – etwa weil eine Beschränkung auf einwilligende Probanden das Forschungsergebnis gefährdet – kommt die gesetzliche Ermächtigung in der Forschungsklausel für eine Datenerhebung, -speicherung oder -übermittlung in Betracht. Dabei ist regelmäßig abzuwägen zwischen dem öffentlichen Interesse an der Durchführung des Forschungsprojekts – dies ist im Gesundheitsbereich oft groß – und dem Interesse der betroffenen Probanden an der Geheimhaltung ihrer Gesundheitsdaten. Letztere genießen gegenüber anderen personenbezogenen Daten einen erhöhten Schutz, wie die Neufassung des Bundesdatenschutzgesetzes deutlich zeigt.

Die oben beschriebenen Fragestellungen können selten direkt aus den gesetzlichen Grundlagen beantwortet werden, sie sind vielmehr im Rahmen der Abwägung jeweils für das konkrete Forschungsprojekt zu entscheiden. So kommt es bei der Frage, wann eine Datenverarbeitung zu Forschungszwecken als ausreichend anonymisiert oder pseudonymisiert gelten kann, z.B. auch darauf an, welche Daten außer den normalen Identifikationsdaten wie Name, Adresse, Geburtdatum zu einem Wiedererkennen der betroffenen Person beitragen können – etwa die Größe, das Gewicht, die Patientennummer im Krankenhaus, taggenaue Aufnahme-, Operations-, Entlassungs- und andere Termine, Kinderzahl, Staatsangehörigkeit u.a. Zu klären ist auch, ob der Empfänger der Daten über eigene Datenbestände zu den Probanden verfügt, die Zusatzwissen zur Re-Identifizierung darstellen können.

Diese Fragen spielen eine große Rolle bei den immer „beliebter" werdenden Proben- und Datenbanken „auf Vorrat": Patientendaten werden gesammelt, um sie Instituten, Arzneimittelunternehmen oder auch Versicherungen zur wissenschaftlichen Auswertung nach ihren eigenen Vorstellungen anzubieten. So gründete der LBK eigens für diesen Zweck das Institut für klinische Forschung und Entwicklung Ikfe, nun umbenannt in „proresearch", um auch ausländischen Kunden die Instituts-Aufgabe deutlich zu machen. Diese Daten- und Probenpools werden nicht zuletzt und zunehmend auch für genetische Analysen genutzt. Um so wichtiger ist aus unserer Sicht die Sicherstellung der Anonymisierung oder Pseudonymisierung der gesammelten Daten.

21.6 Der verräterische Arztstempel auf dem Attest

Der Praxis-Stempel „Drogenambulanz..." oder „Dr. Freud, Psychiater" auf einer Arbeitsunfähigkeitsbescheinigung offenbart dem Arbeitgeber des Patienten unnötigerweise sensible Gesundheitsdaten und verstößt damit gegen den Datenschutz.

Die Drogenambulanzen Hamburg GmbH, eine Gesellschaft des Landesbetriebs Krankenhäuser (LBK), hatte sich bereits 1999 mit dem Hinweis an uns gewandt, sie halte ihren Praxis-Stempel „Drogenambulanz..." auf Arbeitsunfähigkeitsbescheinigungen (AU) für datenschutzrechtlich problematisch, müsse ihn aber nach Auffassung der Kassenärztlichen Vereinigung Hamburg (KVH) verwenden (vgl. 17.TB, 17.7). Wir teilen die datenschutzrechtlichen Bedenken, weil das Sozialgesetzbuch ausdrücklich differenziert zwischen der Arbeitsunfähigkeitsbescheinigung mit Diagnose für die Krankenkasse und dem Attest ohne Begründung für den Arbeitgeber. Gerade bei süchtigen Patienten, die mit Methadon substituiert werden, um ihre Eingliederung in das soziale Umfeld zu erhalten, kann die indirekte Offenbarung der Drogenabhängigkeit gegenüber dem Arbeitgeber den Verlust des Arbeitsplatzes bedeuten und die Therapie insgesamt gefährden.

Nach den auf Bundesebene vereinbarten AU-Richtlinien sind die Atteste mit dem Praxis-Stempel des Arztes zu versehen. Wie dieser zu gestalten ist, vereinbaren die Kassen mit den Kassenärztlichen Vereinigungen in sog. Gesamtverträgen auf Landesebene. So heißt es in § 8 des Vertrages zwischen der KVH und der AOK Hamburg, die KVH stelle jedem Vertragsarzt einen Arztstempel zur Verfügung, der neben dem Namen des Arztes „in der behördlich beurkundeten Form“ auch (Fach-)“Gebiets- und/oder Teilgebiets- bzw. Zusatzbezeichnungen ...“ enthält. Die von der KVH ermächtigten ärztlich geleiteten Substitutionseinrichtungen des LBK heißen entsprechend der behördlich beurkundeten Registereintragung „Drogenambulanzen Hamburg GmbH“.

Nach langwieriger erfolgloser Korrespondenz mit der KVH und dem LBK machten wir das Problem im August 2001 bei unserer Halbjahres-Pressekonferenz öffentlich. Kurz danach erhielten wir vom LBK die Mitteilung, dass die Drogenambulanzen Hamburg GmbH beabsichtige, „in Kürze eine Änderung ihres Firmennamens vorzunehmen.“ Dabei werde man sich „bemühen, die zwischen uns und der KVH diskutierten datenschutzrechtlichen Aspekte zu berücksichtigen“.

Ist damit das Hamburger Problem – hoffentlich – zunächst entschärft, bleibt das allgemeine Problem der Facharztbezeichnungen auf den AU nach wie vor offen: So können Bezeichnungen wie „Psychiater, Neurologe“, aber auch „Onkologe“, „Humangenetiker“, „Gynäkologe“ oder Zusatzbezeichnungen wie „plastische Operationen“, „Homöopathie“ oder „Allergologie“ den Arbeitgeber zu weitgehenden Schlussfolgerungen verleiten, die über die erforderliche „Krankschreibung“ hinausgehen. Auch ist daran zu denken, dass AU nicht selten durch die Hände von Kolleginnen und Kollegen gehen, die möglicherweise ebenfalls in ihrem Verhältnis zu dem krankgeschriebenen Kollegen beeinflusst werden.

Richtig ist sicherlich, dass die Authentizität einer AU durch einen Praxisstempel mit dem Namen des Arztes gewährleistet werden muss und dass über ein Telefonbuch oder eine Telefon-CD die Facharztrichtung dieses Arztes schnell zu erfahren ist. Richtig ist auch, dass zumindest in kleineren Orten ohnehin bekannt ist, welcher Fachrichtung ein nur namentlich genannter Arzt angehört. Die Facharztbezeichnung auf dem Stempel drängt aber dem Leser (Arbeitgeber, Kollegen) die Information über die Art der Krankheit des Krankgeschriebenen in vielen Fällen geradezu auf. Dagegen wird der bloße Arztname beim Leser jedenfalls in einer Großstadt nur in Ausnahmefällen zu einem weiteren Rechercheaufwand führen.

Wir haben dieses Problem den Datenschutzbeauftragten des Bundes und der anderen Länder vorgetragen und Zustimmung erfahren. Bei geeigneter Gelegenheit will der Bundesbeauftragte eine mögliche Änderung der AU-Richtlinie auf Bundesebene anregen.

Datenschutz im nicht-öffentlichen Bereich

22. Versicherungswirtschaft

22.1 Versicherungen im Internet

Mit der Versicherungswirtschaft wurden Standards für einen datenschutzgerechten Internetauftritt von Versicherungsunternehmen erarbeitet, die nunmehr von der Versicherungswirtschaft umgesetzt werden.

Bei Durchsicht der Internet-Angebote einiger Versicherungsunternehmen wurden Datenschutzdefizite festgestellt, die vor allem auf einer nicht vollständigen Umsetzung der Datenschutzvorschriften des Teledienstedatenschutzgesetzes (TDDSG) und des Mediendienste-Staatsvertrages (MDSTV) beruhen. Dabei handelte es sich insbesondere um die Verwendung von Cookies, unzureichende Kundeninformationen, unvollständige oder fehlende Anbieterkennzeichnungen und fehlende Hinweise auf mögliche Verschlüsselungen.

Zur Erarbeitung von Standards für einen datenschutzgerechten Internetauftritt von Versicherungsunternehmen wurde eine Arbeitsgruppe mit Vertretern der Aufsichtsbehörden und der Versicherungswirtschaft gebildet. Die Arbeitsgruppe hat einen Kriterien-Katalog für den Internetauftritt von Versicherungsunternehmen entworfen, der an die Versicherungsunternehmen als Empfehlung weitergegeben wird.

Zu den einzelnen Punkten der Empfehlung gehören einvernehmliche Aussagen über Anbieterkennzeichnung, Datenschutzpolitik, Grundsatz der Datensparsamkeit und Datenvermeidung sowie Verwendung von personenbezogenen Daten bei Informationsangeboten. Zwischen den Aufsichtsbehörden und den Vertretern der Versicherungswirtschaft konnte dagegen keine Einigung über das Schriftformerfordernis für die Einwilligungserklärung zum Datenschutz und eventuelle Formerfordernisse für die Schweigepflichtentbindungserklärung erzielt werden.

Die Aufsichtsbehörden vertreten die Auffassung, dass auch bei Abschluss eines Versicherungsvertrags im Internet für die Unterzeichnung der Einwilligungserklärung zum Datenschutz nach § 4 a Abs. 1 Satz 3 BDSG die Schriftform einzuhalten ist. Die Einwilligungserklärung zum Datenschutz kann in Einzelfällen zwar gemäß § 28 Abs. 1 Satz 1 Nr. 1 BDSG entbehrlich sein, wenn die zur Durchführung des Vertrags erforderlichen personenbezogenen Daten vom Versicherer erhoben und nur von ihm im Rahmen des Vertragsverhältnisses verarbeitet werden. In der Regel liegen diese Voraussetzungen jedoch nicht vor, da die Datenverarbeitung durch Versicherungsunternehmen meist unternehmensübergreifend zentral erfolgt und ein Datenaustausch im Rahmen von Antrags- oder Schadensprüfung mit anderen Versicherern erfolgt.

Die Versicherungswirtschaft teilt die Auffassung der Aufsichtsbehörden nicht. Sie hält wegen der besonderen Umstände des Mediums Internet entsprechend § 4 a Abs. 1 Satz 3 BDSG eine elektronische Abgabe der Einwilligungserklärung zum Datenschutz für ausreichend. Hintergrund ist dabei vor allem der zunehmende Wettbewerb im Internet um Vertragsabschlüsse.

Die Aufsichtsbehörden haben darauf hingewiesen, dass nach Änderung der Vorschriften des BGB die gesetzlich vorgeschriebene schriftliche Form durch eine dort genannte elektronische Form ersetzt werden kann. Diese Änderung des BGB ist inzwischen erfolgt (siehe 3.6).

Auch hinsichtlich einer formlosen Abgabe der Schweigepflichtentbindungserklärung im Internet haben die Aufsichtsbehörden Bedenken. Zwar gibt es keine Formvorschrift für die Abgabe der Erklärung. Die Entbindung von der Schweigepflicht durch bloßes Anklicken stellt aber nicht sicher, dass die Schweigepflichtentbindungserklärung nur durch dazu Befugte abgegeben wird. Die Anforderungen an die Datensicherheit nach § 9 BDSG und der Anlage zu § 9 sind daher nicht erfüllt.

Wegen der besonderen Tragweite dieser Einwilligung sind die Aufsichtsbehörden zudem der Auffassung, dass auch ohne ausdrückliche gesetzliche Vorgabe zumindest die Formvorschrift des § 3 Abs. 7 TDDSG 1997 erfüllt sein müsste. Nach dieser Vorschrift ist die elektronische Erklärung einer Einwilligung u.a. erst dann möglich, wenn der Diensteanbieter sicherstellt, dass sie nur durch eine eindeutige und bewusste Handlung des Nutzers erfolgt, nicht unerkennbar verändert werden kann und die Urheber der Erklärung festgestellt werden können. Diese Anforderungen können letztlich nur durch eine digitale Signatur erfüllt werden.

Der Kriterien-Katalog für den Internet-Auftritt der Versicherungsunternehmen, der nach Aussagen des Gesamtverbandes der Versicherungswirtschaft (GDV) den Unternehmen bereits zur Verfügung gestellt wurde, enthält eine Darstellung der unterschiedlichen Auffassungen der Aufsichtsbehörden und der Versicherungswirtschaft.

22.2 Weitergabe von Versichertendaten im Rahmen der Entschädigung für Holocaust-Opfer

Auf der Grundlage sogenannter Holocaust-Versicherungsgesetze zahlreicher US-Bundesstaaten sind mehrere europäische Versicherungsgesellschaften von amerikanischen Behörden zur Übermittlung oder Veröffentlichung im Internet von Listen sämtlicher Vorkriegspolicen der unterschiedlichen Versicherungssparten aufgefordert worden. Einer Datenweitergabe in dem geforderten Umfang durch deutsche Versicherungsunternehmen stehen die Vorschriften des BDSG entgegen.

Im Berichtszeitraum haben mehrere amerikanische Behörden europäische Versicherungsgesellschaften unter Verweis auf die sogenannten Holocaust-Versicherungsgesetze zahlreicher US-Bundesstaaten aufgefordert, sämtliche Versichertendaten aller Versicherungspolicen aus den Jahren 1920 bis 1945 in die USA zu übermitteln bzw. ins Internet einzustellen. Die Aufforderungen, die u.a. an Versicherungsunternehmen in Deutschland, Frankreich, Belgien, Polen, Tschechien, Österreich und Italien gingen, waren nicht beschränkt auf die Datenübermittlungen aus Policen jüdischer oder anderer Holocaust-Opfer, sondern betrafen den gesamten Bestand, unabhängig davon, ob die Policen bereits ordnungsgemäß abgewickelt wurden.

Die Obersten Datenschutzaufsichtsbehörden haben sich in der Arbeitsgruppe Versicherungswirtschaft auf der Grundlage des Bundesdatenschutzgesetzes alter Fassung eingehend mit der Thematik befasst. Sie sind mehrheitlich der Auffassung, dass eine Übermittlung aller von den US-amerikanischen Gesetzen geforderten Daten, soweit sie in automatisierten oder nicht-automatisierten Dateien gespeichert sind, nach den Vorschriften des BDSG unzulässig gewesen wäre. Datenschutzrechtlich unbedenklich war im Rahmen des § 28 Abs. 2 Nr. 1b BDSG (a.F.) nur die Übermittlung oder Nutzung der personenbezogenen Daten ausschließlich von Holocaust-Opfern. Eine darüber hinausgehende Datenübermittlung ist weder nach § 28 Abs. 1, noch nach § 28 Abs. 2 Nr. 1a oder § 28 Abs. 2 Nr. 1b BDSG (a.F.) zulässig, weil schutzwürdige Interessen der betroffenen, nicht zum Kreis der Holocaust-Opfer gehörigen Versicherungsnehmer entgegenstehen. Auch auf der Grundlage des novellierten BDSG ergibt sich keine andere datenschutzrechtliche Bewertung.

Die Aufsichtsbehörden sind der Auffassung, dass die Klärung, ob noch Ansprüche von Holocaust-Opfern gegen deutsche Versicherungen bestehen, auf unterschiedliche Weise unter Beachtung von datenschutzrechtlichen Vorschriften verwirklicht werden kann. Ein in dieser Hinsicht vertretbares Verfahren wäre z.B. die Öffnung der versicherungseigenen Archive für Nachforschungen durch Dritte ähnlich den bei einigen Staatsarchiven durchgeführten Nachforschungen durch das Facts & Files Historical Research Institute Berlin. Rechercheure müssten in diesem Fall auf das Datengeheimnis verpflichtet werden. Überwiegende schutzwürdige Interessen von Versicherungsnehmern oder Begünstigten gegen die Einsichtnahme würden nicht bestehen, soweit sich eine anschließende Veröffentlichung auf den Namen, Vornamen, letzten Wohnsitz und die Art der Versicherung der Holocaust-Opfer, deren Begünstigte oder Erben beschränkt. In diesem Fall könnte von einem berechtigten Interesse der überlebenden Opfer und Begünstigten oder deren Erben an der Veröffentlichung ausgegangen werden, vorbehaltlich zu beachtender Widersprüche in Einzelfällen. Datenschutzrechtlich hätte ein solches Verfahren den Vorteil, dass Daten über die Vielzahl von Versicherungsnehmern, die nicht Holocaust-Opfer sind, bei den Versicherern verbleiben könnten.

Als weitere Lösung käme eine Recherche im Wege der Auftragsdatenverarbeitung in Deutschland in Betracht. In diesem Fall würde eine Auswertung nicht durch Dritte im Rechtssinne erfolgen. Die Versicherungswirtschaft wurde über die Auffassung der Obersten Aufsichtsbehörden unterrichtet.

Mittlerweile hat der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) vorgeschlagen, eine neutrale vertrauenswürdige Stelle im Geltungsbereich der EU-Datenschutzrichtlinie im Wege der Auftragsdatenverarbeitung mit dem in dieser Angelegenheit erforderlichen Abgleich zu beauftragen. Die dieser Stelle zur Verfügung zu stellenden Listen sollen dann nach einem festzulegenden Verfahren mit einer bestimmten Vorgabe aufbereitet werden. Veröffentlicht werden soll anschließend eine Trefferliste mit den Namen derjenigen Holocaust-Opfer, die nachweislich Vertragsbeziehungen zu Versicherungsunternehmen hatten.

Die Obersten Aufsichtsbehörden haben der Versicherungswirtschaft mitgeteilt, dass dieses Verfahren keinen datenschutzrechtlichen Bedenken begegnet, aber auch andere Lösungen denkbar sind. Zu beachten sind allerdings in diesem Zusammenhang eingehende Widersprüche von Opfern des Holocaust. Dabei erscheint es durchaus sachgerecht, durch geeignete Veröffentlichungen vor der Einstellung in das Internet auf entsprechende Widerspruchsmöglichkeiten hinzuweisen.

22.3 Datentransfer innerhalb international tätiger Versicherungsunternehmen

Der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) hat den Entwurf einer Unternehmensrichtlinie für den Datentransfer innerhalb international tätiger Versicherungsunternehmen vorgelegt. Dieser Entwurf muss noch grundlegend überarbeitet werden.

Wir haben uns in den Arbeitsgruppen Versicherungswirtschaft und Internationaler Datenverkehr der Obersten Aufsichtsbehörden mit dem Entwurf des GDV beschäftigt und eine umfassende Überarbeitung gefordert. Der Entwurf bietet keine ausreichenden Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte für die Betroffenen. Er enthält nicht die Mindestanforderungen, die von der Europäischen Kommission als verbindliche Datenschutzgrundsätze im Zusammenhang mit den beschlossenen Standardvertragsklauseln benannt werden. Die Arbeitsgruppen sind der Auffassung, dass diese Grundsätze auch bei der Erstellung einer Unternehmensrichtlinie beachtet werden müssen und bei deren Beachtung ausreichende Garantien im Sinne von § 4 c Abs. 2 BDSG und Artikel 26 Abs. 2 EG-Datenschutzrichtlinie geschaffen werden können.

Der vorgelegte Entwurf enthält keine Aussagen zur Zweckbindung der Datenverarbeitung, zum Auskunftsrecht der Betroffenen und zur Beschränkung der Weiterübermittlung. Außerdem fehlen Aussagen darüber, wie und bei welcher

Stelle die Rechte der Betroffenen durchgesetzt werden können. Unklar ist auch der Anwendungsbereich der Unternehmensrichtlinie. Er soll für den Datentransfer europäischer Versicherungsunternehmen in Drittländer gelten. Allerdings wird dabei die Geltung des BDSG vorausgesetzt, was bei Datenübermittlungen aus EU-Ländern außerhalb der Bundesrepublik nicht nachvollziehbar ist. Obwohl dem GDV rechtzeitig mitgeteilt wurde, in welchen Punkten eine Nachbesserung erforderlich ist, wurden diese in einer vorgelegten Neufassung nicht berücksichtigt.

Dem GDV wurden daher noch einmal die einzelnen datenschutzrechtlichen Mängel mitgeteilt, um eine datenschutzgerechte Überarbeitung der Unternehmensrichtlinie zu gewährleisten. Das ist schon deswegen erforderlich, weil die einzelnen Unternehmen sich nach § 4 c Abs. 2 BDSG bestimmte Datenübermittlungen ins Ausland von den zuständigen Aufsichtsbehörden genehmigen lassen müssen und in diesem Zusammenhang ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorzuweisen haben.

Noch nicht endgültig geklärt ist seitens der Versicherungswirtschaft die Frage, ob es sich bei dem vorgelegten Muster einer Unternehmensrichtlinie lediglich um Vorgaben für die Unternehmen im Rahmen der Sicherstellung ausreichender Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte im Rahmen der Genehmigungsvoraussetzung des § 4 c Abs. 2 BDSG handeln soll. Denkbar ist auch die Verwendung einer überarbeiteten Fassung als Verhaltensregel i.S.d. § 38 a BDSG.

22.4 Service-Center bei Krankenversicherungen

Der Aufsichtsbehörde wurde bekannt, dass private Krankenversicherungen in datenschutzrechtlich bedenklicher Weise personenbezogene Kundendaten an sog. Service-Center übermitteln und auch von dort erheben.

Von der Aufsichtsbehörde eines anderen Bundeslandes erhielten wir den Hinweis, dass ein Service-Unternehmen über das Internet für die Versicherten privater und gesetzlicher Krankenversicherungen die Möglichkeit anbietet, online oder über das Telefon medizinische Anfragen zu stellen. Unsere Recherchen haben ergeben, dass die dort genannte gesetzliche Krankenversicherung im Hamburger Raum dem Service des Unternehmens nicht angeschlossen ist.

Anders sieht es jedoch für eine in unseren Zuständigkeitsbereich fallende private Krankenversicherung aus. Diese übermittelt dem Service-Unternehmen

- Versicherungsnummer
- Name, Vorname

- Geschlecht
- Geburtsdatum
- Postleitzahl
- Ort
- Straße, Hausnummer
- Telefonnummer
- eMail-Adresse

sämtlicher Versicherungsnehmer, also auch derjenigen, die nie den Service in Anspruch nehmen. Der Grund für die weitreichende Datenübermittlung besteht für die Krankenversicherung darin, dass sie dem Service-Unternehmen eine jährliche Pauschalsumme auf Basis der berechtigten Kunden zahlt. Damit soll sicher gestellt werden, dass ausschließlich die berechtigten Versicherten die Auskunft gebenden Ärzte des Unternehmens in Anspruch nehmen können. Das Service-Unternehmen kann anhand der übermittelten Daten diese Berechtigung überprüfen.

Schon diese Datenübermittlung ist unserer Auffassung nach unzulässig. Sie ist jedenfalls nicht von dem Krankenversicherungsvertrag umfasst. Inhalt eines solchen Vertrages ist es nicht, eine umfassende Beratung in medizinischen Angelegenheiten anzubieten. Die von dem Service-Unternehmen angebotene Leistung ist vielmehr als Zusatzangebot zu verstehen. Daher ist datenschutzrechtlich eine Abwägung zwischen der Wahrung berechtigter Interessen der Krankenversicherung und den schutzwürdigen Interessen der betroffenen Versicherungsnehmer im Rahmen des § 28 Abs. 1 Nr. 2 BDSG vorzunehmen.

Es liegt sicherlich im berechtigten Interesse der Versicherung, im Rahmen eines von ihr den Kunden zur Verfügung gestellten zusätzlichen Angebots auch sicher zu stellen, dass dieses Angebot ausschließlich von dem berechtigten Kundenkreis genutzt werden kann. Dem stehen jedoch die schutzwürdigen Interessen der Kunden gegenüber. Zwar werden mit den oben aufgeführten Daten keine besonders sensiblen Geheimnisse preisgegeben. Es hätte jedoch zur Zweckerfüllung ausgereicht, lediglich die Versicherungsnummer zu übermitteln oder die Berechtigung des Versicherungsnehmers im Einzelfall online zu prüfen. Darüber hinaus werden aber auch die Daten all derjenigen weitergegeben, die den Service nie in Anspruch nehmen werden. Es entsteht auf diese Weise also eine Vorratsdatenhaltung auf Seiten des Service-Unternehmens, die völlig unnötig ist. Darüber hinaus könnte das Service-Unternehmen die Berechtigung auf andere Weise feststellen, etwa durch Abfrage im Einzelfall. Infolgedessen überwiegt das schutzwürdige Interesse der Versicherten. Die Übermittlungen sind daher unzulässig.

Obwohl sich das Krankenversicherungs-Unternehmen der rechtlichen Beurteilung durch die Aufsichtsbehörde nicht anschließen wollte, erklärte es sich bereit, das Verfahren einer Online-Prüfung der Anrufberechtigung weiterzuverfolgen und bis zum Ende des Jahres 2001 umzusetzen.

Bei der Erörterung vorstehender Probleme wurde deutlich, dass die Ärzte des eingeschalteten Service-Unternehmens den Betroffenen am Telefon den Eindruck vermitteln, mit ihrer eigenen Krankenversicherung verbunden zu sein. Nach den Vorschriften des neuen Bundesdatenschutzgesetzes muss eine verantwortliche Stelle – und um eine solche handelt es sich bei dem Service-Unternehmen als Call-Center – dem Betroffenen gegenüber nach § 4 Abs. 3 Nr. 1 BDSG ihre Identität offenbaren. Da das Service-Unternehmen seinen Sitz in Nordrhein-Westfalen hat, wurde auch die dortige Aufsichtsbehörde informiert, die die Angelegenheit weiterverfolgen wird. Eine Lösung dieser Frage erscheint besonders wichtig, weil davon auch alle anderen Service-Unternehmen betroffen sind, die Funktionen von anderen Unternehmen übernehmen.

Zur Zeit erhebt die Krankenversicherung noch keine Daten über den Inhalt der Beratung durch die Mitarbeiter des Service-Unternehmens. Angesichts der Tatsache, dass die Gespräche schon der ärztlichen Schweigepflicht unterliegen, könnten die Daten über diese Inhalte auch von der Versicherung nach keiner Vorschrift rechtmäßig erhoben werden. In einer eingehenden Erörterung stellte sich jedoch heraus, dass eine solche Datenerhebung über die Ärzte des Service-Center für wünschenswert gehalten wird.

Das Krankenversicherungs-Unternehmen hat zwar geltend gemacht, es sei für erneute Kundenkontakte erforderlich, einen vollständigen Kenntnisstand über den Inhalt der Arztkontakte zu erhalten. Dem ist jedoch entgegenzuhalten, dass es nicht Aufgabe einer privaten Krankenversicherung ist, sich Kenntnisse über den Inhalt von Arztgesprächen ihrer Versicherten zu verschaffen. Zulässigerweise könnten solche Daten nur mit einer wirksamen Schweigepflicht-Entbindungserklärung jedes einzelnen Betroffenen übermittelt werden. Die Krankenversicherung hat mitgeteilt, dass sie weiterhin eine Übermittlung von Daten ihrer Versicherungsnehmer durch das Service-Center an sich anstrebt, sich aber der datenschutzrechtlichen sowie der strafrechtlichen Problematik bewusst sei.

Auch die angebotene medizinische Beratung über das Internet begegnet erheblichen datenschutzrechtlichen Bedenken. Es sind jedoch Planungen vorgestellt worden, die jedenfalls eine künftig datenschutzgerechtere Handhabung dieses äußerst sensiblen Bereichs erwarten lassen.

Da die aufgeführten Probleme noch nicht endgültig gelöst sind, wird die Aufsichtbehörde die Angelegenheit weiter verfolgen und die Umsetzung der angekündigten Änderungen kontrollieren.

22.5 Sonstiges

– Darüber hinaus hat sich die Datenschutzaufsichtsbehörde im Bereich der Versicherungswirtschaft mit der Zulässigkeit der sog. Rennlisten beschäftigt. Darunter versteht man Leistungsübersichten, in die Handelsvertreter von den Versicherungsunternehmen aufgenommen werden. Diese Listen sind angesichts des Inhalts zumindest dann problematisch, wenn die Handelsvertreter nicht über diese ständige Praxis und die Freiwilligkeit ihrer Mitwirkung ausreichend informiert sind. Die Versicherungswirtschaft hat eine Vereinheitlichung der Praxis, die auch die Vorgaben des BDSG zur Datenvermeidung und Datensparsamkeit sowie ausreichende Transparenz berücksichtigt, zugesichert.

– Thematisiert wurden im Bereich der Kfz-Haftpflichtversicherung Fragen zum Umfang der Datenerhebung bei Abschluss der Versicherung und der Erforderlichkeit der Vorlage einer Führerscheinkopie zur Rabattübertragung.

23. Schufa und Auskunfteien

23.1 Neufassung der Schufa-Klausel

Die Schufa-Klausel für Girokonten wurde datenschutzkonform neu gefasst.

Nachdem sich eine Arbeitsgruppe aus Teilnehmern der Obersten Aufsichtsbehörden und der Schufa zur Formulierung einer neuen Schufa-Klausel gebildet hatte (vgl. 17. TB, 20.3), konnte die neue Formulierung relativ zügig verabschiedet werden. Längere Diskussionen hat es zunächst über einige Einzelheiten des Textes, insbesondere über die Aufnahme von Informationen über das Scoring-Verfahren gegeben.

Der Schufa wurde mit der Formulierung scheinbar neu die Möglichkeit eröffnet, Daten auch an andere Kredit gewährende Unternehmen, wie etwa Telekommunikationsunternehmen, und nicht nur an Kreditinstitute selbst zu übermitteln. Es ist jedoch festzuhalten, dass Auskunfteien grundsätzlich – auch ohne Einwilligung – unter bestimmten Umständen befugt sind, zulässigerweise erhobene personenbezogene Daten an Dritte weiterzugeben, die daran ein berechtigtes Interesse haben. Die Klausel nimmt also Sachverhalte auf, die jedenfalls teilweise nicht der Einwilligung bedürfen.

In diesem Zusammenhang kann man an der Neufassung der Schufa-Klausel auch kritisieren, dass sie dem Kunden suggeriert, die Entscheidung über die Unterzeichnung oder Nicht-Unterzeichnung der Klausel zu haben. In der Praxis wird aber kaum ein Kreditinstitut, unverständlicherweise nicht einmal bei Guthabenkonten, ein Girokonto ohne Unterzeichnung der Schufa-Klausel vergeben.

Positiv ist daran jedoch zu vermerken, dass hier zumindest eine Information des Kunden über den Umgang mit seinen personenbezogenen Daten erfolgt und auf diese Weise die Transparenz des Schufa-Verfahrens insgesamt erhöht wird. Es ist also für den Betroffenen bei Unterzeichnung der Klausel erkennbar, welche Folgen möglicherweise auf ihn zukommen und wie seine Daten künftig verwendet werden.

23.2 Score-Wert der Schufa

23.2.1 Informationen über den Score-Wert

In der Neufassung des Schufa-Merkblatts sind auch Informationen über das Scoring-Verfahren des Unternehmens enthalten.

Die Kreditwirtschaft hat das Merkblatt zum Schufa-Verfahren im Berichtszeitraum erneut überarbeitet und insbesondere auch deutliche Informationen zum Score-Verfahren gegeben. Die Frage, ob die Schufa oder das kreditgebende Institut den Score-Wert beauskunften muss, wurde von den Obersten Aufsichtsbehörden weiterhin außerordentlich intensiv und auch kontrovers sowohl mit der Schufa als auch mit Vertretern der Kreditwirtschaft erörtert.

Seitens der Kreditwirtschaft wurde mitgeteilt, dass dieser Wert teilweise überhaupt nicht gespeichert oder sonst aufbewahrt wird und es daher Probleme mit der Nachvollziehbarkeit einzelner Werte zu bestimmten Zeitpunkten gebe. Gleichwohl wurde zugesagt, den Score-Wert immer dann auch zu beauskunften, wenn er in irgend einer Form – ggf. auch in Aktenform – noch unproblematisch rekonstruierbar sei. Eine Rechtspflicht sollte damit jedoch nicht begründet werden.

Die Schufa gab zunächst an, angesichts der verschiedenen Möglichkeiten, nach denen die Score-Werte für die unterschiedlichen Vertragspartner jeweils individuell und für einen bestimmten Zeitpunkt errechnet würden, könne keinesfalls eine verbindliche Auskunft gegeben werden. Nunmehr hat die Schufa jedoch mitgeteilt, dass sie zur weiteren Erhöhung der Transparenz des Score-Verfahrens denjenigen Betroffenen, die dies wünschen, eine Score-Berechnung nach verschiedenen Score-Karten, die jeweils unterschiedlich aufgebaut sind, anbieten wird. Diese Score-Werte können allerdings im Einzelfall von denjenigen abweichen, die zu früheren Zeitpunkten bereits an Vertragspartner der Schufa übermittelt wurden. Das Verfahren wird kostenpflichtig sein.

23.2.2 Einflüsse auf den Score-Wert

Die Geltendmachung des gesetzlichen Rechts auf Selbstauskunft hat bei der Schufa zu einer Verschlechterung der Score-Werte Betroffener geführt.

Durch eine Eingabe wurde offenbar, dass das Einholen einer oder mehrerer Selbstauskünfte durch Betroffene bei der Schufa zu einer deutlichen Verschlechterung des Score-Wertes führte. Entscheidend ist in diesem Zusam-

menhang, dass das Bundesdatenschutzgesetz einen Anspruch auf Erteilung einer solchen Selbstauskunft vorsieht, der in der Häufigkeit der Geltendmachung auch nicht beschränkt ist. Daraus ergibt sich, dass die Inanspruchnahme des Rechts auf Auskunft über die gespeicherten Daten nicht zu Nachteilen des Betroffenen führen darf.

Die Schufa hielt dem zunächst entgegen, es gebe Erfahrungswerte dahingehend, dass eine hohe Zahl der Selbstauskünfte in Wahrheit in wirtschaftlicher Weise, z.B. für Kredite, die der Schufa nicht gemeldet würden, verwendet würden. Aus diesem Grund erhöhe jede zusätzliche Selbstauskunft auch das Kreditrisiko und damit den Score-Wert des Betroffenen. Die Beeinflussung des Score-Wertes durch die Selbstauskünfte sei daher sachlich gerechtfertigt.

Nach mehreren kontrovers geführten Gesprächen mit Vertretern der Schufa gab diese bekannt, künftig auf die Einbeziehung der Anzahl der Selbstauskünfte in die Score-Wertberechnung zu verzichten. In diesem Zusammenhang wurde seitens der Schufa erläutert, dass die Wahrnehmung weiterer datenschutzrechtlicher Betroffenenrechte, wie etwa Anträge auf Berichtigung, Löschung oder Sperrung von Daten, keinen Einfluss auf die Berechnung des Score-Wertes haben. Angesichts der Komplexität von Score-Wertberechnungen und der damit zusammenhängenden Neugestaltung der sogenannten Scorekarten ist die Umstellung des Verfahrens jedoch noch nicht abgeschlossen.

23.3 Schufa-Auskünfte an die Wohnungswirtschaft

Das in Hamburg durchgeführte Pilotverfahren zum Anschluss von Wohnungsunternehmen an die Schufa konnte erfolgreich abgeschlossen werden. Bei der bundesweiten Umsetzung ergaben sich weitere Datenschutzfragen.

Unter engen Voraussetzungen war es im Rahmen eines Testverfahrens Wohnungsunternehmen möglich, von der Schufa Informationen über künftige Mieter zu erhalten (zu den Einzelheiten vgl. 17. TB, 20.4). Dabei stellte sich heraus, dass die Einholung von Selbstauskünften, die mehr Daten enthalten, als die Vermieter zur Beurteilung der wirtschaftlichen Leistungsfähigkeit künftiger Mieter benötigen, deutlich zurückging. Gleichzeitig erreichte die Aufsichtsbehörde auch keine Beschwerde mehr über das Verlangen von Schufa-Selbstauskünften durch Vermieter.

Mittlerweile hat die Schufa mit der bundesweiten Einführung des Anschlusses von Wohnungsunternehmen an das Schufa B-Verfahren begonnen. Zunächst war in diesem Zusammenhang den Obersten Aufsichtsbehörden für den Datenschutz zugesagt worden, dass dabei die für die Testphase vereinbarten Voraussetzungen eingehalten würden. Es hat sich jedoch herausgestellt, dass kein vollständiger Verzicht auf Nachmeldeverfahren stattfindet. Seitens der Datenschutzaufsichtsbehörden war davon ausgegangen worden, dass die Vermieter nach Abschluss eines Mietvertrages weitere Angaben nicht mehr

benötigen und insoweit deren berechtigtes Interesse fehlt. Die Vertreter der Schufa haben jedoch vorgetragen, ein berechtigtes Interesse liege jedenfalls dann vor, wenn eine Kündigung wegen Zahlungsverzugs hinsichtlich unstreitiger Mietrückstände von zwei Raten erfolgt sei. Unter der Voraussetzung, dass streitige Rückstände nicht zu einer Meldung führen, erhoben die Obersten Aufsichtsbehörden gegen diese Form der Nachmeldungen keine Einwände.

Darüber hinaus ist jedoch ein weiteres, noch mit der Schufa zu klärendes Problem aufgetreten: Im Rahmen des in Hamburg durchgeführten Pilotverfahrens wurde eine Einwilligungsklausel entwickelt, die nach Auffassung der Datenschutzaufsichtsbehörden auch bundesweit eingesetzt werden sollte. Wie sich jetzt jedoch herausstellte, legen die Vermieter ihren Interessenten eine andere, von der Schufa vorgegebene Erklärung zur Unterzeichnung vor. In einem Gespräch der Obersten Aufsichtsbehörden für den Datenschutz mit der Schufa wurde klargestellt, dass eine Einwilligungserklärung, die die Erhebung von mehr Daten erlaubt, als sie für die Wohnungswirtschaft nach den in dem Pilotprojekt vereinbarten Zwecke erforderlich ist, als unzulässig angesehen wird. Zwar hat die Schufa zugesichert, die Klausel in der den Betroffenen vorgelegten Form nicht zu nutzen. Die Obersten Aufsichtsbehörden machten jedoch deutlich, dass sie eine Einschränkung des Wortlauts auf das unbedingt erforderliche Maß für notwendig erachten.

In diesem Zusammenhang teilte die Schufa mit, dass auch Überlegungen dahingehend bestehen, den Vermietern mitzuteilen, welche finanziellen Belastungen die Mietanwärter monatlich haben. Derartige Übermittlungen wären äußerst kritisch zu betrachten, weil bei der Schufa keine vollständigen aussagekräftigen Daten zu diesem Punkt vorliegen und daher der Wert einer Übermittlung zweifelhaft ist. Jedenfalls wären solche Übermittlungen ohne transparente Information des künftigen Mieters und darauf basierender freiwilliger Einwilligung unzulässig. Die Vertreter der Schufa haben zugesichert, die weitere Entwicklung in diesem Punkt mit den Obersten Aufsichtsbehörden für den Datenschutz abzustimmen.

23.4 Sonstiges

Die wirtschaftliche Entwicklung hat dazu geführt, dass sich immer mehr Unternehmen im Rahmen von Risikovertragsabschlüssen hinsichtlich der Seriosität und Zahlungsfähigkeit ihrer Kunden absichern. Daraus ergeben sich zwei unterschiedliche Folgen für die Aufgaben der Aufsichtsbehörde:

– Einerseits erweitern die vorhandenen Auskunfteien ihre herkömmlichen Geschäftsbereiche erheblich. Dies gilt zum Beispiel für die Telekommunikationsbranche, aber auch für Stromlieferungsgeschäfte. Daneben erhoffen sich neue Unternehmen, bisher nicht erkannte Geschäftsfelder bearbeiten zu können. In beiden Fällen ist einerseits Kontrolle und anderer-

seits auch Beratung durch die zuständigen Aufsichtsbehörden gefragt, was zu einer deutlichen Erhöhung insbesondere der Beratungstätigkeit führt.

– Andererseits sind aber auch die Bürger von der Tätigkeit der Auskunfteien stärker betroffen. Durch die zunehmende Absicherung der Unternehmen kommt es zu mehr Datenübermittlungen und teilweise auch zu fehlerhaften Auskünften. An der Eingabenentwicklung im nicht-öffentlichen Bereich (vgl. 30.4) ist ablesbar, dass die Betroffenheit der Bürger erheblich zugenommen hat.

24. Kreditwirtschaft

24.1 Abschaffung des Bankgeheimnisses?

Eingriffe in das Bankgeheimnis müssen wie jeder Eingriff in das Recht auf informationelle Selbstbestimmung auf einer verfassungsmäßigen Rechtsgrundlage beruhen.

Nach den Anschlägen des 11. September 2001 wurde deutlich, dass sich diese nur unter Einsatz erheblicher finanzieller Mittel durchführen ließen. Um weltweit operierenden Terrororganisationen den Boden entziehen zu können, wird als eine Maßnahme von vielen das Aufspüren und Austrocknen von Terror unterstützenden Finanzquellen als erforderlich angesehen. Zur Durchsetzung dieses Ziels ist – neben der Errichtung eines zentralen Kontenregisters beim Bundesaufsichtsamt für das Kreditwesen (siehe 13.1) – auch die Abschaffung des so genannten Bankgeheimnisses im Gespräch. Hiermit ist in diesem Zusammenhang der staatliche Zugriff auf Kontoinformationen gemeint.

Unter dem Bankgeheimnis wird die Pflicht des Kreditinstituts verstanden, Informationen, die ihm aus dem Geschäftsverhältnis mit seinen Kunden bekannt werden, grundsätzlich vertraulich zu behandeln. Das Bankgeheimnis ist in der Bundesrepublik Deutschland nicht ausdrücklich einfachgesetzlich geregelt, sondern folgt aus dem Vertrag mit dem Kreditinstitut und letztlich aus dem verfassungsrechtlich geschützten Recht des Kunden auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.

Der besondere Schutz des Bankkunden hat seine Ausprägung auch in § 30 a AO gefunden, wonach die Finanzbehörden bei der Ermittlung eines steuerrechtlichen Sachverhalts besondere Rücksicht auf das Vertrauensverhältnis zwischen den Kreditinstituten und deren Kunden zu nehmen haben. Insbesondere dürfen die Finanzbehörden von den Kreditinstituten zum Zwecke der allgemeinen Überwachung die einmalige oder periodische Mitteilung von Konten bestimmter Art oder bestimmter Höhe nicht verlangen.

Darüber hinaus ist das Bankgeheimnis in der Rechtsbeziehung zwischen dem Kreditinstitut und seinen Kunden in den Allgemeinen Geschäftsbedingungen der Banken geregelt. Das Bankgeheimnis kann jedoch durchbrochen werden,

wenn eine gesetzliche Grundlage das Kreditinstitut verpflichtet, Informationen über seinen Kunden bekannt zu geben oder der Kunde eine entsprechende Einwilligung erteilt hat.

Die Staatsanwaltschaft kann im Rahmen des Ermittlungsverfahrens den Sachverhalt erforschen und in diesem Zusammenhang auch von Kreditinstituten Auskünfte erhalten; außerdem kann sie gegebenenfalls Durchsuchungen und Beschlagnahmen durchführen. Voraussetzung für die Einleitung eines Ermittlungsverfahrens ist jedoch stets das Vorliegen eines Anfangsverdachts. Die Staatsanwaltschaft darf keine Ermittlungen „ins Blaue“ betreiben und somit keine Daten auf Vorrat sammeln.

Nach § 23 des Gesetzes über die Datenverarbeitung der Polizei darf die Polizei für die Rasterfahndung von öffentlichen und nicht öffentlichen Stellen die Übermittlung von personenbezogenen Informationen bestimmter Personengruppen aus Dateien zum Zwecke des Abgleichs mit anderen Datenbeständen oder zur Auswertung verlangen, soweit dies zur Abwehr einer unmittelbar bevorstehenden Gefahr für den Bestand des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person erforderlich ist. Das Ermittlungsersuchen muss sich dabei auf Namen, Vornamen, Geburtsdatum, Geburtsort und Anschrift sowie auf im Einzelfall festzulegende Merkmale beschränken. Bei dieser Rasterfahndung sind die Kreditinstitute unter den genannten Voraussetzungen schon nach geltendem Landesrecht zur Auskunftserteilung verpflichtet.

Darüber hinaus können Kreditinstitute bereits nach § 28 Abs. 3 BDSG Kundendaten an die Sicherheits- und Strafverfolgungsbehörden weiterleiten, wenn dies für die Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

Im Entwurf des Terrorismusbekämpfungsgesetzes ist eine Ausweitung der bisher schon vorhandenen Befugnisse vorgesehen. Danach sollen Banken und Geldinstitute explizit zur Erteilung von Auskünften an das Bundesamt für Verfassungsschutz verpflichtet werden. Dies würde bedeuten, dass der Verfassungsschutz ohne besondere Anhaltspunkte und ohne Wissen der Betroffenen Auskünfte über Kontenbewegungen erhalten könnte und diese Daten bis zu 15 Jahre speichern dürfte. Eine derart ausufernde Auskunftsverpflichtung ist verfassungsrechtlich bedenklich. Die Konferenz der Datenschutzbeauftragten hat daher in ihrer Grundsatzentschließung vom 24. bis 26. Oktober 2001 (siehe Einleitung) gefordert, dass Freiheits- und Persönlichkeitsrechte bei der Terrorismusbekämpfung nicht verloren gehen dürften. Sie hat ausdrücklich als Beispiel für geplante pauschale problematische Eingriffsbefugnisse die vorgesehene Auskunftsverpflichtung für Kreditinstitute gegenüber dem Verfassungsschutz genannt.

Der Entwurf des Bundesinnenministeriums ist anschließend in der Kabinettsvorlage vom 7. November 2001 aufgrund der öffentlichen Kritik deutlich eingeschränkt worden. Danach dürfen Auskünfte insbesondere nur noch verlangt werden, wenn tatsächliche Anhaltspunkte für schwerwiegende Gefahren z.B. durch terroristische Aktivitäten bestehen. Außerdem wurde eine Mitteilungspflicht gegenüber den Betroffenen eingefügt. Wesentliche Mängel wurden damit beseitigt.

24.2 Elektronische Geldkarte

Ob die von den Aufsichtsbehörden abgegebenen Empfehlungen zur Verbesserung des Datenschutzes bei dem Zahlungssystem Geldkarte von den Kreditinstituten umgesetzt werden, ist weiterhin kritisch zu beobachten.

Mit den datenschutzrechtlichen Anforderungen an die 1997 in Einsatz gebrachte elektronische Geldkarte haben wir uns schon in den letzten Tätigkeitsberichten intensiv befasst (vgl. 17. TB, 21.2; 16. TB 21.2; 14. TB 25.1). Wir haben die Thematik auch in diesem Berichtszeitraum weiter verfolgt und im Kreise der Obersten Datenschutzaufsichtsbehörden gemeinsam mit den Vertretern des Zentralen Kreditausschusses diskutiert. Derzeit sind ca. 55 Mio. Geldkarten im Umlauf, und es ist zu erwarten, dass sich die Anzahl nach Wegfall der eurocheque-Garantie am 1. Januar 2002 weiter erhöhen wird. Zu erwarten ist auch, dass die Geldkarte neben der bisherigen bloßen Zahlfunktion zukünftig zusätzliche Anwendungen umfassen wird. Der Chip kann beispielsweise als elektronischer Fahrschein eingesetzt werden. Ein solches Pilotprojekt wurde bereits im Jahre 1999 in Bremen durchgeführt (vgl. 17. TB, 21.2); die Geldkarte kann auch z.B. in den HHA-Bussen zur bargeldlosen Bezahlung verwendet werden.

Die Datenschutzaufsichtsbehörden haben im Berichtszeitraum das System Geldkarte beurteilt und der Kreditwirtschaft Vorschläge zur datenschutzfreundlichen Anwendung unterbreitet.

Nach der neuen Regelung in § 3 a BDSG haben sich die Gestaltung und Auswahl von Datenverarbeitungssystemen an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Daher empfehlen die Datenschutzaufsichtsbehörden, dass die Nutzung der Geldkarte soweit wie möglich anonym bzw. pseudonym gestaltet wird. Hieraus ergibt sich die von uns schon seit Langem – jedoch noch immer nicht flächendeckend umgesetzte – Forderung, kontoungebundene Geldkarten bereit zu stellen. Diese sogenannte „White Card“, die ohne Personenbezug ausgegeben wird, gewährleistet einen datenschutzfreundlichen anonymen Zahlungsverkehr. Leider wissen die Kunden nur in den wenigsten Fällen, dass es überhaupt eine solche Karte gibt.

Auch wenn bislang noch keine Fälle der Erstellung von Nutzerprofilen bekannt sind, eröffnen kontogebundene Geldkarten, bei deren Nutzung Datenspuren gespeichert werden, zumindest die Möglichkeit, Rückschlüsse auf die Person des Nutzers zu ziehen. Möglicherweise wird dies eine noch größere Bedeutung erlangen, wenn neben der Zahlfunktion weitere Zusatzanwendungen auf der Geldkarte zur Verfügung gestellt werden.

Ein weiteres datenschutzrechtliches Anliegen ist die Sicherstellung einer transparenten Datenverarbeitung. Die Nutzer einer kontogebundenen Geldkarte müssen insbesondere darüber aufgeklärt werden, welche Stellen die mit der Nutzung der Karte anfallenden Daten speichern und wie lange die Daten dort vorgehalten werden. Der Zentrale Kreditausschuss teilt diese Auffassung und hat die Kreditinstitute auf die Erforderlichkeit der Transparenz des Datenlaufs hingewiesen. Leider haben noch nicht alle Kreditinstitute diese Vorgaben in befriedigendem Maße umgesetzt. Unsere Aufgabe wird es sein, möglichst alle Kreditinstitute zu einer Umsetzung unserer datenschutzfreundlichen Forderungen zu bewegen.

24.3 Ausforschung von Girokonten

Jede Verarbeitung personenbezogener Kontodaten, die über den konkreten Verwendungszweck der Girokontoführung hinaus geht, ist nicht von § 28 Abs. 1 Nr. 2 BDSG gedeckt. Ein Kreditinstitut darf daher die personenbezogenen Kontodaten ohne wirksame Einwilligung der Kunden nicht zu Akquisitions- oder Werbezwecken nutzen.

Während des Berichtszeitraums hat ein Mitarbeiter eines Kreditinstituts einzelne Überweisungen von und auf Girokonten eines Kunden beobachtet und für die Zwecke des eigenen bzw. eines dritten Unternehmens ausgewertet. In dem uns bekannt gewordenen Fall wurde ein Kunde angerufen, auf eine von ihm veranlasste Überweisung für seine Unfallversicherung angesprochen und schließlich darauf hingewiesen, dass eine mit dem Kreditinstitut kooperierende Versicherung diese Unfallversicherung zu einem weitaus günstigeren Beitrag anbieten könne.

Dieses Vorgehen ist datenschutzrechtlich nicht zulässig. Nach der allein in Betracht kommenden Rechtsgrundlage § 28 Abs. 1 Nr. 2 BDSG ist die Nutzung personenbezogener Daten als Mittel für die Erfüllung eigener Geschäftszwecke nur zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.

Der gezielten Auswertung der Girokontobewegungen zu Werbe- und/oder Akquisitionszwecken wird hingegen regelmäßig ein schutzwürdiges Interesse des Girokontokunden entgegen stehen und das Vermittlungsinteresse des Kreditinstituts überwiegen. Der Kunde bringt gerade seinem Girovertragspart-

ner besonderes Vertrauen entgegen. Insbesondere das Institut, bei dem möglicherweise die einzige Girokontoverbindung besteht, erhält durch die verschiedenen, teilweise sensiblen, Kontobewegungen in besonders enger Weise Kenntnis von den Lebensumständen des Betroffenen. Der Kunde wird in der Regel davon ausgehen, dass von diesen häufig sehr sensiblen Daten nur im Zusammenhang mit der Durchführung der Transaktionen Kenntnis genommen wird. Jede darüber hinaus gehende Auswertung wird er als Ausforschung empfinden, die sein Vertrauen in die vertragsgerechte Behandlung seiner Daten erschüttert.

Daher darf ohne das Wissen und den eindeutigen Willen des Kunden, dass er eine solche „Beratung" seines Kreditinstituts wünscht, eine Ausforschung nicht erfolgen. Diese Auffassung ist von uns in den Kreis der Obersten Aufsichtsbehörden für den Datenschutz eingebracht worden und wird von dort bestätigt. Auch der Zentrale Kreditausschuss, der darauf hingewiesen hat, dass es sich hierbei nicht um die Angelegenheit des Zentralverbandes oder der einzelnen Verbände, sondern um die einzelner Kreditinstitute handele, sieht die Problematik. Wir haben daher das betreffende Kreditinstitut auf die datenschutzrechtliche Unzulässigkeit der Verfahrensweise hingewiesen. Das Kreditinstitut betont, dass es sich bei der uns bekannt gewordenen Angelegenheit um einen Einzelfall gehandelt habe, vertritt jedoch grundsätzlich die Auffassung, dass eine Auswertung der Verwendungszwecke zur Akquisition ohne ausdrückliche Einwilligung des Kunden zulässig sei.

24.4 EC-Karte mit Altersangabe

Jede nicht zwingend erforderliche Ausweitung der Speicherung personenbezogener Daten auf EC-Karten ist abzulehnen.

Das Bundesgesundheitsministerium verfolgt das Ziel, den Tabakkonsum unter Jugendlichen zu reduzieren. Um dieses Ziel zu erreichen, soll Jugendlichen unter 16 Jahren der Zugang zu Zigarettenautomaten möglichst verwehrt, zumindest aber erschwert werden. Zur Durchsetzung der Zugangssperre favorisieren das Bundesgesundheitsministerium und der Verband der Automatenaufsteller das Aufbringen eines Altersmerkmals auf der kontogebundenen Geldkarte. Der Nutzer des Zigarettenautomaten muss sich vor der Warenausgabe dadurch authentifizieren, dass sein Alter mit über 16 Jahren angegeben ist. Ist die Authentifizierung erfolgreich, kann der Kauf mit Bargeld oder bargeldlos abgewickelt werden.

Aus Sicht der Aufsichtsbehörden bestehen gegen dieses Vorhaben datenschutzrechtliche Bedenken. Unter Anwendung des Grundsatzes der Datensparsamkeit stellt sich zunächst die Frage, ob zum Erreichen des Ziels, Jugendlichen den Zugang zu Zigarettenautomaten zu erschweren, das Aufbringen eines Altersmerkmales auf der EC-Karte überhaupt geeignet ist. Es ist zu berücksichtigen, dass nicht der Jugendliche nach seiner Zugangs-

berechtigung beurteilt wird, sondern lediglich die von dem Jugendlichen verwendete EC-Karte. Es ist ohne Weiteres vorstellbar, dass der Jugendliche, der an sich nicht zum Zigarettenkauf berechtigt ist, entsprechende Karten von Freunden oder Eltern nutzen wird. Die Eignung eines auf der EC-Karte aufgebrachten Altersmerkmales zur Durchsetzung der Zugangssperre erscheint daher höchst zweifelhaft.

Selbst wenn das Aufbringen des Altersmerkmales als geeignet angesehen werden könnte, bestehen darüber hinaus auch Zweifel an der Erforderlichkeit dieser Maßnahme. Der Anteil der Jugendlichen unter 16 Jahren, die ein eigenes Konto mit EC- oder Bankkarte besitzen, beträgt weniger als 1%. Das wiederum bedeutet, dass 99% der Automatennutzer ohnehin das zum Tabakkauf erforderliche Mindestalter aufweisen würden. Aus diesem Grunde könnte es zur Erreichung des Ziels ausreichen, lediglich die herkömmliche EC-Karte – ohne Altersmerkmal – zur Authentifizierung am Automaten einzusetzen. Ein dementsprechendes Pilotprojekt wird bereits in Bayern getestet. Wir werden dieses Projekt im Kreis der Aufsichtsbehörden weiter begleiten.

25. Handel und Verkehr

25.1 E-Commerce – Zahlungsverfahren im Internet

Aus datenschutzrechtlicher Sicht sollten sich Zahlungssysteme im Internet an den Kriterien Datensparsamkeit und Datenvermeidung, Datensicherheit sowie Transparenz gegenüber dem Kunden orientieren.

Viele Unternehmen nutzen mittlerweile auch das Internet zum Warenabsatz. Ob die Verbraucher das Internet als Marktplatz akzeptieren und den Unternehmen eine neue Einnahmequelle eröffnen, hängt entscheidend von der Vertrauenswürdigkeit der Kaufabwicklung ab. Der Verbraucher möchte alle Vorteile des virtuellen Einkaufs nutzen, ohne gleichzeitig Nachteile im Vergleich zum herkömmlichen Bargeschäft zu erfahren. Über den Erfolg eines Internetangebots entscheiden in nicht unerheblichem Umfang datenschutzrechtliche Aspekte.

Das Bundesdatenschutzgesetz enthält den Grundsatz der Datensparsamkeit und Datenvermeidung. Als Möglichkeiten der Datensparsamkeit und -vermeidung nennt das Gesetz in § 3 a insbesondere die Anonymisierung und Pseudonymisierung. Eine datenschutzrechtliche Bewertung der unterschiedlichen Systeme muss sich daher auch an den von den Systemen diesbezüglich eingeräumten Möglichkeiten orientieren. Die Zahlungssysteme sind grob in bargeld- und transaktionsorientierte Verfahren zu trennen.

Mit bargeldorientierten Zahlungssystemen wird der Zahlungsvorgang der Bargeschäfte des täglichen Lebens nachgebildet. Der Kunde kann seine Einkäufe vollständig anonym tätigen. Aus diesem Grunde sind diese Systeme datenschutzrechtlich zu begrüßen.

Bei transaktionsorientierten Zahlungsverfahren fallen hingegen personenbezogene Daten an, aus denen sich grundsätzlich Käuferprofile erstellen lassen können. Aus datenschutzrechtlicher Sicht sollten diese Systeme zumindest die Möglichkeit einer pseudonymen Nutzung gewährleisten.

Weiterhin ist bei diesen Systemen zu beachten, dass nur diejenigen Stellen von den anfallenden Daten Kenntnis erlangen, die von ihnen zur Kaufabwicklung zwingend benötigt werden. So wird es in der Regel nicht erforderlich sein, dass das Kreditinstitut im Einzelnen Kenntnis über die vom Verbraucher gekauften Waren hat. Zur Wahrung des Grundsatzes der Datensparsamkeit wird daher nur die Endsumme an das Kreditinstitut übermittelt werden müssen. Da es mittlerweile viele unterschiedliche Zahlungssysteme gibt, die auf unterschiedlichen Grundlagen arbeiten und bei denen unterschiedliche Arten personenbezogener Daten erhoben und teilweise auch übermittelt werden, sollte dem Verbraucher das zum Einsatz gebrachte Zahlungssystem transparent gemacht werden. Nur ein informierter Verbraucher wird entscheiden können, ob und zu welchen Konditionen er einen virtuellen Einkauf wünscht.

Auch der Zentrale Kreditausschuss hat mittlerweile ein internetfähiges Chipkartenterminal zugelassen, mit dem im Internet per Geldkarte bezahlt werden kann. Der Zentrale Kreditausschuss hat zugesichert, dass bei der Abwicklung von Geldkartenzahlungen über das Internet keine Differenzierung zwischen kontogebundenen und kontoungebundenen Karten mit Geldkarten-Funktion vorgesehen ist, sodass auch immer eine Zahlung mittels kontoungebundener Karte möglich ist. Dies entspricht einer datenschutzfreundlichen Regelung (vgl. 24.2) – zumindest wenn der Verbraucher über die Möglichkeit des Einsatzes einer kontoungebundenen Karte informiert wird.

Wir werden die Entwicklung der Zahlungssysteme weiterhin beobachten und auf die Möglichkeiten datenschutzfreundlicher Anwendungen hinweisen.

25.2 Kundenkarten

Kundenkartenanträge sind transparent und datensparsam zu gestalten.

Bereits im 17. TB (22.3) hatten wir über den Einsatz so genannter Kundenkarten berichtet. Die Ausgabe dieser Karten hat auch im Berichtszeitraum weiter zugenommen. Grund dafür waren unter anderem der Wegfall des Rabattgesetzes und der Zugabeverordnung im Juli 2001.

Bei der Ausgabe von Kundenkarten ist datenschutzrechtlich zu beachten, dass in den Anträgen ohne ausdrückliche Einwilligung des Kunden nur die personenbezogenen Daten erhoben werden dürfen, die zur Erfüllung des Vertragszweckes erforderlich sind. Vertragszweck ist es in der Regel, Kunden über die Gewährung eines Rabatts an das Unternehmen zu binden. Dafür dürften grundsätzlich Name und Anschrift und gegebenenfalls das Geburtsdatum des Kunden ausreichend sein. Jedes darüber hinaus gehende Datum – wie z.B.

Angaben zu Hobbys, Beruf etc. – darf nur mit der ausdrücklichen Einwilligung des Kunden erhoben werden. Der Kunde muss folglich darüber aufgeklärt werden, dass die entsprechende Angabe freiwillig erfolgen kann. Auch dürfen dem Kunden keine Nachteile entstehen, wenn er nicht bereit ist, diese Angaben zu machen.

Besorgte Bürger berichteten uns von einem Hamburger Unternehmen, das in den Kundenkartenanträgen eine Fülle von Daten verlangt hatte, ohne die Kunden darauf hinzuweisen, dass viele der Angaben lediglich auf freiwilliger Basis erhoben werden. Wir wiesen das Unternehmen auf die datenschutzrechtliche Unzulässigkeit der Datenerhebung hin und unterbreiteten Vorschläge zu einer datenschutzfreundlichen Gestaltung des Antrags. Aus datenschutzrechtlicher Sicht war es für uns wichtig, dass der Grundsatz der Datensparsamkeit schon im Kartenantrag umgesetzt wird und nur die Daten als Pflichtangaben erhoben werden, die für die Vertragsabwicklung erforderlich sind.

Ein weiteres datenschutzfreundliches Anliegen war uns eine für den Kunden transparente Antragsgestaltung. Der Kunde kann nur dann frei entscheiden, welche persönlichen Daten er preisgibt, wenn er darüber aufgeklärt wird, was mit seinen Angaben geschieht. Auch sollte der Kunde informiert werden, welche weiteren Daten beim Einsatz der Kundenkarte anfallen werden. Das Hamburger Unternehmen hat die Anträge entsprechend unseren Vorschlägen umgestaltet, sodass unsere datenschutzrechtlichen Bedenken ausgeräumt wurden.

25.3 Videoüberwachung

25.3.1 Videoüberwachung im Hauptbahnhof

Die von der Deutschen Bahn AG geplanten bundesweit einheitlichen Piktogramme zur Videoüberwachung setzen das datenschutzrechtliche Transparenzgebot in erfreulicher Weise um.

Im 17. TB (23.3) hatten wir darüber berichtet, dass sich bei der Videoüberwachung des Hamburger Hauptbahnhofes durch sogenannte „Dome-Kameras“ das Problem stellte, die Videoüberwachung nicht ausreichend zu kennzeichnen. Nach Gesprächen mit der für den Hauptbahnhof zuständigen Station und Service AG, eines Tochterunternehmens der Deutschen Bahn AG, konnte erreicht werden, dass Hinweise auf den Kameraeinsatz in ausreichender Zahl und Größe angebracht wurden. Dabei wurden auch die Eingänge zum Bahnhof berücksichtigt, so dass nunmehr gewährleistet ist, dass die Betroffenen bereits beim Eintreten in den videoüberwachten Bereich davon Kenntnis erhalten.

Aus datenschutzrechtlicher Sicht besonders erfreulich ist die Tatsache, dass sich die Deutsche Bahn AG entschlossen hat, die Gestaltung der Hinweise

bundesweit optisch zu verändern. So wird künftig mit einem für alle Betroffenen deutlich sichtbaren, verständlichen Piktogramm auf die Videoüberwachung in Bahnhöfen hingewiesen.

25.3.2 Videoüberwachung in U-Bahnen

Der Testversuch der Hamburger Hochbahn (HHA) zur Videoüberwachung in öffentlichen Verkehrsmitteln wird unter Beachtung von Auflagen in erweiterter Form fortgeführt.

Die HHA hat im Berichtszeitraum den Testbetrieb der Videoüberwachung fortgeführt und weitere Wagen in den U-Bahnen mit Videokameras und digitalen Aufzeichnungsgeräten ausgerüstet. Die Wagen werden im Wechsel auf allen U-Bahnlinien eingesetzt. Hintergrund ist, dass die Zahl der Sachbeschädigungen in den beiden zunächst im Rahmen des Testversuchs überwachten Wagen (vgl. 17.TB, 23.3) praktisch völlig zurückgegangen ist. Der erweiterte Testbetrieb soll neben der Abschreckung potentieller Straftäter und einer Beweissicherung dazu führen, das Sicherheitsgefühl der Fahrgäste zu steigern und die Kosten der Videoüberwachung zu ermitteln.

Die Aufnahmen erfolgen durch zwei festeingestellte Kameras pro Wagen. Die Datenaufzeichnungen werden nach 24 Stunden automatisch überschrieben, falls die Aufnahmen nicht wegen eines Schadensfalls sichergestellt und ausgewertet werden. Dies ist der Fall, wenn Fahrgäste eine Meldung machen oder Schäden in einem Fahrzeug gefunden werden. Eine ständige Beobachtung der Videoaufnahmen erfolgt nicht. An den überwachten Wagen ist ein Hinweisschild mit dem Text „Dieser Wagen wird zu Ihrer Sicherheit videoüberwacht“ angebracht.

Die Ausgestaltung des Verfahrens ist von Anfang an mit uns erörtert worden. Auch die Ausdehnung der Videoüberwachung auf weitere Wagen haben wir eingehend mit der HHA besprochen. Aus datenschutzrechtlicher Sicht haben wir zusätzliche Videokameras unter den nachfolgenden Auflagen für vertretbar gehalten: Es muss gewährleistet sein, dass Fahrgäste die Möglichkeit haben, in einem Wagen des videoüberwachten Fahrzeugs auch unbeobachtet zu fahren. Zum anderen sind Sicherungsmaßnahmen zu ergreifen, die das Missbrauchsrisiko der aufgezeichneten Aufnahmen gering halten. Die HHA hat zugesagt, im erweiterten Testbetrieb diese Auflagen zu beachten.

Die datenschutzrechtliche Bewertung des Vorhabens richtet sich grundsätzlich nach der bis zum 22. Mai 2001 geltenden Fassung des BDSG, da es sich bei der Videoüberwachung durch die HHA um eine Verarbeitung personenbezogener Daten handelt, die noch vor dem Inkrafttreten der geänderten Fassung des BDSG am 23. Mai 2001 begonnen wurde. Als Rechtsgrundlage für die Videoüberwachung wurde § 28 Absatz 1 Satz 1 Nr. 2 BDSG herangezogen.

Zur Bewertung der Frage, inwieweit ein erweiterter Testbetrieb aus datenschutzrechtlicher Sicht zulässig ist, war das rechtliche Interesse der HHA an der geplanten Ausweitung der Videoüberwachung sowie das allgemeine Persönlichkeitsrecht der davon betroffenen Fahrgäste zu berücksichtigen und gegeneinander abzuwägen. Dabei war insbesondere zu beachten, dass eine ständige Videoüberwachung eines öffentlich zugänglichen Raumes nach der Rechtsprechung des BGH einen weitreichenden Eingriff in das allgemeine Persönlichkeitsrecht darstellt und allenfalls dann zulässig sein kann, wenn keine anderen zumutbaren Mittel zur Verfügung stehen, um schwerwiegende Beeinträchtigungen der Rechte Dritter abzuwehren (vgl. BGH NJW 1995, 1955ff). Eine dauerhafte, wiederholte und ständige Videoüberwachung, der sich ein Betroffener nicht entziehen kann, greift stärker in das allgemeine Persönlichkeitsrecht ein als eine nur punktuelle und gelegentliche Überwachung. Zu berücksichtigen war dabei, dass die HHA als öffentliches Unternehmen Grundrechte der Fahrgäste besonders zu beachten hat und dass es sich bei öffentlichen Verkehrsmitteln um einen Aspekt der Daseinsvorsorge handelt, auf den viele Menschen angewiesen sind.

Da durch die Videoüberwachung nicht nur Sachbeschädigungen in beträchtlicher Schadenshöhe sondern auch gewalttätige Übergriffe auf Fahrgäste verhindert werden sollen, hat die Aufsichtsbehörde eine Erweiterung der Videoüberwachung durch die HHA als zulässig erachtet, solange die betroffenen Fahrgäste nicht flächendeckend überwacht werden, sondern weiterhin bei Bedarf die Möglichkeit besteht, unbeobachtet U-Bahn zu fahren. Zur Gewährleistung der Persönlichkeitsrechte der Betroffenen hat die HHA zugesagt, pro Zug mindestens in einem Wagen keine Kameraaufzeichnungen durchzuführen. Die Wagen werden entsprechend deutlich gekennzeichnet. Die HHA hat zudem die von der Aufsichtsbehörde geforderten Maßnahmen gemäß § 9 BDSG zur Verhinderung eines Missbrauchs der Videoaufzeichnungen getroffen. Dazu gehört insbesondere eine Verschlüsselung der Bilddaten, eine begrenzte Zugriffsberechtigung für ausgewählte Mitarbeiter und eine Dienstanweisung, die diese Vorgaben verbindlich regelt.

Inzwischen ist zum 23. Mai 2001 das novellierte BDSG in Kraft getreten, in dem der neu eingefügte § 6 b die Zulässigkeit der Videoüberwachung regelt. Auch bei Zugrundelegung dieser neuen Vorschrift wäre die Erweiterung der Videoüberwachung durch die HHA unter den genannten Auflagen zulässig.

Kurz vor Redaktionsschluss dieses Tätigkeitsberichts hat uns die HHA mitgeteilt, dass sie nach Abschluss des Projekts nunmehr die Einführung einer flächendeckenden Videoüberwachung in U-Bahnen beabsichtigt. Wir werden die weitere Entwicklung des Vorhabens datenschutzrechtlich begleiten.

26. Werbung/Adresshandel

26.1 AG Internetauftritt der Werbewirtschaft

Die Verbände der Werbewirtschaft haben Kriterien für einen datenschutzgerechten Internetauftritt kommerzieller Anbieter vorgelegt.

Werbung im Bereich des Internet nimmt stetig zu und wirft neben wettbewerbs- auch zahlreiche datenschutzrechtliche Fragen auf. Unsicherheiten für die Praxis ergeben sich nicht zuletzt aufgrund einer unübersichtlichen und aus einer Vielzahl verschiedener Regelungsmaterien bestehenden Gesetzgebung.

Die Verbände der Werbewirtschaft – Deutscher Direktwerbe – und Direktmarketing Verband (DDV), Zentralverband der deutschen Werbewirtschaft (ZAW) und Deutscher Multimedia Verband (dmmv) – haben mit dem Entwurf eines Handlungsleitfadens für die Werbewirtschaft Kriterien entwickelt, um diese Unsicherheiten zu beseitigen und eine Orientierungshilfe für die Praxis zu bieten. Der Leitfaden behandelt folgende Themen:

- Anbieterkennzeichnung
- Einwilligung
- Auskunftsrechte
- Cookies
- Übermittlung in Drittstaaten
- Datenschutzpolitik
- Datensicherheit

Eine Arbeitsgruppe aus einigen Aufsichtsbehörden für den Datenschutz und den Vertretern der Werbewirtschaft wird diesen Entwurf weiter diskutieren. Wir werden über den Fortgang berichten.

26.2 Sonstiges

Weitere Themen zur Werbung und zum Adresshandel waren:

– Unverlangt zugesandte Werbefaxe

– E-Mail-Werbung

– Gewinnspiele und Nutzung der Adressen zu Werbezwecken

27. Arbeitnehmerdatenschutz

27.1 Internet und E-Mail am Arbeitsplatz

Sofern der Arbeitgeber seinen Mitarbeitern die private Nutzung von Internet und E-Mail am Arbeitsplatz erlaubt, sind zusätzliche rechtliche Anforderungen zu beachten.

Bei der dienstlichen Nutzung von Internet und E-Mail ist das Teledienstegesetz (TDG) und das Teledienstedatenschutzgesetz (TDDSG) nicht anzuwenden, da es sich nicht um ein Angebot oder eine Nutzung eines Dienstes durch Dritte handelt. Die Anwendbarkeit der Vorschriften würde voraussetzen, dass Anbieter und Nutzer von Telediensten zwei verschiedene Instanzen sind; jedoch ist zumindest im Falle der ausschließlich dienstlichen Überlassung von Telediensten durch den Arbeitgeber an die Arbeitnehmer genau diese Voraussetzung zweifelhaft („In-sich-Verhältnis“).

Der Arbeitgeber wäre damit insbesondere nicht verpflichtet, den Arbeitnehmern die anonyme oder pseudonyme Nutzung dieser Dienste einzuräumen. Bezogen auf die dienstliche Nutzung von Telediensten im Arbeitsverhältnis fänden lediglich die Vorschriften des BDSG Anwendung.

Gegen eine solche eingeschränkte Definition des Anwendungsbereichs wird angeführt, dass der Begriff des „Angebots“ nicht zwingend ein Außenverhältnis im Sinne einer Kundenbeziehung voraussetze und lediglich als technisch-organisatorisches Bereithalten oder Vermitteln von Telediensten zu sehen sei.

Der Gesetzgeber hat hier mittlerweile im Rahmen der Novellierung des TDDSG eine Klärung vorgenommen (siehe 3.5.1). Danach sollen die Vorschriften des TDDSG nicht bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten in Dienst- und Arbeitsverhältnissen gelten, soweit die Nutzung zu ausschließlich beruflichen oder dienstlichen Zwecken erfolgt.

Auch im Falle der Nichtanwendbarkeit der Vorschrift auf die rein dienstliche Nutzung von Telediensten in Dienst- und Arbeitsverhältnissen wird die Erhebung, Verarbeitung und Nutzung der Nutzungsdaten nicht ohne Einschränkung zulässig sein, denn die Daten könnten zur Kontrolle der Arbeitsleistung der Beschäftigten verwendet werden. Die Eingriffe in das Persönlichkeitsrecht der Beschäftigten müssen auch bei der Nutzung von Kommunikationsmedien im Rahmen der Verhältnismäßigkeit bleiben.

Zudem müssen in jedem Fall die Mitbestimmungsrechte der Mitarbeitervertretungen beachtet werden. Mitbestimmungsrechte gemäß §87 BetrVG sind gegeben, wenn eine technische Einrichtung zur Überwachung des Verhaltens oder der Leistung der Mitarbeiter bestimmt ist. Für die konkrete Regelung auf Ebene des Betriebs oder der Dienststelle bietet sich dann wegen des ohnehin bestehenden Mitbestimmungsrechts der Abschluss einer Dienstvereinbarung an, in der sowohl die generellen Regeln zur Nutzung von Telediensten durch

die Beschäftigten als auch zur Erhebung, Verarbeitung und Nutzung der bei der Inanspruchnahme der Dienste anfallenden Daten festgelegt werden.

Wer Internet und E-Mail am Arbeitsplatz für private Zwecke nutzen darf und in welchem Umfang, entscheidet der Arbeitgeber. Einen Rechtsanspruch auf die private Nutzung der dienstlich zur Verfügung gestellten Kommunikationsmittel gibt es nicht. Soweit Beschäftigten eine private Nutzung der Dienste erlaubt ist, bestehen – nach derzeitigem und nach zukünftigem Recht – keine Zweifel daran, dass die Vorschriften in vollem Umfang anzuwenden sind; der Arbeitgeber bzw. Dienstherr ist als Anbieter von Telediensten anzusehen, die Beschäftigten als Nutzer. Dies hat nicht automatisch die Konsequenz, dass sich die private Inanspruchnahme einer Regelung durch Dienst- oder Betriebsvereinbarungen entzieht; allerdings sind an die Datenschutzbestimmungen dieser betrieblichen Vorschriften strengere Ansprüche zu stellen als bei ausschließlich dienstlicher Nutzung, speziell was die Überwachung dieser privaten Kommunikation anbelangt.

Insbesondere ist der Arbeitgeber zur Wahrung des Fernmeldegeheimnisses gemäß § 85 TKG verpflichtet, soweit er zusammen mit dem Teledienst auch einen Telekommunikationsdienst erbringt. Davon ist in der Regel auszugehen, weil auch die telekommunikative Basis der Teledienste (lokale Netze, Übergänge zu öffentlichen Netzen usw.) den Beschäftigten im Regelfall durch den Arbeitgeber bzw. Dienstherrn zur Verfügung gestellt wird.

Eine generelle Protokollierung oder gar Überwachung der privaten Inanspruchnahme von Telediensten durch den Arbeitgeber bzw. Dienstherrn würde die verfassungsmäßig garantierten Rechte sowohl der betroffenen Beschäftigten als auch der (gegebenenfalls betriebsexternen) Nutzer beeinträchtigen. Sie ist daher unzulässig.

Die Umsetzung der Rechtslage (Anwendbarkeit der Vorschrift nur auf die private Nutzung der Teledienste durch Beschäftigte, nicht jedoch auf die dienstliche Inanspruchnahme) stößt in der Praxis auf erhebliche Probleme. Zum einen haben viele Unternehmen, die ihren Beschäftigten den Zugriff auf das Internet und die Nutzung von E-Mail und anderer Teledienste erlauben, keine ausdrücklichen Vorgaben hinsichtlich der dienstlichen oder privaten Nutzung aufgestellt.

Zum anderen ist die Unterscheidung des jeweiligen Nutzungsvorgangs als dienstlich oder als privat schwierig. Eine derartige Unterscheidung könnte im Einzelfall ohne (unzulässige!) Inhaltskontrolle nicht vorgenommen werden. Schließlich ist auch im Hinblick auf die Interessen der Unternehmen bzw. Dienstherrn an einem effektiven Schutz der betrieblichen Datenverarbeitung vor Störungen von außen (etwa gegen das Einschleusen von „Trojanischen Pferden“, Viren oder sonstigen Schadprogrammen) die Festlegung verschiedener Schutzmaßnahmen je nach privater oder dienstlicher Nutzung der Teledienste dem Arbeitgeber kaum zumutbar.

Gegebenenfalls kann der Problemlage dadurch Rechnung getragen werden, dass für die kritischen Vorgänge (Vertretung, ungeplante Abwesenheit, Aufklärung von Dienstvergehen) spezielle Regelungen getroffen werden, die zwischen privaten und dienstlichen Kommunikationsvorgängen unterscheiden. Auf jeden Fall müssen die betroffenen Beschäftigten darüber ins Bild gesetzt werden, dass im Ausnahmefall auch Dritte (wenn auch unter definierten restriktiven Bedingungen) auf E-Mail zugreifen können.

Zudem sollten sie darauf hingewiesen werden, mit welchen Hilfsmitteln sie ihre Kommunikationsvorgänge gegen einen unberechtigten Zugriff schützen können (Verschlüsselung, Kennzeichnung von Vorgängen als privat usw.). Schließlich müssen die technischen Systeme so gestaltet werden, dass das Risiko eines unberechtigten Zugriffs minimiert wird, insbesondere durch Gewährleistung einer effektiven Datenlöschung sowohl auf Mailservern als auch auf Festplatten lokaler Systeme.

Eine Muster-Betriebsvereinbarung ist abgedruckt in der Zeitschrift RDV 2001, Heft 1. Weitere Muster-Betriebsvereinbarungen können u.a. abgerufen werden unter www.tse-hamburg.de und www.soliserv.de.

27.2 Sonstiges

Weitere Themen zum Arbeitnehmerdatenschutz waren:

- Rücksendung von Bewerbungsunterlagen
- Vorlage von polizeilichen Führungszeugnissen
- Schweigepflichtentbindungserklärung bei Einstellungsuntersuchungen
- Personalfragebogen

28. Internationaler Datenverkehr

Die Übermittlung personenbezogener Daten ins – insbesondere außereuropäische – Ausland bedarf in jedem Fall einer sorgfältigen datenschutzrechtlichen Zulässigkeitsüberprüfung.

Angesichts der Neuregelung der Übermittlung personenbezogener Daten ins Ausland ist für die Unternehmen ein zunehmender Beratungsbedarf durch die Aufsichtsbehörden entstanden. Gerade bei Konzernen mit internationalen Verflechtungen wird versucht, insbesondere die Personaldatenverarbeitung so zu vereinheitlichen, dass sowohl die Datenverarbeitung innerhalb Deutschlands und Europas als auch sämtliche Übermittlungen ins außereuropäische Ausland datenschutzrechtlich abgedeckt sind. Dabei wird in der Regel verkannt, dass im Hinblick auf datenschutzrechtliche Zulässigkeiten jede Transaktion gesondert auf den Zweck und die Erforderlichkeit zu untersuchen ist. Darüber hinaus ist in der Mehrzahl der Fälle auch das schutzwürdige Interesse der Betroffenen gegen die berechtigten Interessen der verantwortlichen Stelle

abzuwägen. Zur Veranschaulichung werden im Folgenden zwei Beispiele wiedergegeben, wie unterschiedlich Unternehmen mit diesem Problem umgehen.

28.1 Personalinformationssysteme und Betriebsvereinbarung

Der Datenschutzbeauftragte eines Konzerns hat die Datenschutzaufsichtsbehörde um Beurteilung der Zulässigkeit eines konzernweit einzuführenden Personalinformationssystems gebeten. Bei der Überprüfung hat sich herausgestellt, dass eine Vielzahl sensibler Mitarbeiter- und auch z.B. Hinterbliebenendaten der deutschen Konzernunternehmen in dieses, in den USA installierte, System eingespeist und dem Zugriff der verschiedenen verantwortlichen Stellen ausgesetzt werden sollen. Als Rechtsgrundlage sollte eine Rahmenbetriebsvereinbarung dienen. Da die Übermittlung derartiger personenbezogener Daten innerhalb der Europäischen Union grundsätzlich zulässig ist, sollte die Vereinbarung ein konzernweites Datenschutzniveau im Sinne der EG-Datenschutzrichtlinie herstellen.

Der datenschutzrechtlichen Bewertung durch die Aufsichtsbehörde lagen die Vorschriften des novellierten Bundesdatenschutzgesetzes (BDSG) zugrunde. Nach § 4 Abs. 1 BDSG ist die Datenerhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, sofern dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder der Betroffene eingewilligt hat. Neben den Vorschriften des BDSG und der Einwilligung der Betroffenen sind dabei auch Betriebsvereinbarungen als sonstige Rechtvorschriften relevant.

Als gesetzliche Erlaubnisnorm für die Datenweitergabe innerhalb der Mitgliedstaaten der Europäischen Union kommt § 28 BDSG in Betracht (vgl. § 4b Abs. 1 BDSG). Die Übermittlung personenbezogener Daten an ausländische Stellen ist ebenfalls zunächst nach § 28 BDSG zu beurteilen. Sowohl die Datenweitergabe an Stellen innerhalb Europas als auch an Stellen in Drittländer hat nach dieser Vorschrift zu unterbleiben, soweit die Betroffenen schutzwürdige Interessen an dem Ausschluss der Übermittlung haben. Die Aufsichtsbehörde ist davon ausgegangen, dass der vorgesehenen umfangreichen Datenübermittlung überwiegende schutzwürdige Interessen der Betroffenen entgegenstehen. Einer Bewertung, ob durch die internationale konzernweite Datenschutzvereinbarung ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte im Sinne des § 4c Abs. 2 BDSG auch in Drittländern gewährleistet werden kann, bedurfte es daher nicht mehr. Nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG ist die Datenerhebung, -verarbeitung und -nutzung von personenbezogenen Daten als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit den Betroffenen dient. Die weltweite Datenweitergabe durch Einräumung des lesenden Zugriffs für einen großen Personenkreis stellt eine Datenübermittlung dar. Derartig umfassende

Datenübermittlungen entsprechen nicht der Zweckbestimmung der Vertragsverhältnisse mit den Betroffenen, da sie keinen Bezug zur konkreten Tätigkeit aufweisen. Es war nicht ersichtlich, dass die Datenübermittlungen in dem vorgesehenen Umfang geeignet sind, der Erfüllung der Rechte und Pflichten aus dem Vertragsverhältnis zu dienen. Sie sind daher nicht nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG zulässig.

Als weiterer Erlaubnistatbestand wurde § 28 Abs. 1 Satz 1 Nr. 2 BDSG geprüft. Danach ist die Datenübermittlung zur Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass schutzwürdige Interessen des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegen. Der Begriff berechtigte Interessen der verantwortlichen Stelle ist dabei weit auszulegen, so dass auch die Verbesserung der Qualität des konzernweiten Personalmanagements als berechtigtes Interesse des deutschen Konzernunternehmens angesehen werden kann. Dieses Interesse bezieht sich allerdings auf die aktiven Arbeitnehmer, die davon profitieren könnten – möglicherweise auch auf Bewerber – und beschränkt sich auf die Daten, die zu diesem Zweck erforderlich sind. Nicht erforderlich sein dürften z.B. Privatanschrift, Sozialversicherungsnummer, Bankverbindung oder der Anstellungsvertrag. Angehörige von Mitarbeitern, ausgeschiedene Arbeitnehmer und Hinterbliebene werden von dem berechtigten Interesse nicht erfasst, so dass es insofern auch noch an der Erforderlichkeit der Datenweitergabe fehlt.

Auch wenn ein berechtigtes Interesse der verantwortlichen Stellen bestehen würde, überwiegen in jedem Fall die schutzwürdigen Interessen der Betroffenen an dem Ausschluss der Weitergabe ihrer Daten, da diese zu sensibel und nicht nach Erforderlichkeitskriterien für einen konkreten Zweck differenziert sind (z.B. Bankverbindung, Sozialversicherungsnummer). Soweit es schließlich um statistische Erfassungen und Auswertungen durch andere Unternehmen geht, sind personenbezogene Daten überhaupt nicht erforderlich und überwiegende berechtigte Interessen der Betroffenen am Ausschluss der Weitergabe gegeben.

Die konzernweite Datenweitergabe ist auch nicht nach § 28 Abs. 3 Satz 1 Nr. 1 BDSG zulässig. Es ist zweifelhaft, ob der lesende Zugriff auf sämtliche der angegebenen Daten zur Wahrung berechtigter Interessen der Konzerngesellschaften überhaupt erforderlich ist. Selbst bei weiter Auslegung des Begriffs berechtigte Interessen kämen für eine Weitergabe nur wenige differenzierte Daten von Mitarbeitern in Betracht (s.o. zu § 28 Abs. 1 Satz 1 Nr. 2 BDSG). Auch bei Vorliegen von berechtigten Interessen der Konzerngesellschaften ist allerdings wegen der Sensibilität der zu übermittelnden personenbezogenen Daten davon auszugehen, dass die Betroffenen ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung ihrer Daten an andere Konzerngesellschaften haben.

Nach Auffassung der Aufsichtsbehörde wäre die Übermittlung der personenbezogenen Arbeitnehmerdaten in dem vorgesehenen Umfang auch dann nicht zulässig, wenn sie Gegenstand einer Betriebsvereinbarung wäre. Betriebsvereinbarungen werden nach überwiegender Ansicht als eine „andere Rechtsvorschrift“ im Sinne des § 4 Abs. 1 BDSG und damit als Erlaubnistatbestand angesehen. Zweifelhaft ist allerdings, ob Betriebsvereinbarungen die Übermittlungen personenbezogener Daten in Drittstaaten rechtfertigen können.

Unabhängig von der Klärung dieser Rechtsfrage stellt sich jedoch zunächst die Frage, ob Betriebsvereinbarungen die Übermittlung personenbezogener Daten rechtfertigen können, wenn sie das durch das BDSG gewährleistete Schutzniveau unterschreiten. Dieses Schutzniveau würde im vorliegenden Fall durch eine Betriebsvereinbarung eingeschränkt werden. Die vorgesehenen Datenübermittlungen greifen unverhältnismäßig in die Rechte der Betroffenen ein, da sie überwiegend für die Erreichung der Unternehmenszwecke nicht erforderlich sind und den schützenswerten Interessen der Betroffenen nicht ausreichend Rechnung getragen wird. Die Aufsichtsbehörde ist wie die überwiegende Literatur der Auffassung, dass Betriebsvereinbarungen den Datenschutz gegenüber dem BDSG nicht einschränken können. Betriebsvereinbarungen können nur soweit vom BDSG abweichen, wie sie die dort getroffenen Regelungen durch Schutzvorkehrungen ersetzen, die den besonderen Beschäftigungsbedingungen besser angepasst, allerdings mindestens so weitreichend sind. Diese Voraussetzungen lagen aber nicht vor, da nach den gesetzlichen Erlaubnistatbeständen des BDSG eine so weitreichende Datenverarbeitung nicht zulässig wäre.

Wir haben die vorstehende Problematik in die Arbeitsgruppe Internationaler Datenverkehr eingebracht, die die Angelegenheit rechtlich aufgreifen und einer bundesweit einheitlichen Rechtsauffassung zuführen wird.

28.2 Einzeleinwilligungen

Einen anderen Weg der generellen Regelung versuchte ein weiterer Konzern. Durch die Einholung einer umfassenden Einwilligungserklärung von jedem einzelnen Mitarbeiter sollte eine datenschutzgerechte weltweite Übermittlung der Mitarbeiterdaten ermöglicht werden. Grundsätzlich können Einwilligungen sowohl fehlende Rechtsgrundlagen ersetzen als auch anderenfalls nicht zulässige Datenübermittlungen in Drittländer ermöglichen.

Problematisch wird die Erteilung solcher Einwilligungen jedoch dann, wenn es sich nicht mehr um einzeln von einem Unternehmen eingeholte Erklärungen handelt, sondern alle Mitarbeiter pauschal in sämtliche denkbaren Übermittlungen einwilligen sollen. In dem von der Aufsichtsbehörde zu beurteilenden Fall hatte die Konzernleitung zulässige, unzulässige, völlig unproblematische und sensibelste Verarbeitungen der Mitarbeiterdaten nebeneinander auf-

gezählt und wollte „freiwillig“ von allen eine Unterschrift. Die Befürchtung mancher Mitarbeiter, es seien vermutlich Übermittlungen geplant, die ihnen letztlich schaden könnten, konnte in dieser Pauschalität nach Durchsicht von der Aufsichtsbehörde nicht geteilt werden. Zwar war nicht auszuschließen, dass solche Nachteile sich langfristig ergeben könnten. Zunächst machte die Einwilligung jedoch den Anschein, als wolle man sich lediglich vorsorglich gegen alle Eventualitäten absichern.

Obwohl es im Einzelfall, insbesondere z.B. bei leitenden Mitarbeitern, auf freiwilliger Basis durchaus zulässig sein kann, in die Übermittlung sensibler Personaldaten an einen bestimmten Personenkreis einzuwilligen, erscheint dies im Falle aller Mitarbeiter ohne Ansehen der Erforderlichkeit datenschutzrechtlich unzulässig. Insbesondere fehlt es gegenüber dem Arbeitgeber an der für die Freiwilligkeit notwendigen Unabhängigkeit, im Zweifel die Unterschrift auch verweigern zu können. In dem zur Beurteilung anstehenden Einzelfall kam hinzu, dass auch in Übermittlungen an staatliche Stellen eingewilligt werden sollte, so dass der Verdacht entstand, das Unternehmen wolle sich von der Prüfung des Vorliegens der gesetzlichen Voraussetzungen befreien.

29. Meldepflicht und Prüftätigkeit

29.1 Meldepflicht

Die Aufsichtsbehörde führt nach § 38 Abs. 2 BDSG ein Register der Stellen, die der Meldepflicht unterliegen. Bis zur Novellierung des Bundesdatenschutzgesetzes waren Stellen, die geschäftsmäßig personenbezogene Daten zum Zwecke der personenbezogenen oder anonymisierten Übermittlung speichern oder im Auftrag als Dienstleistungsunternehmen verarbeiten oder nutzen, nach § 32 BDSG meldepflichtig.

Im novellierten BDSG wurde die Meldepflicht vollkommen neu geregelt. Grundsätzlich müssen nicht-öffentliche Stellen alle Verfahren automatisierter Verarbeitungen personenbezogener Daten bei der Datenschutzaufsichtsbehörde melden. Allerdings sind auch einige Ausnahmen vorgesehen. Lediglich Verfahren automatisierter Verarbeitungen, in denen personenbezogene Daten geschäftsmäßig

- zum Zweck der Übermittlung (§ 29 BDSG, z. B. Auskunfteitätigkeit, Adresshandel) oder
- zum Zweck der anonymisierten Übermittlung (§ 30 BDSG, z.B. Markt- und Meinungsforschung)

gespeichert werden, unterfallen ohne Ausnahme der Meldepflicht (§ 4d Abs. 4 BDSG).

Das Merkblatt zur Meldepflicht und die entsprechenden Formulare stehen in unserem Internet-Angebot zum Abruf zur Verfügung.

29.1.1 Register nach § 32 BDSG

Bis zum 22. Mai 2001 waren zu diesem Register 255 Unternehmen gemeldet. Unterteilt nach der Art der meldepflichtigen Tätigkeit ergibt sich folgendes Bild:

- Speicherung zum Zwecke der Übermittlung
  - Auskunfteien/Warndienste 19
  - Adresshändler 3
- Speicherung zum Zwecke der anonymisierten Übermittlung
  - Markt- und Meinungsforschung 24
- Auftragsdatenverarbeitung
  - Direktmarketing 27
  - Servicerechenzentren 24
  - Akten- und Datenträgervernichter 11
  - Mikroverfilmer 5
  - Datenerfasser 19
  - sonstige Auftragsdatenverarbeitung 123

29.1.2 Register nach § 4d BDSG

Nach dem 23. Mai 2001 haben bisher 19 Unternehmen ihre Angaben zur Meldepflicht entsprechend den Vorgaben des § 4e BDSG angepasst oder sich überhaupt zum ersten Mal zum Register gemeldet. Allerdings haben noch nicht alle von uns angeschriebenen, auch nach der Novellierung meldepflichtigen Unternehmen ihre Meldung aktualisiert. Unterteilt nach der Art der meldepflichtigen Verfahren ergibt sich derzeit folgendes Bild:

- Speicherung zum Zwecke der Übermittlung
  - Auskunfteien/Warndienste 9
  - Adresshändler 0
- Speicherung zum Zwecke der anonymisierten Übermittlung
  - Markt- und Meinungsforschung 10

29.2 Prüfungen

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

Auskunfteien/Warndienste	0
Direktmarketing/Adresshändler	1
Markt- und Meinungsforschung	7
Servicerechenzentren	4
Akten- und Datenträgervernichter	1
Mikroverfilmer	2
Datenerfasser	1
sonstige Auftragsdatenverarbeitung	19
gesamt	35

29.3 Bußgeldverfahren

Im Berichtszeitraum wurde gegen ein Unternehmen aus dem Bereich Direktmarketing ein Bußgeldverfahren gemäß § 44 Abs. 1 Nr. 2 BDSG a.F. wegen Verstoßes gegen die Meldepflicht durchgeführt.

Bürgerservice und die Dienststelle

30. Unterstützung der Bürgerinnen und Bürger

Die Eingaben haben erneut deutlich zugenommen. Unsere Veranstaltungen und die Öffentlichkeitsarbeit hatten eine beachtliche Resonanz.

Offenbar fühlen sich die Bürgerinnen und Bürger immer häufiger als – wie es in den Datenschutzgesetzen heißt – „Betroffene“ aufgrund von Datenschutzverstößen. Im Jahr 2000 betrug die Zahl der schriftlichen Eingaben 509 und im Jahr 2001 sogar 610. Wir haben außerdem die Zahl der persönlichen, telefonischen und schriftlichen Beratungen der Bürgerinnen und Bürger ganzjährig seit dem Jahr 2000 festgehalten. Demnach haben wir im Jahr 2000 in fast 1.900 Fällen beraten und im Jahr 2001 in über 2.000 Fällen. Im Sinne unserer vorrangigen Zielsetzung, den Bürgerinnen und Bürgern unmittelbar zu helfen, hat sich dieser Beratungsbereich erneut ausgeweitet.

Hinzu kommen unsere Beratungen öffentlicher und nicht-öffentlicher Stellen mit über 1.600 Fällen im Jahr 2000 und über 1.700 Fällen im Jahr 2001. Auch diese Beratungen kommen unmittelbar oder mittelbar vielen Bürgerinnen und Bürgern zugute.

30.1 Eingaben

Von Anfang Dezember 2000 bis Ende November 2001 gingen 1.119 schriftliche Eingaben ein. Sie betrafen – getrennt für die Jahre 2000 und 2001 – folgende Datenschutzbereiche:

	2000	2001
Versicherungswirtschaft	21	21
Kreditwirtschaft	15	38
private Wohnungswirtschaft	16	11
Versandhandel	9	7
sonst. Handel	11	19
Werbung, Direktmarketing	51	79
Schufa, Auskunfteien	40	47
Markt- und Meinungsforschung	3	6
Vereine	5	7
freie Berufe	4	6
Soziales und Gesundheitswesen, nichtöffentlich	21	19
Personaldatenschutz, nichtöffentlich	20	20
Verkehrswesen, nichtöffentlich	9	5
Sonstiges, nichtöffentlich	47	32
Justiz	19	14
Strafvollzug	12	6
Sicherheitsüberprüfung	-	1
Verfassungsschutz	2	15
Polizei	27	26
Staatsanwaltschaft	8	11
Meldewesen	20	32
Wahlen	-	10
MDK, Kranken- und Pflegedienste	4	15
andere Sozialbereiche	39	32
Gesundheitswesen, öffentlich	12	15
Personaldatenschutz, öffentlich	20	27
Verkehrswesen, öffentlich	7	8
Ausländerwesen	4	12
Finanz-, Steuerwesen	8	4
Bildungswesen	6	4
Wirtschaftsverwaltung	4	2
Telekommunikation	7	15
Teledienste	46	78
Medien	6	5
Personenstandswesen	5	4
Statistik	2	1
Bau-, Vermessungswesen	4	4

	2000	2001
Hochschulen	6	4
Umweltschutz	2	2
Sonstiges, öffentlich	12	7

30.2 Veranstaltungen

Die von mir mitgegründete Hamburger Datenschutzgesellschaft (HDG) unter ihrem 1. Vorsitzenden Rechtsanwalt Dr. Ivo Geis hat ihre Veranstaltungen fortgesetzt. Besondere Resonanz finden dabei die Foren zusammen mit der Handelskammer Hamburg, die zu aktuellen Datenschutzthemen für die Wirtschaft jeweils im Frühjahr durchgeführt werden. Im Mai 2000 stand die Veranstaltung in der Handelskammer unter dem Thema „Datenschutz und Datensicherheit beim Electronic Banking“; im Juni 2001 fand das Forum zum Thema „Bezahlen im Internet“ statt. Bei unseren Herbstveranstaltungen im Warburg-Haus hielt Frau Prof. Kollek, Universität Hamburg, am 28. September 2001 einen Vorträg über „Genanalyse und Datenschutz“; Anfang Dezember 2001 sprach dort Dr. Brühann von der Europäischen Kommission über „Datenschutz in Europa – die Perspektiven nach der Richtlinie“.

Im Jahr 2001 haben wir außerdem eigene Veranstaltungen aus Anlass „20 Jahre Datenschutz in Hamburg“ durchgeführt, nachdem das erste Hamburgische Datenschutzgesetz am 1. Mai 1981 in Kraft getreten war. Im Mai 2001 wurde im DAG-Gebäude als erstem Sitz des Hamburgischen Datenschutzbeauftragten eine Podiumsveranstaltung „Datenschutz im Wandel“ mit Vertretern aus Politik, Verwaltung, Wirtschaft und Medien durchgeführt; nach einem Rückblick auf die vergangenen 20 Jahre ging es dabei insbesondere um die Zukunftsaussichten des Datenschutzes. Ende Mai 2001 haben wir zum zweiten Mal einen Bürgernachmittag in der Dienststelle am Baumwall mit Einzelberatungen und Internet-Demonstrationen veranstaltet. Außerdem haben wir mit Bürgerberatungen in den Kundenzentren der Bezirksämter begonnen, erstmals an einem Nachmittag im September 2001 in Bezirksamt Hamburg Nord.

30.3 Öffentlichkeitsarbeit

Nach der erneuten Novellierung des Hamburgischen Datenschutzgesetzes (2.2.1) haben wir die Broschüre „Hamburgisches Datenschutzrecht 2001“ herausgegeben. Dort ist das Hamburgische Datenschutzgesetz mit den Änderungen vom 30. Januar 2001 wiedergegeben; daran schließen sich ausführliche Erläuterungen zum Gesetz insbesondere anhand der amtlichen Begründungen an. Die Broschüre enthält außerdem erstmals eine Liste der Hamburgischen Gesetze und Verordnungen mit den Bezeichnungen und Fundstellen von rund 70 bereichsspezifischen Datenschutzregelungen, von den Datenschutzbestimmungen für die Hamburgische Bürgerschaft bis zu Datenschutzvorschriften für den Gesundheitsbereich.

Nach der Novellierung des Bundesdatenschutzgesetzes gemäß der EG-Datenschutzrichtlinie (2.1.2) haben wir unser überarbeitetes Datencheckheft – nunmehr mit dem Titel „Kennen Sie Ihre neuen Datenschutzrechte?“ – im Mai 2001 in 6. Auflage mit diesmal 10.000 Exemplaren veröffentlicht. Davon gingen allein 6.000 Exemplare an zahlreiche Stellen in der Stadt zur unmittelbaren Weitergabe an die Bürgerinnen und Bürger, darunter mit dem größten Anteil die Bezirksämter, aber auch die Staats- und Universitätsbibliothek, die Handelskammer Hamburg und die Öffentlichen Bücherhallen. Das Datencheckheft mit 48 Briefkarten wird weiterhin gemeinsam mit dem Datenschutzbeauftragten des NDR herausgegeben.

Zugleich haben wir unser Informationsblatt „Was tun wir für Sie?“ in aktualisierter Form veröffentlicht. Dort wird wiedergegeben, welche Bereiche unsere rund 20 Mitarbeiterinnen und Mitarbeiter betreuen und wie sie erreichbar sind. Das Faltblatt ist ebenso wie das Datencheckheft auch über unser Internet-Angebot abrufbar.

Unser Angebot im Internet haben wir in neuer Aufmachung so gestaltet, dass es für die Bürgerinnen und Bürger und für alle sonstigen Interessenten noch informativer geworden ist. Unsere Internet-Adresse lautet: www.hamburg.datenschutz.de. Dieses Angebot ist auch über das Virtuelle Datenschutzbüro als ein gemeinsamer Service der Datenschutzbeauftragten und weiterer Datenschutzinstitutionen unter www.datenschutz.de erreichbar.

Im Jahr 2000 haben wir außerdem eine neue Broschüre zum Datenschutz bei Windows NT herausgegeben, ein neues Faltblatt zur Telefonwerbung mit dem Titel „Datenschutz und Verbraucherschutz rund ums Telefon“ und – als gemeinsame Broschüre der Datenschutzbeauftragten des Bundes und der Länder – Empfehlungen zum Datenschutz beim E-Government unter dem Titel „Vom Bürgerbüro zum Internet“. Im Jahre 2001 haben wir gemeinsam mit der Verbraucher-Zentrale ein weiteres Faltblatt „Datenschutz und Verbraucherschutz rund um die Internet-Nutzung“ herausgebracht sowie eine Broschüre „Datenschutz bei Windows 2000“ vorbereitet.

Auf unserer Halbjahres-Pressekonferenz im Sommer 2000 erläuterte ich die weitere Beanstandung an den Senat wegen der Datenverarbeitung durch die Ausländerbehörden (siehe 16.2); außerdem gingen wir auf die Themen Datenschutz bei hamburg.de (3.5.5) und auf die Datenschutzprobleme der Genomforschung (21.3) ein. Im Sommer 2001 waren aktuelle Themen auf der Halbjahres-Pressekonferenz die neue Daueraufsicht über die Wirtschaft in Hamburg (2.1.2, 2.2.1 und 31.), die Datenschutzanforderungen bei E-Mails im Dienst- und Arbeitsverhältnis (3.3, 11.1, 27.1) und die elektronische Beantragung von Wahlscheinen (3.1.3) sowie die Probleme bei ärztlichen Krankschreibungen für den Arbeitgeber mit Arztstempeln, die auch Fachgebietsbezeichnungen enthalten oder sogar auf die Drogenbehandlung der Arbeitnehmer hinweisen (21.6).

Nachdem Mitte 1998 erstmals die Ergebnisse einer bundesweiten Meinungsumfrage zum Datenschutz vorgestellt worden waren, wurde die Repräsentativbefragung bundesweit bei 2.000 Personen im Jahr 2001 erneut durchgeführt. Die wesentlichen Ergebnisse der Umfrage, die für die Arbeit der Datenschutzbeauftragten und auch für die öffentliche Meinungsbildung wichtig ist, wurden von Prof. Opaschowski vom BAT Freizeit-Forschungsinstitut auf der Kieler Sommerakademie unseres schleswig-holsteinischen Nachbarn im September 2001 erläutert. In einer Presseerklärung habe ich hervorgehoben, dass sich die Mehrheit der Bürger mit 53 % dafür ausspricht, dass der Datenschutz künftig noch stärkere Bedeutung bekommt.

31. Entwicklung der Dienststelle

Die Stellenausstattung der Dienststelle wurde endlich verbessert.

Nach meinen mehrjährigen Bemühungen hat die Bürgerschaft Mitte Dezember 2000 eine zusätzliche Stelle für IuK-Angelegenheiten im öffentlichen Bereich beschlossen. Die Personalkosten für diese Stelle, zu deren Aufgabenbereich die Datenschutzbetreuung der hamburgischen Verwaltung gehört, werden nach einem Umlageschlüssel von hamburgischen Behörden getragen.

Gemäß dem Ersuchen der Bürgerschaft an den Senat bereits von Mitte Dezember 1999 hat die Bürgerschaft schließlich im Sommer 2001 eine weitere Stelle für die Daueraufsicht über die Wirtschaft in Hamburg gebilligt. Nach dem in-Kraft-Treten des novellierten Bundesdatenschutzgesetzes ermöglicht diese neu eingeführte Daueraufsicht (2.1.2 und 2.2.1) systematische Datenschutzprüfungen. Wir beabsichtigen, mit anderen Datenschutzbeauftragten auch automatisierte Prüfungen im Internet vorzunehmen. Dabei werden wir Schwerpunkte gemäß den Datenschutzproblemen bilden, die für die Bürgerinnen und Bürger besonders relevant sind.

Geschäftsverteilung (Stand: 1. Dezember 2001)

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

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

		Durchwahl
Dienststellenleiter:	Dr. Hans-Hermann Schrader	– 2044 –
Stellvertreter:	Peter Schaar	– 2231 –
Vorzimmer:	Heidi Niemann	– 2045 –
Verwaltungsangelegenheiten der Dienststelle	Rolf Nentwig	– 2563 –
Informationsmaterial	Irene Heinsohn	– 2047 –
	Heidi Niemann	– 2045 –
Grundsatzfragen des Datenschutzrechts, Datenschutzgesetze, Parlamentsangelegenheiten, Justiz, Strafvollzug, Verfassungsschutz, Sicherheitsüberprüfungen, Meldewesen, Wahlen und Volksabstimmungen, Ausweis- und Passangelegenheiten, Archivwesen	Dr. Harald Wollweber	– 2046 –
Polizei, Feuerwehr, Staatsanwaltschaft, Straßenverkehrsverwaltung, Verkehrsordnungswidrigkeiten, Gewerbeaufsicht, Wirtschaftsverwaltung	Herbert Janßen	– 2581 –
Bauen, Wohnen, Vermessungswesen, Personenstandeswesen, Umwelt, Statistik, Finanz-, Steuer- und Rechnungswesen	Gunnar Hansen	– 223 –
Grundsatzfragen, Telekommunikation, Medien, Internet, technisch-organisatorische Beratung und Prüfung, Ausländerwesen	Peter Schaar	– 2231 –
Landesamt für Informationstechnik (LIT), SAP, IuK-Leitung, IuK-Planung, technisch-organisatorische Beratung und Prüfung	Dietmar Nadler	– 2236 –

DV-Verfahren der Dienststelle,
Systemadministration, Internetangebot

Martin Schemm – 2063 –

Betriebssysteme, Netzwerke, Chipkarten,
Verschlüsselungstechnik, Elektronische Signatur,
technisch-organisatorische Beratung und Prüfung

Dr. Sebastian Wirth – 1769 –

Ulrich Kühn – 2564 –

Standard-Software und Dokumentenmanagement /
Archivierung, technisch-organisatorische Beratung
und Prüfung, Vertretung IuK-Leitung

Jutta Gebers – 1373 –

Gesundheitswesen, Forschung, Kultur

Dr. Hans-Joachim Menzel – 2558 –

Soziales, Bildungswesen, Allgemeine
Bezirksangelegenheiten, Vereine, Kirchen

Detlef Melessa – 2089 –

Auskunfteien, SCHUFA, Kreditwesen

Helga Naujok – 2556 –

Versicherungswirtschaft, Handel, Industrie

Elisabeth Duhr – 2541 –

Adresshandel, Werbung, Markt- und
Meinungsforschung

Birgit Danker – 2562 –

Arbeitnehmerdatenschutz / Personalwesen,
Auftragsdatenverarbeitung, Meldepflicht

Evelyn Seiffert – 2468 –

Meldepflicht / Register, Transport und Verkehr,
gewerbliche Dienstleistungen, Freie Berufe

Bernd Uderstadt – 2276 –

Stichwortverzeichnis

Veröffentlichungen zum Datenschutz

Beim Hamburgischen Datenschutzbeauftragten können derzeit folgende Veröffentlichungen kostenlos abgeholt werden oder per Post gegen Einsendung von Briefmarken im Wert von 0,77 € angefordert werden:

Broschüren

Hamburgisches Datenschutzrecht 2001
Datenschutz in der Arztpraxis
Datenschutz bei Multimedia und Telekommunikation
Datenschutz bei Windows NT
Datencheckheft
Mehr Service – weniger Datenschutz
Vom Bürgerbüro zum Internet

Berichte

18. Tätigkeitsbericht 2000/2001
17. Tätigkeitsbericht 1998/1999

Informationsblätter

Was tun wir für Sie?
Handels- und Wirtschaftsauskunfteien
Die Gesundheits-Chipkarte
Datenschutz und Verbraucherschutz rund ums Telefon
Virtuelles Datenschutzbüro
Surfen, Klicken und Bestellen

Internet

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

Verlagsveröffentlichungen

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

Bäumler, Breinlinger, Schrader (Hrsg.), Datenschutz von A – Z, Loseblattwerk, Luchterhand Verlag, 1999

Kühn, Schläger, Datenschutz in vernetzten Computersystemen, Datakontext-Fachverlag, 1997

Schaar, Datenschutz im Internet, Beck-Verlag, 2002

Schaar, Kommentierungen zum TDDSG und MDStV in: Roßnagel (Hrsg.) Recht der Multimediadienste, 2000

Schaar, Die Möglichkeiten der Datenschutzaufsichtsbehörden, in: Bäumler (Hrsg.), E-Privacy, Vieweg-Verlag, 2000