BÜRGERSCHAFT
DER FREIEN UND HANSESTADT HAMBURG **Drucksache 13/7120**

13. Wahlperiode **19. 11. 90**

Der Hamburgische Datenschutzbeauftragte

An die
Frau Präsidentin der Bürgerschaft

9.

Betr.: Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten

Gemäß § 23 Absatz 3 Satz 2 des Hamburgischen Datenschutzgesetzes übersende ich der Bürgerschaft den neunten Tätigkeitsbericht* des Hamburgischen Datenschutzbeauftragten.

Dem Senat habe ich den Tätigkeitsbericht gleichzeitig zugeleitet.

Manfred Krause

* Verteilt nur an die Abgeordneten der Bürgerschaft

Bürgerschaftsdrucksachen — außer Senatsvorlagen — sind zu beziehen bei:
Druckerei Wartenberg & Söhne GmbH, Theodorstraße 41 w, 2000 Hamburg 50, Telefon 89 39 48

Neunter Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten

Zugleich Tätigkeitsbericht der Aufsichtsbehörde für den nicht-öffentlichen Bereich

vorgelegt im November 1990

Herausgegeben vom Hamburgischen Datenschutzbeauftragten
Baumwall 7 · 2000 Hamburg 11 · Tel.: 35 04 20 44

Druck: Lütcke & Wulff, Hamburg 1

GLIEDERUNG

Seite

1. Zur Lage des Datenschutzes

1.1 Neues Datenschutzrecht in Hamburg

Am 1. August 1990 ist das neue Hamburgische Datenschutzgesetz in Kraft getreten. Wer die Regelungen mit den Vorschlägen und Anregungen des Hamburgischen Datenschutzbeauftragten zur Novellierung (7. TB, 1.3, S. 2 ff, 8. TB, 1.1–1.2, S. 1 ff) vergleicht, wird verstehen, daß das neue Recht bei uns nicht nur ungeteilte Freude ausgelöst hat. Gleichwohl haben wir zu akzeptieren, daß sich der Gesetzgeber nach breiter parlamentarischer Beratung zu der jetzt vorliegenden Lösung entschlossen hat und es gibt genügend Regelungen, die es verdienen, als deutliche Verbesserungen gegenüber dem bisherigen Rechtszustand hervorgehoben zu werden.

So begrüßen wir es ausdrücklich, daß die Unterscheidung der Verarbeitung personenbezogener Daten in Akten einerseits und in Dateien andererseits aufgegeben wurde. Das neue Gesetz regelt die Verarbeitung personenbezogener Daten ohne Rücksicht auf die Form der Verarbeitung. Nur dies wird dem Grundrecht auf informationelle Selbstbestimmung voll gerecht, denn auch der Rechtsprechung des Bundesverfassungsgerichts zu dieser Ausprägung des Persönlichkeitsschutzes war eine solche Differenzierung nicht zu entnehmen.

Aber auch sonst hat das Gesetz Lücken geschlossen, die in der Vergangenheit nicht nur unsere Arbeit sondern auch die der anwendenden Behörden erschwert haben. Besonders zu erwähnen ist in diesem Zusammenhang die Regelung über die Datenverarbeitung zum Zwecke wissenschaftlicher Forschung (§ 27) sowie der Einstieg in den Arbeitnehmerdatenschutz (§ 28).

Wir beabsichtigen, im Zusammenwirken mit der Justizbehörde das neue Recht in einer Informationsschrift den interessierten Bürgern und den Rechtsanwendern in den Behörden mit einigen Erläuterungen vorzustellen.

1.2 Neues Bundesdatenschutzgesetz — Eingriff in das hamburgische Recht

Wenige Tage vor Redaktionsschluß zu diesem Bericht haben die parlamentarischen Gremien des Bundes — unter Einschluß des Vermittlungsausschusses — das Artikel-„Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes" verabschiedet, mit dem nicht nur die notwendigen gesetzlichen Grundlagen für die Geheimdienste des Bundes (Bundesamt für Verfassungsschutz, MAD, BND) geschaffen wurden, sondern auch das Bundesdatenschutzgesetz novelliert wurde. Wir hatten noch keine Zeit, die neuen Gesetze abschließend zu beurteilen (ein zusammenhängender Text lag uns bis jetzt noch nicht vor). Auf eine — bisher einmalige — Besonderheit soll jedoch hingewiesen werden.

Gemäß § 24 Absatz 2 Nummer 2 des neuen Gesetzes soll der Bundesbeauftragte für den Datenschutz die Verarbeitung personenbezogener Daten in bestimmten Bereichen dann nicht kontrollieren dürfen, wenn der Betroffene der Kontrolle der auf ihn bezogenen Daten im Einzelfall ihm gegenüber widerspricht. Über ihr Widerspruchsrecht sind die Betroffenen in allgemeiner Form zu unterrichten.

Erstaunlich daran ist, daß es für diese Einschränkung des Kontrollrechts gar keinen Anlaß gibt: Uns ist in der bisherigen hamburgischen Praxis kein Fall bekannt geworden, in dem sich ein Betroffener durch eine datenschutzrechtliche Kontrolle beschwert gefühlt hätte. Auf der anderen Seite kann das Widerspruchsrecht systematische Querschnittskontrollen erheblich beeinträchtigen. Bemerkenswert ist weiter, daß die Betroffenen zwar einer Datenschutzkontrolle, nicht aber der Rechnungsprüfung, einer fachaufsichtlichen Kontrolle und auch nicht — worauf der schleswig-holsteinische Datenschutzbeauftragte hingewiesen hat — der Einbeziehung ihrer Daten in eine Rasterfahndung widersprechen können.

Darüber hinaus läßt das Gesetz die Anwender völlig im unklaren darüber, in welcher Form und vor allem wann die Betroffenen über ihr Widerspruchsrecht aufzuklären sind.

Es dürfte wohl nicht gewollt sein, durch das mögliche Widerspruchsrecht Einzelner unangemeldete Kontrollen in den genannten Bereichen auszuschließen.

Völlig unakzeptabel ist aber, daß diese erstaunlichen und widersprüchlichen Einschränkungen der Kontrollbefugnisse des Bundesbeauftragen für den Datenschutz über § 24 Absatz 6 BDSG auch für sämtliche Landesbeauftragten gelten sollen. Wir stimmen der Konferenz der Datenschutzbeauftragten zu, die im Vorfeld der Abstimmung darauf hingewiesen hat, daß eine derartige Einwirkung auf das Landesrecht verfassungswidrig ist, und hoffen, daß die berufenen hamburgischen Verfassungsorgane diesen Eingriff in ihre Rechtshoheit in der gebotenen Form zurückweisen.

2. Entwicklung der Dienststelle

2.1 Personeller Umbruch

Am 21. Juni 1990 hat die neue niedersächsische Landesregierung den bisherigen Hamburgischen Datenschutzbeauftragten, Claus Henning Schapper, zum Staatssekretär in das Innenministerium berufen. Damit hat die Runde der Datenschutzbeauftragten eine weitere profilierte Persönlichkeit verloren. Die Etablierung des Datenschutzes in der hamburgischen Rechtswirklichkeit ist untrennbar mit dem Namen von Claus Henning Schapper verbunden.

Der mit dem Ausscheiden des bisherigen Amtsinhabers entstandenen Situation hat der Senat dadurch Rechnung getragen, daß er gemäß § 19 Absatz 3 HmbDSG bis zur Neuwahl einer Nachfolgerin oder eines Nachfolgers durch die Bürgerschaft einen Vertreter mit der Wahrnehmung der Geschäfte beauftragt hat, der auch für den vorliegenden Tätigkeitsbericht verantwortlich ist.

Neben Herrn Schapper scheiden während des laufenden Berichtsjahres vier weitere verantwortliche Mitarbeiter bei der Dienststelle des Hamburgischen Datenschutzbeauftragten aus und übernehmen neue Aufgaben in der Justiz oder in der hamburgischen Verwaltung, unter ihnen auch eine Mitarbeiterin der ersten Stunde. Mit dem dadurch verursachten personellen Umbruch wird die Dienststelle einen deutlich spürbaren Einschnitt verkraften müssen. Trotz des mit dem Weggang bewährter Mitarbeiter verbundenen Verlustes an Wissen und Erfahrung liegt darin jedoch auch eine Chance. Die neuen Mitarbeiter können mit ihrer Kreativität und ihren Ideen die Arbeit der Dienststelle befruchten — zugunsten des Datenschutzes, der eine Verkrustung am wenigsten verträgt.

2.2 Neue Aufgaben durch das Bundesdatenschutzgesetz

Bekanntlich hat der Senat dem Hamburgischen Datenschutzbeauftragten auch die Aufgaben der Aufsichtsbehörde für die Datenverarbeitung im nicht-öffentlichen Bereich nach den §§ 30 und 40 BDSG a. F. übertragen. In diesem Bereich kommen nun durch die Novelle zum Bundesdatenschutzgesetz (vgl. 1.2) neue Aufgaben auf die Dienststelle zu.

Bisher durfte die Aufsichtsbehörde nach § 30 Absatz 1 BDSG a. F. nur dann die Datenverarbeitung bei einem privaten Unternehmen überprüfen, wenn ein Betroffener begründet dargelegt hatte, daß er bei der Verarbeitung seiner personenbezogenen Daten in seinen Rechten verletzt worden war (sog. Anlaßkontrolle). Dies führte in der Praxis dazu, daß die Aufsichtsbehörde Verstöße gegen datenschutzrechtliche Bestimmungen hinnehmen mußte, wenn es an einer Betroffenenbeschwerde fehlte. Überprüfungen, die wir für erforderlich gehalten haben, konnten nicht stattfinden.

Nach der neuen Regelung in § 38 Absatz 1 BDSG n. F. reicht es für eine Überprüfung nunmehr aus, wenn hinreichende Anhaltspunkte für eine Gesetzesverletzung vorliegen. Damit ist die Aufsichtsbehörde gesetzlich verpflichtet, Anhaltspunkten für Datenschutzverstöße nachzugehen, auch wenn keine Beschwerde eines unmittelbar Betroffenen vorliegt.

Desweiteren kann die Aufsichtsbehörde nach § 38 Absatz 5 BDSG n. F. eine Reihe von Anordnungen treffen, die bisher nicht vorgesehen waren:

— Maßnahmen zur Beseitigung technischer und organisatorischer Mängel,

— Untersagung des Einsatzes einzelner Verfahren,

— Abberufung des betrieblichen Datenschutzbeauftragten.

Da diese Aufgaben zwangsläufig zu einem deutlichen Anwachsen sowohl der Fallzahlen als auch der technischen wie juristischen Probleme führen werden, wird es unerläßlich sein, Senat und Bürgerschaft um eine entsprechende Verbesserung der personellen Ausstattung der Aufsichtsbehörde zu ersuchen. Entsprechende Anträge werden wir rechtzeitig zu den Haushaltsberatungen für das Jahr 1992 einbringen.

3. Automatisierte Datenverarbeitung

3.1 Stand und Fortentwicklung der Regelungen für die automatisierte Datenverarbeitung

3.1.1 Bereich der zentralen ADV-Verfahren — Neue Freigaberichtlinie

Im 8. Tätigkeitsbericht (2.1, S. 9 ff.) haben wir darauf hingewiesen, daß es inzwischen sogar für Mitarbeiter schwierig geworden ist, die für die Entwicklung und Pflege sowie den Betrieb von IuK-Verfahren einschlägigen Vorschriften überhaupt zu überblicken. Der Senat hat in seiner Stellungnahme dazu angekündigt, den Beschäftigten solle der Zugang zu den Vorschriften durch ein Suchregister nach Art einer Loseblattsammlung erleichtert werden.

Zu den dargestellten Mängeln des Regelungswerks im übrigen hat der Senat darauf verwiesen, daß die Regelungen den Veränderungen der Technik und ihrer Nutzung schrittweise angepaßt werden müßten.

In diesem Sinne wurde mit den Arbeiten zur Neufassung der Freigaberichtlinie begonnen. Die vom Arbeitskreis Freigaberichtlinie beim Senatsamt für den Verwaltungsdienst — Organisationsamt — erarbeiteten Entwürfe sind mit besonders betroffenen ADV-Gruppen diskutiert worden, und es hat bereits ein Behördenabstimmungsverfahren stattgefunden. Vorschläge und Bedenken der beteiligten ADV-Gruppen und Behörden haben zu einem weiteren Entwurf geführt.

Mit dem Entwurf für eine neue Freigaberichtlinie wird die der geltenden Richtlinie zugrunde liegende Vorstellung aufgegeben, die Sicherheit der ADV-Verfahren und des Rechenzentrumsbetriebs mache es erforderlich, das Freigabeverfahren nicht nur inhaltlich, sondern auch hinsichtlich des formalen Verfahrens detailliert und abschließend vorzuschreiben. Dies hat sich in der Praxis bekanntlich nicht bewährt. Der Arbeitskreis Freigaberichtlinie ist zu der Erkenntnis gelangt, daß bloße Formalien — zumal, wenn gegen sie sanktionslos verstoßen werden kann — keinen Sicherheitsgewinn erwarten lassen. Mit dem Entwurf der neuen Freigaberichtlinie wird daher auf starre Verfahrensvorschriften verzichtet. Er enthält vielmehr einen Rahmen, innerhalb dessen Modifikationen zulässig sein sollen. Die wichtigsten mit ihm verfolgten Intentionen wurden wie folgt beschrieben:

— Die Freigaberichtlinie soll stärker als bisher auf die organisatorischen Grundsätze und materiellen Voraussetzungen der Freigabe konzentriert werden. Sie soll von der Senatskommission für den Verwaltungsdienst beschlossen werden.

— Die verfahrensmäßige Umsetzung soll davon abgesetzt in Durchführungshinweisen des Senatsamtes für den Verwaltungsdienst konkretisiert werden. Die Durchführungshinweise sollen insbesondere Erläuterungen, Realisierungsalternativen und Vorgaben für die Einheitlichkeit der betrieblichen Durchführung in der DVZ enthalten.

— Die Freigabeverpflichtung knüpft an eine tatsächlich für ein DV-Verfahren bestehende Arbeitsteilung zwischen der für die Aufgabenerfüllung verantwortlichen („fachlich zuständigen") Stelle, der programmierenden Stelle und/oder der Datenverarbeitungszentrale (oder einer anderen Rechenstelle) an. Die Verantwortung der fachlich zuständigen Stelle zur Aufgabenerfüllung erstreckt sich auch auf die Aufgaben, die mit Hilfe von DV-Verfahren erfüllt werden. (Dies wurde bisher nicht immer ausreichend berücksichtigt.) DV-Verfahren sind damit stets von der fachlich zuständigen Stelle freizugeben.

— Von der fachlich zuständigen Stelle zu verantworten ist stets das DV-Verfahren als Ganzes. Das gilt auch, wenn nur Teile davon geändert werden.

— Deutlicher als bisher wird zwischen Freigabe und Test unterschieden. Die fachlich verantwortliche Stelle hat sich vor der Freigabe davon zu überzeugen, daß das DV-Verfahren den rechtlichen, sonstigen fachlichen und organisatorischen Anforderungen entspricht. Das hierfür geeignete Mittel ist in der Regel ein Test mit systematisch entwickelten Testfällen. Art und Umfang der Funktions- und Abnahmetests sollen nicht mehr vorgeschrieben werden, sondern der Entscheidung der Behörde in eigener Verantwortung überlassen bleiben. Für die Praxis wichtig ist der Hinweis, daß die Freigabe eines DV-Verfahrens als Ganzes — z. B. nach Änderung nur eines Teilprogramms oder bei Erweiterungen — nicht zwingend einen Test des gesamten DV-Verfahrens erfordert. Die verantwortliche Behörde kann zulassen, daß der Test (nicht die Freigabe) auf einzelne Programmprodukte beschränkt wird, wenn die Auswirkungen auf das DV-Verfahren eindeutig darstellbar sind.

— Die betriebliche Durchführung des Abnahmetests soll nicht mehr zwingend festgelegt werden.

— Die Anforderungen an die Dokumentation der Tests sollen der technischen Weiterentwicklung (Dialogverfahren) angepaßt werden. Es soll ein Weg eröffnet werden, die im Freigabeverfahren erforderlichen Erklärungen mit Dokumentencharakter auch auf elektronischem Wege zu übermitteln.

— Für den Fall, daß ein DV-Verfahren zwangsläufig kurzfristig geändert werden muß, aber nicht zeitgerecht freigegeben werden kann, soll eine befristete Ausnahme möglich sein.

Der Hamburgische Datenschutzbeauftragte war im Arbeitskreis Freigaberichtlinie vertreten. Die im Entwurf vorliegende neue Richtlinie haben wir grundsätzlich begrüßt, uns jedoch dagegen ausgesprochen, in der Freigaberichtlinie explizit darauf hinzuweisen, daß auch die Gestaltung von Tests dem Gebot der Wirtschaftlichkeit unterliegt und deshalb der Aufwand für die Durchführung in einem angemessenen Verhältnis zum Gewinn an Verfahrenssicherheit stehen muß. Das Wirtschaftlichkeitsgebot gilt selbstverständlich für jegliches Verwaltungshandeln. Wir befürchten, die an dieser Stelle nicht gebotene Betonung des Wirtschaftlichkeitsgebots könnte zu einem Mißverständnis führen und als Vorwand für nicht ausreichenden Testaufwand benutzt werden.

3.1.2 Behördeninterne Regelungen zum PC-Einsatz

Trotz einer Vielzahl von Regelungen für die automatisierte Datenverarbeitung in der hamburgischen Verwaltung (vgl. 8. TB, 2.1, S. 9 ff.) gibt es bisher keine verbindliche Richtlinie über organisatorische und technische Datensicherungsmaßnahmen für die Verarbeitung personenbezogener Daten auf PC. Das Senatsamt für den Verwaltungsdienst hat lediglich 1987 „Vorläufige Hinweise für die Verarbeitung personenbezogener Daten auf Personalcomputern (PC) in der Verwaltung" herausgegeben (MittVw 1988, S. 61). Diese „vorläufigen Hinweise" sind sehr allgemein, jedoch mit dem Ziel formuliert worden, daß die jeweiligen Behörden ihrerseits eigenverantwortlich die Ausführung der Datenschutzbestimmungen durch behördeninterne Dienstanweisungen sicherstellen. Auf diese, sich aus dem Hamburgischen Datenschutzgesetz ergebende Verpflichtung der Behörden haben wir bereits im 7. Tätigkeitsbericht (3.1.2, S. 10 f.) ausdrücklich hingewiesen.

Dennoch haben wir in den letzten Jahren in Einzelfallprüfungen regelmäßig das Fehlen praktikabler, behördeninterner Regelungen festgestellt. Um einen umfassenden Überblick über derartige Regelungen zu bekommen, haben wir eine behördenübergreifende Erhebung durchgeführt, die auch Fragen zu organisatorischen und technischen Sicherungsmaßnahmen auf Personalcomputern enthält.

Hierbei fiel auf, daß entweder entsprechende Dienstvorschriften gänzlich fehlen oder sich die bestehenden Regelungen — mit Ausnahme der Regelung der Behörde für Schule, Jugend und Berufsbildung (BSJB) — im wesentlichen auf die Festlegung von Verantwortlichkeiten und räumlichen Zugangssicherungen beschränken. Die detaillierten Richtlinien der BSJB können als richtungsweisend angesehen werden, da sie allgemeingültige datenschutzrechtliche Regelungen mit behördenspezifischen Aspekten verbinden. Die darin aufgeführten technischen und organisatorischen Maßnahmen sind geeignet, die in § 8 Absatz 2 HmbDSG genannten Forderungen behördenspezifisch zu erfüllen.

Hinsichtlich der von den Behörden getroffenen technischen und organisatorischen Maßnahmen kann festgestellt werden, daß nur ein Teil der befragten Dienststellen spezielle Datenschutzsoftware zur Zugriffskontrolle einsetzt. Überwiegend wird auf rein räumliche Sicherungsvorkehrungen vertraut. Dieses Ergebnis ist unbefriedigend. Angesichts der steigenden Anzahl von PC-Anwendungen mit sensiblen personenbezogenen Daten entsteht der Eindruck, daß die Notwendigkeit geeigneter Sicherungsmaßnahmen nicht von allen Behörden in dem erforderlichen Maß gesehen wird. Das Ergebnis unserer Umfrage bestätigt die Einschätzung, die wir in den letzten Jahren aufgrund von Einzelprüfungen im PC-Bereich gewonnen haben. Im einzelnen ergibt sich folgendes Bild:

Behörde	Datenschutz-Richtlinien	Technische und organisatorische Maßnahmen
Senatskanzlei	keine internen Dienstvorschriften	keine Angaben über PC-Einsatz
Senatsamt für den Verwaltungsdienst	keine internen Dienstvorschriften	Zugriffskontrolle durch Benutzeridentifikation innerhalb der Anwendungssoftware (bezieht sich auf den Bereich Vorbereitung und Durchführung der zentralen Anpassungs- und Führungsfortbildung, berufliche Fortbildung, Einführung von Mitarbeitern)
Senatsamt für Bezirksangelegenheiten	keine internen Dienstvorschriften	Zugriffskontrolle durch Datensicherungs-Software
Staatsarchiv	keine internen Dienstvorschriften	keine Datensicherungs-Software im Einsatz
Justizbehörde	Benutzerordnung für Datenschutz- und Datensicherungsmaßnahmen im Amt für Allgemeine Verwaltung, sonst keine weiteren internen Dienstvorschriften	— Benutzerkontrolle mittels Schlüsselschalter — Zugriffskontrolle durch Datensicherungs-Software
Behörde für Schule, Jugend und Berufsbildung	sehr detaillierte Regelungen: — seit 24. 1. 85 gültige Geschäftsordnungsbestimmung Nr. 16 — Hinweise zur Datenverarbeitung und Datensicherung in Schulen und Dienststellen vom 10. 4. 85	— räumliche Zugangskontrolle durch Sicherheitsschlösser — Zugriffskontrolle durch Benutzeridentifikation innerhalb der Anwendungssoftware (bezieht sich auf das Pilotprojekt „Vereinfachung der Schulverwaltung") — Im Unterricht eingesetzte Anlagen dürfen nicht für außerunterrichtliche Zwecke verwendet werden — Gesundheitsdaten, Ergebnisse von Intelligenz- und Persönlichkeitstests sowie Daten über Ordnungsverstöße und Religionszugehörigkeit dürfen nicht auf automatisierten Anlagen gespeichert werden
Behörde für Wissenschaft und Forschung	amtsinterne Regelungen: — UKE-Dienstanweisung (in Vorbereitung) — TU Hamburg-Harburg: Merkblatt zu „Datenschutz und Datensicherung — Arbeit am PC"	— räumliche Zugangskontrolle durch Sicherheitsschlösser — zum Teil Benutzerkontrolle mittels Schlüsselschalter — zum Teil Zugriffskontrolle durch Datensicherungs-Software

Behörde	Datenschutz-Richtlinien	Technische und organisatorische Maßnahmen
Kulturbehörde	interne Verfügung vom 26. 5. 89, beschreibt technische und organisatorische Sicherungsvorkehrungen	— Zugangskontrolle durch abschließbare Räume — Benutzerkontrolle mittels Schlüsselschalter — Aufbewahrung von Sicherungsdisketten im Tresor
Behörde für Arbeit, Gesundheit und Soziales	keine amtsspezifischen Regelungen, weder für den Bereich, der früher der BAJS angehörte, noch für das Amt für Gesundheits- und Veterinärwesen	für den Bereich, der früher der BAJS angehörte: — Zugangskontrolle durch abschließbare Räume — Aufbewahrung von Sicherungsdisketten im abschließbaren Schrank — Installation von PC nur in Ausnahmefällen vorgesehen, im wesentlichen zur Unterstützung von Planungs- und Statistikaufgaben für das Gesundheits- und Veterinärwesen: — Zugriffskontrolle durch Datensicherungs-Software ist geplant
Baubehörde	interne Dienstvorschrift in Vorbereitung	— räumliche Zugangskontrolle durch Sicherheitsschlösser — Zugriffskontrolle durch softwaremäßige Benutzeridentifikation — Aufbewahrung der Sicherungsdisketten in abschließbaren Schränken
Behörde für Wirtschaft, Verkehr und Landwirtschaft	keine internen Dienstvorschriften	— Zugangskontrolle durch abschließbare Räume, die teilweise mit Sicherheitsschlössern ausgestattet sind — Benutzerkontrolle mittels Schlüsselschalter — Aufbewahrung von Sicherungsdisketten im Stahlschrank — Zugriffskontrolle durch Datensicherungs-Software sowie Paßwort-Abfrage innerhalb der Anwendungssoftware
Umweltbehörde	Vermerk zu Grundsatzfragen des Datenschutzes vom 8. 8. 83	keine Datensicherungs-Software im Einsatz

Behörde	Datenschutz-Richtlinien	Technische und organisatorische Maßnahmen
Behörde für Inneres	keine internen Dienstvorschriften, allerdings polizeispezifische Regelungen zum Thema — „Aufstellung und Sicherung von Datenstationen und organisatorische Regelungen zum Datenschutz" in der Polizeidienstvorschrift — „Datenerhebung und Datenschutz für autonome ADV-Systeme" vom 29. 1. 88	— Zugangskontrolle durch abschließbare Räume — Benutzerkontrolle durch Schlüsselschalter — sichere Verfahrung der Sicherungsdisketten — Führung von Sicherungsprotokollen — Zugriffskontrolle durch Datensicherungs-Software (lediglich bei neueren Modellen) — Trennung zwischen anwendender und programmierender Stelle
Finanzbehörde • Allgemeine Verwaltung, Ausschreibungsabteilung	amtsinterne Regelungen Datenschutzbestimmungen im Anwenderhandbuch des automatisierten Ausschreibungsverfahrens	amtsinterne Maßnahmen Zugriffskontrolle durch Benutzeridentifikation innerhalb des Ausschreibungsverfahrens
• Allgemeine Verwaltung, DVZ	Anweisung zum Einsatz von PC im Rahmen des ADV-Handbuchs, Teil 3	— Dokumentation und Kontrolle sämtlicher Datenträger — Zugriffskontrolle durch softwaremäßige Benutzeridentifikation — Dokumentation sämtlicher Zugriffe auf personenbezogene Daten — Freigabe entsprechend geprüfter Programme — Kennung von Disketten zwecks Bindung an bestimmte Geräte
• Finanzverwaltung	keine interne Dienstvorschrift	keine Angaben über PC-Einsatz
• Vermögens- und Beteiligungsverwaltung	Dienstanweisung bzw. Verfahrens-Handbuch	— Zugriffskontrolle durch Benutzeridentifikation innerhalb der Anwendungssoftware — Aufbewahrung von Sicherungsdisketten im Tresor
• Liegenschaftsverwaltung	interne Dienstanweisung in Vorbereitung	bei Umstellung der Eigenheimbewerberdatei sind geplant: — Verschlüsselung der Daten auf der Festplatte — Zugriffskontrolle durch softwaremäßige Benutzeridentifikation

Behörde	Datenschutz-Richtlinien	Technische und organisatorische Maßnahmen
• Oberfinanzdirektion	„Vorläufige Dienstanweisung für PC-Einsatz in den Betriebsprüfstellen der Finanzämter und im Finanzamt für Prüfdienste" vom 8. 3. 88	— Zugangskontrolle durch angemessene Raumsicherungsmaßnahmen — Zugriffskontrolle durch Datensicherungs-Software — ausschließliche Menüsteuerung — Daten, die dem Steuergeheimnis unterliegen, dürfen nur temporär auf der Festplatte gespeichert werden — Disketten werden verschlossen
Bezirksamt Hamburg-Nord	umfangreiche Zuständigkeitsregelungen, keine internen Dienstvorschriften	Zugriffskontrolle durch Datensicherungs-Software
Bezirksamt Hamburg Mitte	Datenschutz-/Datensicherungskonzept in Vorbereitung	geplant sind: — ausreichender Schutz der Räumlichkeiten — Zugriffskontrolle durch Datensicherungs-Software — sichere Aufbewahrung von Datenträgern
Bezirksamt Altona	umfangreiche Zuständigkeitsregelungen, keine internen Dienstvorschriften	— räumliche Zugangskontrolle durch Sicherheitsschlösser — Benutzerkontrolle mittels Schlüsselschalter — Zugriffskontrolle durch Datensicherungs-Software
Bezirksamt Bergedorf	keine internen Dienstvorschriften	— Zugangskontrolle durch abschließbare Räume — Benutzerkontrolle mittels Schlüsselschalter — Zugriffskontrolle durch Datensicherungs-Software
Bezirksamt Harburg	umfangreiche Zuständigkeitsregelungen, keine internen Dienstvorschriften	— Zugangskontrolle durch abschließbare Räume — Benutzerkontrolle mittels Schlüsselschalter — Zugriffskontrolle durch Datensicherungs-Software — Aufbewahrung von Disketten in abschließbaren Schränken — Führung eines PC-Logbuchs, in dem Inhalt und Verbleib der Arbeitsdisketten sowie Art und Umfang der auf der Festplatte gespeicherten Daten festgehalten sind

Behörde	Datenschutz-Richtlinien	Technische und organisatorische Maßnahmen
Bezirksamt Eimsbüttel	umfangreiche Zugständigkeitsregelungen, keine internen Dienstvorschriften	— räumliche Zugangskontrolle durch Sicherheitsschlösser — Benutzerkontrolle mittels Schlüsselschalter — Zugriffskontrolle durch Datensicherungs-Software
Bezirksamt Wandsbek	umfangreiche Zuständigkeitsregelungen, keine internen Dienstvorschriften	— räumliche Zugangskontrolle durch Sicherheitsschlösser — Zugriffskontrolle durch Datensicherungs-Software
TÜV Norddeutschland	organisatorische Regelungen, insbesondere Verantwortlichkeitsregelungen	— Benutzerkontrolle mittels Schlüsselschalter — Verschluß der Disketten
Schornsteinfegerinnung	keine internen Dienstvorschriften	— Zugangskontrolle durch abschließbare Räume — Zugriffskontrolle durch softwaremäßige Benutzeridentifikation — Aufbewahrung von Sicherungsdisketten im Tresor

3.2 Datensicherungskonzept bei Einzelplatz-PC

3.2.1 PC-Einsatz in der hamburgischen Verwaltung

Wir haben oft darauf hingewiesen, daß der Einsatz von Personalcomputern in der hamburgischen Verwaltung aus datenschutzrechtlicher Sicht zunehmend problematisch geworden ist. Die kritische Situation im PC-Bereich hat mehrere Ursachen:

— Ausdehnender PC-Einsatz: Mittlerweile hat der PC verstärkt Einzug in die Bereiche gehalten, die bisher Großrechnern vorbehalten waren. Während PC bis vor einigen Jahren hauptsächlich für Textverarbeitung eingesetzt wurden, weitet sich deren Einsatz nunmehr auch auf speziellere Datenbank-Anwendungen aus, bei denen zum Teil sehr sensible personenbezogene Daten verarbeitet werden.

— PC-erfahrene Benutzer: Im Verhältnis zu Großrechner-Wissen, das auf wenige Spezialisten beschränkt ist, sind PC-Kenntnisse mittlerweile weit verbreitet, so daß etwa Datenmißbrauch zumindest nicht mehr an zu geringer EDV-Erfahrung scheitert.

— Geringer Stellenwert der Datensicherheit: Datensicherungsmaßnahmen werden in vielen Verwaltungen immer noch als kostenverursachendes Hindernis angesehen, so daß Mittel für entsprechende Maßnahmen und Stellen nur in seltenen Fällen von vornherein Bestandteil neuer EDV-Projekte sind.

— Schlecht organisierter PC-Einsatz: Der PC-Einsatz findet teilweise so unkoordiniert statt, daß die zuständigen Stellen manchmal keinen vollständigen Überblick darüber haben, wer welchen PC zu welchen Zwecken wo einsetzt und welche personenbezogenen Daten hierbei verarbeitet werden (vgl. 8. TB, 3.13.2.1, S. 106).

— Aufhebung der Arbeitsteilung: Die im Großrechner-Bereich zu beobachtende Trennung von Maschinenbediener, Systemprogrammierer, Anwendungsprogrammierer und Benutzer ist beim PC-Einsatz weitgehend aufgehoben. Oftmals werden sämtliche Tätigkeiten von einer Person wahrgenommen, so daß das traditionelle Vier-Augen-Prinzip nicht mehr greift.

— Unübersichtliche Regelungen: Datenschutz ist für den einzelnen Benutzer in der hamburgischen Verwaltung kaum umsetzbar, da er sich inzwischen einer Vielzahl von schwer überschaubaren Regelungen gegenübergestellt sieht, die zum Teil veraltet oder unverbindlich sind. Es fehlen behördeninterne Regelungen, die den PC-Einsatz und entsprechende technisch-organisatorische Maßnahmen anwendungsspezifisch und abschließend festlegen (s. o. 3.1.2).

— Einsatz von Betriebssystemen (z. B. MS-DOS), die ohne erforderliche Sicherungssysteme erhebliche Schwachstellen aufweisen (fehlende Benutzeridentifikation; kein physikalisches Löschen von Dateien; fehlende Differenzierung von Lese-, Schreib-, Lösch- und Ausführungsberechtigung; unkontrollierbarer Diskettenbetrieb; fehlende Protokollierung).

Angesichts dieser Situation ist es aus unserer Sicht unbedingt notwendig, den Einsatz technischer und organisatorischer Datensicherungsmaßnahmen mehr als bisher differenziert zu regeln. Deshalb haben wir ein Schutzstufenkonzept zu PC-Sicherungsmaßnahmen entwickelt, das einerseits die Sensibilität und somit das Gefährdungspotential zu schützender Daten berücksichtigt, andererseits unnötige bürokratische Zwänge vermeidet. Dieses Konzept dient als Grundlage der Prüfungs- und Beratungstätigkeit des Hamburgischen Datenschutzbeauftragten.

3.2.2 Grundlegende Aspekte des Schutzstufenkonzepts

3.2.2.1 Sensibilität von Daten und Klassifikation von Sicherheitsstandards

Das Hamburgische Datenschutzgesetz geht in § 8 Absatz 2 davon aus, daß technische und organisatorische Maßnahmen zur Datensicherung zu treffen sind, die je nach Art der zu schützenden personenbezogenen Daten geeignet sind. Das Gesetz legt somit

nahe, die Sensibilität der Daten bei der Entwicklung eines Datenschutzkonzepts entsprechend zu berücksichtigen.

Neben rechtlichen Aspekten ist die Klassifizierung von Sicherheitsstandards im PC-Bereich auch unter pragmatischen Gesichtspunkten sinnvoll, um einerseits eine für die jeweilige Anwendung angemessene Sicherung zu gewährleisten, andererseits jedoch übertriebene und bürokratisch wirkende Schutzmaßnahmen zu vermeiden. Unangemessene Sicherheitsstandards, die anwendungsunabhängig gefordert oder eingesetzt werden, werden von den Benutzern nicht akzeptiert, als Einschränkung empfunden und deshalb nach Möglichkeit umgangen. Sie wirken dadurch kontraproduktiv.

Die vorliegende abgestufte Standardisierung von weitgehend technischen Maßnahmen kann und soll jedoch nicht ein Gesamtkonzept ersetzen, das räumliche und organisatorische Bedingungen vor Ort konkret einbezieht sowie entsprechende Raumsicherungsmaßnahmen und organisatorische Maßnahmen wie z.B. Vertretungsregelungen beschreibt. Das Schutzstufenkonzept soll auch nicht als schematische Anleitung fehlverstanden werden, sondern als Orientierungshilfe dienen, um eine einheitliche Umsetzung technischer Sicherungsmaßnahmen bei gleichgearteten PC-Anwendungen zu garantieren. Aus diesem Verständnis heraus werden im folgenden durch das Schutzstufenkonzept entsprechende Klassen von Daten definiert und deren mögliche Zuordnung zu speziellen Anwendungen durch einige Beispiele verdeutlicht. Auch dienen die Beispiele nur als Orientierung; eine genaue Zuordnung von Anwendungen kann erst im Einzelfall unter genauer Kenntnis des Verwendungszwecks der gespeicherten Daten erfolgen. Auf die systemspezifischen Sicherungsmaßnahmen wird unten (3.2.3) produktunabhängig eingegangen. Insgesamt wird zwischen folgenden Daten unterschieden:

— Stufe A: personenbezogene Daten, deren Mißbrauch keine besondere Beeinträchtigung erwarten läßt, z.B.
  - Adreßangaben (Name, Anschrift, Tel.-Nr.),
  - Berufs-, Branchen- oder Geschäftsbezeichnungen;

— Stufe B: personenbezogene Daten, deren Mißbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann, z.B.
  - Daten über Mietverhältnisse,
  - Daten über Geschäftsbeziehungen;

— Stufe C: personenbezogene Daten, deren Mißbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigen kann, bzw. die einem Berufs- oder besonderen Amtsgeheimnis (§ 45 Satz 2 Nummer 1 BDSG a.F.) unterliegen, z.B. Daten über
  - gesundheitliche und soziale Verhältnisse,
  - strafbare Handlungen,
  - Ordnungswidrigkeiten,
  - religiöse oder politische Anschauung;

— Stufe D: personenbezogene Daten, deren Mißbrauch für den Betroffenen Gefahren für Leib und Leben bedeuten, z.B.
  - Adressen von polizeilichen V-Leuten,
  - Adressen von Zeugen in bestimmten Strafverfahren.

3.2.2.2 Schutzrichtung zu treffender Maßnahmen

Personenbezogene Daten sollen grundsätzlich vor unberechtigtem Zugriff, unberechtigter Verwendung und unberechtigter Weitergabe geschützt werden. Unbefugte können in diesem Sinne sowohl Externe als auch die Benutzer selbst sein. Als Externe gelten aus Sicht einer Anwendung auch diejenigen Benutzer, die im Rahmen des Mehr-

benutzer-Betriebs lediglich für andere Anwendungen autorisiert sind und darüber hinaus keine weitere Zugriffsberechtigung haben.

Das vorliegende Schutzstufenkonzept geht davon aus, daß die Daten der Stufe A lediglich vor unberechtigtem Zugriff durch Externe geschützt werden müssen. Die Hauptverantwortung für die Datensicherheit hinsichtlich der Stufe A trägt somit der Benutzer selbst, es bedarf keiner zusätzlichen Kontrolle. Gleichzeitig wird dem Benutzer der PC als weitgehend universell einsetzbarer Rechner zur Verfügung gestellt.

Personenbezogene Daten der Klasse B und C sollten zusätzlich vor unberechtigter Weitergabe durch den Benutzer selbst geschützt werden (interner Mißbrauch). Dies hat u.a. zur Konsequenz, daß der Benutzer im Gegensatz zum Konzept für Daten der Klasse A lediglich menügesteuert die Funktionalität auf dem PC erhält, die er für die Aufgabenbearbeitung tatsächlich benötigt. Diese Regelung führt zu einer restriktiveren PC-Nutzung. Daten der Stufe D, deren Mißbrauch Leib und Leben des Betroffenen gefährden kann, sollten überhaupt nicht auf PC gespeichert werden, da auf diesen Geräten die erforderlichen Schutzmaßnahmen faktisch nicht getroffen werden können.

3.2.2.3 Stellenwert der Systemverwaltung

Mittlerweile sehen viele auf dem Markt befindliche PC-Sicherungssysteme die Autorisierung von mehreren Benutzern und somit die Funktion eines Systemverwalters vor, wie sie von Großrechnersystemen bekannt ist. Durch eine Systemverwaltung wird insbesondere im Mehrbenutzer-Betrieb die Zugriffskontrolle erhöht.

Beim Sicherungskonzept für Daten der Stufe A und B kann die Funktion des Systemverwalters bei entsprechender Schulung von einem Benutzer selbst wahrgenommen werden. Da Daten der Stufe B zusätzlich gegen internen Mißbrauch geschützt werden sollen, ist es bei dieser Stufe notwendig, die Aktivitäten des Systemverwalters zusätzlich zu protokollieren und die Protokolle durch eine zweite Person auszuwerten. Zur Auswertung der Protokolle sollten geeignete Hilfsmittel zur Verfügung stehen.

Um gegenüber Stufe B weitere Sicherheit zu erreichen, unterliegt die Systemverwaltung im Rahmen der Stufe C zusätzlich dem Vier-Augen-Prinzip. Die Systemverwaltung darf nicht von einem Benutzer selbst wahrgenommen werden. Dieser sollte lediglich dem Systemverwalter den Systemzugriff über ein zweites Paßwort freigeben und somit die Systemverwaltung indirekt kontrollieren.

3.2.2.4 Mehrbenutzer- bzw. multifunktionaler Betrieb

Die Benutzerkontrolle (ausschließlicher Zugriff auf die der Zugriffsberechtigung unterliegenden Daten) gewinnt in dem Maße an Bedeutung, wie der Computer zur Unterstützung unterschiedlicher Aufgaben mit aufgabenspezifischen Dateien genutzt wird. Während im Einbenutzer-Betrieb insbesondere bei monofunktionaler Nutzung lediglich der Zugang zum PC kontrolliert werden muß, erweitern sich bei multifunktionalem Betrieb (Nutzung des PC zu verschiedenen Zwecken) mit mehreren Benutzern die Sicherungsmaßnahmen um die gegenseitige Abschottung der für die jeweiligen Aufgaben benötigten Dateien. Benutzer anderer Anwendungen gelten in diesem Konzept als Externe, denen der Zugriff auf Dateien anderer Anwendungen, selbst bei Stufe A verwehrt werden sollte.

Bei Schutzstufe C bezieht sich die Zugriffskontrolle nicht nur auf Personen, sondern auf die verschiedenen funktionalen Rollen, die ein Benutzer wahrnimmt und die entsprechend gegeneinander abgeschottet werden müssen. Um eine aufgabenübergreifende Nutzung zu vermeiden bzw. diese auch durch entsprechende Protokolle besser kontrollieren zu können, ist es notwendig, auch bei nur einem Benutzer die jeweiligen Anwendungen über eine eigene Benutzerkennung abzuwickeln.

Falls Anwendungen mit unterschiedlichen Schutzstufen auf einem Rechner abgewickelt werden, sollen sich die Sicherungsmaßnahmen an den Daten orientieren, die der Klassifizierung entsprechend am stärksten zu schützen sind.

3.2.2.5 Betriebssystemzugriff

Personalcomputer zeichnen sich vor allem durch ihren flexiblen Einsatz aus, der nicht zuletzt durch den direkten Betriebssystemzugriff realisiert wird. So stellt sich etwa MS-DOS auch mit zusätzlicher Datenschutzsoftware als offenes System dar, wenn dem Benutzer der Zugang auf Betriebssystemebene erlaubt wird: Unterverzeichnisse können nicht wirkungsvoll geschützt werden, beim Einsatz von speziellen Dienstprogrammen kann auch auf versteckte Dateien weiterhin zugegriffen werden.

Daher wird dem Benutzer lediglich bei Stufe A der Betriebssystemzugriff gewährt. Nutzen jedoch mehrere Benutzer den PC für verschiedene Zwecke, so muß auch in Stufe A verhindert werden, daß über Betriebssystemebene verzeichnisübergreifend auf sämtliche PC-Dateien zugegriffen werden kann. Aus diesem Grund sollte der Aufruf von Betriebssystemkommandos im Mehrbenutzer-Betrieb mittels spezieller Datenschutzsoftware abgewickelt werden, die im Rahmen ihrer Dateiverwaltung die Funktionalität der jeweils benötigten MS-DOS-Befehle bereitstellt.

Um den in Stufe B und C geforderten Schutz gegen internen Mißbrauch umzusetzen, sollte in diesen Stufen dagegen auf direkten Betriebssystemzugriff vollständig verzichtet und der Benutzer per Menü gesteuert werden.

3.2.2.6 Protokollierung

Nachträgliche Zugangs-, Zugriffs-, Eingabe- und Datenabgangskontrollen erfordern eine umfassende Protokollierung aller Systemaktivitäten, insbesondere der Funktionen, die vom Systemverwalter aufgerufen werden. Die Auswertung entsprechender Protokolle sollte durch geeignete Werkzeuge unterstützt und darf in Stufe B und C nicht vom Systemverwalter selbst vorgenommen werden. Wahlweise sollten die Veränderung von Benutzerrechten, erfolgreiche und fehlgeschlagene Anmeldeversuche, Dateizugriffe sowie der Aufruf von Programmen protokolliert werden können.

3.2.2.7 Verschlüsselung von Daten

Neben der Zugangs- und Zugriffskontrolle mittels Paßwort-Vergabe benutzen einige Datensicherungssysteme das Instrument der Datenverschlüsselung. Zusätzliche Datenverschlüsselung ist dann notwendig, wenn die zu speichernden Daten derart schutzwürdig sind, daß sie selbst nach Diebstahl des Geräts bzw. nach umständlicher und zeitintensiver Umgehung der Zugriffskontrolle weiterhin nicht lesbar sein sollen. Personenbezogene Daten, die auf tragbaren Geräten gespeichert sind, sollten in jedem Fall verschlüsselt werden.

Die mit Laufzeitverzögerungen verbundene Verschlüsselung von Daten ist jedoch nur dann gegenüber dem Benutzer vertretbar, wenn die jeweiligen Daten nicht ausdrücklich vor jedem Zugriff durch ein entsprechendes Batch-Programm ver- bzw. entschlüsselt werden müssen. Dieses umständliche Verfahren würde beispielsweise beim Verändern eines Datums einer Datenbank zum Entschlüsseln der gesamten Datenbank und nach erfolgter Änderung wieder zu deren gesamten Entschlüsselung führen. Um unnötige Laufzeitverzögerungen zu vermeiden, ist es notwendig, daß die zu schützenden Daten hardwaremäßig online-verschlüsselt werden, das heißt die Daten werden während des Zugriffs auf die Festplatte durch eine zusätzliche Steckkarte chiffriert. Hierfür werden hauptsächlich zwei Verschlüsselungstechniken eingesetzt:

— Das XOR-Verfahren soll z. B. Wartungstechnikern das Lesen der Festplatte erschweren, ist jedoch aufgrund des relativ einfachen Verschlüsselungsalgorithmus nicht allzu sicher und von Spezialisten leicht zu erkennen.

— Die DES-Verschlüsselung (Data Encryption Standard) ist weitaus sicherer als das XOR-Verfahren. Als symmetrisches Verfahren benutzt es sowohl beim Verschlüsseln als auch beim Entschlüsseln nur einen Schlüssel. Angesichts der Komplexität des Verfahrens ist zur Online-Verschlüsselung eine spezielle Steckkarte mit einem sehr schnellen Prozessor erforderlich.

3.2.3 Datensicherungsmaßnahmen für einzelne Schutzstufen

3.2.3.1 Datensicherungsmaßnahmen für Stufe A

Benutzerkontrolle bei Einbenutzer-Betrieb:

— Schloß mit Sicherung der Tastatur, unterschiedliche Schlösser vorausgesetzt

Benutzerkontrolle bei Mehrbenutzer-Betrieb:

— Paßwort-Abfrage

— Starten des Betriebssystems ausschließlich über Festplatte (Bootschutz für Diskettenlaufwerk)

Zugriffskontrolle (lediglich bei Mehrbenutzer-Betrieb):

— jeweils eigene Unterverzeichnisse für einzelne Anwendungen

— Zugriff auf Betriebssystemkommandos nur innerhalb der jeweiligen Anwendung

Datenabgangskontrolle:

— Geschützte Aufbewahrung der Sicherungsdisketten

3.2.3.2 Datensicherungsmaßnahmen für Stufe B

Benutzerkontrolle:

— Paßwort-Abfrage

— Starten des Betriebssystems ausschließlich über Festplatte (Bootschutz für Diskettenlaufwerk)

— Gehäuseschloß oder Verplomben des Gerätes

Zugriffskontrolle:

— jeweils eigene Unterverzeichnisse für einzelne Anwendungen

— ausschließliche Menüsteuerung, kein Betriebssystemzugriff

— Bildschirm-Verdunkelung durch den Benutzer bei Arbeitsunterbrechung, Weiterarbeit erst nach erneuter Paßwort-Eingabe

Eingabekontrolle:

— Protokollierung gescheiterter Zugriffsversuche

— Protokollierung der Aktivitäten des Systemverwalters:

- Veränderung von Zugriffsrechten
- Lese- und Schreibzugriff auf Dateien mit personenbezogenen Daten
- Aufruf von Programmen

— Auswertung der Protokolle durch eine Person, die nicht Systemverwalter ist

Datenabgangskontrolle:

— menügesteuerte Datensicherung

— Verschlüsselung der Sicherungsdisketten

— Aufbewahrung der Sicherungsdisketten in Sicherheitsschränken

— Zugriff auf das Diskettenlaufwerk nur über Menüsteuerung innerhalb der Anwendung

— Sicherung der seriellen Schnittstelle vor unberechtigtem Zugriff

3.2.3.3 Datensicherungsmaßnahmen für Stufe C

Benutzerkontrolle:

— Paßwort-Abfrage

— Starten des Betriebssystems ausschließlich über Festplatte (Bootschutz für Diskettenlaufwerk)

— Gehäuseschloß oder Verplomben des Gerätes

Zugriffskontrolle:

— jeweils eigene Unterverzeichnisse für einzelne Anwendungen

— ausschließliche Menüsteuerung, kein Betriebssystemzugriff

— Systemverwaltung durch dritte Person nach dem Vier-Augen-Prinzip (Vier-Augen-Prinzip kann über zwei Paßwörter, die jeweils dem Systemverwalter und Benutzer bekannt sind, umgesetzt werden)

— automatische Bildschirm-Verdunkelung bei längerer Arbeitsunterbrechung, Weiterarbeit erst nach erneuter Paßwort-Eingabe

— Verschlüsselung der Festplatte nach dem DES-Verfahren

— physikalisches Löschen personenbezogener Daten

Eingabekontrolle:

— Protokollierung gescheiterter Zugriffsversuche

— Protokollierung der Aktivitäten des Systemverwalters und sämtlicher Benutzer:
  - Veränderung von Zugriffsrechten
  - Lese- und Schreibzugriff auf Dateien mit personenbezogen Daten
  - Aufruf von Programmen

— Auswertung der Protokolle durch eine Person, die nicht Systemverwalter ist

Datenabgangskontrolle:

— menügesteuerte Datensicherung nur durch den Systemverwalter

— Verschlüsselung der Sicherungsdisketten nach dem DES-Verfahren

— Aufbewahrung der Sicherungsdisketten im Tresor

— Zugriff auf das Diskettenlaufwerk nur durch den Systemverwalter

— Sicherung der seriellen Schnittstelle vor unberechtigtem Zugriff

3.2.3.4 Datensicherungsmaßnahme für Stufe D

Aus sicherheitstechnischen Gründen wird die Verarbeitung von Daten der Stufe D auf PC abgelehnt.

3.3 Sicherheitsaspekte beim Betrieb von UNIX-Rechnern

In der Verwaltung werden zunehmend mittlere Datenverarbeitungssysteme eingesetzt. Der überwiegende Teil dieser Systeme läuft unter dem Betriebssystem UNIX bzw. einer Variante dieses Betriebssystems (SINIX).

Im Unterschied zu dem PC-Betriebssystem MS-DOS können bei UNIX mehrere Benutzer gleichzeitig am System arbeiten. Jeder Benutzer kann zudem gleichzeitig verschiedene Dienstleistungen nutzen, also z.B. zugleich einen Text bearbeiten und einen anderen Text ausdrucken. Die Benutzer können auf gemeinsame Datenbestände zugreifen.

Stark gesunkene Preise von mittleren UNIX-Anlagen, ihre benutzerfreundlichen Menüoberflächen und die vermeintlich einfache Installation und Systemverwaltung tragen zu ihrer raschen Verbreitung bei. UNIX-Systemen wird häufig dort der Vorzug gegeben, wo verschiedene Benutzer auf eine gemeinsame Datenbasis zugreifen sollen und die Einrichtung von PC-Netzwerken als zu aufwendig erscheint. Zudem können Anwender einem von der zentralen Administration vorgegebenen Nutzungskonzept unterworfen und so an einer Verselbständigung gehindert werden, was bei autonom betriebenen PC kaum möglich ist.

Andererseits sind vor dem Einsatz von UNIX-Systemen erhebliche Anforderungen an die Planung der organisatorischen Einbindung und an die Qualifikation des Systemmanagements zu stellen. Andernfalls sind erhebliche — z.T. kaum noch beherrschbare

— Datenschutzrisiken die unvermeidliche Folge. Von uns durchgeführte Prüfungen haben ergeben, daß diesen Risiken auch in der Hamburger Verwaltung nicht immer Rechnung getragen wird, weil bei den für die Installation und den Betrieb derartiger Rechner zuständigen Stellen z.T. nicht die erforderlichen Kenntnisse vorhanden sind, um den bestehenden Gefahren in jedem Fall zuverlässig zu begegnen.

3.3.1 Die Rolle des Systemverwalters

UNIX gibt dem — Super-User genannten — Systemverwalter umfassende Zugriffsrechte auf sämtliche Ressourcen. Er kann alle Dateien lesen, die Zugriffsrechte auf sie und die Eigentumsrechte an ihnen verändern sowie Systeminformationen über Dateien manipulieren (z.B. Datum der letzten Dateiänderung). Er kann auch die Paßworttabelle bearbeiten, also Benutzer hinzufügen, sperren, ihre Berechtigungen verändern oder löschen, und hat die Möglichkeit, ohne Einschränkung in jede Benutzerkennung zu wechseln.

Andererseits ist der Super-User praktisch nicht zu kontrollieren, denn er hat nicht nur Zugriff auf eventuell vorhandene Systemprotokolle, sondern kann diese auch verändern. Diese Stellung des „allmächtigen" Super-Users stellt die entscheidende Schwachstelle von UNIX dar.

Das vom Super-User ausgehende Risiko läßt sich durch eine konsequente Funktionstrennung zwar begrenzen, nicht aber völlig ausschließen. So können bestimmte Aufgaben der Systemverwaltung einem weniger privilegierten Unterverwalter übertragen werden, der zudem seine Aufgaben menügeführt wahrnimmt. Ferner ist daran zu denken, das Paßwort des Super-Users zu teilen oder die Super-User-Kennung mit zwei Paßwörtern zu versehen, so daß nur zwei Personen gemeinsam sich unter der entsprechenden Kennung anmelden können.

Ein weiteres Problem ergibt sich daraus, daß UNIX wahlweise im Einbenutzermodus oder im Mehrbenutzermodus betrieben werden kann. Während im Mehrbenutzermodus der Systemzugang durch die Paßwortkontrolle geschützt wird, findet im Einbenutzermodus keine Paßwortabfrage statt und die Konsole (der Bildschirmarbeitsplatz, von dem aus das System gewöhnlich administriert wird und auf dem die Systemmeldungen ausgegeben werden) hat automatisch Super-User-Status und verfügt damit über umfassende Privilegien. Es müssen deshalb Maßnahmen getroffen werden, die verhindern, daß das System unkontrolliert in den Einbenutzermodus heruntergefahren wird. Die Zentraleinheit und die Konsole müssen besonders gegen unberechtigten Zutritt gesichert werden.

3.3.2 Lückenhafte Menüsteuerung

UNIX-Systeme werden zumeist mit einer „Menüoberfläche" ausgeliefert, d.h. der Zugriff auf Programme und Dateien erfolgt nicht durch Eingabe von Betriebssystemkomandos, sondern durch Auswahl von Menüpunkten aus einer vorgegebenen Liste.

Nur bestimmten Benutzern wird der Zugang zur Betriebssystemebene gestattet. Damit soll gewährleistet werden, daß die Anwender das System nur im Rahmen ihrer Berechtigungen nutzen können. Ein unkontrollierter Zugang zum Betriebssystem könnte irreversible Schäden am Datensystem entstehen lassen; Sicherungsmechanismen könnten umgangen oder außer Kraft gesetzt werden. So sind — anders als bei DOS — mit Betriebssystemkommandos gelöschte Dateien oder Dateisysteme nicht mehr rekonstruierbar, sofern nicht zuvor auf Diskette oder auf Magnetband Sicherungskopien gezogen wurden. Die Paßworttabelle und andere sicherheitsempfindliche Dateien können gelesen, kopiert oder ausgedruckt werden. Dadurch wäre es Benutzern möglich, Informationen, die nicht für sie bestimmt sind, zur Kenntnis zu nehmen und weitere Sicherheitslücken ausfindig zu machen.

Ferner könnten „Trojanische Pferde" (Programme mit gleichem Namen, aber unterschiedlicher Funktionsweise als die zugelassenen Programme) und Programmviren

(sich in andere ausführbare Programme fortpflanzende Programmsegmente) in den Rechner eingeschleust werden.

Leider weisen verschiedene in der Hamburger Verwaltung standardmäßig eingesetzte Softwarepakete Ausgänge zum Betriebssystem auf, durch die Benutzer — auch wenn dies ihren vom Systemverwalter vergebenen Rechten widerspricht — auf die Betriebssystem-Ebene gelangen können. Solche Programme stellen ein erhebliches Sicherheitsrisiko dar, insbesondere deshalb, weil die Anwender davon ausgehen, daß durch das Menüsystem ein unkontrollierter Zugang zur Betriebssystemebene unterbunden wird. Die Menüsteuerung suggeriert somit häufig eine tatsächlich gar nicht gegebene Systemsicherheit.

Aus diesem Grund müssen Menüsysteme „wasserdicht", d.h. ohne unverschlossene Hintertüren zur Betriebssystemebene gestaltet werden. Anwendungsprogramme mit nicht verschließbaren Ausgängen zum Betriebssystem sollten nicht eingesetzt werden. Standardprogramme (für Textverarbeitung, Tabellenkalkulation, Datenbankverwaltung und Bürokommunikation) sollten an zentraler Stelle — möglicherweise durch das IuK-Informationszentrum des Senatsamtes für den Verwaltungsdienst — eingehend geprüft und erst dann für den allgemeinen Einsatz in der Verwaltung empfohlen werden, wenn festgestellt wurde, daß sicherheitsrelevante Schwachstellen nicht bestehen.

3.3.3 UNIX in sicherheitsempfindlichen Bereichen?

Die erwähnten und andere — hier aus Sicherheitserwägungen heraus nicht beschriebene — Schwachstellen von UNIX-Systemen wiegen in solchen Bereichen besonders schwer, in denen sensible personenbezogene Daten verarbeitet werden oder in denen aus anderen Gründen der Systemsicherheit besondere Bedeutung zukommt.

Derartige Verfahren sind nur zu verantworten, wenn der Rechnereinsatz in ein umfassendes Sicherheitskonzept eingebettet ist und Maßnahmen ergriffen werden, um die Sicherheitsrisiken zu minimieren. Den verantwortlichen Stellen muß bewußt sein, daß gleichwohl ein Restrisiko bestehen bleibt, das sich auch mit restriktiven Regelungen und Maßnahmen nicht ausschalten läßt. Sollte dieses Risiko im Hinblick auf die Sensibilität der zu verarbeitenden Daten zu hoch sein, sollte von einer Verarbeitung auf UNIX-Systemen abgesehen werden.

3.4 Prüfung der Datenverarbeitungszentrale (DVZ)

3.4.1 Vorgeschichte

Die Behörden der Freien und Hansestadt Hamburg haben, soweit sie keine eigenen Rechner betreiben, in der Regel keine Möglichkeit, einen Auftragnehmer für die Durchführung ihrer automatisierten Verfahren „unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen", wie es § 3 Absatz 1 Satz 2 HmbDSG vorschreibt, sondern sind insoweit auf die DVZ als Auftagnehmer angewiesen. Die zur Finanzbehörde gehörende DVZ ist das Rechenzentrum der hamburgischen Verwaltung. Vor diesem Hintergrund ist die Datensicherheit in der DVZ von grundlegender Bedeutung für die Gewährleistung des Datenschutzes in der gesamten hamburgischen Verwaltung.

Nachdem der Hamburgische Datenschutzbeauftragte in den Jahren 1984/85 in der DVZ eine Prüfung durchgeführt hatte (4. TB, 3.6, S. 21 ff.), haben wir im Berichtsjahr mit einer weiteren Prüfung der DVZ begonnen. Auch jetzt steht wieder — wie schon 1984/85 — die Sicherheit der Datenverarbeitung in der DVZ im Mittelpunkt und nicht die bei einzelnen automatisierten Verfahren zu treffenden und von den zuständigen Behörden zu verantwortenden Sicherungsmaßnahmen. Mit Sicherheit der Datenverarbeitung ist die Betriebssicherheit gemeint, wie sie in § 8 HmbDSG und in der DS-Richtlinie (MittVw 1977 S. 205) umschrieben ist.

Seit unserer ersten Prüfung sind erhebliche Veränderungen hinsichtlich der ADV-Verfahren, der in der DVZ eingesetzten Betriebssysteme, der systemnahen Software ein-

schließlich der Sicherheitssoftware sowie der Organisation des Rechenzentrums zu verzeichnen. Diese Veränderungen beruhen auf der allgemeinen technischen Weiterentwicklung und stehen im Zusammenhang mit den vom Senat im Juli 1985 getroffenen Grundsatzentscheidungen zur Neuorganisation der Nutzung von IuK-Technik.

Mit der Entwicklung einer neuen Organisation für die DVZ soll der Tatsache Rechnung getragen werden, daß die Informations- und Kommunikationstechnik heute einen Stand erreicht hat, der eine angemessene Automatisierung des Rechenzentrumsbetriebs erfordert, die wir schon 1985 in unserem Prüfungsbericht empfohlen hatten. Diese Automatisierung, aber auch die Zunahme von Dialogverfahren und die Vielfalt der von der hamburgischen Verwaltung betriebenen Datenfernverarbeitungsnetze, stellen sehr hohe Anforderungen an die Qualifikation des im Rechenzentrum tätigen Personals. Um diesen Anforderungen gerecht werden zu können, muß der Betrieb der DVZ inhaltlich und qualitativ schrittweise weiterentwickelt werden, wozu — wie sich gezeigt hat — die Neueinstellung hinreichend ausgebildeten Personals sowie die Weiterentwicklung geeigneter Kräfte aus dem vorhandenen Mitarbeiterstamm erforderlich ist. Die DVZ geht davon aus, daß der Prozeß der Umgestaltung sich über vier Jahre erstrecken wird. Davon ist bisher etwa ein Jahr verbraucht.

Mit der Neuorganisation der DVZ wird keine Veränderung bei der Verteilung der Kompetenzen zwischen DVZ und Senatsamt für den Verwaltungsdienst — Organisationsamt — verbunden sein. Es bleibt bei der Zuständigkeit des Senatsamtes für die Planung von Hard- und Software, die Systemprogrammierung einschließlich der Implementation der Sicherheitssoftware (deren Administration obliegt weiterhin der DVZ) und für die zentrale Steuerung der IuK-Planung. Die Anwendungsentwicklung bleibt Aufgabe der für die jeweilige Verwaltungsaufgabe zuständigen Behörden. Die DVZ ist bestrebt, die aus der Sicht des eigenen Betriebs an die Verfahrensgestaltung zu stellenden Anforderungen rechtzeitig und wirkungsvoller als in der Vergangenheit in die Planungen einzubringen. Deshalb entsendet sie neuerdings Kontaktpersonen in bedeutende Projekte.

3.4.2 Prüfungsgegenstand und Vorgehen

Schwerpunktmäßig befassen wir uns bei der derzeitigen Prüfung mit der Frage, wie die diversen in der DVZ eingesetzten sicherheitsrelevanten Softwareprodukte (Betriebssystem, systemnahe Software, Sicherheitssoftware, der Sicherheit dienende Komponenten in der Anwendungssoftware) zusammenwirken und in welchem Maße dadurch Betriebssicherheit erreicht wird.

Die Sachverhaltsermittlung erfolgt im wesentlichen in Form von „Expertengesprächen". An den Gesprächen nehmen sachkundige Vertreter der DVZ und des Senatsamtes teil. Weil unser Prüfungsgegenstand im wesentlichen die „Allgemeine Software" ist, die vom Senatsamt für den Verwaltungsdienst bereitgestellt wird und für die die Systemprogrammierer des Senatsamtes zuständig sind, ist die Beteiligung des Senatsamtes an dieser Untersuchung geboten.

Folgende Themenbereiche haben wir bisher behandelt:

— Zusammenwirken des Betriebssystems MVS mit dem TP-Monitor COMPLETE und der Datenbanksoftware ADABAS/NATURAL,

— Zusammenwirken des Betriebssystems BS2000/UTM mit der Datenbanksoftware ADABAS/NATURAL,

— Zusammenwirken von MVS und der Sicherungssoftware TSS,

— Sicherungen im Betriebssystem BS2000,

— Sicherheitsfunktion der Software UTM (einer Komponente des BS2000).

Weitere Untersuchungsbereiche werden sein:

— die Funktionsweise und Sicherungen der Netze [Transdata, SNA, BULL, Datex-P, DVS (ein in Nordrhein-Westfalen betriebenes Netz, das vom Statistischen Landesamt mitgenutzt wird), ISDN]

— Anschluß dezentraler Rechner,

— Probleme der Abstrahlung von DV-Geräten,

— Probleme bei potentieller Zulassung von Wählanschlüssen und Fernwartung.

Nach Abschluß der Sachverhaltsermittlung werden wir die Ergebnisse analysieren und datenschutzrechtlich bewerten. Wir gehen davon aus, daß die Prüfung im nächsten Jahr abgeschlossen und voraussichtlich im nächsten Tätigkeitsbericht ausführlich dargestellt werden kann.

3.5 Telekommunikation

3.5.1 Datenspeicherung in ISDN-Nebenstellenanlagen

Wir haben schon im letzten Tätigkeitsbericht darauf hingewiesen, daß die ISDN-Technik neuartige datenschutzrechtliche Gefahren in sich birgt (8. TB, 2.3.1, S. 15), die vor allem mit der Frage verbunden sind, wie die durch Artikel 10 GG rechtlich geschützte Vertraulichkeit der übertragenen Informationen und der Verbindungsdaten gewährleistet werden kann.

Da es sich bei ISDN-Anlagen um softwaregesteuerte Datenverarbeitungsanlagen handelt, hängt die Lösung der auftretenden Probleme entscheidend von den eingesetzten Programmen ab.

Im Zusammenhang mit der Einrichtung behördlicher ISDN-Nebenstellenanlagen haben wir deshalb im Januar 1990 eine Reihe von Fragen, die sich auf die eingesetzten Programme, die verarbeiteten Kommunikationsdaten und die getroffenen Datensicherungsmaßnahmen bezogen, an die fachlich zuständige Baubehörde gestellt. Insbesondere wollten wir erfahren,

— welche personenbezogenen Daten (Bestands-, Verbindungs- und Inhaltsdaten) gespeichert werden,

— welche Maßnahmen getroffen werden, um den Datenschutz sicherzustellen (§ 8 Abs. 2 HmbDSG),

— ob und gegebenenfalls wie der Systemzustand revisionssicher protokolliert wird und

— durch welche Regelungen die Einhaltung der Datensicherungsmaßnahmen gewährleistet wird.

Die Baubehörde hat zunächst den Standpunkt vertreten, auf ISDN-Anlagen würden keine personenbezogenen Daten verarbeitet und somit sei das Hamburgische Datenschutzgesetz nicht anzuwenden. Deshalb bestünden auch keine Auskunftspflichten gegenüber dem Hamburgischen Datenschutzbeauftragten. Dem haben wir entschieden widersprochen und deutlich gemacht, daß es sich bei Kommunikationsdaten, die einzelnen Anschlüssen zuzuordnen sind, um personenbezogene Daten handelt. Hierzu gehören sowohl Rufnummern als auch die für die Anschlüsse jeweils verfügbaren Leistungsmerkmale, denn auch diese Informationen können einzelnen Personen zugeordnet werden. Personenbezogen sind ferner Inhaltsdaten, die mit der Anlage übertragen werden oder die — z. B. im Sprachinformationssystem — gespeichert werden und die ebenfalls einem Anschluß, Teilnehmer oder Kommunikationspartner des Teilnehmers zugeordnet werden können.

Erst kurz vor Redaktionsschluß für diesen Tätigkeitsbericht hat die Baubehörde schließlich Unterlagen über die Kommunikationsdatenverarbeitung auf ISDN-fähigen Nebenstellenanlagen vorgelegt. Die inhaltliche Prüfung dieser Unterlagen konnte deshalb für diesen Bericht noch nicht abgeschlossen werden. Allerdings kann schon jetzt auf folgendes hingewiesen werden: Obwohl ISDN-fähige Nebenstellenanlagen zur Überwachung des Verhaltens der Benutzer geeignet sind, gibt es weder behördenspezifische noch behördenübergreifende Regelungen, die einen Mißbrauch von in ISDN-Nebenstellenanlagen anfallenden Kommunikationsdaten (Verbindungs- und Inhaltsdaten) wirksam unterbinden. Der Senat hat die entsprechenden Anstöße des Daten-

schutzbeauftragten und der Gewerkschaften lediglich zum Anlaß genommen, eine Überarbeitung der „Telekommunikationsrichtlinie" von 1976 (MittVw 8/1976, S. 169) anzukündigen. Ob und inwieweit Datenschutzgesichtspunkte hierbei berücksichtigt werden, bleibt abzuwarten.

3.5.2 Pilotprojekt Telekommunikationsanlage als Kommunikationsdrehscheibe

Für die Erprobung einer digitalen Nebenstellenanlage (Telekommunikationsanlage) als Kommunikationsdrehscheibe wurde einem Senatsauftrag (Senatsdrucksache 77/1988) entsprechend eine Projektgruppe unter Federführung der Baubehörde eingesetzt (8. TB, 2.3.4, S. 18 f.).

Der Hamburgische Datenschutzbeauftragte ist in der Projektgruppe vertreten. Im Rahmen seiner Beratungsfunktion nach dem Hamburgischen Datenschutzgesetz beurteilt er bei den Pilotanwendungen auftretende und bei einer potentiellen allgemeinen Einführung solcher Anwendungen in der hamburgischen Verwaltung möglicherweise zu erwartende datenschutzrechtlich relevante Risiken. Er formuliert Anforderungen an die Technik und Organisation zur Vermeidung bzw. Beherrschung dieser Risiken und beteiligt sich an der Erarbeitung von Lösungsvorschlägen. An Entscheidungen der Projektgruppe kann er sich wegen seiner gesetzlich verankerten Unabhängigkeit nicht beteiligen.

Die Projektgruppe hat inzwischen ein Rahmenkonzept erarbeitet, das als Basis für das Pilotprojekt zur Fortentwicklung der Telekommunikationsinfrastruktur in der hamburgischen Verwaltung dienen soll. Das Rahmenkonzept ist offen für Weiterentwicklungen. Es umfaßt in Form von sogenannten Kommunikationsmodellgruppen (KMG) technisch realisierbare und für die Verwaltung möglicherweise sinnvolle Anwendungen sowohl im sprachlichen als auch im nichtsprachlichen Bereich. Aufgabe der Behörden ist es, jeweils ihre Anwendungen zu planen und zu organisieren. Die Behörden haben dabei die rechtliche Zulässigkeit eigenverantwortlich zu prüfen und bestehende Mitbestimmungsrechte der Personalvertretungen zu beachten. Die Baubehörde prüft dann, ob die gewünschte Anwendung technisch realisierbar ist und stellt die entsprechenden Übertragungs- und Vermittlungseinrichtungen gegebenenfalls zur Verfügung. Der Schwerpunkt des Pilotversuchs wird bei der TK-Anlage der Baubehörde liegen.

Wir haben zu dem Rahmenkonzept im Juni 1990 eine Stellungnahme abgegeben. Weil eine Reihe von Fragen zu technischen Details der eingesetzten Telekommunikationsanlagen und -software, denen wir datenschutzrechtliche Relevanz beimessen, noch nicht geklärt sind (s. o. 3.5.1), hat diese Stellungnahme vorläufigen Charakter. Wir haben dargelegt, daß wir von einem befristeten Pilotversuch ausgehen und daß erst nach Beendigung des Versuchs und Auswertung der gewonnenen Erkenntnisse darüber entschieden werden kann, welche der einzelnen erprobten Anwendungen zeitlich verlängert und welche davon auch für andere Anwendungsfälle zugelassen werden sollen. Es darf nicht die Möglichkeit ausgeschlossen werden, daß der Pilotversuch hinsichtlich einzelner Anwendungen zu dem Ergebnis führt, sie sollten nicht generell eingeführt werden.

Eine Reaktion auf unsere Stellungnahme ist bisher nicht erfolgt. Uns ist auch nicht bekannt, ob von anderer Seite zu dem Rahmenkonzept Stellung genommen worden ist.

Nach dem Rahmenkonzept sollen im Pilotversuch KGM unter anderem folgende Anwendungen erprobt werden:

3.5.2.1 Digitales Behördennetz

Ziel ist eine ISDN-fähige Kommunikationsinfrastruktur im Behördennetz. Das digitale Behördennetz soll nach derzeitigen Vorstellungen

— eine höhere Übertragungskapazität, eine bessere Übertragungsgüte sowie größere Silbenverständlichkeit bieten,

— anlagenübergreifende Leistungsmerkmale in der Sprachkommunikation und

— Mischkommunikation (Sprach- und Datenübertragung) ermöglichen,

— eine wirtschaftlichere Nutzung der vorhandenen Kabelstrecken zulassen und

— die Wartungskosten reduzieren.

Zum digitalen Behördennetz vertreten wir die Auffassung, daß offengelegt werden muß, welche Art von Daten in den Vermittlungsstellen und dem geplanten digitalen Behördenknoten gespeichert und verarbeitet werden. Falls es sich dabei — wie wir vermuten — auch um personenbezogene Daten handelt, müssen die erforderlichen Maßnahmen getroffen werden, um einen Mißbrauch dieser Daten auszuschließen und das Fernmeldegeheimnis zu gewährleisten. Dazu gehören sowohl technische (z.B. Raumsicherung, Speicherungs- und Benutzungskontrolle) als auch organisatorische Maßnahmen (z.B. Festlegung von Zuständigkeiten). Die Benutzer der an TK-Anlagen angeschlossenen Endgeräte müssen darüber unterrichtet werden, welche Leistungsmerkmale anlagenübergreifend verfügbar sind und welche Daten verarbeitet werden (z.B. Übermittlung der Rufnummer des anrufenden Teilnehmers).

3.5.2.2 Korporative Anlage

Alle Dienststellen einer Behörde sollen unter einer Rufnummer erreicht werden können. Bisher sind Dienststellen von Behörden, die räumlich getrennt untergebracht sind, unter Umständen an verschiedene Fernsprechzentralen angeschlossen und daher nur über verschiedene Rufnummern zu erreichen.

3.5.2.3 Endgeräte

Es sollen verschiedene Fernsprechapparate (analoge sowie digitale) und multifunktionale Endgeräte (z.B. für Mischkommunikation) erprobt werden.

3.5.2.4 TK-Management

— Fernrevision (Fernverwaltung, Fernwartung, Endstörungshandling, Softwarepflege, System-Update)

— und Fernadministration (Anpassung der TK-Anlage an den Bedarf im Hinblick auf Leistungsmerkmale, Rufnummern und Berechtigungen)

durch die Zentrale Servicestelle sollen eine schnellere Anpassung der TK-Anlagen an den Bedarf, verbesserte Verwaltung der Netzunterlagen, schnellere Entstörung und damit geringere Ausfallzeiten und schließlich Revisionssicherheit ermöglichen.

Beim TK-Management halten wir eine Dokumentation über die erteilten Berechtigungen sowie eine revisionssichere Aufzeichnung der jeweiligen Aktivitäten zur Fernrevision und Fernadministration für erforderlich.

Im Rahmen dieser KGM soll auch ein Verbund der Elektronischen Telefonbücher (ETB) verschiedener TK-Anlagen erprobt werden. Zur Zeit sind einige Behörden dabei, elektronische Telefonbücher jeweils für ihren Bereich aufzubauen. Mit einem Verbund wird eine qualitative Verbesserung der Behördennetz-Auskunft bei der Baubehörde angestrebt.

3.5.2.5 Kommunikationskosten

Die ISDN-Technik ermöglicht eine differenzierte Erfassung der bei der Telekommunikation anfallenden Nutzungsgebühren. So ist es z.B. möglich, die entstehenden Gebühren so zu erfassen, daß sie einzelnen Kostenstellen zugeordnet werden können. Dabei können als Kostenstellen definiert werden

— Behörden,

— Ämter der betreffenden Behörden,

— Hauptabteilungen,

— Abteilungen,

— einzelne Anschlüsse.

Die jeweils definierten Kostenstellen könnten mit den tatsächlich von ihnen verursachten Gebühren belastet werden. Die Gebühren könnten in einer Summe oder als Auflistung aller Einzelgebühren dargestellt werden, wobei es möglich wäre, für bestimmte Kostenstellen die Einzelpositionen aufzulisten und für andere Kostenstellen nur Gesamtsummen anzugeben.

Es könnten Berechtigungen — z. B. zur Wahl von Ferngesprächen national, kontinental, interkontinental — differenziert und im erforderlichen Umfang freigegeben werden.

Dienstlich veranlaßte Gespräche und Privatgespräche könnten anhand einer Kennziffer unterschieden und getrennt abgerechnet werden.

Hinsichtlich der Kommunikationskosten halten wir eine Speicherung der kompletten Verbindungsdatensätze (einschließlich vollständiger Zielnummern) für nicht erforderlich. Mit der Zielnummerspeicherung wird in das informationelle Selbstbestimmungsrecht beider Kommunikationspartner eingegriffen. Zulässig ist aus unserer Sicht allenfalls die Speicherung verkürzter Zielnummern. Im übrigen sollten die aufgelaufenen Gebühreneinheiten in einer Summe gespeichert werden.

3.5.2.6 Wählverbindungen und Festverbindungen

Ziel ist der Test von Wählverbindungen und Festverbindungen im Behördennetz. Wählverbindungen sind gewählte Verbindungen (analog oder digital) zwischen beliebigen Endstellen (angeschaltet an Wähl- oder Universalanschlüssen). Festverbindungen können in drei Varianten geschaltet werden: als analoge, permanente Festverbindungen (Gruppe 1), als digitale, permanente Verbindung (Gruppe 2) oder als digitale, semipermanente Verbindung (Gruppe 3). Festverbindungen der Gruppe 1 kommen nicht zur Anwendung.

Zu dem Versuch mit Wählverbindungen und Festverbindungen haben wir auf Datensicherungsaspekte hingewiesen: Sofern auch Datenverarbeitungsanlagen über Wählverbindungen erreichbar sein sollen, muß das Sicherheitssystem dieser Anlagen gewährleisten, daß unberechtigter Zugang zuverlässig unterbunden wird und daß abgewiesene Zugangsversuche protokolliert werden. Ferner muß sichergestellt werden, daß nur autorisierte Benutzer ausschließlich auf diejenigen Datenbestände zugreifen können, für die sie berechtigt sind.

3.5.2.7 Non-Voice-Services

Der Datentransfer zwischen an das Behördennetz angeschlossenen Datenendeinrichtungen und einer externen Datenbank (z. B. „JURIS") soll erprobt und Möglichkeiten der elektronischen Post im hamburgischen Behörden-Telekommunikationsnetz sollen ausgelotet werden.

Es muß geklärt werden, ob und welche personenbezogenen Daten verarbeitet werden sollen. Die Erprobung der „elektronischen Post" sollte sich wegen der damit verbundenen Datensicherungsprobleme zunächst auf den an eine TK-Anlage angeschlossenen Teilnehmerkreis beschränken. Die Datex-P-Nutzung sollte aus den gleichen Erwägungen zunächst auf solche Anwendungen beschränkt werden, in denen keine personenbezogenen oder sonst besonders zu schützenden Daten verarbeitet werden. Es wäre dabei sicherzustellen, daß in das Behördennetz eingebundene PAD-Einrichtungen nur von autorisierten Benutzern aus dem Behördennetz benutzt werden können.

3.5.2.8 Kommunikation mit einem LAN (Inhouse-Netz, Lokal Area Network)

Im Rahmen dieser Anwendung soll von einer Datenendeinrichtung aus über das Telekommunikationsnetz der hamburgischen Verwaltung eine Verbindung zu einem Rechner aufgebaut werden, der an ein lokales Netz angeschlossen ist. So soll z. B. von

einem Terminal in der Baubehörde aus das Bibliothekssystem der Technischen Universität Hamburg-Harburg mitbenutzt werden können.

Dazu haben wir angemerkt, daß unberechtigter Zugang zum LAN über eine Wählverbindung zuverlässig ausgeschlossen werden muß. Das setzt voraus, daß ein Zugang über Wählverbindung nur eröffnet wird, wenn zuvor festgelegt worden ist, wer Zugang haben soll, und wenn technisch sichergestellt ist, daß andere keinen Zugang erhalten. Denkbar ist eine Lösung in der Weise, daß eine Verbindung zum LAN nur von bestimmten Anschlüssen (Telefonanschluß — definiert durch die Telefonnummer des anrufenden Partners) aus zugelassen wird. Dies wäre ein Anwendungsbeispiel für eine geschlossene Benutzergruppe.

Eine andere Lösung wäre es, den Zugang zu Komponenten des LAN von einem Paßwort abhängig zu machen. Diese Sicherung des Zugangs zum LAN ist jedoch nur durch eine Softwarekomponente des LAN zu realisieren, die TK-Anlage leistet dieses nicht.

3.5.2.9 Geschlossene Benutzergruppe

Es soll ausprobiert werden, durch Definition einer geschlossenen Benutzergruppe nur bestimmten Benutzern eine Anwendung zugänglich zu machen und alle anderen Benutzer von dieser Anwendung auszuschließen.

3.5.3 Übertragung vertraulicher Dokumente mittels Telefax

Telefax ist ein von der Deutschen Bundespost — Telekom — angebotener Dienst zur Übertragung von Textkopien (Faksimiles) über das Telefonnetz. Über nichtöffentliche Netze (z.B. das Hamburgische Behördentelefonnetz) können Fernkopien ebenfalls versandt werden, sofern die entsprechenden Endgeräte installiert sind.

Auch der Telefax-Verkehr unterliegt dem Schutz des Fernmeldegeheimnisses (Art. 10 GG und § 10 Fernmeldeanlagengesetz), seine Realisierung bereitet in der Praxis jedoch erhebliche Probleme. Anders als das Telefon befindet sich das Telefax-Gerät in der Regel nicht direkt am Arbeitsplatz der Kommunikationspartner, sondern in zentralen, häufig allgemein zugänglichen Räumlichkeiten innerhalb einer Dienststelle (z.B. Kopiererraum). Die Datenübertragung erfolgt bei Telefax immer offen, d.h. sowohl am Sende- als auch beim Empfangsgerät sind die übertragenen Seiten offen einsehbar. Es ist vom Absender nicht zu steuern, welche Personen bei der empfangenden Stelle Kenntnis von der Fernkopie erhalten. Die Vertraulichkeit der Informationen ist deshalb — ohne zusätzliche organisatorische Sicherheitsmaßnahmen — nicht gegeben.

Auch die Geheimhaltung der Tatsache einer Telefax-Kommunikation ist im Regelfall nicht gewährleistet, da sämtliche Übertragungsvorgänge mit den beiderseitigen Anschlußkennungen in Journalen des Sendegeräts und des Empfängers aufgezeichnet und damit die Kommunikation nachvollzogen werden kann. Allerdings ist in diesem Zusammenhang darauf hinzuweisen, daß aufgrund der noch geringen „Telefaxdichte" eine personenbezogene Zuordnung der Anschlußnummern nicht ohne weiteres möglich sondern meist nur nachzuvollziehen ist, welche Institutionen miteinander Verbindung hatten.

Ein weiterer Unsicherheitsfaktor ist in der durch Eingabefehler oder durch Fehler beim Vermittlungsvorgang verursachten Fehlleitung von Fernkopien zu sehen. Während beim Telefonat von den Betroffenen sofort erkannt wird, daß man nicht mit dem gewünschten Partner verbunden ist, ist beim Telefax-Verkehr der Fehler erst beim Auswerten der Übermittlungsprotokolle oder durch eine Meldung des Empfängers ersichtlich.

Selbst die Identifikation des Absenders ist mit Unsicherheiten verbunden, denn die Kennung des Absenders wird nicht — wie etwa bei ISDN — vom Fernmeldenetz an den Empfänger gesendet. Vielmehr handelt es sich um eine Meldung des Sendegerätes, die an das Empfangsgerät übertragen und dort aufgezeichnet wird. Durch einfache Manipulation am Sendegerät kann die Absenderkennung verändert werden.

Aus diesen Gründen ist die Übertragung vertraulicher Dokumente — hierzu gehören auch Dokumente mit personenbezogenen Daten — per Telefax problematisch. Sofern solche Dokumente gleichwohl übertragen werden sollen, gehört zu den erforderlichen Datensicherungsmaßnahmen stets die telefonische Anmeldung der Sendung beim Empfänger, damit dieser den Eingang der Fernkopien persönlich überwachen und die übertragenen Dokumente selbst aus dem Gerät entnehmen kann.

4. Einzelne Probleme des Datenschutzes im öffentlichen Bereich

4.1 Sozialwesen

4.1.1 Projekt Sozialhilfe-Automation (PROSA)

Wir haben in den letzten beiden Tätigkeitsberichten (7. TB, 4.1.6, S. 36 und 8. TB, 3.1.2, S. 26) über das Vorhaben berichtet. Danach ist geplant, die Arbeitsabläufe in den Sozialdienststellen der Bezirke durch umfassende Technik-Unterstützung zu reorganisieren. In dem im Dezember 1986 vom Senat beschlossenen IuK-Gesamtplan 1987—1989 wurde dieses Projekt bereits als dringlich und unabweisbar ausgewiesen. Ziel des Projektes ist es, eine umfassende Arbeitsunterstützung für rund 1000 Sozialhilfe-Sachbearbeiter/innen zu schaffen. Dies soll durch Dialogisierung des operativen Verfahrens „Sozialhilfe" und durch Einführung von IuK-Technik zur Bürounterstützung und -kommunikation erreicht werden.

Weiteres Ziel ist daneben, die Transparenz der mit der Sozialhilfe verbundenen sozialpolitischen und finanziellen Aspekte inhaltlich zu verbessern und zeitnäher zu gewährleisten. Darüber hinaus mißt der Senat diesem Projekt grundsätzliche Bedeutung im Rahmen seiner auf Modernisierung der Verwaltung durch umfassende und konsequente Nutzung von IuK-Technik gerichteten Organisationspolitik bei (vgl. 3. TB, 3.1). So sollen im Rahmen von PROSA Standards zur Schaffung einer ausbaubaren, zukunftssicheren Infrastruktur für die Informationsverarbeitung im Bürobereich der gesamten Verwaltung gewonnen werden. Deshalb sollen alle in diesem Bereich vorhandenen Bürofunktionen (wie z. B. Textverarbeitung, Aktenhaltung, Dokumentation, Terminverwaltung, Bürokommunikation) technisch unterstützt werden. Daß durch die automatisierte Verarbeitung sensibler Sozialdaten Gefahren für das informationelle Selbstbestimmungsrecht der Hilfeempfänger/innen entstehen, ist offensichtlich. Deshalb kommt dem Datenschutzkonzept für PROSA besondere Bedeutung zu.

Den ersten Entwurf eines (allerdings noch unvollständigen) Datenschutzkonzeptes haben wir im Mai dieses Jahres erhalten. Er wird seither laufend überarbeitet. Schwerpunkte unserer Beratungstätigkeit liegen bei der technischen Datensicherung, bei der geplanten Verarbeitung von Daten zu Zwecken der Statistik/Sozialplanung sowie bei der Verarbeitung von medizinischen Daten.

4.1.1.1 Verbesserung der technischen Datensicherung — PROSA-Zugriffssicherung

Die Verarbeitung sensibler Sozialdaten stellt hohe Anforderungen an die Datensicherheit. Es muß u. a. gewährleistet sein, daß die Sachbearbeiter über ein nur ihnen bekanntes Paßwort lediglich auf die Daten der Hilfeempfänger zugreifen können, für die sie zuständig sind. Die ersten Entwürfe des Datenschutzkonzeptes sahen zunächst eine Zugriffssicherung auf zwei Eingabe-Ebenen vor: Einerseits eine zentral von der Datenverarbeitungszentrale verwaltete Paßwort-Abfrage auf Betriebssystemebene

durch das Produkt TSS (Top Secret System), andererseits eine dezentral in den Sozialhilfeabteilungen administrierbare Paßwort-Abfrage, die integraler Bestandteil der PROSA-Anwendungssoftware ist.

Der damit suggerierte doppelte Schutz verkehrt sich in der Praxis allerdings in eine unsichere Lösung, weil eine zentrale Verwaltung vergessener Paßwörter von etwa 1000 Anwendern faktisch nicht zu realisieren ist. Paßwörter werden häufig vergessen, so daß es zu erheblichen Verzögerungen im Verwaltungsvollzug käme. Aus diesem Grund würden die meisten Sachbearbeiter ihr TSS-Paßwort auf beiden Ebenen benutzen und damit den TSS-Schutz weitgehend zunichte machen. Damit würde die eigentliche Zugriffssicherung auf der dezentral verwalteten Anwendungsebene stattfinden. Im Gegensatz zur TSS-Ebene, auf die lediglich Systemprogrammierer der DVZ Zugriff haben, ist die Anwendungsebene allerdings gegen unerlaubten Datenzugriff wesentlich weniger geschützt, da beispielsweise Paßwörter unverschlüsselt in nicht besonders gesicherten Dateien gespeichert werden, die z.B. von PROSA-Anwendungsprogrammierern gelesen werden können.

Um eine sichere und gleichermaßen dezentrale Zugriffssicherung zu realisieren, haben wir vorgeschlagen, die bisher auch in anderen Verfahren der hamburgischen Verwaltung existierende Praxis einer zentralen TSS-Verwaltung aufzugeben und eine Dezentralisierung der TSS-Paßwort-Vergabe zu ermöglichen. Der Vorschlag wurde von der Projektgruppe aufgegriffen und wird inzwischen in Zusammenarbeit mit der DVZ realisiert.

4.1.1.2 Verarbeitung zu Zwecken der Statistik und Sozialplanung

Die Behörde für Arbeit, Gesundheit und Soziales (BAGS) hat beklagt, es stünden fachlich und politisch benötigte statistische Sozialhilfedaten in quantitativer und qualitativer Hinsicht nicht in ausreichendem Maße zur Verfügung. Ein Ziel des Projekts ist es deshalb, „einen nach einheitlichen Regeln aufgebauten Datenbestand zu schaffen, der allen Ansprüchen hinsichtlich der Aktualität genügt und eine für alle beteiligten Behörden gleichermaßen geltende Planungs- und Informationsgrundlage darstellt".

Die Notwendigkeit eines solchen Informationssystems wird aus den Zielvorgaben des Bundessozialhilfegesetzes hergeleitet: Vermeidung von Hilfebedürftigkeit, Hilfeleistung zur Beseitigung bestehender Notlagen, Hilfeleistung zur Stärkung der Selbsthilfe. Aus diesen Zielvorgaben kann jedoch nicht die Befugnis zur Erhebung von Daten zu statistischen Zwecken abgeleitet werden, die über das „Gesetz über die Durchführung von Statistiken auf dem Gebiet der Sozialhilfe, der Kriegsopferfürsorge und der Jugendhilfe" hinausgehen. Für Statistiken nach diesem Gesetz sind jedoch die Daten ausreichend, die für die Fallbearbeitung ohnehin vorhanden sind.

Die BAGS hat nach unserem Eindruck inzwischen im wesentlichen akzeptiert, daß Datenerhebungen ausschließlich für statistische/planerische/politische Zwecke wegen fehlender Rechtsgrundlagen für die Erreichung der oben genannten Ziele nicht zulässig sind. Ausgewertet werden dürfen nur solche Daten, die befugt für die Gewährung von Sozialhilfeleistungen erhoben werden. Der Begriff der „Leistung" wird allerdings unserer Meinung nach von der BAGS unzulässig weit ausgelegt. Leistungserheblich sollen nach ihrer Interpretation alle Daten sein, die dem Sachbearbeiter ermöglichen, einen effektiven und zielorientierten Hilfeprozeß — Stichwort „Hilfe zur Selbsthilfe" — einzuleiten und zu unterstützen. Darunter fallen dann auch Informationen zu den Ursachen der Hilfebedürftigkeit, zur schulischen und beruflichen Ausbildung und zu den Gründen, die zum Ausscheiden aus der Sozialhilfe geführt haben.

Unserer Meinung nach muß die auswertbare Speicherung von Daten der Hilfeempfänger enger an spezifische Leistungen geknüpft werden: Gründe für die Beendigung der Sozialhilfe braucht der Hilfeempfänger deshalb nicht anzugeben. Die Schulausbildung sowie berufliche Qualifikationen und Tätigkeiten können im Einzelfall leistungsrelevant sein, dürfen aber nicht generell abgefragt und gespeichert werden. Einzelne Ursachen für Sozialhilfebedürftigkeit können für die Beratung und die Begründung des

Anspruchs von Bedeutung sein, sollten aber nur in groben Kategorien erfaßt werden. Im übrigen lassen sich viele Informationen zur Ursache aus der konkreten Leistung ableiten.

Soweit Daten, die zur Leistungserbringung erhoben wurden, zu statistischen und planerischen Zwecken ausgewertet werden (Sekundärstatistik), ist wegen der damit verbundenen Zweckänderung sicherzustellen, daß der Personenbezug gelöscht und die Daten so aggregiert werden, daß eine Beeinträchtigung schutzwürdiger Belange der Betroffenen ausgeschlossen ist. Auf die Dauer der Speicherung von Daten darf es keinen Einfluß haben, daß sie möglicherweise für statistische Zwecke genutzt werden sollen. Eine Beurteilung, ob diesen datenschutzrechtlichen Vorgaben hinreichend Rechnung getragen wird, wird erst möglich sein, wenn ein detailliertes Auswertungskonzept vorliegt.

4.1.1.3 Verarbeitung medizinischer Daten

Sozialhilfe umfaßt auch Hilfe für die Überwindung von Notlagen, die im Zusammenhang mit Krankheit oder Behinderung stehen. Für die Gewährung von Leistungen kann es deshalb in unterschiedlichem Umfang erforderlich sein, Gesundheitsdaten der Hilfeempfänger/innen zu verarbeiten. Daten, die der Sozialleistungsträger von einem Arzt oder einer anderen in § 203 Absatz 1, 3 StGB genannten Person erhalten hat, die also einem besonderen, strafbewehrten Berufsgeheimnis wie der ärztlichen Schweigepflicht unterliegen, sind als besonders schutzwürdig anzusehen und werden vom SGB X besonderen Offenbarungsvoraussetzungen unterworfen (§ 76 SGB X). Aber auch Informationen, die der Hilfesuchende zur Begründung von gesundheitlich bedingten Mehrbedarfen den Sozialdienststellen offenbart, enthalten sehr sensible medizinische Daten. Die besondere Schutzwürdigkeit ist in jeder Phase der Datenverarbeitung zu beachten. Zur Sicherstellung des Datenschutzes haben wir mit der BAGS und der Projektgruppe vereinbart, daß die medizinischen Daten, die im Rahmen der vorbeugenden Gesundheitshilfe und der Krankenhilfe anfallen, sinngemäß nach den datenschutzrechtlichen Vorschriften des Rechts der gesetzlichen Krankenversicherung (SGB V) behandelt werden, da die Sozialhilfe insoweit die Funktion der Krankenversicherung für den Hilfeempfänger hat. Das gilt insbesondere für die Zweckbindung der Erhebung und Speicherung sowie für Löschungsfristen.

Für gesundheitlich begründete Mehrbedarfe wird angestrebt, über die Fachlichen Weisungen Fallgruppen zu bilden, in denen mehrere Erkrankungen zusammengefaßt sind, so daß möglichst kein Rückschluß auf Einzeldiagnosen des Bedürftigen gezogen werden kann. Dadurch könnte gleichzeitig das Problem der Offenbarung von Diagnosen durch das begutachtende Gesundheitsamt gelöst werden: Der Gutachter würde als Ergebnis nur die Zuordnung zu einer Mehrbedarfsklasse vorschlagen.

Eine automatisierte Speicherung von Einzelfalldiagnosen und ihr Ausdruck in Bewilligungsbescheiden soll nicht stattfinden. Statt dessen wird auch hier jeweils nur die Mehrbedarfsklasse gespeichert, die auf den Bewilligungsbescheiden aus Gründen der Transparenz für die Hilfeempfänger/innen durch eine Zusatzinformation erläutert wird. Auch wenn eine kurzfristige Umstellung der Mehrbedarfsregelungen nicht möglich ist, soll das Datenverarbeitungskonzept die Gruppenbildung schon jetzt vorsehen. Ähnliche Probleme wie bei den Gesundheitsdaten traten auch bei den Eingliederungshilfen für Behinderte auf, die aber durch Zusammenfassung von Leistungsarten weitgehend ausgeräumt sind.

Wir möchten in diesem Zusammenhang hervorheben, daß die bisherige Zusammenarbeit mit der Projektgruppe als vorbildlich bezeichnet werden kann. Wir haben deshalb Anlaß zu der Erwartung, daß es bei der allseits — auch bei der BAGS — vorhandenen Kooperationsbereitschaft gelingen kann, die Interessen der Verwaltung und die schutzwürdigen Belange der betroffenen Hilfeempfänger/innen zu einem angemessenen Ausgleich zu bringen.

4.1.2 Richtlinien zum Bewilligungsverfahren bei medikamentengestützten Drogentherapien

Im letzten Tätigkeitsbericht (8. TB, 3.1.3, S. 27) hatten wir über das Verfahren der BAGS bei der Abrechnung von Leistungen für psychosoziale Betreuung Drogenabhängiger berichtet. Die „Richtlinie zum Bewilligungsverfahren bei medikamentengestützten Drogentherapien" (sog. Methadon-Substitution) sah vor, daß das Landessozialamt die von den psychosozialen Beratungsstellen eingereichten Rechnungen bezahlt und sie danach zu den einzelnen Sozialamtsakten weiterreicht, damit (erst) dort die sachliche und rechnerische Richtigkeit geprüft wird. Die Abrechnungen sollten in der Akte verbleiben.

Wir waren mit der BAGS seinerzeit darüber einig, daß bei diesem Verfahren nicht ausgeschlossen werden kann, daß Unbefugte Zugriff auf die Daten nehmen. Wir begrüßen es deshalb, daß die BAGS zwischenzeitlich unseren Vorschlag aufgegriffen hat, das gesamte Bewilligungsverfahren in der BAGS abzuwickeln. Die entsprechende Richtlinie lautet jetzt:

„Die anerkannten Träger der psychosozialen Begleitung rechnen ihre Leistungen unter Vorlage der ärztlichen Verordnung direkt mit dem Landessozialamt ab. Eine Weiterleitung von abgerechneten ärztlichen Verordnungen an die Sozialdienststellen der Bezirke erfolgt in keinem Falle. Die Bewilligung im Einzelfall erfolgt zentral durch die Fachbehörde."

Diese Verfahrensweise gilt nur im Rahmen von psychosozialer Betreuung bei medikamentengestützten Drogentherapien. Die Problematik der Verarbeitung sensibler Gesundheitsdaten bei den Sozialämtern soll im Rahmen des Projekts „Automation der Sozialhilfe" (PROSA) (vgl. 4.1.2) gelöst werden.

4.1.3 Offenbarung von Sozialdaten nach dem Tod von Hilfeempfängern

Von Sozialamtsmitarbeitern und von Angehörigen verstorbener Hilfeempfänger/innen wird häufig die Frage an uns gerichtet, ob und gegebenenfalls in welchem Umfang Auskunft über verstorbene Hilfeempfänger/innen gegeben werden darf. Ungeklärt ist, ob die Offenbarungsvorschriften nach dem SGB X auch nach dem Tod des Betroffenen relevant sind und wer gegebenenfalls für den Verstorbenen in eine Offenbarung einwilligen darf. In der Literatur wird zum Teil die Auffassung vertreten, diese Befugnis entfalle (als höchstpersönliche Befugnis) mit dem Tod des Betroffenen, könne also von Rechtsnachfolgern oder Angehörigen nicht ausgeübt werden. Die Konsequenz bleibt unklar: Soll damit der Schutz des Sozialgeheimnisses völlig wegfallen oder — im Gegenteil — der Schutz dadurch verstärkt werden, daß Offenbarungen nur auf die gesetzlichen Befugnisse der §§ 68-77 SGB X gestützt werden können?

Nach einer anderen Auffassung soll den Angehörigen oder Rechtsnachfolgern insoweit eine Einwilligungsbefugnis zustehen, als sie in dieser Eigenschaft ein berechtigtes Interesse an der Offenbarung haben. Dagegen ist einzuwenden, daß eigene Interessen mit dem Instrument der Einwilligung ohne Rücksicht auf den Verstorbenen durchgesetzt werden könnten.

Das Bundessozialgericht hat die postmortale Geltung des Sozialgeheimnisses grundsätzlich anerkannt (aber die Frage offengelassen, wem unter welchen Voraussetzungen die Einwilligungsbefugnis für den Verstorbenen zusteht). Für diese Auffassung spricht, daß auch das strafbewehrte Verbot für Ärzte und andere Berufs- und Personengruppen, Privatgeheimnisse unbefugt zu offenbaren, nach dem Tode des Betroffenen weiterbesteht (§ 203 Abs. 4 StGB).

Da diese Problematik bereits mehrfach an uns herangetragen wurde, werden wir Gespräche mit der BAGS mit dem Ziel aufnehmen, eine praxisgerechte und datenschutzkonforme Lösung zu finden. Es ist aber nicht auszuschließen, daß das Ergebnis sein kann, daß eine Gesetzeslücke besteht, die nur vom Gesetzgeber geschlossen werden kann.

4.1.4 Amtspflegschaft und Amtsvormundschaft bei nichtehelichen Kindern

Im 6. (6. TB, 4.1.2, S. 32 f.) und 7. Tätigkeitsbericht (7. TB, 4.1.4, S. 35) hatten wir das an Hamburger Jugendämtern von Amtspflegern und -vormündern praktizierte Verfahren bei der Beschaffung von Informationen über das Einkommen von Vätern nichtehelicher Kinder kritisiert.

Die (ehemalige) Behörde für Arbeit, Jugend und Soziales — inzwischen ist das Amt für Jugend Teil der Behörde für Schule, Jugend und Berufsbildung (BSJB) — war seinerzeit nicht bereit, zur Feststellung des Arbeitseinkommens von unterhaltspflichtigen Vätern auf Anfragen bei Arbeitgebern zu verzichten, obwohl es nach unserer Auffassung (die von der BAJS nicht geteilt wurde) für die mit dieser Anfrage verbundene Datenübermittlung keine Rechtsgrundlage gab.

Das Gesetz zur Neuordnung des Kinder- und Jugendhilferechts (Kinder- und Jugendhilfegesetz) vom 26. Juni 1990, das zum 1. Januar 1991 in Kraft tritt, klärt diese Frage. Nach § 68 dürfen Amtspfleger und Amtsvormünder im Rahmen ihrer Tätigkeit personenbezogene Daten erheben und verwenden, soweit dies zur Erfüllung der jeweiligen Aufgabe erforderlich ist.

Unstreitig ist die Geltendmachung von Unterhaltsansprüchen gemäß § 1706 BGB Aufgabe des Amtspflegers oder — wenn die Mutter des Kindes noch minderjährig ist — des Amtsvormundes. Um einen Unterhaltsanspruch in angemessener Höhe geltend machen zu können, ist es notwendig, das Einkommen des Unterhaltspflichtigen zu kennen, da dessen Lebensstellung gemäß § 1615 c BGB bei der Bemessung des Unterhalts zu berücksichtigen ist. Sofern der Unterhaltsverpflichtete seiner Auskunftspflicht gemäß § 1605 BGB i. V. m. § 1615 a BGB nicht nachkommt, ist das bisher schon praktizierte Verfahren, den Arbeitgeber um Übermittlung der Einkommensdaten zu bitten, ab 1991 auch rechtlich zulässig.

Da die Rechtsordnung aber keine Auskunftspflicht des Arbeitgebers normiert, muß der Arbeitgeber auf die Freiwilligkeit der Auskunft hingewiesen werden (§ 9 Abs. 2 Bundesdatenschutzgesetz). Darüber besteht mit der BSJB Einigkeit.

4.2 Personalwesen

4.2.1 Beihilfesachbearbeitung in Heimarbeit

Im Mai des Berichtsjahres erhielten wir von dritter Seite davon Kenntnis, daß die Besoldungs- und Versorgungsstelle (BVSt) beabsichtigte, Beihilfeanträge an Wochenenden von den Beihilfesachbearbeitern in Heimarbeit bearbeiten zu lassen, um erhebliche Rückstände abzubauen. In den uns übersandten Unterlagen fand sich der Hinweis, daß dieses Verfahren in der Behörde für Schule, Jugend und Berufsbildung (BSJB), in der ebenfalls Rückstände bei der Beihilfesachbearbeitung vorhanden waren, schon seit April dieses Jahres praktiziert wurde.

In der Besoldungs- und Versorgungsstelle mußte die Heimarbeit eingestellt werden, weil der Personalrat einer Verlängerung dieser Bearbeitungspraxis über den Monat Juni 1990 hinaus nicht mehr zustimmte.

In der BSJB dagegen wurde die Praxis fortgesetzt, obwohl wir diese mehrfach gerügt und im weiteren eine formelle Beanstandung gegenüber dem Senat angekündigt haben. Zur Erläuterung wies die BSJB darauf hin, daß es nicht gelungen sei, die erheblichen Rückstände in der Beihilfesachbearbeitung durch andere Maßnahmen zu beseitigen. Zur Gewährleistung des Datenschutzes seien sämtliche Mitarbeiterinnen und Mitarbeiter noch einmal ausdrücklich darauf hingewiesen worden, bei der Heimarbeit besonders die Vertraulichkeit der Vorgänge zu beachten und Vorkehrungen zu treffen, daß keine Unbefugten, insbesondere auch keine Familienmitglieder, Einsicht in die Beihilfeunterlagen erhielten. Zur Sicherung auf dem Transport würden die Mitarbeiter die von der BVSt zur Verfügung gestellten Aktenkoffer mit Zahlenschlössern benutzen, die auch im Hause einen zusätzlichen Schutz gegen fremde Einsicht in die Akten

böten. Es sei auch darauf hinzuweisen, daß Heimarbeit im öffentlichen Dienst nichts Ungewöhnliches sei. Sowohl Lehrer als auch Richter erfüllten ihre dienstlichen Obliegenheiten nur teilweise in den Dienststellen.

Da diese Praxis nach unserer Auffassung mehrfach gegen Bestimmungen des Hamburgischen Datenschutzgesetzes verstößt, mußten wir sie formell gegenüber dem Senat beanstanden.

Die in den Beihilfeanträgen und den jeweils beigefügten Belegen enthaltenen Daten gehören zu den sensibelsten Daten, die die Bediensteten über sich und/oder ihre Familienangehörigen überhaupt im Rahmen ihres Beschäftigungsverhältnisses offenbaren. Arzt- und Krankenhausrechnungen sowie Arzneimittelverordnungen lassen entweder direkt durch Angabe der Diagnose und der Therapiemaßnahmen oder indirekt Rückschlüsse auf den konkreten Gesundheitszustand der Bediensteten und deren Angehörigen zu. Damit ist der intimste Kernbereich der personenbezogenen Information berührt. Daten aus Beihilfeanträgen erfordern deshalb einen besonders hohen Standard der Datensicherheit. Hieran fehlt es bei einer Beihilfesachbearbeitung in Heimarbeit: Die Anträge und Unterlagen werden zunächst aus dem der Öffentlichkeit nicht zugänglichen Bereich der besonders geschützten Diensträume herausgebracht. Ein abschließbarer Koffer hindert zwar ungewolltes Öffnen oder Zugreifen von Dritten, er kann jedoch verloren gehen, bei einem Wegeunfall beschädigt und/oder durch unbefugte Dritte „sichergestellt", auch gestohlen werden. Besonders gefährdet sind die Beihilfedaten jedoch während der Sachbearbeitung zu Hause. Es kann unterstellt werden, daß die wenigsten Sachbearbeiter ein eigenes Arbeitszimmer haben oder auch nur einen eigenen Schreibtisch in der Wohnung, so daß weder die Einsichtnahme durch Unbefugte noch die Beschädigung der Unterlagen hinreichend sicher ausgeschlossen werden können.

Erschwerend kommt hinzu, daß die Dienststelle während des Wochenendes keinerlei Kontrolle über die datenschutzrechtlich besonders sensible Tätigkeit ihrer Mitarbeiter ausüben kann; dies gilt in gleicher Weise für die gesetzlich vorgesehene Kontrolle durch den Hamburgischen Datenschutzbeauftragten.

In dieser objektiven Gefährdung sehr sensibler Daten bei gleichzeitigem Ausschluß einer wirksamen Aufsicht liegt ein schwerer „Mangel bei der Verarbeitung personenbezogener Daten" im Sinne von § 21 Absatz 1 Seite 1 a. F. HmbDSG.

Den Hinweis auf die Heimarbeit von Lehrern und Richtern halten wir nicht für gerechtfertigt. Die zu bearbeitenden Schülerunterlagen sind in der Regel von erheblich geringerer Sensibilität. Die Möglichkeiten der Richter zur Heimarbeit werden unmittelbar aus der ebenfalls verfassungsrechtlich geschützten richterlichen Unabhängigkeit abgeleitet, die ihrerseits auch keine datenschutzrechtliche Kontrolle zuläßt. Im übrigen haben sehr viele Angehörige dieser Berufsgruppen — steuerlich geförderte — private Arbeitszimmer.

Um aber die Belange der Betroffenen und die Interessenlage der BSJB zu einem angemessenen Ausgleich zu bringen, haben wir zugleich mit der Beanstandung vorgeschlagen, die Beihilfeanträge solcher Antragsteller in Heimarbeit bearbeiten zu lassen, die dieser Bearbeitung ausdrücklich schriftlich zugestimmt haben. Es erschien uns denkbar, daß Antragsteller zugunsten einer schnelleren Antragsbearbeitung die durch Heimarbeit entstehenden Risiken für ihre persönlichen Daten bewußt in Kauf nahmen.

Der Senat hat die Beanstandung im Ergebnis nicht akzeptiert. Er ist der Auffassung, daß Heimarbeit in dieser Sondersituation zulässig ist und hält die getroffenen Maßnahmen zur Datensicherung für ausreichend. Im übrigen hätten sich die Mitarbeiter/innen damit einverstanden erklärt, eine Datenschutzkontrolle in ihrer Wohnung zuzulassen. Eine Einwilligung der Betroffenen wolle der Senat nicht einholen. Die Verwaltung sollte sich nach seiner Auffassung „nicht ohne zwingenden Anlaß von den Antragstellern vorschreiben lassen müssen, in welcher Art und Weise sie ihre Aufgaben (korrekt) erfüllt."

Obwohl wir diese Auffassung des Senats weiterhin nicht teilen, sind die gesetzlichen Möglichkeiten des Hamburgischen Datenschutzbeauftragten zur Klärung der grundsätzlichen Rechtmäßigkeit dieses Verfahrens erschöpft. Allerdings hat uns der mehrfache Hinweis des Senats, die Mitarbeiter der Beihilfestelle hätten sich über unsere Bedenken deutlich betroffen geäußert, Veranlassung zur Ausräumung eines offensichtlichen Mißverständnisses gegeben.

Die Bemühungen des Hamburgischen Datenschutzbeauftragten um effektiven Datenschutz beruhen auf einem gesetzlichen Auftrag und nicht auf persönlichem Mißtrauen gegenüber Bediensteten oder der Unterstellung drohender Dienstpflichtverletzungen. Wir hatten und haben keinerlei Anlaß zu Zweifeln an der Integrität der Mitarbeiter der BSJB — niemand ist uns persönlich bekannt. Das Vertrauen auf die gewissenhafte Erfüllung der Dienstpflichten durch die Bediensteten vermag weder die datenverarbeitende Stelle noch den Hamburgischen Datenschutzbeauftragten von ihrem jeweiligen Gesetzesauftrag zu befreien.

Ob dies in der BSJB hinreichend bewußt ist, muß weiterhin zweifelhaft erscheinen. So mußten wir noch im September bei einer Kontrolle des Verfahrens in der Beihilfestelle feststellen, daß nicht einmal eine Übersicht darüber hergestellt werden kann oder kontrolliert wird, welche/r Sachbearbeiter/in an welchem Wochenende welche Akten mit nach Hause nimmt. Lediglich zur Abrechnung der Überstunden wird am Montag die Anzahl der zurückgebrachten Akten gezählt. Der denkbare Verlust einer bestimmten Beihilfeakte wird so möglicherweise erst durch eine Nachfrage der antragstellenden Person entdeckt. Dies kann selbstverständlich nicht als ordnungsgemäßes Verfahren angesehen werden. Wir haben deshalb die BSJB aufgefordert, vor der Bearbeitung zu Hause schriftlich festzuhalten, welche/r Sachbearbeiter/in wann welche Beihilfeakte mitnimmt, und die Rückgabe zu kontrollieren. Die Besoldungs- und Versorgungsstelle, die nach dem Senatsbeschluß und mit Zustimmung des Personalrats die Heimarbeit in modifizierter Form und auf 8 Wochen befristet wieder zugelassen hat, schreibt die geforderte Kontrolle bereits vor. Gleichwohl hat die BSJB selbst die einfache Vorsichtsmaßnahme unter Hinweis auf das nahe Ende der Heimarbeit abgelehnt.

4.2.2 Telefonvermittlungsdaten

Gegenstand zweier parlamentarischer Anfragen sowie zahlreicher Presseberichte war ein Vorgang in der Telefonvermittlungszentrale des Bezirksamtes Harburg: Ein Lehrer, der außerhalb Hamburgs wohnt, hatte auf dem Weg zu seiner Schule einen Autounfall und wollte dies seiner Frau telefonisch mitteilen. Bei der zuständigen Vermittlungszentrale des Bezirksamtes Harburg meldete er das Ferngespräch als Dienstgespräch an. Da bei Anwahl der Zielnummer die Ehefrau des Lehrers am Apparat war, fragte die Vermittlungsperson noch einmal nach, ob es sich tatsächlich um ein Dienstgespräch handele, stellte die Verbindung dann her, teilte ihrem Vorgesetzten jedoch ihre weiterhin bestehenden Zweifel mit. Dieser informierte die Leitung der Schule des betroffenen Lehrers. Ob das Gespräch mitgehört wurde, ließ sich bei unserer Prüfung nicht mehr aufklären. Allerdings berichtete uns aus Anlaß dieses Falles eine andere Lehrerin derselben Schule, sie sei einmal mitten in einem längeren Gespräch mit einem Schulbuchverlag von der Vermittlung unterbrochen worden mit der Begründung, es handele sich ja gar nicht um ein Dienstgespräch.

In den folgenden Gesprächen mit dem Bezirksamt und bei einer Prüfung der Telefonvermittlungszentrale ließen wir uns die Praxis der Ferngesprächsvermittlung und die Möglichkeit der Gesprächsunterbrechung und des Mithörens vorführen. Das Einschalten in vermittelte Gespräche ist bei ankommenden dringenden Fernanrufen sowie bei sehr langen Ferngesprächen zur Kontrolle vorgesehen und wird den Gesprächsteilnehmern durch ein akustisches Zeichen deutlich gemacht.

Bei der Kontrolle der Vermittlungsunterlagen privater Ferngespräche stellten wir fest, daß die Zielnummern der angerufenen Teilnehmer vollständig gespeichert werden und daß früher geführte Vermittlungskladden mit personenbezogenen Daten seit über 10 Jahren aufbewahrt werden. Dies habe der Rechnungshof gefordert. Gegenwärtig wer-

den private Ferngespräche auf einer Karteikarte mit dem Namen des Anmeldenden vermerkt und einmal im Jahr abgerechnet. Dieses Verfahren wird von der Anordnung „Einrichtung und Benutzung von Fernsprechanlagen" vom 29. Januar 1976 (MittVw 76, S. 169) festgelegt.

Auf unsere Anregung und nach Rücksprache mit dem Rechnungshof hat das Bezirksamt Harburg inzwischen die alten Vermittlungskladden vernichtet und für die Karteikarten eine Aufbewahrungsfrist von einem Jahr nach der Abrechnung bestimmt, um den Zahlungseingang sicherzustellen.

Darüber hinaus haben wir für die neue Telekommunikationsrichtlinie angeregt, die folgenden Regelungen für die gesamte Hamburger Verwaltung verbindlich festzulegen:

— So sollte eine Verkürzung der gespeicherten privaten Zielnummern um die letzten beiden Ziffern vorgesehen werden. Dies haben wir bereits in unserem 3. Tätigkeitsbericht (4.7.5, S. 125) für den nicht-öffentlichen Bereich gefordert. Die verkürzte Speicherung ist für die Klärung von Meinungsverschiedenheiten zwischen Dienstherrn und Mitarbeiter über die Zahlungspflicht ausreichend und verhindert aber, daß der konkret angerufene Teilnehmer für den Dienstherrn identifizierbar ist.

— Eine Aufbewahrung der Karteikarten mit den Telefondaten (vgl. Anordnung von 1976) ist nur bis zur Bezahlung der privaten Ferngespräche erforderlich. Allenfalls der Beleg über die Zahlung mag haushaltsrechtlich bis zu fünf Jahren aufzubewahren sein, nicht jedoch die Aufstellung der einzelnen Telefongespräche.

— Das Aufschaltsignal zur Kenntlichmachung, daß die Vermittlung sich in das Gespräch eingeschaltet hat, gleicht heute eher einem regelmäßigen technischen Knacken als einem Warnsignal. Es sollte — z. B. durch eine Tonfolge — eindeutig gestaltet und in der Richtlinie allen Bediensteten beschrieben und in seiner Funktion bekanntgemacht werden.

Eine inhaltliche Antwort auf unsere Anregung haben wir bislang nicht erhalten.

4.2.3 Personalaktenrecht

4.2.3.1 Änderung der Beamtengesetze

Mit dem „Entwurf eines Neunten Gesetzes zur Änderung dienstrechtlicher Vorschriften" (Bundestagsdrucksache 11/7390 vom 13. Juni 1990) will die Bundesregierung das Personalaktenrecht erstmals im Bundesbeamtengesetz und im Beamtenrechtsrahmengesetz verankern (vgl. 8. TB, 3.2.6, S. 35). Gegenüber der im letzten Tätigkeitsbericht erläuterten Fassung ergeben sich in dem nun vorgelegten Gesetzentwurf nur Änderungen im Detail. So wird nun der neue Begriff der „Personalaktendaten" definiert, deren Verwendung ausdrücklich auf Zwecke der Personalverwaltung oder Personalwirtschaft beschränkt und ihre vertrauliche Behandlung und ihr Schutz vor unbefugter Einsicht festgelegt. Auskünfte aus dem Bundeszentralregister sind nun grundsätzlich nach 3 Jahren und nicht erst nach Tilgungsreife zu entfernen und zu vernichten. Ein automatisierter Abruf von Personalaktendaten muß nach dem neuen Entwurf durch eine „besondere Rechtsvorschrift" zugelassen sein. Dagegen wurde die Abschottung der Personalverwaltung von der Beihilfesachbearbeitung zur Soll-Vorschrift abgeschwächt und die Weitergabe von Personalakten ohne Einwilligung des Betroffenen auch an Behörden eines anderen Geschäftsbereichs desselben Dienstherren zugelassen, „soweit diese an einer Personalentscheidung mitzuwirken haben". Potentiell nachteilige Unterlagen über „Beschwerden, Behauptungen und Bewertungen" sollen nun grundsätzlich erst nach 3 (bisher 2) Jahren entfernt und vernichtet werden und auch nur dann, wenn sie nicht für die nächste dienstliche Beurteilung benötigt werden. Das ausdrückliche Verbot, Personalaktendaten zur Erstellung von Persönlichkeitsprofilen oder zur lückenlosen Kontrolle der Leistung heranzuziehen, ist entfallen, dürfte aber in der oben genannten Zweckbestimmung mit enthalten sein.

Die im 8. Tätigkeitsbericht beschriebenen Kritikpunkte (Personalakteneinsicht durch Vorgesetzte, Ausnahmen zur Weitergabe von Beihilfedaten, Schutz vor Bedienerdaten, Regelung der Datenerhebung) müssen wir auch gegenüber dem neuen Gesetzentwurf leider aufrechterhalten und haben sie zusammen mit dem Bundesbeauftragten und den anderen Landesbeauftragten für den Datenschutz in die Behördenabstimmung eingebracht. In den parlamentarischen Beratungen wird das Bemühen um eine Verbesserung des Gesetzentwurfs fortgesetzt werden.

4.2.3.2 Weitergabe von Personalakten durch Clearingstelle

Die von uns seit längerem (vgl. 6. TB, 4.2.1, S. 37; 7. TB, 4.2.2, S. 45) kritisierte Personalaktenversendung zwischen den Behörden ohne ausdrückliche Einwilligung der/des Betroffenen hat bei einem Petenten nun zu einer Verzögerung der Einstellung und damit zu einem finanziellen Verlust geführt: Der Betroffene hatte im Hamburger Staatsdienst seine Ausbildung absolviert, war danach zunächst aus dem Dienst ausgeschieden und bewarb sich dann später beim Personalamt um Wiedereinstellung in den Verwaltungsdienst der Hansestadt. Das Schreiben enthielt die — von falschen Voraussetzungen ausgehende — Bitte, „die Ihnen vorliegende Personalakte einzusehen". Der Petent bewarb sich daneben aber auch noch bei anderen öffentlichen und privaten Stellen. Das Personalamt teilte dem Betroffenen mit, daß es seine Bewerbung an andere Fachbehörden weitergeleitet habe. Später fragte der Petent noch einmal beim Personalamt nach, machte deutlich, daß er weiterhin an einer Einstellung — egal in welcher Fachbehörde — interessiert sei, und verwies „nochmals auf meine Personalakte, die zuletzt bei der Behörde X geführt wurde". Anläßlich eines Vorstellungsgespräches in einem Bundesamt gab der Petent diesem die Einwilligung zur Einsicht in die Personalakte. Sie konnte jedoch nicht gleich übersandt werden, weil sie auf Veranlassung des Personalamtes von der Behörde X ohne Wissen des Betroffenen an ein Bezirksamt verschickt worden war, das bei der Clearingsstelle des Personalamtes nach Kandidaten für eine freigewordene Stelle nachgefragt hatte. Die Einstellung beim Bundesamt verzögerte sich um 2 Wochen.

Das Personalamt rechtfertigte die Weiterleitung der Personalakte an das Bezirksamt im wesentlichen mit dem „wohlverstandenen Interesse" des Betroffenen. Es entnahm den Schreiben des Petenten die „zweifelsfreie" Einwilligung in die Weiterleitung der Bewerbung an die einzelnen Behörden „und daß dabei auch auf die bei der Behörde X geführte Personalakte zurückgegriffen werden konnte".

Wir teilen diese Auffassung nicht. Wie die Eingabe deutlich macht, sah der Petent in den zitierten Formulierungen keineswegs eine Pauschaleinwilligung an die Behörde X, die Personalakte an jede interessierte Stelle weiterzugeben. Vielmehr wollte er lediglich dem Personalamt die Einsicht gewähren, um ihm zu ermöglichen für ihn, den Petenten, eine passende Stelle auszuwählen. Das „wohlverstandene" Interesse deckte sich hier nicht mit dem tatsächlichen. Angesichts der Sensibilität von Personalaktendaten sind eindeutige Einwilligungen für deren Übersendung zu fordern. Ergibt sie sich nicht zweifelsfrei aus der Bewerbung, muß der Betroffene hierauf aufmerksam gemacht werden. Im übrigen ist zu fragen, warum überhaupt das Personalamt von sich aus für eine Personalaktenübermittlung sorgt. Hätte sich das Personalamt im vorliegenden Fall damit begnügt, dem Betroffenen das Angebot des Bezirksamtes weiterzuleiten und ihm die weitere Initiative überlassen, wäre es zu Schäden nicht gekommen.

4.2.3.3 Lebensläufe

Im letzten Tätigkeitsbericht (3.2.5, S. 34) berichteten wir vom Beginn der datenschutzrechtlichen Diskussion um Erforderlichkeit und Gestaltung von Lebensläufen. Unsere Position dabei ist einfach zu beschreiben: Soweit nicht ohnehin schon in einem Bewerbungsfragebogen die Ausbildungs- und Berufstätigkeitszeiten abgefragt werden, ist nur ein tabellarischer Lebenslauf für die Auswahlentscheidung erforderlich. Im übrigen kann es weder auf die „Ausführlichkeit" oder auf die Handschrift noch darauf ankommen, daß der Lebenslauf „selbstverfaßt" bzw. „eigenhändig geschrieben" wurde. Darf

die Behörde somit nur einen tabellarischen Lebenslauf fordern, so kann dem/der Bewerber/in andererseits nicht verwehrt werden, von sich aus freiwillig im Anschreiben oder im Lebenslauf zusätzliche persönliche Daten zu offenbaren.

Diese Position wird von der Justizbehörde und — jedenfalls auf telefonische Nachfrage — nun wohl auch vom Personalamt grundsätzlich geteilt. Einer Umsetzung in die tägliche Praxis stehen zur Zeit jedoch noch die verschiedenen Laufbahnvorschriften entgegen. Sie stellen hinsichtlich des Lebenslaufes als notwendige Bewerbungsunterlage ganz unterschiedliche Anforderungen, wobei ein sachlicher Grund für die Differenzierungen nicht ersichtlich ist. Die Varianten:

— überhaupt keine Regelung (z.B. bei Polizei und Feuerwehr),

— „selbstverfaßter und eigenhändig geschriebener Lebenslauf" (z.B. beim mittleren und gehobenen allgemeinen Verwaltungsdienst),

— „selbstverfaßter und eigenhändig geschriebener ausführlicher Lebenslauf" (nur bei Wirtschafts- und Sozialwissenschaftlern im höheren Verwaltungsdienst),

— „handgeschriebener Lebenslauf" (Lehrer an Sonderschulen),

— „Lebenslauf" (Vorbereitungsdienst und zweite Staatsprüfung für Lehrämter).

Das Personalamt sagte zu, die Laufbahnverordnungen im Zuge der Umsetzung der geplanten Beamtenrechtsnovellierung (s. o.) zu überarbeiten und dabei einheitlich eine Beschränkung auf einen tabellarischen Lebenslauf vorzusehen. Wir begrüßen dies, zumal die Diskussion bis zu diesem Punkt sehr schwierig war.

4.2.3.4 Weitergabe von Personaldaten an Versicherungen

In den letzten Jahren hatten sich immer wieder einzelne Bedienstete bei uns darüber beschwert, daß sie kurz nach der Einstellung oder anderen personalrechtlichen Maßnahmen Besuch von Versicherungsvertretern erhalten hätten, die nicht offenbarten, woher sie Namen und Adresse des/der Besuchten erfahren hatten. Eine „undichte Stelle" konnte bisher nie identifiziert werden.

Aufgrund der Beharrlichkeit eines von einem Versicherungsvertreter besuchten Bediensteten und der datenschutzrechtlichen Sensibilität eines Vorgesetzten wurde nun ein Mitarbeiter in einer Personalabteilung der Weitergabe von Personaldaten an eine Versicherung überführt. Obwohl es sich nach unserer Auffassung bei derartigen Übermittlungen nach bisherigem Recht um eine Straftat nach § 25 Absatz 1 HmbDSG handelte, haben wir angesichts personalabteilungsinterner Maßnahmen auf weitere Schritte und auch auf die Offenbarung des Namens gegenüber dem Petenten verzichtet.

4.2.3.5 Entfernung von Unterlagen aus der Personalakte

Die Frage, wie lange eine für den Betroffenen potentiell nachteilige Unterlage (hier: ein personalärztliches Gutachten) in der Personalakte verbleiben muß, warfen wir bereits im letzten Tätigkeitsbericht (8. TB, 3.2.7, S. 36) auf. Eine Stellungnahme der Oberfinanzdirektion hierzu macht deutlich, wie wenig die Bedeutung des informationellen Selbstbestimmungsrechts für die tägliche Personalverwaltungspraxis erkannt wird: „Ärztliche Äußerungen über medizinische Befunde behalten dienstliche Relevanz und können auch nach längerer Zeit nicht als „überholt" aus der Personalakte entfernt werden . . . Als Beamter haben Sie keinen Anspruch darauf, daß das rechtmäßig in Ihre Personalakte gelangte Gutachten wieder entfernt wird . . . Das Recht auf informationelle Selbstbestimmung . . . greift gegenüber der gesetzlich geregelten Befugnis des Dienstherrn zur Führung von Personalakten nicht Platz, da diese anderenfalls ihren Zweck, ein möglichst lückenloses Bild der Entstehung und Entwicklung des Dienstverhältnisses als historischen Geschehensablauf zu vermitteln, nicht mehr erfüllen könnten." Obwohl die angebliche gesetzliche Regelung zur Personalaktenführung zur Zeit gerade noch fehlt, werden hier tradierte verwaltungsorganisatorische Prinzipien dem

im allgemeinen Persönlichkeitsrecht wurzelnden Grundsatz der Erforderlichkeit von Datenspeicherungen zu Unrecht übergeordnet. Die geplante Änderung des Beamtenrechts sieht eine Entfernung und Vernichtung von potentiell nachteiligen „Unterlagen über Beschwerden, Behauptungen und Bewertungen" grundsätzlich nach 3 Jahren vor. Im vorliegenden Fall ist das Gutachten 9 Jahre alt.

Das Personalamt trat zwar der Auffassung der Oberfinanzdirektion ausdrücklich bei. Für den konkreten Einzelfall wurde jedoch insofern eine Lösung gefunden, als bei späteren Bewerbungen des Petenten bei anderen Behörden das Gutachten und der dazu geführte Schriftverkehr vor Abgabe der Personalakte „vorübergehend zu einer Sonderakte" genommen werden soll. Wir gehen davon aus, daß das Inkrafttreten des neuen Beamtenrechts die endgültige Entfernung des Gutachtens aus der Personalakte erzwingen wird.

Wesentlich datenschutzbewußter zeigte sich die Personalabteilung eines Bezirksamtes, die bei der Bearbeitung eines Verkehrsunfalles einer Mitarbeiterin vom Unfallgegner erfuhr, daß diese während der unfallbedingten Arbeitsunfähigkeit eine Fehlgeburt erlitten hatte. Der darüber entstandene Schriftwechsel wurde zunächst in einer Sachakte geführt und nach der Abwicklung der Unfallfolgen vernichtet.

4.2.4 Einsicht in Bußgeldakten von Arbeitnehmern

Ein anderer Verkehrsunfall eines Bediensteten warf die Frage auf, ob der Arbeitgeber — hier vertreten durch die Personalabteilung eines Bezirksamtes — die Bußgeldakte von der Innenbehörde — Einwohnerzentralamt — anfordern darf, um die Angaben des Arbeitnehmers in der dienstlichen Unfallmeldung mit den Ergebnissen der polizeilichen Ermittlungen zu vergleichen.

Wir haben die Frage mit folgender Begründung bejaht: Bei einem Unfall eines Arbeitnehmers im öffentlichen Dienst trägt der Arbeitgeber das Krankengeld bzw. die Lohnfortzahlung im Ergebnis nur insoweit, als der Mitarbeiter den Unfall selbst verschuldete. Etwaige Schadenersatzansprüche gegen Dritte leitet der Arbeitnehmer entsprechend dem Tarifvertrag auf den Arbeitgeber über. Daraus ergibt sich für die sachbearbeitende Personalabteilung ein berechtigtes Interesse an der Einsichtnahme in die Bußgeld-/Strafermittlungsakte. Ihr kann entnommen werden, ob ein Dritter den Unfall (mit-)verschuldete, ob den Mitarbeiter — oft entgegen seiner Unfallmeldung — ebenfalls eine Mitschuld trifft, wer gegebenenfalls in Anspruch genommen werden kann und welche Versicherung beteiligt ist. Dementsprechend sehen auch die Richtlinien zum Straf- und Bußgeldverfahren, Ziffer 185 Absatz 2 und 3 ein Akteneinsichtsrecht sowohl für die Anwälte der Versicherungen als auch für Behörden vor. Im Streit um die Schadenersatzansprüche müssen beide Parteien gleiche Ermittlungs- und Verhandlungschancen haben.

Die Anforderung der Bußgeld- oder Ermittlungsakte vom Einwohnerzentralamt ist jedoch zu begründen, damit dieses als übermittelnde Stelle ihrer Verantwortung nach § 14 Absatz 3 HmbDSG n. F. gerecht werden kann. Zur Sicherstellung der Transparenz für den/die Betroffene/n sollte im Formular für die Unfallmeldung darüber hinaus ein Hinweis aufgenommen werden, daß der Arbeitgeber die Angaben des/der Bediensteten gegebenenfalls durch Einsicht in die Bußgeld-/Ermittlungsakte überprüft.

4.2.5 Bewerberdaten

4.2.5.1 Polizei

Nachdem uns Anfang des Jahres die neuen mit uns abgestimmten Bewerber- und Personalbögen der Justizbehörde für den Strafvollzugsdienst zugegangen waren (vgl. 7. TB, 4.2.3, S. 47), konnten auch Erhebung und Speicherung von Bewerberdaten bei der Polizei weitgehend einverständlich geklärt werden. Angesichts der großen Anzahl von Bewerbern (5000 schriftliche Anfragen und 2500 Bewerbungen im Jahr), die zum großen Teil nicht in Hamburg wohnen, haben wir Abweichungen von dem Muster-Fra-

gebogen akzeptiert, die den Anforderungen des Massenverfahrens und des erhöhten Sicherheitsbedürfnisses Rechnung tragen.

Die im Bewerbungsbogen nach wie vor gewünschten Angaben zum Familienstand und zur Kinderanzahl werden nun ausdrücklich als freiwillige Angaben hervorgehoben. Dasselbe gilt erstmals für Angaben über nicht in das Führungszeugnis aufgenommene Verurteilungen, Zuchtmittel oder Maßregelverhängungen sowie für Angaben über schwebende Verfahren. Die bisherige Formulierung im Bewerbungsbogen, Verurteilte hätten „auch Sachverhalte anzugeben, die nicht in das Führungszeugnis aufgenommen werden, soweit Behörden ein Recht auf unbeschränkte Auskunft haben", war in diesem Zusammenhang rechtlich unzutreffend. Die Verweigerung von Angaben zu diesen Punkten führt nach unserer Kenntnis nicht automatisch zum Abbruch des weiteren Bewerbungsverfahrens. Allerdings wird darüber hinaus bei der Polizeidienststelle des Wohnortes des Bewerbers nach Erkenntnissen gefragt, die gegen eine mögliche Einstellung sprechen könnten. Dabei wird das Auskunftssystem POLAS/INPOL genutzt, das über abgeschlossene oder schwebende Ermittlungsverfahren informiert. Zu dieser Leumundsanfrage ist im Bewerbungsbogen eine ausdrückliche Einwilligungserklärung vorgesehen. Offen bleibt, ob dieses Einverständnis tatsächlich freiwillig gegeben wird oder ob die Bewerbungssituation nicht zu einem faktischen Zwang führt, der dem/der Bewerber/in die freie Entscheidung weitgehend nimmt. Dann könnte nur eine gesetzliche Ermächtigung eine solche Leumundsanfrage rechtfertigen. Hierzu sind wir mit den Datenschutzbeauftragten der anderen Länder noch in der Diskussion.

Trotz unserer grundsätzlichen Bedenken haben wir der geschilderten polizeilichen Praxis zunächst zugestimmt, weil auf unsere Anregung nun wenigstens zwei Einschränkungen im Bewerbungsbogen festgeschrieben sind: „Befragungen Dritter aus meinem persönlichen Umfeld erfolgen nicht" und „Sollten die Auskünfte zu einer Ablehnung der Bewerbung führen, werde ich über den Inhalt der Auskünfte unterrichtet". Letzteres wird auch der angefragten Polizeidienststelle des Wohnortes des Bewerbers mitgeteilt.

4.2.5.2 Staatliche Gewerbeschule

Wer sich bei der staatlichen Gewerbeschule zum Fachlehrer im Werkstattunterricht ausbilden lassen will, mußte bislang neben der Geburtsurkunde auch ein aktuelles Lichtbild, einen Lebenslauf, den Antrag eines Führungszeugnisses zur Vorlage bei einer Behörde sowie eine Erklärung darüber vorlegen, „ob er gerichtlich vorbestraft ist oder ob gegen ihn ein gerichtliches Strafverfahren oder ein staatsanwaltliches Ermittlungsverfahren anhängig ist oder anhängig gewesen ist". Gegen diese Anforderungen haben wir bei der Behörde für Schule, Jugend und Berufsbildung Bedenken angemeldet. Insbesondere die Frage nach schwebenden Verfahren erschien uns nicht erforderlich.

Der Datenschutzbeauftragte der Schulbehörde teilte unsere Zweifel weitgehend und kündigte eine Änderung des entsprechenden Merkblattes an: Anstelle des Lebenslaufes wird nur noch eine tabellarische Übersicht über den Bildungsgang abgefordert, auf das Lichtbild und auf die Erklärung über Straf- oder Ermittlungsverfahren wird in Zukunft ganz verzichtet. Als Begründung für das erweiterte Führungszeugnis, an dem festgehalten werden soll, wies die Schulbehörde darauf hin, daß nur das Führungszeugnis zur Vorlage bei einer Behörde, nicht aber das Führungszeugnis für eigene Zwecke z. B. den Entzug der Ausbildungsbefugnis vermerkt. Dies haben wir im vorliegenden Zusammenhang als relevant anerkannt.

4.2.5.3 Psychologischer Dienst

Im 2. Tätigkeitsbericht (3.3.1, S. 47) hatten wir die Verarbeitung der Bewerberdaten durch das Prüfungsamt für den öffentlichen Dienst vorgestellt. Mit Wirkung vom 1. Januar 1990 wurde dieses Amt in den „psychologischen Dienst" beim Senatsamt für den Verwaltungsdienst — Personalamt — umgewandelt und das Verfahren für einzelne Bewerbergruppen geändert. Dies war für uns Anlaß, die Praxis einmal vor Ort zu prüfen. Dabei haben wir unter anderem folgende Feststellungen getroffen:

Die Einladung zur Prüfung enthält folgende Datenschutzinformationen: „Die vom Psychologischen Dienst gespeicherten Daten werden vernichtet, sobald feststeht, daß eine Einstellung nicht zustande kommt, in jedem Fall nach vier Jahren; ausgenommen hiervon sind jedoch Daten der Bewerber/innen, bei denen eine uneingeschränkte Eignung festgestellt worden ist. Diese Daten werden weitere vier Jahre aufbewahrt, um bei einer eventuell nötigen zweiten Eignungsuntersuchung zu Ihren Gunsten auf das Ergebnis der ersten Eignungsuntersuchung zurückgreifen zu können." § 28 Absatz 5 HmbDSG n.F. lautet demgegenüber allgemein: „Personenbezogene Daten, die vor der Eingehung eines Beschäftigungsverhältnisses erhoben wurden, sind unverzüglich zu löschen, sobald feststeht, daß ein Beschäftigungsverhältnis nicht zustande kommt."

In der Praxis werden die Bewerbungsunterlagen nur dann vor Ablauf von 4 Jahren vernichtet, wenn der Bewerber dies ausdrücklich wünscht. Die 8jährige Aufbewahrung wird nicht von der Einwilligung des Bewerbers abhängig gemacht.

Zu den 4 bzw. 8 Jahre aufbewahrten Unterlagen gehören eine auf den Namen bezogene Bewerberkarteikarte mit Prüfnummer, Prüfungstermin und -ergebnis sowie — nur auf die Prüfnummer, nicht auf den Namen bezogen — ein Leistungsbericht mit einem differenzierten Leistungsprofil und gegebenenfalls dem Ergebnis der psychologischen Exploration und Auffälligkeiten aus dem Lebenslauf. Ferner unterliegen auch die von den Prüfern ausgefüllten Signierbögen mit Prüfnummer und Geburtstag des Bewerbers den genannten Aufbewahrungsfristen. Sie dienen der Erstellung einer automatisierten Prüfungsergebnisdatei. Die jährlichen Ausdrucke dieser Datei offenbaren ebenfalls Prüfungsnummer und Geburtsdatum, sind im übrigen jedoch weitgehend verschlüsselt. Der Direktor des Psychologischen Dienstes verwahrt diese Ausdrucke nebst einzelnen Sonderauswertungen seit seit 1978 in seinem Dienstzimmer.

Bei Angestelltenbewerbern und Anwärtern wird das vom Psychologischen Dienst erstellte Leistungsprofil den Beschäftigungsbehörden bzw. den zentralen Ausbildungsstellen zur Erläuterung der Eignungsempfehlung vorübergehend zur Verfügung gestellt. Der Rücklauf und das ausdrücklich vermerkte Fotokopierverbot werden allerdings nicht (mehr) kontrolliert.

In einem gebundenen „Hauptbuch" werden nach den fortlaufenden Prüfnummern der Bewerbername, die Bewerbergruppe, das Prüfungsdatum und die Abkürzung für den Prüfer/Gutachter vermerkt. Da hier zwischen geeigneten und ungeeigneten Bewerbern nicht unterschieden wird, werden die Hauptbücher solange aufbewahrt, bis die letzte Eintragung 8 Jahre zurückliegt. Das älteste Hauptbuch reicht dementsprechend mit seinen ersten Eintragungen bis zum März 1981 zurück.

Die Prüfungsergebnisse von Schwerbehinderten einschließlich der Resultate aus der psychologischen Exploration werden mit Einverständnis der Bewerber in eine Liste aufgenommen, aus der der Psychologische Dienst Anfragen von Dienststellen beantwortet oder in die Personalleiter Einsicht nehmen zur Auswahl eines geeigneten Behinderten. Diese Liste wird über Jahre geführt. Eine Löschung erfolgt nur, wenn der Bewerber von sich aus ausdrücklich mitteilt, er wolle die Bewerbung zurückziehen.

Eine abschließende rechtliche Bewertung der von uns getroffenen Feststellungen steht noch aus, da wegen des Wechsels des Leiters des Psychologischen Dienstes noch keine Einigkeit über den Sachverhalt erzielt werden konnte.

4.2.6 Ausfallzeitenstatistik im Landesbetrieb Krankenhäuser

Ziel und Probleme der Ausfallzeitenstatistik im Landesbetrieb Krankenhäuser stellten wir im letzten Tätigkeitsbericht dar (8. TB, 3.2.3, S. 33). Im wesentlichen ging es um die Sicherstellung der Anonymität der Statistik und der Verhinderung einer technischen Leistungs- und Verhaltenskontrolle der Mitarbeiter. Um die Einhaltung unserer datenschutzrechtlichen Vorgaben zu überprüfen, ließen wir uns im Februar eine vorläufige Systemversion vorführen. Dabei stellten wir fest, daß sich die von uns geforderte Aggregierung zu Angaben über mindestens 4 Personen ausschließlich auf die ausgedruckten Listen bezog. Der Statistikdatensatz im System enthielt jedoch weiterhin Informatio-

nen über Jahr, Monat, Dienstart, Kostenstelle, Ausfallzeiten, Ausfallarten und tatsächliche Monatsarbeitszeit. Jede Person mit Zugriff auf das Betriebssystem war danach in der Lage, in sehr vielen Fällen auch ohne Namensangabe eine Reidentifikation des/der betroffenen Mitarbeiter/in vorzunehmen. Wir teilten dem Landesbetrieb unsere Auffassung mit, daß es sich bei der beabsichtigten Ausfallzeitenstatistik um personenbeziehbare Daten handele, auf die das Hamburgische Datenschutzgesetz anwendbar sei. Zugleich sei damit partiell eine Verhaltens- und Leistungskontrolle möglich, was nach § 84 Absatz 1 Nummer 4 HmbPersVG Mitbestimmungsrechte des Personalrats auslösen könnte. Wir rieten dazu, entweder auch den Statistikdatensatz im System zu aggregieren oder ein Mitbestimmungsverfahren mit dem Personalrat einzuleiten.

Im Mai erhielten wir die Mitteilung, daß der zweite Weg beschritten werden sollte. Die uns im Juli zugegangene Dienstvereinbarung versucht, personenbezogene Auswertungen dadurch unmöglich zu machen, daß Name und Personenkennziffer auf dem Dienstzeitnachweis bereits vom direkten Vorgesetzten durch eine besondere Identifikationsnummer ersetzt werden, die Zugangsberechtigung auf vier verschiedene Funktionsbereiche aufgeteilt, die Verarbeitung der Ausfallzeiten von der Personalverwaltung getrennt und die Gestaltung der Statistik genau festgelegt wird. „Dabei werden Informationen aus Einzelstatistiken, die sich auf weniger als vier Personen beziehen, ‚geweißt'". Angesichts der Einigung zwischen Dienststelle und Personalrat und der detaillierten Datenschutzregelungen sehen wir auch aus unserer Sicht keinen Anlaß mehr für Bedenken. Die Dienstvereinbarung kann nach § 5 Absatz 1 Ziffer 1 HmbDSG n.F. als „andere Rechtsvorschrift" ebenso wie ein Gesetz und die Einwilligung der Betroffenen die Verarbeitung personenbezogener Daten rechtfertigen.

4.2.7 Personaldatenverarbeitung außerhalb der Personalabteilungen

4.2.7.1 Baurechtsamt

Aufgrund einer Eingabe überprüften wir Ende letzten Jahres die interne Personalverwaltung im Baurechtsamt. Dabei haben wir folgendes festgestellt: Auf einer Grundkarteikarte werden die Personalien der Amtsmitarbeiter einschließlich Name und Geburtstag des Ehepartners und der Kinder vermerkt. Eine Krankheitskarteikarte offenbart jeden krankheitsbedingten Ausfalltag seit Eintritt ins Baurechtsamt. Nach Ausscheiden des/der Betroffenen aus dem Amt wird sie neben anderen Unterlagen zu Stellenbesetzung, Beurlaubungen usw. in einer Hilfspersonalakte verwahrt, die nach längeren, aber nicht festgelegten Zeiträumen (meist mehrere Jahre) aufgelöst wird. Die Grundkarteikarte wird ebenfalls über das Ausscheiden hinaus aufbewahrt — bei Ruheständlern bis zu deren Tod, bei Versetzungen oder ähnlichem bis zum 60. Lebensjahr der/des Betroffenen. Bei Stellenbesetzungen fordert der Personalsachbearbeiter die Personalakten der Bewerber an und erstellt daraus einen Bewerberspiegel für den Amtsleiter.

Wir äußerten Kritik an der Speicherung einiger nicht erforderlicher Daten auf der Grundkarteikarte, an der langen Aufbewahrung dieser Karte und der Krankheitsdaten sowie an der Einsicht in die Personalakten der zukünftigen bzw. potentiellen Kollegen/innen durch den Sachbearbeiter. Wir regten an, die Speicherung von nicht (mehr) erforderlichen persönlichen Daten und deren Nutzung für Jubiläumsansprachen und ähnliches von der ausdrücklichen Einwilligung des/der (ehemaligen) Bediensteten abhängig zu machen.

Im Ergebnis konnten wesentliche Änderungen der Praxis vereinbart werden: Die Hilfspersonalakte wird in Zukunft bereits beim Ausscheiden des/der Betroffenen aufgelöst und vernichtet, die Grundkarteikarte zwei Jahre danach — allerdings nur bei Versetzungen, nicht bei Ruheständlern. Die Krankheitsdaten werden nur noch für 3 Jahre gespeichert. Hinsichtlich des Datenumfangs auf der Grundkarteikarte wies das Baurechtsamt auf eine neue „Zuständigkeitsregelung in Personalangelegenheiten" der Baubehörde hin, die insbesondere die Genehmigung von Sonderurlaub und Arbeitsbe-

freiung auf die Amtsleiter delegiert und eine Weiterdelegation zuläßt. Für diesen Zweck läßt sich die Erhebung und Speicherung zusätzlicher persönlicher Daten rechtfertigen. Dies gilt allerdings nicht für Ruheständler. Hier konnte bezüglich der ohne Einwilligung erfolgenden Aufbewahrung und Nutzung der Grundkarteikarte bis zum Tod des/der Betroffenen keine Einigung erzielt werden. Zur Personalakteneinsicht durch den Sachbearbeiter mußten wir auf die genannte Zuständigkeitsregelung hinweisen, die den Amtsleitern eine Weiterübertragung des Rechts auf Einsicht in Personalakten ausdrücklich nicht gestattet. Eine abschließende Äußerung des Baurechtsamtes steht noch aus.

4.2.7.2 Registratur der Justizbehörde

Aufgrund des Hinweises eines Bediensteten überprüften wir einen Teil der allgemeinen (Sachakten-)Registratur der Justizbehörde nach personenbezogenen Datensammlungen. Zutritt hierzu hat grundsätzlich jeder Mitarbeiter der Justizbehörde; eine Sachbearbeiterin der allgemeinen Verwaltung ist für die Ablage und Aktenvorlage verantwortlich. Wir stellten folgendes fest:

In den offenen Aktenschränken werden folgende personenbezogene Vorgänge aufbewahrt:

— Nebentätigkeiten (Anträge, Schriftwechsel, Genehmigungen),

— Stellenausschreibungen mit Bewerbersiegel, zum Teil mit Auswahlbegründungen und Schriftwechsel,

— Sammlung gelöschter Dienststrafen seit 1967,

— Akte „Rechte und Pflichten der Beamten" (seit 1961) mit Disziplinar-Ermittlungsvorgängen, Richterdienstgerichtsentscheidungen, Schriftwechsel über Dienstpflichtverletzungen, (z.B. Bestechlichkeitsvorwürfe),

— Vorgänge über Täuschungshandlungen bei juristischen Prüfungen,

— Rückforderung von Dienstbezügen,

— Generalakten zu Ermittlungsverfahren gegen Richter und Staatsanwälte wegen ihrer Justiztätigkeit in der NS-Zeit.

Im Inhaltsverzeichnis zu einigen der genannten (Sammel-)Akten ist der Name des/der Betroffenen als Suchbegriff aufgeführt. So wird bei der „Löschung von Dienststrafen" erstmals in der Registratur der Name erfaßt und ins Inhaltsverzeichnis eingetragen. Im übrigen sind die Akten über einen ausliegenden detaillierten Aktenplan zu erschließen, der — in einzelnen Aktentiteln — ebenfalls Namen von Betroffenen enthält. Die Einsicht in viele der genannten Akten eröffnet einen tiefen Einblick in zum Teil äußerst sensible Vorgänge und Vorwürfe hinsichtlich bestimmter Personen, wobei es sich teilweise um 20 Jahre zurückliegende, teilweise um aktuelle Angelegenheiten handelt.

Der Registraturraum war nicht besonders gesichert, die Tür mit dem allgemeinen Generalschlüssel zu öffnen. Die Aktenschränke werden nie verschlossen, die Aktenpläne liegen auch nach Dienstschluß offen aus. Zur Zeit der Prüfung war das Gebäude eingerüstet, wobei eine Laufplanke direkt am Fenster des Registraturraumes vorbeiführte. Nach Aussage der Sachbearbeiterin war bereits in das Gebäude eingebrochen worden.

Im Mai 1990 wiesen wir die Justizbehörde darauf hin, daß es sich bei den aufgefundenen Akten materiell um Personalakten handelt, die eines besonderen Schutzes und besonderer Sicherheitsmaßnahmen bedürfen. Nach einer telefonischen Zwischennachricht erhielten wir 2 Monate später die schriftliche Mitteilung, als Sofortmaßnahme sei der Raum mit einem Sicherheitsschloß versehen worden. Die übrigen Punkte bedürften eingehender Prüfung. Mehr als 4 Monate nach unserem Hinweis an die Justizbehörde steht eine Stellungnahme immer noch aus.

4.2.8 Sicherheitsrichtlinien

Unsere im 8. Tätigkeitsbericht (3.2.9, S. 37) dargestellte Stellungnahme zur Neufassung der Hamburger Sicherheitsrichtlinien führte zu einem neuen Entwurf, der unseren Bedenken weitgehend Rechnung trägt. So wurde klargestellt, daß für die Sicherheitsüberprüfung der Geheimschutzbeauftragte der jeweiligen Behörde zuständig ist und das Landesamt für Verfassungsschutz (LfV) in seinem Auftrag tätig wird. Anfragen des LfV werden nicht mehr an die „örtlich zuständigen Polizeidienststellen" (mit der Möglichkeit der Weitergabe von sogenannten „Milieu-Kenntnissen") gerichtet, sondern an das Landeskriminalamt. Bei der erweiterten Sicherheitsüberprüfung dürfen nur noch bestimmte „andere geeignete staatliche Stellen" befragt werden, nicht aber private. Bedeutsam ist ein Verzicht auf die Nutzung und Weitergabe anfallender Informationen für „Zwecke der straf- oder disziplinarrechtlichen Verfolgung sowie erforderliche dienst- oder arbeitsrechtliche Maßnahmen". Inzwischen wurde auch die pauschale Bezugnahme auf die „kommunistisch regierten Länder" durch eine Liste von „Staaten mit besonderen Sicherheitsrisiken" ersetzt.

Nicht durchsetzen konnten wir, daß das LfV bei der einfachen Sicherheitsüberprüfung auf eine NADIS-Abfrage bezüglich des Lebenspartners des/der Betroffenen verzichtet. Unserer Forderung, dies dann aber wenigstens im Merkblatt zur Sicherheitsprüfung dem/der Betroffenen mitzuteilen, stand die Behörde für Inneres jedoch aufgeschlossen gegenüber. Ebenfalls nicht erreicht haben wir eine ausnahmslose Trennung von Geheimschutz und Personalverwaltung, wie sie die Sicherheitsrichtlinien des Bundes vorsehen. In Hamburg gebe es keine hauptamtlichen Geheimschutzbeauftragten und viele Verwaltungseinheiten seien so klein, daß ausnahmsweise ein Verwaltungsleiter auch einmal sowohl für den Geheimschutz als auch für die Personalverwaltung zuständig sein dürfte.

Insgesamt stellen die neuen Hamburger Sicherheitsrichtlinien gegenüber den Bundes-Richtlinien jedoch einen nicht unerheblichen Fortschritt im Sinne einer liberaleren und datenschutzfreundlicheren Verfassungsschutzpraxis dar. Nicht eingelöst ist mit ihnen allerdings das verfassungsrechtliche Gebot, die mit der Sicherheitsüberprüfung verbundenen tiefgehenden Eingriffe in das Persönlichkeitsrecht der Betroffenen auf gesetzlicher Grundlage zu regeln.

4.3 Statistik

4.3.1 Entwurf eines Hamburgischen Statistikgesetzes

Die Behörde für Inneres hat Ende Juli 1990 die überarbeitete Entwurfsfassung für ein Hamburgisches Landesstatistikgesetz vorgelegt. Leider ist festzustellen, daß unsere zum ersten Referentenentwurf aus den Oktober 1989 geäußerten Kritikpunkte und Anregungen (vgl. 8. TB, 3.3.1, S. 38) im wesentlichen nicht aufgegriffen wurden.

Lediglich für die Abschottungsregelung ist die Behörde für Inneres unserer Argumentation gefolgt. Nach dem neugefaßten § 7 Abs. 1 ist die Wahrnehmung statistischer Aufgaben organisatorisch und personell von der Erfüllung anderer Aufgaben des Verwaltungsvollzugs zu trennen. Dies gilt allerdings nicht für Geschäftsstatistiken, deren Erstellung nur räumlich (nicht aber organisatorisch und personell) von anderen Verwaltungsaufgaben zu separieren ist.

Problematisch sind vor allem die Regelungen über die Geschäftsstatistiken, die keiner spezialgesetzlichen Grundlage bedürfen: Gemäß § 8 Abs. 1 sollen bei der rechtmäßigen Aufgabenerfüllung angefallene Daten für die Erstellung von Geschäftsstatistiken genutzt werden können. Die datenschutzrechtliche Relevanz solcher Statistiken wäre in der Tat gering, wenn es sich — wie in der Begründung zur ersten Entwurfsfassung ausgeführt — dabei bloß um Strichlisten handeln würde, die z. B. über den Arbeitsanfall in einer Verwaltungseinheit Auskunft geben sollen. Tatsächlich erstellen verschiedene Verwaltungszweige eine Fülle unterschiedlicher, z. T. personenbezogener Statistiken, die sie als Geschäftsstatistiken bezeichnen, obwohl es sich um regelmäßige, z. T. län-

derübergreifend koordinierte oder aus verschiedenen Sachzusammenhängen und sogar von unterschiedlichen öffentlichen Stellen stammende Daten handelt.

Die Zusammenführung von personenbezogenen Daten mit unterschiedlichem Sachbezug greift tief in das Recht auf informationelle Selbstbestimmung des Betroffenen ein und bedarf deshalb einer spezialgesetzlichen Grundlage. Die von der Verwaltung für die Erfüllung von Fachausgaben erhobenen Daten stellen keineswegs einen für „geschäfts-"statistische Zwecke von den öffentlichen Stellen beliebig verknüpfbaren und auswertbaren Fundus dar.

Wenn § 8 Abs. 1 S. 3 das Zusammenführen von Daten über dieselbe natürliche oder juristische Person aus Geschäftsgängen mit unterschiedlichem Sachbezug im Rahmen von Geschäftsstatistiken, „soweit dies zur Erreichung des mit der Geschäftsstatistik verfolgten Zwecks zwingend geboten ist", erlaubt, so stellt dies eine bedenkliche Ausweitung zweckentfremdeter Datenverarbeitung dar. Da die Abschottungsregelungen des § 7 Abs. 1 nicht für Geschäftsstatistiken gelten sollen, dürften also Daten, die im Rahmen des Verwaltungsvollzugs gegeneinander zu isolieren wären, nunmehr für „Geschäftsstatistiken" nicht nur miteinander verknüpft sondern auch anderen Organisationseinheiten innerhalb derselben öffentlichen Stelle zur Kenntnis gebracht werden.

Auch die Vorschrift des § 8 Abs. 4 stößt aus den gleichen Gründen auf erhebliche Bedenken. Bei den dort erwähnten „zusammenfassenden Landesstatistiken" aus Daten verschiedener öffentlicher Stellen (Bezirksämter, Schulen, Hochschulen und Gerichte) handelt es sich nicht um Geschäftsstatistiken, sondern um Landesstatistiken, für die gem. § 2 eine Anordnung durch Gesetz erforderlich ist.

4.3.2 Bevölkerungsstatistikgesetz

Das Bundesinnenministerium hat im November 1989 einen Referentenentwurf für ein neues Gesetz über die Bevölkerungsstatistik vorgelegt. Gegen diesen Entwurf bestehen erhebliche datenschutzrechtliche Bedenken, die von der Behörde für Inneres leider nicht geteilt werden.

Bei der Bevölkerungsstatistik handelt es sich — wie bei der Volkszählung — um eine Vollerhebung, also um eine Erhebung, bei der Daten über die gesamte Bevölkerung verarbeitet werden. Die Daten beziehen sich nicht auf einen bestimmten Stichtag, sondern fließen immer dann an die Statistischen Landesämter, wenn bestimmte Ereignisse (z. B. Geburten, Eheschließungen, Scheidungen und Sterbefälle) eintreten.

Auch wenn die Bürger nur in geringem Umfang selbst zur Auskunft herangezogen werden, greift das Erhebungsprogramm der Bevölkerungsstatistik tief in die Persönlichkeitssphäre des einzelnen ein: Einige Erhebungsmerkmale beziehen sich auf den intimen Bereich der privaten Lebensgestaltung. So sollen z. B. Daten über die Ehelichkeit/Nichtehelichkeit von Neugeborenen und die Erwerbstätigkeit der Mutter (§ 2), die Religionszugehörigkeit (§§ 2-5) und die Tatsache von Urteilen in Ehesachen (§ 6) erhoben werden.

Besonders gravierend ist, daß ein Rückschluß auf die Betroffenen anhand des Merkmals Geburtsdatum in Verbindung mit dem Merkmal Gemeinde/Gemeindeteil und dem Merkmal Geschlecht möglich ist, die in den einzelnen Erhebungsbereichen (Geburten, Eheschließungen, Sterbefälle, Zu- und Fortzüge, Ehescheidungen) jeweils als Erhebungsmerkmale erfragt werden. Damit ist die Anonymität der Erhebungsergebnisse auch nach Löschung der Hilfsmerkmale nicht gewährleistet.

Über die Erhebungsmerkmale Geburtsdatum, Geschlecht und Gemeinde/Gemeindeteil ließe sich zudem eine Verlaufsstatistik bilden. Die erhobenen Sachverhalte könnten miteinander verknüpft und ausgewertet werden. So könnten anhand der Geburts- und Ortsangaben Daten über Eheschließungen, Wohnungswechsel, Geburten, Scheidungen und Todesfälle miteinander verknüpft werden. Diese Möglichkeit ist im Hinblick auf die Unzulässigkeit von tiefenscharfen Persönlichkeitsprofilen nicht hinzunehmen, auch dann nicht, wenn derartige Auswertungen derzeit nicht praktiziert werden.

Wir haben vorgeschlagen, die Erhebungs- und Hilfsmerkmale zu reduzieren. Insbesondere sollte darauf geachtet werden, daß nicht das genaue Geburtsdatum, das genaue Hochzeitsdatum und das genaue Umzugsdatum erfaßt werden, die einen Rückschluß auf den Betroffenen zulassen. Es wäre aus unserer Sicht völlig ausreichend, wenn die bevölkerungsstatistischen Untersuchungen auf das Geburtsjahr zur Altersbestimmung abstellen würden, zumal auch die Volkszählungsergebnisse, deren Fortschreibung die Bevölkerungsstatistik nach Auskunft der Behörde für Inneres vornehmlich dient, ebenfalls nicht das genaue Geburtsdatum enthalten.

Die Behörde für Inneres war dagegen der Auffassung, unsere Ausführungen zu den Möglichkeiten einer nachträglichen Re-Identifizierung entbehrten der praktischen Bedeutung, da die Geburtsdaten keine Veröffentlichungstatbestände darstellten, und ließen die gesetzlich vorgeschriebenen Maßnahmen zur Datensicherung außer acht.

Dem ist entgegenzuhalten, daß das vom Bundesverfassungsgericht in seinem Volkszählungsurteil postulierte Gebot zur möglichst frühzeitigen faktischen Anonymisierung statistischer Daten unterlaufen wird, wenn — wie hier — praktisch alle Datensätze mit nur geringem Zusatzwissen leicht wieder den einzelnen Bürgern zuzuordnen sind. Das gilt erst recht, wenn sowohl das erforderliche Zusatzwissen als auch die Erhebungsmerkmale auf automatisiert auswertbaren Datenträgern vorliegen.

Ferner hatten wir einen Verzicht auf die Merkmale Zugehörigkeit zu einer Religionsgesellschaft (§§ 2-5), Ehelichkeit/Nichtehelichkeit (§§ 2, 4), Erwerbstätigkeit der Mutter (§ 2), Jahr und Monat der Auflösung einer vorausgegangenen Ehe (§ 3), vorgeschlagen, da diese Daten in unzumutbarer Weise in den Privatbereich der Bürger eingreifen.

Auch diesem Vorschlag wollte die Behörde für Inneres nicht folgen, da diese Merkmale — mit Ausnahme des Merkmals der Ehelichkeit bzw. Nichtehelichkeit von Neugeborenen — an das Verhalten der Betroffenen in der Außenwelt anknüpften und zudem anonymisiert ausgewertet würden.

Unserem Vorschlag, auf Angaben über rechtskräftige Urteile in Ehesachen (§ 6) bei der Erhebung der Bevölkerungsstatistik zu verzichten, hat die Behörde für Inneres entgegengehalten, ohne diese Erhebung würde die Fortschreibung der Bevölkerung nach Familienstand unmöglich werden. Sie hat sich aber nicht dazu geäußert, weshalb für diesen Zweck die Erhebungsmerkmale Antragsteller oder Kläger, nichteinverständliche oder einverständliche Scheidung, Dauer der Trennung vor der Scheidung erforderlich sind.

Die Reaktion der Innenbehörde läßt befürchten, daß Hamburg diesem bedenklichen Gesetzentwurf im Bundesrat nicht entgegentreten wird.

4.3.3 Strafverfolgungsstatistikgesetz

Im April des Berichtsjahres hat der Bundesminister für Justiz einen Arbeitsentwurf für ein Strafverfolgungsstatistikgesetz vorgelegt, mit dem die bisher als „koordinierte Länderstatistik" erstellte Strafverfolgungsstatistik die dringend erforderliche gesetzliche Grundlage erhalten sollte.

Wir haben der Justizbehörde mitgeteilt, daß einzelne Vorschriften des Entwurfes unter datenschutzrechtlichen Gesichtspunkten kritisch zu beurteilen sind. Unsere Bedenken richten sich hauptsächlich gegen

- die vorgesehene Regelung für die Speicherung von Opferdaten,
- die Benutzung der Geschäftsnummer der aktenführenden Stelle als Hilfsmerkmal während der gesamten Aufbereitungsphase, wodurch ein jederzeitiger Rückgriff auf die jeweiligen Strafverfahrensakten erfolgen könnte,
- die mangelnden Abschottungsregelungen für die statistische von der sonstigen Datenverarbeitung,
- die mißverständlichen Bestimmungen über Zuständigkeit für die Datenschutzkontrolle.

Wie wir mittlerweile erfahren haben, ist mit einer Verabschiedung des Gesetzes durch den Bundestag in dieser Legislaturperiode nicht mehr zu rechnen, so daß die Strafverfolgungsstatistik — wie eine Reihe anderer Justizstatistiken — auch weiterhin ohne gesetzliche Grundlage durchgeführt werden wird.

4.3.4 Deutsch-deutsche Statistik

Die Herstellung der staatlichen Einheit zwischen der DDR und der Bundesrepublik hat auch Auswirkungen auf den Bereich der Statistik. Der Vertrag über die Herstellung der deutschen Einheit enthält Bestimmungen zur Überleitung von statistischen Rechtsvorschriften. Danach sollen das Bundesstatistikgesetz und nahezu sämtliche bundesstatistischen Einzelgesetze auch für das Gebiet der DDR gelten.

Problematisch ist, daß nach den Regelungen des Staatsvertrages die bisher bei Erhebungen in der DDR angefallenen Hilfsmerkmale, Ordnungsnummern und laufenden Nummern bis zum 31. Dezember 1994 weiterverwendet werden dürfen, wenn die statistische Aufbereitung und Auswertung des vorhandenen statistischen Materials noch nicht abgeschlossen worden ist. Damit dürfen bereits erhobene Daten der bisherigen DDR-Bürger auch dann weiterverarbeitet werden, wenn sie ohne Rechtsgrundlage erhoben und die Statistiken auch nicht fortgeführt werden sollen. Bedenkt man ferner, daß ein solches „Hilfsmerkmal" auch das bisher in der DDR gebräuchliche einheitliche Personenkennzeichen ist, mit dem diverse andere Dateien zu erschließen sind, muß diese Regelung als äußerst problematisch angesehen werden. Es ist nicht erkennbar, wie vor diesem Hintergrund das Statistikgeheimnis für die neuen Bürger der Bundesrepublik gewahrt werden soll.

4.4 Archivwesen

Im 7. Tätigkeitsbericht (4.4, S. 58) hatten wir von dem Entwurf eines Hamburgischen Archivgesetzes berichtet. Im Jahr darauf versandte das Staatsarchiv eine überarbeitete Fassung; ein weiteres Jahr später, im Juli 1990, folgte schließlich der Entwurf einer Senatsdrucksache. Ob das Gesetz allerdings noch in dieser Legislaturperiode verabschiedet werden kann, erscheint zweifelhaft.

Inhaltlich ist das Staatsarchiv vielen unserer Anregungen gefolgt. Angesichts des Rahmens, den die Systematik des Bundesarchivgesetzes und der Archivgesetze einzelner Bundesländer vorgeben, konnten wir uns auf die Kritik an unklaren und interpretationsbedürftigen Bestimmungen beschränken. Nach wie vor unvollkommen ist die Regelung von „Zwischenarchivgut". Es muß durch eine entsprechende Ergänzung des Gesetzes vermieden werden, daß eine Behörde dem Staatsarchiv Unterlagen zur Zwischenarchivierung überläßt, ohne daß dieses innerhalb einer vorgegebenen Zeit eine Aussonderung der archivwürdigen Teile vornehmen und die anderen — bei personenbezogenen Unterlagen zur Vernichtung — zurückgeben muß. Anderenfalls könnten durch die Zwischenarchivierung die Löschungsfristen des § 19 Absatz 3 HmbDSG unterlaufen werden. Nicht eindeutig ist ferner das Verhältnis von § 6 des Archivgesetzentwurfes („Auskunft und Gegendarstellung") zu § 18 HmbDSG („Auskunft"). Einerseits enthält § 6 ArchivGE für das Auskunfts- und Einsichtsrecht des Betroffenen bereichsspezifische Einschränkungen; andererseits erklärt die Gesetzesbegründung § 18 HmbDSG für „unberührt". Inzwischen hat das Staatsarchiv uns versichert, diese auch von ihm erkannten Unklarheiten im endgültigen Gesetzentwurf, zumindest in der Begründung, auszuräumen.

Insgesamt kann der Entwurf des Hamburgischen Archivgesetzes als ein weitgehend gelungener Versuch gewertet werden, die Belange des Datenschutzes mit den Interessen von Wissenschaft und Forschung zu versöhnen. Es kommt jetzt darauf an, daß dieser Ausgleich auch geltendes Recht wird.

4.5 Schulwesen

Seit unserem 3. (3.5.1, S. 36 f) und zuletzt in unserem 6. Tätigkeitsbericht (4.18, S. 117) wiesen wir auf die Notwendigkeit bereichsspezifischer Datenschutzbestimmungen für

das Schulwesen hin. Bisher hat es mehrere Entwürfe zur Ergänzung des Schulgesetzes gegeben, doch wird auch diese Legislaturperiode zu Ende gehen, ohne daß entsprechende Regelungen verabschiedet sein werden.

Inzwischen haben wir erfahren, daß in der Behörde für Schule, Jugend und Berufsbildung an einem neuen Referentenentwurf für die nächste Legislaturperiode gearbeitet wird. Wir haben der Behörde dazu das Gesetz der Freien Hansestadt Bremen zum Datenschutz im Schulwesen übersandt, das sich nicht mit einer eher allgemeinen Verordnungsermächtigung begnügt, sondern selbst die wichtigsten Regelungen über den Umfang der Datenverarbeitung in der Schulverwaltung trifft. Wir gehen davon aus, daß wir wie bisher von der Behörde für Schule, Jugend und Berufsbildung in die Erarbeitung der bereichsspezifischen Regelungen einbezogen werden. Wir würden es begrüßen, wenn möglichst bald für die betroffenen Eltern, Schüler und Lehrer transparente, normenklare Datenverarbeitungsbestimmungen in Kraft treten könnten.

4.6 Steuerwesen

4.6.1 Kontrollbefugnis des Hamburgischen Datenschutzbeauftragten im Bereich der Abgabenordnung

Über unsere Auseinandersetzungen mit der Finanzbehörde wegen der Frage, ob dem Datenschutzbeauftragten bei der Erfüllung seiner Kontrollaufgaben das Steuergeheimnis der Abgabenordnung (AO) entgegengehalten werden kann, haben wir mehrfach berichtet (1. TB, 6.2; 2. TB, 3.4.1.1; 3. TB, 3.3.1 und 3.3.2.1). Wir haben stets den Standpunkt vertreten, § 30 AO ist eine „andere Vorschrift über den Datenschutz" im Sinne von § 20 Absatz 1 Satz 1 HmbDSG a. F. bzw. § 23 Absatz 1 Satz 1 HmbDSG n. F., deren Einhaltung der Datenschutzbeauftragte nach dem erklärten Willen des Gesetzgebers kontrollieren soll. Die Finanzbehörde teilte zwar unsere Auffassung, der Datenschutzbeauftragte müsse die notwendigen Kontrollen lückenlos wahrnehmen können, hatte aber Bedenken gegen nicht auf den Einzelfall beschränkte Kontrollen. Sie bezweifelte, daß die mit Kontrollen im Steuerbereich zwangsläufig verbundene Offenbarung von Daten, die dem Steuergeheimnis unterliegen, durch § 30 Absatz 4 Nr. 2 AO i. V. m. § 20 HmbDSG gerechtfertigt sei. Zwar sei nach § 30 Absatz 4 Nr. 2 AO die Offenbarung von Daten dann zulässig, wenn sie durch ein Gesetz ausdrücklich zugelassen ist; dafür reiche jedoch ein Landesgesetz nicht aus, vielmehr müsse sich die Befugnis aus einem Bundesgesetz ergeben.

Obwohl im Bundesdatenschutzgesetz — jedenfalls für den Zuständigkeitsbereich des Bundesbeauftragten für den Datenschutz — eine entsprechende bundesgesetzliche Regelung vorhanden war, sah sich der Senat nicht in der Lage, das Problem der unterschiedlichen Rechtsauffassungen in Hamburg zu lösen. Er hielt eine Lösung durch den Bundesgesetzgeber für erforderlich. Ein Antrag des Senats zum Steuerbereinigungsgesetz 1985, nach dem im Anwendungsbereich der Abgabenordnung klargestellt werden sollte, daß den Datenschutzbeauftragten bei ihren Kontrollen das Steuergeheimnis nicht entgegengehalten werden dürfe, blieb jedoch erfolglos.

Jetzt ist diese Klarstellung endlich erfolgt. Im Rahmen des nun beschlossenen Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes wurde in § 24 Absatz 2 Satz 1 BDSG bestimmt: „Die Kontrolle des Bundesbeauftragten erstreckt sich auch auf personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis, insbesondere dem Steuergeheimnis nach § 30 AO, unterliegen". Zwar wird — gegen den mehrfach erklärten Widerstand der Datenschutzbeauftragten — auch in der nun beschlossenen Fassung des Bundesdatenschutzgesetzes in § 24 Absatz 2 Satz 4 die Befugnis des Bundesbeauftragten für den Datenschutz zur Kontrolle der Verarbeitung personenbezogener Daten in bestimmten Bereichen durch ein Widerspruchsrecht der Betroffenen begrenzt, dies gilt — entgegen der ursprünglichen Planung — ausdrücklich aber nicht im Bereich der Abgabenordnung.

Nun kann nicht mehr bestritten werden, daß auch für Steuerdaten die uneingeschränkte verfahrensmäßige Absicherung in Form einer jederzeit möglichen Datenschutzkontrolle gilt.

4.6.2 Nachtrag zum Fall „Zinsen aus Sparguthaben und Aufnahme von Ermittlungen durch die Steuerfahndung"

Im 8. Tätigkeitsbericht (3.6.1, S. 44 ff) haben wir über einen Fall berichtet, in dem die Steuerfahnung aufgrund einer im Landeskriminalblatt veröffentlichten Meldung über einen Einbruch in eine Etagenwohnung gegen die Bestohlenen ein Ermittlungsverfahren wegen Steuerhinterziehung eingeleitet hatte. Wir hatten uns mit der Frage auseinandergesetzt, unter welchen Voraussetzungen die Aufnahme von Ermittlungen durch die Steuerfahndung zulässig ist und waren zu folgendem Ergebnis gekommen: Sie ist zulässig, wenn aufgrund konkreter Momente des Einzelfalls oder relevanter allgemeiner Erfahrungen der Finanzämter über eine klar zu definierende Personengruppe die Möglichkeit objektiver Steuerverkürzung in Betracht kommt.

Es war nicht erkennbar, worin gerade in dem beschriebenen Einzelfall die „konkreten Merkmale" bestehen sollten, die die „Möglichkeit objektiver Steuerverkürzung in Betracht kommen" ließen, und zu welcher „besonderen Personengruppe, über die die Finanzbehörde spezielle, im Hinblick auf Steuerhinterziehung relevante allgemeine Erfahrungen hat", die Geschädigten gehören sollten. Deshalb haben wir keinen „hinreichenden Anlaß" für die Aufnahme der Ermittlungen gesehen, sondern darin einen Verstoß gegen den Grundsatz der Verhältnismäßigkeit erblickt und sie für nicht gerechtfertigt gehalten.

Die von uns um Stellungnahme gebetene Finanzbehörde teilt unsere Auffassung zu den Voraussetzungen für die Aufnahme von Ermittlungen durch die Steuerfahndung, soweit diese abstrakt herausgearbeitet wurden. Sie weist jedoch darauf hin, daß — entgegen unserer Auffassung — gerade in dem angesprochenen Fall sehr wohl „konkrete Merkmale" und „Erfahrungen hinsichtlich einer besonderen Personengruppe" vorlagen, die als Anlaß für die Aufnahme von Ermittlungen hinreichten: Die konkreten Merkmale ergaben sich aus der Höhe des Gesamtguthabens auf den gestohlenen Sparbüchern (ca. 90 000 DM), die auf steuerlich relevante Zinseinkünfte hindeuteten, und die Vermutung für die Möglichkeit einer Steuerverkürzung gründete sich auf die allgemeine Erfahrung der Steuerverwaltung, daß Zinseinkünfte — insbesondere aus höheren Sparguthaben — häufig nicht versteuert werden. Sparguthaben sind als Kapitalanlage wegen des niedrigen Zinssatzes an sich unwirtschaftlich, es sei denn, es wird auf ihre „Steuerfreiheit" spekuliert.

Die Finanzbehörde hat auf unsere Nachfrage weiter mitgeteilt, die Steuerfahndung werte weder das Landeskriminalblatt noch andere (öffentliche) Quellen routinemäßig aus. Es gäbe auch keine Kriterien speziell für die Aufnahme von Ermittlungen gegen durch Straftaten Geschädigte oder Inserenten, weil weder die einen noch die anderen eine irgendwie besonders geartete Gruppe von Steuerpflichtigen darstellten, von der vermutet werden müßte oder könnte, daß sie Steuern verkürze. Gegen diese Ausführungen der Finanzbehörde haben wir nichts einzuwenden.

Dennoch bleibt ein Aspekt des dargestellten Falles problematisch, auf den bisher noch nicht eingegangen wurde: Von dem Diebstahl der Sparbücher und der Höhe der Sparguthaben hatte die Steuerfahndungsstelle durch eine Veröffentlichung im Landeskriminalblatt Kenntnis erhalten, und es war zu klären, ob diese Dienststelle darauf in zulässiger Weise zurückgreifen darf.

Das Landeskriminalblatt wird von der Behörde für Inneres — Landeskriminalamt Hamburg — herausgegeben. Es erscheint einmal wöchentlich und ist Informationsmittel zur Ausschreibung von polizeilich interessierenden Sachverhalten und Informationen sowie Fahndungsmittel. Ausschreibungen im Landeskriminalblatt dienen

— der Fahndung nach Personen und Sachen,

— dem Erkennen von Tatzusammenhängen und der Zuordnung der von Wiederholungstätern begangenen Straftaten,

— der Ermittlung der Herkunft sichergestellter, vermutlich aus Straftaten stammender Gegenstände,

— der Übermittlung von Informationen über polizeilich interessierende Personen,

— der Ermittlung von Vermißten, der Identifizierung von unbekannten Toten und unbekannten hilflosen Personen,

— der Personenfeststellung.

Darüber hinaus dient das Blatt der Veröffentlichung polizeilicher Informationen über

— Praktiken und Tatausführungsmerkmale von Straftätern,

— Kriminalitätsentwicklungen,

— Entwicklungen auf dem Gebiet der Kriminaltechnik und -taktik,

— polizeiliche Organisationen und Einrichtungen.

Es trägt auf der Vorderseite den Aufdruck: „Sicher aufbewahren! Weitergabe, Abdruck und Auswertung außerhalb des Bezieherkreises auch auszugsweise nicht gestattet."

Als Empfänger des Landeskriminalblattes wurden uns öffentliche Stellen benannt, für deren Aufgabenerfüllung der Bezug erforderlich erscheint. Jede Erweiterung des Empfängerkreises geschieht nach Aussage der Behörde für Inneres aufgrund einer Einzelfallprüfung unter Berücksichtigung der Belange des Datenschutzes. Die Steuerfahndung gehört(e) nicht zu den berechtigten Empfängern.

Das Zollfahndungsamt Hamburg, das zu den regelmäßigen Beziehern des Landeskriminalblattes gehört, hatte jeweils ein Exemplar an die Steuerfahndungsstelle weitergeleitet. Dies entsprach offenbar einer eingefahrenen Praxis des Zollfahndungsamtes, deren Ursprung nicht mehr festzustellen ist und die dem Landeskriminalamt erst aufgrund unserer Nachfragen bekannt wurde. Das Landeskriminalamt hat dem Zollfahndungsamt die Weitergabe des Landeskriminalblattes an die Steuerfahndungsstelle unverzüglich untersagt.

Da das Zollfahnungsamt eine Behörde des Bundes ist, die der Kontrolle des Bundesbeauftragten für den Datenschutz unterliegt, haben wir diesem die Angelegenheit mit der Bitte um Prüfung unterbreitet. Als Ergebnis bleibt festzuhalten, daß nicht nur der Bundesbeauftragte für den Datenschutz sondern auch der Bundesminister der Finanzen unsere Auffassung teilt, daß die Übermittlung des Landeskriminalblattes durch das Zollfahndungsamt an die Steuerfahndungsstelle unzulässig war. Der Minister hat das Zollfahndungsamt Hamburg angewiesen, derartige Weiterleitungen zu unterlassen.

Danach muß jedenfalls festgestellt werden, daß die Steuerfahndung ihre Ermittlungen gegen die Betroffenen aufgrund von Kenntnissen aufgenommen hat, die sie durch eine unzulässige Datenübermittlung erlangt hat.

4.7 Wissenschaft und Forschung

4.7.1 Genomanalysen

Im letzten Tätigkeitsbereicht (8. TB, 3.11.1.1, S. 98) hatten wir die datenschutzrechtlichen Gefahren von Genomanalysen bei Strafverfahren, im Arbeitsverhältnis und für Versicherungen aufgezeigt und für den sogenannten genetischen Fingerabdruck eine gesetzliche Grundlage gefordert. Im Januar leitete uns die Justizbehörde einen „Diskussionsentwurf" des Bundesjustizministeriums zur Ergänzung der Strafprozeßordnung zu. Die neuen §§ 81 e und f StPO sollen den genetischen Fingerabdruck zugleich legitimieren und datenschutzgerecht eingrenzen. Danach muß die — erzwingbare — genetische Untersuchung von Beschuldigten zur Identifizierung von Spurenmaterial „erforderlich" sein und sich auf die sogenannten nicht-codierenden Teile der Erbsubstanz beschränken, also Bereiche ausschließen, die Aufschluß über Erbanlagen, Krankheiten oder persönliche Merkmale geben können. Nach „äußerlich sichtbaren Körpermerkmalen" sollen allerdings Tatspuren genetisch analysiert werden dürfen. Der genetische Fingerabdruck muß nach dem Entwurf durch einen Richter angeordnet werden, der auch die genetische Methode zu bezeichnen und die mit der Untersu-

chung zu beauftragende Stelle zu bestimmen hat. Diese soll Amtsträger oder öffentlich bestellte/r Sachverständige/r sein. Das untersuchte Zellen- und Spurenmaterial sowie zusätzlich alle Analyseunterlagen von untersuchten Dritten dürfen nur für Zwecke des Strafverfahrens verwendet werden und sind so bald wie möglich zu vernichten.

In unserer Stellungnahme zu dem Entwurf sind wir auf folgende Punkte eingegangen: Die „Erforderlichkeit" des genetischen Fingerabdrucks läßt offen, ob er nur dann angeordnet werden darf, wenn die herkömmlichen Methoden eine zuverlässige Identifizierung von Spurenmaterial nicht zulassen. Hier sollte eine klare Subsidiarität der Genomanalyse festgeschrieben werden.

Für äußerst bedenklich halten wir die Ermächtigung, Spurenmaterial nach „äußerlich sichtbaren Körpermerkmalen" zu untersuchen. Die Mißbrauchgefahr wird durch diesen Zugriff auf codierende Genombereiche sprunghaft erhöht: Jedes äußerliche Merkmal benötigt eine andere Gen-Sonde; die Begrenzung auf das eine Verfahren des genetischen Fingerabdrucks würde — weitgehend unkontrollierbar — aufgegeben. Darüber hinaus ist auch die mögliche Verbindung von „äußerlichen Merkmalen" zu Persönlichkeits-, Krankheits-, Rassemerkmalen bzw. zu entsprechenden Vorurteilen nicht zu leugnen. Um hier den Anfängen zu wehren, muß eine Genomanalyse im Strafverfahren unbedingt auf die nicht-codierenden Teile beschränkt bleiben.

Die dem Entwurf entsprechende derzeitige Praxis, daß Polizeidienststellen („Amtsträger") die Analysen vornehmen, sollte nach unserer Auffassung überdacht werden. Um das Interesse der Polizei an möglichst vielen Informationen zu einem Verdächtigen nicht zum Motiv für eine mißbräuchliche Ausweitung des Untersuchungsumfangs werden zu lassen, schlagen wir eine funktionale Trennung von Strafverfolgung und Genomanalyse vor: Anstelle der Polizei sollten andere staatliche Einrichtungen, etwa die Gerichtsmedizinischen Institute, mit den genetischen Untersuchungen betraut werden. Dabei könnte die Zellprobe dem Institut anonym, d.h. ohne Namen, Aktenzeichen und Akte, sondern nur mit einer Code-Nummer versehen, übermittelt werden. Bei den Untersuchungslabors sollten weder Probenreste noch sonstige Unterlagen verbleiben.

Die Zweckbindung der Untersuchungsunterlagen an das konkrete Strafverfahren sollte nicht nur für Dritte (Zeugen z.B.), sondern auch für den Beschuldigten gelten. Die Ergebnisse der genetischen Untersuchung in Form von Strich-Mustern dürfen nicht auf Vorrat für zukünftige Strafverfolgungen oder gar für präventivpolizeiliche Zwecke gespeichert werden. Andernfalls würde die geforderte Subsidiarität und der Ausnahme-Charakter des genetischen Fingerabdrucks unterlaufen.

Zusätzlich zu den im „Diskussionsentwurf" vorgesehenen Sicherheitsmaßnahmen schlagen wir folgende Regelungen vor:

— eine Strafandrohung für Mißbrauch der Genomanalysen, insbesondere für die Anwendung von Gen-Sonden für den codierenden Teil der Erbsubstanz;

— ein Beschlagnahmeverbot für genomanalytische Befundunterlagen (Ergänzung von § 97 StPO);

— ein Verwertungsverbot für rechtswidrig erhobene genomanalytische Befunde.

In einem jüngst veröffentlichten Grundsatzurteil hat der Bundesgerichtshof den genetischen Fingerabdruck schon aufgrund der bestehenden Rechtslage für zulässig erklärt (Az 5 StR 145/90). Aber auch er machte dies abhängig von der Verhältnismäßigkeit im konkreten Fall und von einer Beschränkung der Untersuchung auf den nicht-codierenden Teil der Erbsubstanz.

4.7.2 Forschungsprojekt „Polizei-Akzeptanz in Altona"

Die neueingerichtete „kriminologische Forschungsgruppe im Landeskriminalamt" befaßte uns mit einer — inzwischen durchgeführten — Bevölkerungsbefragung im Stadtteil Altona. Ziel der Untersuchung war es, Einstellung und Verhalten der Bürger gegenüber Straftaten und Polizei zu erforschen. Das datenschutzrechtliche Problem

lag in einer möglichen Reidentifizierbarkeit der befragten Personen. Der sehr umfangreiche Fragebogen enthielt nämlich einerseits detaillierte Fragen zur eigenen Erfahrung mit Kriminalität, zum Anzeigeverhalten, zur persönlichen Meinung über die Polizei, zum subjektiven Sicherheitsgefühl und andererseits Fragen zu Alter, Geschlecht, Haushaltsgröße, Staatsangehörigkeit, Bildung und Beruf. Es mußte vermieden werden, daß die Kriminalpolizei durch die — unter anderen Vorzeichen gegebenen — Antworten erstmals von Straftaten Kenntnis erhielt, zu deren Verfolgung sie gesetzlich verpflichtet ist, und sich um Nachforschungen bei Opfern oder möglichen Zeugen bemühte. Eine Reidentifikation in diesem Rahmen hätte auch Einstellungen und politische Meinungen der Befragten offenbart.

Dies wurde jedoch zum einen durch die organisatorische und funktionelle Selbständigkeit der Forschungsgruppe ausgeschlossen. Sie unterliegt nicht dem zur Strafverfolgung verpflichtenden Legalitätsprinzip und gibt keinerlei personenbezogene oder personenbeziehbare Daten an andere Polizeidienststellen weiter oder zum Abruf frei. Zum anderen überzeugten wir uns davon, daß eine — für die Untersuchung nicht interessante — Reidentifikation von Tatopfern einen sehr hohen Aufwand erfordern würde (manuelle Durchsicht von über 16 000 Anzeigen bei 5 Revierwachen) und allenfalls bei angezeigten Straftaten möglich wäre. Angesichts der Tatsache, daß in dem mit uns abgestimmten Anschreiben an die Bürger auch ausdrücklich auf die Freiwilligkeit der Teilnahme an der Fragebogenaktion hingewiesen wurde, hatten wir gegen die Untersuchung im Ergebnis keine Bedenken. Nach Auskunft der Leiterin der Forschungsgruppe gab es während und nach der Befragungsaktion keinerlei Beschwerden hinsichtlich datenschutzrechtlicher Belange. Auch uns erreichten zu dieser Aktion keine Eingaben.

4.7.3 Forschungsprojekt „Krankenstand beim Heimpersonal"

Die Behörde für Arbeit, Gesundheit und Soziales führte Ende letzten/Anfang diesen Jahres eine Untersuchung zum Krankenstand in den staatlichen Heimen durch, um Gründe für die hohe Ausfallquote zu ermitteln. Zu diesem Projekt erhielten wir eine kritische Eingabe, die sich im Ergebnis aber als unbegründet erwies.

Kernstück der Untersuchung waren zwei Fragebögen für jeden Krankheitsfall: einer, der von der Stationsleitung (STL) nur gemeinsam mit der Pflegekraft auszufüllen war, wenn der/die Betroffene wieder im Dienst war, und ein zweiter Fragebogen, den die Oberschwester/der Oberpfleger (OSOP) ausfüllte. Im STL-Bogen wurde nach Alter, Geschlecht, Familienstand, Kinderzahl, nach Ausbildungen und Berufstätigkeiten sowie nach Krankheit und Krankmelde-Daten gefragt — mit der hervorgehobenen Bemerkung „Bitte nur festhalten, was die/der Erkrankte mitteilt und alle wissen dürfen!". Schließlich sollte auch ein möglicher Zusammenhang mit einer „Lebenskrise" (ja/nein) angegeben werden. Der OSOP-Fragebogen ermittelte vor allem die zeitliche Verbindung der Krankmeldung zu Wochenenden, Urlaub, Ende der Lohnfortzahlung usw. sowie den Eindruck von Unter- oder Überforderung.

Da diese Untersuchung über die übliche Anwesenheitskontrolle des Dienstherrn hinausging und auch nicht-offenkundige, sehr sensible Daten erhob, war vor allem die Freiwilligkeit der Teilnahme und soweit wie möglich die Anonymität sicherzustellen. Der mit der Untersuchung beauftragte Diplom-Psychologe erläuterte uns das Verfahren: Danach wurde vor Beginn der jeweils 3-monatigen Aktion in einer Stationsversammlung aller Mitarbeiter die Methode erklärt und ausdrücklich auf die Freiwilligkeit hingewiesen. Jede Pflegekraft erhielt darüber hinaus ein Merkblatt mit dem Hinweis, „daß sämtliche im Rahmen dieser Untersuchung gemachten Angaben anonym bleiben. Die Teilnahme an der Untersuchung ist freiwillig". Die Pflegekräfte konnten zudem selbst darüber entscheiden, ob zuerst der OSOP- oder zuerst der STL-Bogen ausgefüllt wurde. Nach der vollständigen Beantwortung wurde ein Kontrollabschnitt mit dem Namen der Pflegekraft abgetrennt und vernichtet bzw. übergeben. Die so anonymisierten Fragebögen erreichten den Untersuchungsleiter per Post in einem verschlossenen Umschlag ohne Absender.

In unserer abschließenden Stellungnahme zu dieser Untersuchung kritisierten wir, daß nicht von vornherein die Reihenfolge der Beantwortung festgelegt wurde: Nur wenn zuerst der OSOP-Bogen ausgefüllt wurde, war sichergestellt, daß die Pflegekraft — bei der dann nachfolgenden Beantwortung des STL-Bogens zusammen mit der Stationsleitung — Einblick und Korrekturmöglichkeit hinsichtlich aller Angaben hatte und die Oberschwester nur „ihren" Fragebogen einsehen konnte. Sowohl der Untersuchungsleiter als auch der zuständige Amtsleiter versicherten uns allerdings, daß die Pflegekräfte auf diese Problematik hingewiesen wurden. Die Prüfung beim Untersuchungsleiter ergab, daß alle Kontrollabschnitte abgetrennt waren und daß viele Fragebögen bei Einzelangaben Leerstellen aufwiesen, was darauf hinweist, daß die Pflegekräfte tatsächlich — auch subjektiv — freiwillig geantwortet hatten. Auch wenn ein STL-Fragebogen die Angabe „zur Zeit noch krank" enthielt — also die geforderte Zusammenarbeit mit der erkrankten Pflegekraft bei der Beantwortung zumindest unwahrscheinlich war —, sahen wir angesichts der intensiven Aufklärung und der überprüften Sicherungsmaßnahmen letztlich keinen Anlaß zu grundsätzlichen Beanstandungen.

4.7.4 Datenbank eines Prüfungsamtes

Das Prüfungsamt eines Fachbereichs der Universität meldete zum Dateiregister vier Dateien an („Adressen", „Prüfungen", „Diplomarbeit", „Prüfer"), die auf einem PC in einer Datenbank verarbeitet werden sollen. Löschungsfristen sind in dem System nicht vorgesehen. Wir haben gegen das Vorhaben eine Reihe von Bedenken geäußert:

Ohne eine Abschottung der vier Dateien untereinander und ohne die Löschung alter Daten wäre es möglich, langfristige Prüferprofile mit Prüfungszahlen, Prüfterminen, ausgegebenen Themen, Benotungen, Honoraren usw. zu erstellen. Prüfer- und Gutachternamen dürfen deswegen außer in der „Prüferdatei" nicht als Suchbegriff genutzt werden können.

Der völlige Verzicht auf Löschungsfristen widerspricht § 19 Absatz 3 HmbDSG. Er ist auch nicht erforderlich. Nach erfolgter Prüfung, Aushändigung der Urkunden und Honorarabrechnung reichen für spätere Nachfragen ein Hinweis auf die Prüfungsakte mit dem Namen des Prüflings als Suchbegriff, eventuell weitere Hinweise auf Prüfungsakten mit dem Namen des Gutachters/Prüfers als Suchbegriff aus. Für die übrigen Daten erscheint eine Löschungsfrist von einem Jahr nach Abschluß der Prüfung angemessen.

Da die Datenbank unterschiedlichen Zwecken dient, sollten die verschiedenen Funktionen (z.B. Terminüberwachung, Abrechnung des Prüferhonorars) unterschiedlichen Zugriffsberechtigungen, gegebenenfalls unterschiedlichen Sachbearbeitern zugeordnet werden.

Schließlich sind an die Sicherheit der Prüfungsdaten angemessene Anforderungen zu stellen. Es muß technisch ausgeschlossen sein, daß durch die mißbräuchliche Verwendung von PC-Dienstprogrammen ein Unbefugter unter Umgehung des Datenbankverwaltungssystems auf das Betriebssystem zugreifen und so z.B. unbemerkt, weil nicht protokolliert, Zensuren ändern kann. Sollte eine entsprechende Sicherungssoftware für den in Aussicht genommenen PC-Typ nicht zur Verfügung stehen, muß eine andere Hardware eingesetzt werden.

Da die geplante Datenbank für andere Prüfungsämter der Universität möglicherweise Vorbildfunktion hat, haben wir die Hochschulverwaltung nicht nur um eine Stellungnahme gebeten, sondern uns auch eine technische Prüfung vor Ort vorbehalten.

4.8 Bauwesen

4.8.1 Hamburgisches Vermessungsgesetz

Hamburg ist bereits seit einigen Jahren das einzige Bundesland ohne Vermessungsgesetz. Ein solches Gesetz ist seit langem überfällig, da § 2 Absatz 2 Grundbuchordnung, § 43 Grundbuchverfügung und das Bodenschätzungsgesetz als Rechtsgrund-

lage für das Liegenschaftskataster, das eine Vielzahl personenbezogener Daten enthält, den verfassungsrechtlichen Vorgaben nicht genügen (vgl. 4. TB, 4.5.3, S. 52). Mit dem Entwurf für ein Gesetz über das Vermessungswesen (VermG), der uns im Berichtszeitraum zugeleitet wurde, soll diese Lücke nunmehr geschlossen werden.

Mit dem Gesetzesentwurf wird angestrebt, abschließend die Aufgaben des Liegenschaftskatasters zu definieren, die im Liegenschaftskataster enthaltenen Daten aufzuführen und festzulegen, wer welche Daten erheben und übermitteln darf. Dabei ist es die ausdrückliche Intention der Verfasser, daß „datenschutzrechtliche Hindernisse für die vereinfachte Weitergabe von personenbezogenen Daten an andere, insbesondere planende Dienststellen, ebenso ausgeräumt werden wie Hindernisse, die bisher der Zusammenfassung flächenbezogener Datensammlungen anderer Behörden mit dem Liegenschaftkataster zu einer einheitlichen Grundstücksdatenbank entgegenstanden". Da diese Absicht auch inhaltlich in dem Entwurf ihren Niederschlag gefunden hatte, mußten wir erhebliche Bedenken geltend machen. Aus datenschutzrechtlicher Sicht darf es nicht darum gehen, wie in der Senatsdrucksache formuliert, verfassungsrechtliche Hindernisse, die zum Schutz der Betroffenen bestehen, lediglich durch den Gesetzgeber beseitigen zu lassen, sondern es muß versucht werden, das informationelle Selbstbestimmungsrecht einer Vielzahl von Einzelnen mit den Interessen der Verwaltung zu einem vertretbaren Ausgleich zu bringen. Dies ist mit dem bisherigen Entwurf leider noch nicht gelungen.

Er zielt vielmehr darauf ab, mit der Einrichtung einer „Raumbezogenen Informationsbasis" einen über das bisherige Liegenschaftskataster hinausgehenden, umfangreichen Datenbestand zu schaffen, der sämtliche Daten zweckunabhängig umfaßt, die in der Verwaltung im Zusammenhang mit Grundstücken erhoben werden. So soll die Informationsbasis umfangreiche Auskunft darüber geben, ob der Grundstückseigentümer Bindungen des Denkmalschutzes beachten muß, durch Baulasten begünstigt oder belastet ist, polizeirechtlich für Altlasten verantwortlich ist, Anliegerbeiträge noch zahlen muß. Allerdings soll im Gesetz nicht geregelt werden, ob die Daten erhebenden Fachverwaltungen oder die Vermessungsämter als speichernde Stellen für die Korrektheit der jeweiligen Daten verantwortlich sind. Dies ist jedoch für die Realisierung der Rechte der Betroffenen auf Auskunft, Berichtigung, Sperrung und Löschung (§§ 18, 19 HmbDSG) von nicht unerheblicher Bedeutung.

Für besonders bedenklich halten wir die geplante Einführung einer Sondermeldepflicht für Grundstückseigentümer, nach der diese verpflichtet sind, auch jede Adreßänderung anzuzeigen. Dies ist angesichts der Pflichten nach dem Hamburgischen Meldegesetz und nach der Grundbuchordnung als ein unverhältnismäßiger Eingriff in die Rechtsposition der Betroffenen abzulehnen.

Der Entwurf vermeidet es, die „Informationsbeziehungen" zwischen der „Raumbezogenen Informationsbasis" und ihrer Nutznießer normenklar zu regeln, sondern beläßt es bei unübersichtlichen und zum Teil sehr weit gefaßten Formulierungen. Der Senat soll darüber hinaus ermächtigt werden, die „Raumbezogene Informationsbasis" um weitere Dateien zu ergänzen. Hierdurch soll ein System der schrankenlosen Datenverarbeitung aufgebaut werden, in dem ausschließlich die Interessen der Verwaltung berücksichtigt werden. Es ist nicht erkennbar, daß den schutzwürdigen Belangen der Betroffenen irgendeine Bedeutung zugemessen wurde. So soll sämtlichen Behörden, die Daten ihres Zuständigkeitsbereichs in der „Raumbezogenen Informationsbasis" gespeichert haben, ein Online-Zugriff zugebilligt werden. Damit entfällt eine Prüfung, ob eine Übermittlung im Einzelfall zulässig ist, da die abrufende Behörde beim Online-Anschluß mit den Daten faktisch in der Weise arbeitet, als ob es sich um eigene Daten handeln würde. Auch der Bürger kann nicht mehr erkennen, wer, was wann und bei welcher Gelegenheit über ihn in Erfahrung gebracht hat. Es ist schon jetzt darauf hinzuweisen, daß auch die Polizei im Rahmen der Behördenabstimmung Interesse an einem Online-Anschluß bekundet hat. Dies muß entschieden abgelehnt werden, denn dafür ist weder eine Notwendigkeit dargelegt noch sonst ersichtlich.

Angesichts der beschriebenen Mängel des Gesetzesentwurfs gehen wir davon aus, daß demnächst ein überarbeiteter Entwurf den beteiligten Behörden übersandt wird. Es muß allerdings bezweifelt werden, daß das Vermessungsgesetz noch in dieser Legislaturperiode verabschiedet werden kann, so daß das anfangs beschriebene Defizit voraussichtlich noch einige Zeit bestehen wird.

4.8.2 Verfahren zur Erhebung der Fehlbelegungsabgabe

Nach langer kontroverser Diskussion über den Nutzen von Fehlbelegungsabgaben ist im Dezember 1989 das Hamburgische Gesetz über den Abbau der Fehlsubventionierung im Wohnungswesen (HmbAFWoG) als gesetzliche Grundlage für die Erhebung dieser Abgabe beschlossen worden. Mit der Durchführung des Erhebungsverfahrens wurde die Mietausgleichszentrale (MAZ) als neu geschaffene Abteilung der Hamburgischen Wohnungsbaukreditanstalt (WK) beauftragt. Der Hamburgische Datenschutzbeauftragte ist weder bei der Behördenabstimmung zum HmbAFWoG noch — trotz mehrfacher Aufforderung — bei der Planung des Verfahrens selbst informiert worden und konnte deshalb seine Vorschläge nicht rechtzeitig einbringen.

4.8.2.1 Durchführung des Verfahrens

Das Verfahren zur Erhebung der Abgabe gliedert sich in drei Hauptphasen: Aufbau einer aktuellen Wohnungsinhaberdatei, Erhebung der Miet- und Einkommensdaten sowie eine automationsgestützte Berechnung und Einziehung der Fehlbelegungsabgabe. Die Erhebung der Wohnungsinhaberdaten soll bis November 1990 abgeschlossen sein, so daß wir derzeit nur zu den ersten beiden Hauptphasen Stellung nehmen können.

— Der Aufbau einer aktuellen Wohnungsinhaberdatei erfolgte durch Abgleich der WK-eigenen Datei über geförderte Wohnungseinheiten mit der seit Jahren existierenden und nun doch noch benötigten Wohnraumdatei (vgl. 4. TB, 4.5.2, S. 49 ff und 7. TB, 4.8.1, S. 66 ff). Dieser Datenbestand wurde schließlich noch um Adressen aus Großraumsiedlungen gekürzt, deren Mieter nicht zur Fehlbelegungsabgabe herangezogen werden. Da nach § 4 Melderegisterauskunftsverordnung vorgesehen ist, daß die Wohnraumdatei von den einzelnen Bezirksämtern regelmäßig auf der Basis des Melderegisters aktualisiert wird, hätte erwartet werden können, daß die Wohnungsinhaberdatei zum Anschreiben der Mieter einigermaßen korrekt ist. Da jedoch dieser Datenbestand einige Mängel aufwies, versucht die Wohnungsbaukreditanstalt nun, nicht zustellbare Anschreiben durch entsprechende Auskünfte beim Vermieter oder bei der Meldebehörde zu korrigieren.

  Gegenüber der Wohnungsbaukreditanstalt ist der Vermieter zwar auskunftsberechtigt, aber nicht auskunftspflichtig. Die Auskunftspflicht kann nicht nach § 2 Absatz 3 Wohnungsbindungsgesetz (WoBindG) abgeleitet werden, wonach Vermieter und Inhaber einer öffentlich geförderten Wohnung Auskunft erteilen müssen, soweit dies zur Sicherung der Zweckbestimmung von Wohnungen nach dem Wohnungsbindungsgesetz erforderlich ist. Das Verfahren zur Erhebung der Fehlbelegungsabgabe dient aber gerade nicht der Sicherstellung der Zweckbestimmung von Wohnungen, sondern geht umgekehrt von der Fehlbelegung aus.

  Nun versucht die Wohnungsbaukreditanstalt, fehlende Informationen über Wohnungsinhaber von geförderten Wohnungen über eine Melderegisterauskunft zu erhalten. Vom Bezirksamt Eimsbüttel wurden Bedenken hinsichtlich solcher Melderegisterauskünfte geäußert, die sich auf sämtliche unter einer Adresse gemeldeten Personen beziehen. Insbesondere in Hochhäusern, in denen nicht immer alle Wohnungen öffentlich gefördert sind, ist die Melderegisterauskunft über sämtliche Hausbewohner ohne Angabe der Etage weder rechtmäßig noch dazu geeignet, den aktuellen Wohnungsinhaber einer geförderten Wohnung zu ermitteln. Diese Bedenken werden von uns geteilt. Falls die MAZ ihr Standardanschreiben an sämtliche Mieter schicken würde, sind schutzwürdige Belange derjenigen Mieter beeinträchtigt, die nicht in einer geförderten Wohnung wohnen, sich aber dennoch zum Ausfül-

len des Erhebungsformulars gezwungen sehen, um einen Bescheid über die Fehlbelegungsabgabe zu entgehen.

Um die aufgezeigten rechtlichen Unzulänglichkeiten zu vermeiden, wäre es notwendig gewesen, Regelungen zur Auskunftspflicht der Vermieter in das HmbAFWoG mit aufzunehmen.

— In den Erhebungsbögen zur Ermittlung der Miet- und Einkommensdaten werden Empfänger von Sozialhilfe, Wohngeld, Arbeitslosenhilfe und Leistungen nach dem Bundesversorgungsgesetz, die von der Fehlbelegungsabgabe befreit sind, aufgefordert, der MAZ vollständige Bewilligungsbescheide vorzulegen. Dies ist nach unserer Auffassung nicht notwendig. Vielmehr dürfte eine einfache Bescheinigung über den Erhalt der Leistungen ausreichen. Eine Verpflichtung der Mieter zur Vorlage der Bewilligungsbescheide wäre unzulässig, da diese gezwungen wären, sie betreffende Sozialdaten an einen Unbefugten zu offenbaren. Die Wohnungsbaukreditanstalt hat sich unserer Auffassung angeschlossen. Die Sachbearbeiter der MAZ wurden angewiesen, die persönlich erscheinenden Wohnungsinhaber auf die Möglichkeit einer einfachen Bescheinigung hinzuweisen. Per Post eingehende Bescheide sollen auf nicht erforderliche Daten durchgesehen und in entsprechendem Umfang „geweißt" werden. Weiterhin haben wir angeregt, die Sozialbehörde und das Arbeitsamt zu bitten, Vordrucke für eine einfache Bescheinigung vorzuhalten. Diese eher umständliche Prozedur hätte vermieden werden können, wenn das Verfahren rechtzeitig mit uns abgestimmt worden wäre.

4.8.2.2 Kontrollzuständigkeit des Hamburgischen Datenschutzbeauftragten

Im Anschluß an das Gesetzgebungsverfahren hat der Senat der Hamburgischen Wohnungsbaukreditanstalt die Erhebung der Fehlbelegungsabgabe durch Zuständigkeitsanordnung übertragen. Da diese Anstalt ein öffentlich-rechtliches Kreditinstitut ist, sind auf sie im Rahmen ihrer kreditwirtschaftlichen Tätigkeit kraft ausdrücklicher Vorschrift des § 2 Absatz 3 HmbDSG nicht die Vorschriften des Hamburgischen Datenschutzgesetzes, sondern die für privatrechtliche Kreditinstitute geltenden Vorschriften des Bundesdatenschutzgesetzes anzuwenden. Dies hat zur Folge, daß die Datenverarbeitung zur Abwicklung von Kreditgeschäften auch bei öffentlich-rechtlichen Kreditinstituten nicht der Kontrolle durch den Hamburgischen Datenschutzbeauftragten gemäß § 23 Absatz 1 HmbDSG, sondern nur den geringeren Kontrollmöglichkeiten der Aufsichtsbehörde unterliegt. Mit dieser Gleichstellung sollen für öffentlich-rechtliche Kreditinstitute Wettbewerbsnachteile vermieden werden.

Die Wohnungsbaukreditanstalt vertritt die Auffassung, daß auch die Mietausgleichszentrale als eine unselbständige Abteilung bei der Erhebung der Fehlbelegungsabgabe vom Privileg des § 2 Absatz 3 HmbDSG erfaßt sei. Dem haben wir widersprochen. Die Erhebung der Fehlbelegungsabgabe liegt nicht im Rahmen der kreditwirtschaftlichen Tätigkeit der Anstalt. Vielmehr handelt es sich um eine normale Verwaltungstätigkeit, die ebenso von der Baubehörde oder etwa von den Bezirksämtern wahrgenommen werden könnte. Wir haben deshalb die Zuständigkeit des Hamburgischen Datenschutzbeauftragten für gegeben erachtet und die für die Fachaufsicht über die Wohnungsbaukreditanstalt zuständige Baubehörde gebeten, sicherzustellen, daß die von uns geplante Prüfung der technisch-organisatorischen Maßnahmen zur Datensicherheit stattfinden kann. Dem hat die Baubehörde, die unsere Auffassung teilt, entsprochen. Da die Wohnungsbaukreditanstalt an ihrer Auffassung festhält, mündet der Konflikt möglicherweise in ein Verfahren der förmlichen Beanstandung.

4.9 Einwohnerwesen

4.9.1 Novellierung des Melderechtsrahmengesetzes

Im 7. Tätigkeitsbericht (4.10.4, S. 82 ff.) haben wir über die Absicht berichtet, das Melderechtsrahmengesetz zu novellieren. Der Gesetzentwurf ist zwar inzwischen in den Deutschen Bundestag eingebracht worden, bei Redaktionsschluß dieses Berichts ließ

sich allerdings noch nicht absehen, ob er noch in dieser Legislaturperiode verabschiedet werden kann. Wir haben im Gesetzgebungsverfahren insbesondere eine Änderung von § 16 des Entwurfs gefordert, wonach an den Meldepflichten beim Aufenthalt im Hotel oder im Krankenhaus festgehalten werden soll.

Zweck der allgemeinen Meldepflicht ist es, die Identität der Einwohner und deren Wohnungen festzustellen und diese Basisinformation für die Bewältigung einer Vielzahl von Verwaltungsaufgaben zur Verfügung zu stellen. Bei einem kurzfristigen Aufenthalt in einem Hotel oder Krankenhaus entfällt dieser Zweck. Lediglich die Polizei hat ein Interesse an der Feststellung dieser Tatsachen. Schon deshalb paßt die Hotel- und Krankenhausmeldepflicht nicht in die Systematik des Melderechts, es handelt sich vielmehr um materielles Polizeirecht.

Polizeiliche Datenverarbeitung setzt aber voraus, daß Gefahren abgewendet oder Straftaten verfolgt bzw. verhütet werden sollen. Hotelgäste und Krankenhauspatienten können jedoch nicht schlechthin als Gefahrenquellen oder (potentielle) Straftäter angesehen werden. Vielmehr handelt es sich im Regelfall um Bürger, die ein Recht darauf haben, von polizeilichen Ausforschungen unbehelligt zu bleiben. Schon deshalb greift eine allgemeine Hotel- und Krankenhausmeldepflicht unverhältnismäßig tief in das informationelle Selbstbestimmungsrecht der Betroffenen ein.

Bei den Beratungen im Bundesrat war jedoch bisher keine Bereitschaft der Länder festzustellen, diese Meldepflichten abzuschaffen oder auch nur wirksam einzuschränken.

4.9.2 Automation des Meldewesens in Hamburg

Die schon im 3. Tätigkeitsbericht (3.7.1.1, S. 48 ff.) ausführlich beschriebene Automation des Meldewesens steht vor ihrem Abschluß. Die bezirklichen Meldedienststellen verfügen über ein modernes Dialogverfahren, mit dem sie die bei An- und Abmeldungen erforderlichen Änderungen im einheitlich geführten automatisierten Meldedatenbestand vornehmen können. Melderegisterauskünfte an Privatpersonen und Übermittlungen von Meldedaten an Behörden aus dem gesamten Datenbestand können bisher allerdings nur vom Einwohnerzentralamt als zentrale Meldestelle aufgrund der manuellen Einwohnerkartei vorgenommen werden.

Während der Beratung des Hamburgischen Meldegesetzes von 1986, das die Grundlage für die Automation darstellen sollte, sind Datenschutzgesichtspunkte noch besonders betont worden. Inzwischen tritt der Aspekt der Rationalisierung immer deutlicher hervor. Stelleneinsparungen waren von vornherein ein besonders wichtiges Ziel der Automation. Allerdings wurden vornehmlich im Bereich des Einwohnerzentralamts Stellen gestrichen, obwohl hier noch kein Dialogverfahren zur Pflege des Datenbestandes und zur Erteilung von Auskünften zur Verfügung stand. Dies hat zur Folge, daß wichtige Aufgaben der zentralen Meldebehörde nicht mehr so wahrgenommen werden können, wie es eigentlich erforderlich wäre: auch einfache Melderegisterauskünfte haben inzwischen eine Bearbeitungszeit von mehr als einem Monat, die Nacherfassung von Nebenwohnungen in den automatisierten Bestand mußte immer wieder zurückgestellt werden, das Einwohnerzentralamt beabsichtigt sogar, die Pflege der manuellen Einwohnerkartei ganz einzustellen. Das Ungleichgewicht zwischen der Arbeitsbelastung im Einwohnerzentralamt und den bezirklichen Meldebehörden führte bereits im Sommer 1989 zu Überlegungen, Aufgaben von der zentralen Meldebehörde auf die örtlichen Meldedienststellen zu verlagern. Insbesondere sollen Melderegisterauskünfte nicht mehr aus der manuellen Einwohnerkartei beim Einwohnerzentralamt, sondern aus den automatisierten Beständen der Bezirke erteilt werden. Über diese Planungen sind wir frühzeitig informiert worden und haben bereits im November letzten Jahres mit den beteiligten Behörden Einvernehmen darüber erzielt, daß gegen eine Aufgabenverlagerung vom Einwohnerzentralamt auf die örtlichen Meldebehörden keine grundsätzlichen datenschutzrechtlichen Bedenken bestehen, wenn das Meldegesetz und die Zuständigkeitsanordnung entsprechend geändert werden und die neue Aufgabenverteilung in ein Sicherungskonzept eingeordnet wird.

Konkrete Schritte zur Schaffung dieser Voraussetzungen sind uns zwischen November 1989 und Mai 1990 nicht bekannt geworden. Im Mai 1990 stellte das Organisationsamt jedoch fest, daß eine Gesetzesänderung unter Umständen zu zeitaufwendig wäre, da die Aufgabenverlagerung wegen der Unzuträglichkeiten im Einwohnerzentralamt bis zum 1. Januar 1991 abgeschlossen sein soll. Nun wurde in Zweifel gezogen, ob eine Änderung des Meldegesetzes überhaupt erforderlich sei, man favorisierte statt dessen den unter Umständen schnelleren Weg einer Änderung der Zuständigkeitsanordnung.

Hiergegen haben wir erhebliche Bedenken geäußert. Das geltende Hamburgische Meldegesetz beschränkt den Zugriff der örtlichen Meldebehörden entsprechend der örtlich begrenzten Zuständigkeit (§ 1 Abs. 4). Lediglich beim Umzug innerhalb Hamburgs kann die Meldedienststelle des neuen Wohnorts den Bestand der bisher zuständigen fortschreiben. Für diesen überörtlichen Zugriff enthält § 30 Abs. 2 die erforderliche Rechtsgrundlage und schreibt auch technische und organisatorische Maßnahmen zur Kontrolle der Zulässigkeit vor. Die Bearbeitung von Ersuchen auf Auskunft aus dem Melderegister, die in der großen Mehrzahl nicht bei den bezirklichen Meldedienststellen, sondern zentral eingehen, kann jedoch nur dann durch die örtlichen Dienststellen erfolgen, wenn diese auf die anderen örtlichen Bestände zugreifen. Ein solcher Zugriff ist im melde- und datenschutzrechtlichen Sinn eine Übermittlung von einer örtlichen Meldebehörde an eine andere. Notwendig wäre daher eine ausdrückliche gesetzliche Regelung im Zusammenhang mit den Vorschriften zur Übermittlung von Daten zwischen den Meldebehörden (§ 30), die bisher fehlt. Auch technische und organisatorische Maßnahmen zur Gewährleistung der Datensicherheit sind für diesen Zugriff erforderlich, aber bisher im Meldegesetz nicht geregelt. Durch bloße Zuständigkeitsanordnung können diese rechtlichen Voraussetzungen nicht geschaffen werden. Wenn tatsächlich die Zeit für eine Gesetzesänderung fehlen sollte, so ist daran zu erinnern, daß der Zeitdruck vor allem durch Stellenstreichungen im Einwohnerzentralamt und dadurch entstanden ist, daß die für die Neuorganisation zuständigen Fachbehörden monatelang untätig geblieben sind.

Die Absicht, die Aufgabenverteilung zwischen zentraler und den örtlichen Meldebehörden allein mit einer Zuständigkeitsanordnung zu ändern und die erforderlichen Zugriffe auf den automatisierten Meldedatenbestand ohne gesetzliche Grundlage zuzulassen, hat darüber hinaus die grundsätzliche Frage aufgeworfen, ob die Entscheidung darüber, wo die Grenzen des zulässigen Zugriffs der Meldebehörden verlaufen sollen, allein vom Gesetzgeber zu treffen ist oder der Organisationsgewalt der Exekutive überlassen werden kann.

Der Hamburger Gesetzgeber hat bei der Beratung und Verabschiedung des Hamburgischen Meldegesetzes von 1986 durchaus berücksichtigt, daß das Bundesverfassungsgericht im Volkszählungsurteil vom Gesetzgeber verlangt hat, unter Wahrung des Verhältnismäßigkeitsprinzips die Voraussetzungen zu schaffen, unter denen die technikgestützte Verarbeitung personenbezogener Daten stattfinden kann. Insbesondere sind auch technische und organisatorische Vorkehrungen getroffen worden, die der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken. Hierzu gehören nach dem geltenden Meldegesetz vor allem die Trennung der Meldebehörden in funktionaler und örtlicher Hinsicht (§ 1 Abs. 1), die Begrenzung der Zugriffsmöglichkeiten (§ 1 Abs. 4) die Festlegung des Umfangs der Daten, die an andere Stellen übermittelt werden dürfen bzw. über die Auskunft erteilt werden kann (§§ 31, 34) sowie Kontroll- und Protokollierungspflichten (§ 30 Abs. 2 und Abs. 6, § 31 Abs. 4).

Damit hat der Gesetzgeber deutlich gemacht, daß die Grenzen des Verwaltungshandelns auf dem Gebiet des Meldewesens nicht nach reinen Zweckmäßigkeitsgesichtspunkten einmal weiter und beim anderen Mal enger gezogen werden dürfen. Vielmehr ist das Verwaltungs- und Rationalisierungsinteresse mit dem Interesse auf Wahrung des Rechts auf informationelle Selbstbestimmung abzuwägen und in Übereinstimmung zu bringen. Das Verwaltungsinteresse tendiert dahin, von möglichst wenigen organisatorischen und verfahrensmäßigen Vorkehrungen behindert zu werden, möglichst umfassend auf einen großen Datenbestand zugreifen zu können und hierbei

möglichst wenige rechtliche Vorgaben beachten zu müssen. Das vom informationellen Selbstbestimmungsrecht geleitete Interesse des Bürgers geht dagegen davon aus, grundsätzlich selbst zu entscheiden wann und innerhalb welcher Grenzen verschiedene Lebenssachverhalte offenbart werden. Überließe man diese Abwägung der Organisationsgewalt der Exekutive, würde voraussichtlich dem Verwaltungsinteresse in der Regel der Vorrang eingeräumt. Eine Interessenabwägung, die dem Grundrecht des Bürgers ebenso gerecht wird wie dem Interesse der Verwaltung, kann daher nur der Gesetzgeber selbst treffen.

Der Senat hat inzwischen beschlossen, eine Änderung des Hamburgischen Meldegesetzes alsbald einzuleiten, um die rechtlichen Voraussetzungen für den überörtlichen Zugriff der örtlichen Meldebehörden zur Erteilung von Melderegisterauskünften und Übermittlungen aus dem Melderegister zu schaffen. Zwar wird die Notwendigkeit einer Gesetzesänderung nicht mehr in Zweifel gezogen, gleichwohl wird für eine Übergangsphase der überörtliche Zugriff ohne Rechtsgrundlage erfolgen müssen. In Zukunft müßte sorgfältiger darauf geachtet werden, daß Rationalisierungsmaßnahmen nur innerhalb des gesetzlichen Rahmens vollzogen werden.

Es ist derzeit vorgesehen, die örtlich eingehenden Auskunftsersuchen unmittelbar örtlich zu erledigen und die zentral eingehenden nach einem Buchstabenmodell auf die örtlichen Meldedienststellen zu verteilen. Der überörtliche Zugriff wird auf den Grunddatensatz beschränkt, der die Erledigung der großen Mehrzahl von Auskünften und Übermittlungen ermöglicht. Die manuelle Einwohnerkartei beim Einwohnerzentralamt wird aufgelöst. Aufgaben, die auch in Zukunft nicht örtlich wahrgenommen werden können (z. B. Übermittlungen, die einen Zugriff über den Grunddatensatz hinaus erfordern), sollen von einer zentralen Stelle, die beim Bezirksamt Harburg eingerichtet werden soll, erledigt werden.

4.9.3 Pläne zur Novellierung des Hamburgischen Meldegesetzes

Abgesehen von der unter 4.9.2 beschriebenen Gesetzesänderung für den überörtlichen Zugriff auf den automatisierten Meldedatenbestand gibt es weitere Pläne für eine umfassende Novellierung des Hamburgischen Meldegesetzes. Dies ist erstaunlich, da die letzte Novelle noch nicht einmal fünf Jahre alt ist. Auch wenn es noch keinen Entwurf für ein neues Meldegesetz gibt, deuten sich bereits jetzt konkrete Wünsche für Gesetzesänderungen an, die alle mit den neuen technischen Möglichkeiten begründet werden, die sich aus der Automation des Meldewesens ergeben.

In der Behörde für Inneres wird überlegt, die Zuständigkeit der örtlichen Meldebehörden nicht allein auf die Erteilung von Auskünften (siehe 4.9.2) zu erweitern. Vielmehr sollen alle Meldedienststellen An- und Abmeldungen unabhängig vom Wohnsitz des Betroffenen vornehmen können. Die hierfür notwendigen überörtlichen Zugriffe auf den Meldedatenbestand wären aus datenschutzrechtlicher Sicht nur dann akzeptabel, wenn eine sorgfältige Analyse ergäbe, daß diese Zuständigkeitserweiterung tatsächlich im überwiegenden Interesse der Bürger und auch der Mitarbeiter in den Meldedienststellen liegt. Auf den ersten Blick sieht das Vorhaben zwar bürgerfreundlich aus. Bei näherer Betrachtung kommen jedoch Zweifel auf, ob nicht eher ein gegenteiliger Effekt einträte. Voraussichtlich würden sich An- und Abmeldungen bei einigen wenigen zentral gelegenen Meldedienststellen in der Innenstadt konzentrieren, während die Dienststellen in den Außenbezirken auch personell ausgedünnt würden. Eine schleichende Zentralisierung wäre gegenüber dem geltenden Zustand ein Rückschrittt. Sollten sich diese Bedenken als nicht gerechtfertigt herausstellen, müßte der überörtliche Zugriff zum Zweck der An- oder Abmeldung nur auf die hierfür zwingend erforderlichen Daten — in erster Linie die Anschrift — beschränkt werden. Ein allumfassender Zugriff mit dem Ergebnis, daß statt bisher einer zentralen und 28 örtlichen Meldebehörden in Zukunft 28 zentrale existieren, wäre keinesfalls hinnehmbar.

Das geltende Hamburgische Meldegesetz läßt nur für die Polizei einen on-line-Zugriff auf das Melderegister (vgl. 4.12.5) zu. Inzwischen sind jedoch Wünsche der Kfz-Zulassungsstelle, der Bußgeldstelle und auch des Projekts Sozialhilfe-Automation (PROSA)

bekannt geworden, im Rahmen ihrer automatisierten Verfahren on-line-Verbindungen zum Melderegister aufzubauen. Im Falle der Polizei ist die Notwendigkeit des on-line-Zugriffs damit begründet worden, daß der Personenkreis, über den zu Zwecken der Gefahrenabwehr oder Strafverfolgung Identifizierungsdaten benötigt werden, nicht vorhersehbar ist, potentiell also der gesamte Einwohnerdatenbestand zur Verfügung gestellt werden muß. Ferner ist die Polizei nach ihrer Auffassung auf diese Daten rund um die Uhr und auch an Wochenenden angewiesen, und braucht unter Umständen innerhalb kürzester Zeit zuverlässige Angaben. Alle diese Argumente entfallen jedoch bei den anderen genannten Stellen. Die Zulassungs- und die Bußgeldstelle haben ebenso wie die Sozialämter die gleichen Arbeitszeiten wie die Meldedienststellen. Es besteht daher immer die Möglichkeit der telefonischen oder schriftlichen Anfrage. Sie benötigen zur Erfüllung ihrer Aufgaben auch jeweils nur die Daten einer Minderheit von Einwohnern. Ein Zugriff auf Meldedaten von Personen, die keine Fahrzeughalter sind, keine Verkehrsordnungswidrigkeit begangen haben und keine Sozialhilfe bekommen, wäre unzulässig, ein entsprechender on-line-Zugriff daher von vornherein völlig unverhältnismäßig.

Denkbar wäre eine technische Verknüpfung der jeweiligen Datenbestände mit dem Melderegister nur unter bestimmten engen Voraussetzungen. Bei der Bußgeldstelle wird im Zusammenhang mit der Automation des Verfahrens zur Verfolgung von Verkehrsordnungswidrigkeiten (OWID) darüber nachgedacht, ob es realisierbar ist, einen systeminternen Datenabgleich der von der Bußgeldstelle gespeicherten Daten mit dem Melderegister vorzunehmen. Beim Zugriff auf die Daten im Bußgeldverfahren würde eine Rückmeldung des Melderegisters erfolgen, ob die Eintragung der Anschrift noch zutrifft. Meldedaten würden nur dann sichtbar, wenn die im Bußgeldverfahren gespeicherte Anschrift nicht mit der im Melderegister übereinstimmt. Die Sachbearbeiter erhielten so die Möglichkeit, die tatsächliche Adresse festzustellen. Diese technisch intelligente Lösung hätte gegenüber dem traditionellen lesenden on-line-Zugriff entscheidende Vorteile. Sie würde nur den Zugriff auf die Daten erlauben, die die abfragende Stelle bereits zur Erfüllung ihrer Aufgaben gespeichert hat. Eine Recherche im Melderegister nach fremden Daten wäre dagegen ausgeschlossen. Das Verfahren wäre im übrigen auch für die Sachbearbeiter erheblich komfortabler, da Anschriftenänderungen automatisch angezeigt würden. Schutzwürdige Belange der Betroffenen würden dagegen nicht berührt, sofern technisch sichergestellt wird, daß nur die Anschriften von Personen überspielt werden, die tatsächlich zur Erfüllung der gesetzlichen Aufgaben der abfragenden Stelle in deren Datei gespeichert sind.

Unter diesen Voraussetzungen, die technisch realisierbar sind und in ihren Grundzügen gesetzlich zu regeln wären, würden aus unserer Sicht die genannten Bedenken gegen on-line-Verbindungen anderer Stellen entfallen können.

Wenn es schon zu einer umfassenden Novellierung des Hamburgischen Meldegesetzes kommen soll, so müssen auch einige dringend erforderliche Verbesserungen zum Schutz von Meldedaten im Gesetz verankert werden. Der Bundesbeauftragte für den Datenschutz hat in seinem 12. Tätigkeitsbericht (3.1, S. 20 f.) die Problematik aufgezeigt, daß § 22 MRRG die Weitergabe von Meldedaten an Parteien im Zusammenhang mit Bundestags- oder Europawahlen derzeit ohne Widerspruchsmöglichkeit der Betroffenen und ohne Regelungen zur Zweckbindung erlaubt. In einer ersten Stellungnahme zur geplanten Änderung des Hamburgischen Meldegesetzes haben auch wir erneut darauf hingewiesen, daß auch die in Hamburg geltende Regelung über Melderegisterauskünfte an Parteien und Wählergruppen nach § 35 HmbMG im Zusammenhang mit Wahlen zur Bürgerschaft und den Bezirksversammlungen unzureichend ist. Wir haben vorgeschlagen, § 35 nach dem Vorbild von § 29 des Berliner Meldegesetzes zu ändern. In Berlin haben die Wahlberechtigten das Recht, der Weitergabe ihrer Daten an politische Parteien und Wählergruppen zu widersprechen; hierauf sind sie bei der Anmeldung und durch öffentliche Bekanntmachung hinzuweisen, wobei Fristen für die Ausübung des Widerspruchsrechts festgesetzt werden können. Die übermittelten Daten dürfen von den Empfängern nur zu Zwecken der Wahlwerbung verwendet werden; sie

sind innerhalb einer Woche nach dem Wahltag zu vernichten. Die Empfänger müssen eine entsprechende schriftliche Verpflichtungserklärung abgeben. Die Meldebehörde kann die Weitergabe von Daten mit zusätzlichen Auflagen verbinden, um sicherzustellen, daß die Empfänger ihren Verpflichtungen nachkommen.

4.9.4 Automatisierter Abgleich privater Dateien mit dem Melderegister?

Nicht nur bei Übermittlungen an öffentliche Stellen wachsen Begehrlichkeiten, technische Möglichkeiten, die sich aus der Automation des Melderegisters ergeben, zu nutzen. Auch einzelne private „Großkunden" (Inkassobüros, Versicherungen, Kreditinstitute) haben gegenüber dem Einwohnerzentralamt ihr Interesse bekundet, ihre elektronisch geführten Kundendateien in regelmäßigen Zeitabständen im automatisierten Verfahren mit dem Melderegister abzugleichen.

Nach Auffassung der Behörde für Inneres in Hamburg handelt es sich bei einem derartigen Abgleich um eine nach § 34 Abs. 1 Satz 2 HmbMG zulässige Sammelauskunft. Aus Rationalisierungsgründen wünscht das Einwohner-Zentralamt, daß Ersuchen um Sammelauskünfte in Form eines Datenträgers gestellt werden, der mit dem Meldedatenbestand abgeglichen werden kann. Das Verfahren wird bereits mit einer Sparkasse praktiziert.

Wir haben dagegen grundsätzliche Bedenken geltend gemacht. Ein Datenabgleich des Melderegisters mit den Beständen öffentlicher Stellen wird unstreitig als eine besondere Form der Übermittlung angesehen. Der Gesetzgeber hat regelmäßige Datenübermittlungen von einer ausdrücklichen bundes- oder landesrechtlichen Zulassung abhängig gemacht (§ 18 Abs. 4 MRRG, § 31 Abs. 5 HmbMG). Diese Einschränkung ist aus Gründen der Normenklarheit, der Durchsetzung der Zweckbindung und zur Wahrung des Verhältnismäßigkeitsprinzips geboten. Wenn im Einzelfall regelmäßige Übermittlungen an öffentliche Stellen durch Rechtsverordnung zugelassen werden, so liegt dem eine Abwägung zwischen den Belangen der Einwohner und den jeweiligen öffentlichen Interessen zugrunde. Es erscheint von vornherein fraglich, ob private Stellen Interessen für sich in Anspruch nehmen können, die denen der öffentlichen Stellen gleichkommen. Es kann im Ergebnis auch keinen Unterschied ausmachen, wenn derartige Ersuchen auf Datenabgleich nicht in konstanten Zeitabständen gestellt werden, sondern nur „hin und wieder", um der Bewertung als regelmäßige Auskunft zu entgehen, da dies an der Eingriffsqualität grundsätzlich nichts ändern würde.

Auch wenn man die Parallele zwischen regelmäßiger Übermittlung an öffentliche Stellen und regelmäßiger Auskunft an Private nicht ziehen will, spricht § 1 Abs. 3 HmbMG gegen die Zulässigkeit dieses Verfahrens. Nach dieser Vorschrift ist die Verarbeitung von Meldedaten nur nach Maßgabe des Meldegesetzes und anderer Rechtsvorschriften zulässig. Der Datenabgleich zum Zweck der Erteilung einer Sammelauskunft stellt jedoch eine gesetzlich nicht geregelte besondere Form der Datenverarbeitung dar.

Auch eine ausdrückliche gesetzliche Zulassung würde unsere Bedenken nicht ausräumen können, da die Beeinträchtigung von Belangen der betroffenen Einwohner nicht mit Sicherheit vermieden werden kann. Wenn eine private Stelle durch den Abgleich in großem Umfang erstmalig erfährt, welche Personen, die sie in ihrem Bestand gespeichert hat, in letzter Zeit umgezogen sind, erhält sie neben ihrer Kundenkartei eine Datei über Umzüge oder Namensänderung, ohne daß die Betroffenen hiervon etwas erfahren. Sie kann diese Informationen ohne großen Aufwand zu Zwecken verwenden, die nicht vom Vertragsverhältnis mit den Kunden abgedeckt sind. Die Meldebehörde kann auch nicht überprüfen, ob die private Stelle die abzugleichenden Daten rechtmäßig gespeichert hat. Läßt sie einen Abgleich von unzulässigen Speicherungen zu, beteiligt sie sich durch eine einmalige Handlung, ohne es zu wollen, an Rechtsverletzungen in einer Vielzahl von Fällen. Zur Zeit sind Melderegisterabgleichen für private Zwecke in großem Umfang noch dadurch Grenzen gesetzt, daß Name, Vorname und Geburtsdatum benötigt werden, um zuverlässige Auskünfte geben zu können. Nur in wenigen privaten Dateien ist das Geburtsdatum gespeichert. Es muß jedoch damit gerechnet werden, daß private Stellen allein zur Durchführung des Melderegisterab-

gleichs von ihren Kunden auch das Geburtsdatum erheben werden, obwohl sie es im Rahmen des Vertragsverhältnisses nicht benötigen.

Die generelle Zulassung des Abgleichs privater Dateien mit dem Melderegister würde dessen Funktion grundsätzlich ändern. Anschriftenänderungen im Melderegister würden in gewissen zeitlichen Abständen automatisch von privaten Stellen übernommen. Das Melderegister würde insoweit zur Zentraldatei für die unterschiedlichsten privaten Dateien. Einwohner könnten nicht mehr darauf vertrauen, daß durch ihren Umzug auch der Kontakt zu einer Stelle, den sie nicht mehr wünschen, abgebrochen ist und nur auf Einzelanfrage wiederherstellbar ist. Die staatlich normierte Meldepflicht würde im Ergebnis zu einer Pflicht, sich auch bei allen privaten Stellen, die am automatisierten Abgleich teilnehmen, umzumelden, womit die informationelle Trennung zwischen Staat und privaten Stellen einseitig zu deren Gunsten aufgehoben würde.

4.10 Ausländerwesen

4.10.1 Das neue Ausländergesetz

Wir hatten schon mehrfach Anlaß zu dem Hinweis, daß der durch das Recht auf informationelle Selbstbestimmung als Teil des allgemeinen Persönlichkeitsrechts gewährte Grundrechtsschutz uneingeschränkt auch den bei uns lebenden Ausländern zusteht. Sie sind auf diesen Schutz auch angewiesen, denn ihre Lebensplanung ist in viel stärkerem Maße von der Informationsverwertung und daraus folgenden Entscheidungen der Verwaltung abhängig, als die ihrer deutschen Mitbürger. Von einem Ausländergesetz muß deshalb erwartet werden, daß es eindeutig regelt, aufgrund welcher Information welche Entscheidungen getroffen werden dürfen. Eine Situation, in der ausländische Bürger nicht mehr erkennen können, welche Informationen aus ihrer Lebenssituation an die Ausländerbehörde weitergegeben und dort möglicherweise zu ihrem Nachteil verwertet werden, ist mit der vom Grundgesetz gewollten Rechtsordnung kaum noch vereinbar.

Diesen Erwartungen ist das im Frühjahr 1990 verabschiedete Gesetz zur Neuregelung des Ausländerrechts, das am 1. Januar 1991 in Kraft tritt, nicht gerecht geworden. Die getroffenen Regelungen dienen unserer Auffassung nach weniger dem Schutz personenbezogener Daten, sondern ermöglichen vielmehr weitgehende Kontrolle und Überwachung.

Der Bundesgesetzgeber hat es nicht für erforderlich gehalten, die bisher schon nur schwer durchschaubare Praxis (vgl. 3. TB 3.7.3, S. 56 ff.) auf ein notwendiges Maß zu reduzieren; er war vielmehr darauf bedacht, eine umfassende Informationsverarbeitung zu gewährleisten und bisher noch bestehende rechtliche Hindernisse zu beseitigen.

So dürfen nach § 75 die Ausländerbehörden zur Ausführung des Ausländergesetzes und anderer ausländerrechtlicher Bestimmungen die personenbezogenen Daten erheben, die zu ihrer gesetzlichen Aufgabenerfüllung erforderlich sind. Eine weitere Konkretisierung wird nicht vorgenommen. Welchen Umfang die Daten haben sollen, erhellt aber die Vorschrift des § 76 (Übermittlungen an Ausländerbehörden).

Zunächst haben öffentliche Stellen (dies sind alle Träger staatlicher Aufgaben, also die gesamte Verwaltung im weitesten Sinne) auf Ersuchen den Ausländerbehörden „ihnen bekannt gewordene Umstände" mitzuteilen. Die Ausländer selbst werden bei diesen Übermittlungen nicht beteiligt. Alle denkbaren Behörden können danach aufgefordert werden, beliebige Sachverhalte mitzuteilen, die auch nur einen entfernten Bezug zur Durchführung des Ausländergesetzes haben. Eine derart weitgehende Verpflichtung der gesamten öffentlichen Verwaltung zu Mitteilungen an eine bestimmte Behörde ist beispiellos. Sie läßt völlig außer acht, daß die anderen Behörden oft nur deshalb über Informationen verfügen, weil sich ihnen Menschen anvertraut haben, die auf Leistungen angewiesen waren oder Beratung brauchten. Vor diesem Hintergrund könnten die Betroffenen in eine Situation geraten, Nachteile in Kauf zu nehmen, weil sie die Hilfe

anderer Behörden beanspruchen, oder aber von vornherein auf solche öffentliche Unterstützung verzichten.

Das Ausländergesetz läßt es jedoch nicht bei Mitteilungen auf Ersuchen der Ausländerbehörde bewenden. Vielmehr sollen in bestimmten Fällen alle öffentlichen Stellen die Ausländerbehörde auf eigene Initiative unterrichten. Eine Mitteilungspflicht bei illegalem Aufenthalt ist noch akzeptabel. Dies gilt aber nicht für die unverzüglichen Mitteilungen bei Kenntnis von „einem sonstigen Ausweisungsgrund". Damit verlangt nämlich das Ausländergesetz völlig undifferenziert bei jedem Kontakt der öffentlichen Verwaltun mit ausländischen Bürgern auch die Prüfung, ob die bekanntgewordenen Sachverhalte einen Ausweisungstatbestand begründen können. Das neue Ausländergesetz kennt aber sehr viele Ausweisungstatbestände. Dazu zählen Gewalttaten ebenso wie Bezug von Sozial- und Jugendhilfe. Darüber hinaus kann ein Ausländer immer dann ausgewiesen werden, wenn sein Aufenthalt die öffentliche Sicherheit und Ordnung oder sonstige erhebliche Interessen der Bundesrepublik Deutschland beeinträchtigt. Hält also eine öffentliche Stelle die Voraussetzungen dieser vagen Generalklausel oder eines besonders genannten Ausweisungsgrundes für erfüllt, muß sie nach dem Wortlaut des Gesetzes die Ausländerbehörde unterrichten.

Wie sich diese Vorschrift in der Praxis auswirken kann, mögen einige Beispiele verdeutlichen: In einem besonders strengen Winter wird an bedürftige deutsche wie ausländische Bürger sogenannte Heizungshilfe geleistet. Dies ist ein Fall von Sozialhilfebezug — bei Ausländern also Ausweisungsgrund nach § 46 Nr. 6 AuslG; die Sozialämter müssen die Ausländerbehörde unverzüglich unterrichten. Gleiches gilt bei der Hilfe für werdende Mütter oder Wöchnerinnen oder Eingliederungshilfe in Fällen schwerer Behinderung von Kindern. Stellt ein ausländischer Arbeitnehmer, der erwerbsunfähig geworden ist, einen Rentenantrag, muß das Versorgungsamt dies der Ausländerbehörde melden, wenn es feststellt, daß die Rente voraussichtlich den Sozialhilfesatz nicht erreicht, der Betroffene somit auf ergänzende Sozialhilfe angewiesen sein wird. Bereits diese Aufzählung macht deutlich, daß eine derartige Pflicht zu Datenübermittlungen an die Ausländerbehörde für die Sachbearbeiter in den jeweiligen Dienststellen zu unzumutbaren Belastungen führen kann und die Masse der Mitteilungen auch von der Ausländerbehörde kaum noch zu verarbeiten wäre.

Die praktisch schrankenlosen Mitteilungspflichten — würden sie allein nach dem Wortlaut befolgt — hätten überdies nicht hinnehmbare Konsequenzen für die rechtmäßige Aufgabenerfüllung aller anderen öffentlichen Stellen. Sie müßten in Kauf nehmen, daß von vornherein ein Vertrauensverhältnis zwischen ihnen und ausländischen Bürgern nicht entstehen könnte. Beratung in sozialen und gesundheitlichen Angelegenheiten würde in Frage gestellt, da Ausländer, die das neue Ausländergesetz und seine Mitteilungspflichten kennen, sich nicht mehr offenbaren könnten, ohne mit erheblichen aufenthaltsrechtlichen Nachteilen rechnen zu müssen. Zahlreiche Stellen müßten sich als „Hilfsorgane" der Ausländerbehörde verstehen, die zuständigen Bediensteten stünden dauernd vor dem Konflikt, sich entweder für ihre eigene Aufgabe oder für die Durchführung des Ausländergesetzes entscheiden zu müssen.

Angesichts dieses Befundes wären Vorschriften geboten, die diese völlig unverhältnismäßigen Mitteilungspflichten einschränken. In der Tat regelt das Gesetz, daß eine Übermittlung personenbezogener Daten nach § 76 unterbleibt, soweit „besondere gesetzliche Verwendungsregelungen" entgegenstehen. Der Begriff „besondere gesetzliche Verwendungsregelungen" ist eine Neuschöpfung des Ausländergesetzes, die in der Praxis noch Schwierigkeiten bringen wird.

Die naheliegende Vermutung, das Sozialgeheimnis stelle eine Verwendungsregelung in diesem Sinne dar, ist nicht zutreffend, denn zusammen mit dem Ausländergesetz wurde auch das Sozialgesetzbuch geändert. Nach § 71 Abs. 2 des Sozialgesetzbuches — Zehntes Buch — (SGB X) ist nunmehr eine Offenbarung von Sozialdaten eines Ausländers im Einzelfall zulässig, soweit Mitteilungen aufgrund von Ersuchen der Ausländerbehörde nach § 76 Abs. 1 AuslG erfolgen sollen, aber auch in allen Fällen der eige-

nen Mitteilungspflichten nach § 76 Abs. 2 AuslG. Damit ist das Sozialgeheimnis für Ausländer seiner Schutzwirkung weitgehend entkleidet.

Als Verwendungsbeschränkung im Sinne von § 77 Abs. 1 AuslG könnte man ferner die Schweigepflichten nach § 203 StGB ansehen. Doch auch dem wird mit einer Sondervorschrift begegnet: Personenbezogene Daten, die von einem Arzt, Psychologen, Ehe-, Erziehungs-, Jugend- oder anerkannten Suchtberater, einem Mitglied einer Beratungsstelle nach § 218a StGB, einem Sozialarbeiter oder Sozialpädagogen einer öffentlichen Stelle zugänglich gemacht worden sind, und die alle der Schweigepflicht unterliegen, dürfen nach § 77 Abs. 2 AuslG von dieser unter bestimmten Voraussetzungen an die Ausländerbehörde weitergegeben werden. Der Perfektionismus, mit dem im Ausländergesetz Vorschriften zum Schutz des informationellen Selbstbestimmungsrechts entwertet werden, ist schon bemerkenswert.

Das neue Ausländergesetz soll — folgt man seiner Begründung — auch einen Beitrag zur Integration der hier lebenden Menschen ohne deutsche Staatsangehörigkeit leisten. Die Regelungen über die Datenverarbeitung der Ausländerverwaltung sind jedoch dazu angetan, das Gegenteil zu bewirken: sie werden zur Benachteiligung und Ausgrenzung der Betroffenen führen, wenn es nicht gelingt, sie in der Praxis auf ein rechtsstaatlich vertretbares Maß einzugrenzen.

Darum will sich eine von uns angeregte und von der Behörde für Arbeit, Gesundheit und Soziales einberufene behördenübergreifende Arbeitsgruppe bemühen, die untersuchen soll, welche Auswirkungen das neue Gesetz auf die in Hamburg lebenden Ausländer und die Verwaltung haben wird, welche Entscheidungsräume in der Praxis vorhanden sind und wie sie ausgefüllt werden können. Einen Schwerpunkt der Erörterungen bilden die datenschutzrechtlichen Probleme.

Ausgangspunkt für die Überlegungen ist die Frage, ob die durch das Gesetz begründeten Mitteilungspflichten nach dem Grundsatz der Verhältnismäßigkeit auf die Fälle eingeschränkt werden müssen, in denen weder die Durchführung des Ausländergesetzes noch die Erfüllung anderer öffentlicher und insbesondere sozialer Aufgaben gefährdet werden. Hierfür könnte § 76 Abs. 5 AuslG, wonach regelmäßige Übermittlungen an die Ausländerbehörden durch Rechtsverordnung bestimmt werden sollen, einen möglichen Ansatz bieten. Möglicherweise können darüber hinaus durch verwaltungsinterne Regelungen Mitteilungen, die die Aufgabenerfüllung anderer Stellen und das Vertrauensverhältnis zu den ausländischen Bürgern gefährden würden, ausgeschlossen werden. Wir haben den Eindruck, daß alle Beteiligten — auch und insbesondere die für die Ausländerverwaltung zuständige Behörde für Inneres — ein großes Interesse an einer gleichermaßen praktikablen wie für die Betroffenen erträglichen Gesetzesanwendung haben. Bei Redaktionsschluß zu diesem Bericht konnten konkrete Ergebnisse der Arbeitsgruppe noch nicht vorliegen, so daß sich derzeit nicht absehen läßt, wie erfolgreich die Bemühungen sein werden.

4.10.2 Ausländerzentralregister

Das Ausländergesetz allein gibt allerdings trotz seiner weiten Regelungen noch keine umfassende Auskunft darüber, in welchem Umfang personenbezogene Daten ausländischer Bürger erhoben, gespeichert und übermittelt werden, da es nur die Datenverarbeitung durch die örtlich zuständigen Ausländerbehörden betrifft. Darüber hinaus werden Daten von Ausländern im Ausländerzentralregister gespeichert und weiterverarbeitet. Die Problematik dieses Registers und der hierzu vorbereiteten gesetzlichen Regelung ist von uns mehrfach (7. TB, 4.10.1, S. 78 ff. und 8. TB, 3.7.1, S. 49 ff.) geschildert worden. Inzwischen ist zwar ein Gesetzentwurf der Bundesregierung beim Deutschen Bundestag eingebracht worden, er konnte jedoch noch nicht inhaltlich beraten werden, da zunächst das neue Ausländergesetz durchgesetzt werden sollte. Ob das AZR-Gesetz noch in dieser Legislaturperiode verabschiedet wird, ist ungewiß. Unsere vielfachen Bedenken gegen die geplante Struktur des Registers, das die zuvor beschriebene Situation für ausländische Mitbürger noch weiter verschlechtert, bestehen fort.

4.10.3 Automation der Ausländerverwaltung in Hamburg

Es ist inzwischen allgemein unstreitig, daß die derzeitige Unterbringung der Ausländerbehörde im Bieberhaus für die betroffenen ausländischen Bürger ebenso wie für die dort beschäftigten Mitarbeiter kaum mehr hinnehmbar ist. Vor diesem Hintergrund wird überlegt, die Ausländerverwaltung zu dezentralisieren. Die erfordert jedoch nach Auffassung der zuständigen Behörde für Inneres eine durch Informations- und Kommunikationstechnik gestützte Automation der Ausländerverwaltung.

Der Senat hat mit dem Entwurf des IuK-Gesamtplanes 1991-1993 ein neues Projekt „Automation der Ausländerabteilung" beschlossen. Es wird noch geprüft, ob ein fertiges Verfahren zur automatisierten Abwicklung ausländerrechtlicher Entscheidungen übernommen werden kann. Diese Prüfung soll bis Ende 1990 abgeschlossen sein. Eine gesicherte Prognose ist derzeit nicht möglich.

Gleichwohl möchten wir schon heute davor warnen, ein mit anderen automatisierten Verfahren vernetztes „Ausländer-Informationssystem" aufzubauen, das jedem Sachbearbeiter den Zugriff auf Sozial-, Gesundheits- und polizeiliche Daten ermöglichen würde. Dies wäre nicht nur eine zusätzliche schwerwiegende Beeinträchtigung der Persönlichkeitsrechte der Betroffenen, sondern würde auch die unter 4.10.1 beschriebenen gemeinsamen Bemühungen wieder in Frage stellen.

4.11 Verkehrswesen

4.11.1 Mängel bei der Durchführung des Ordnungswidrigkeitenverfahrens

Die beim Einwohnerzentralamt angegliederte Bußgeldstelle ist zuständig für die Verfolgung von Ordnungswidrigkeiten im Straßenverkehr. In einem bereits seit längerem betriebenen automatisierten Verfahren (OWI-HH) werden Daten von Personen gespeichert, die eine Verkehrsordnungswidrigkeit begangen haben. Im Berichtszeitraum haben wir einzelne erhebliche Mängel bei der Durchführung dieses Verfahrens festgestellt.

In einer Eingabe schilderte uns ein Bürger folgenden Sachverhalt: Er hatte sein Kraftfahrzeug bereits im Frühjahr 1989 verkauft und unverzüglich ordnungsgemäß abgemeldet. Gleichwohl erhielt er Anfang dieses Jahres ein Anhörungsschreiben der Bußgeldstelle, worin ihm vorgeworfen wurde, er habe als Halter dieses Kraftfahrzeugs im Januar 1990 eine Verkehrsordnungswidrigkeit begangen. Nachdem er mitgeteilt hatte, er sei schon längst nicht mehr der Halter, und die Löschung seiner Daten beantragte, wurde das Ordnungswidrigkeitsverfahren gegen ihn zwar eingestellt, jedoch sonst nichts veranlaßt. Einige Monate später erhielt er erneut ein Anhörungsschreiben zu einer abermaligen Verkehrsordnungswidrigkeit als angeblicher Halter seines früheren Fahrzeugs.

Wir sind der Sache nachgegangen und haben folgendes festgestellt: Bei der Zulassungsstelle in Hamburg ist die Abmeldung des bisherigen und die Anmeldung des neuen Halters ordnungsgemäß vollzogen worden. Daten über Halter von Kraftfahrzeugen werden jedoch nicht nur örtlich gespeichert, sondern auch beim Zentralen Fahrzeugregister (ZEVIS) beim Kraftfahrbundesamt in Flensburg. Die örtliche Zulassungsstelle teilt dem Kraftfahrt-Bundesamt den Halterwechsel mit, was von Hamburg aus zur Zeit noch mit schriftlichen Änderungsformularen erfolgt.

Im Zentralen Fahrzeugregister ist in diesem Fall jedoch keine Änderung vorgenommen worden. Ob dies auf eine Nachlässigkeit der örtlichen Zulassungsstelle oder des Kraftfahrt-Bundesamtes zurückzuführen ist, ließ sich nicht mehr feststellen. Jedenfalls war der Petent zum Zeitpunkt unserer Überprüfung immer noch fälschlicherweise als Halter seines früheren Fahrzeugs gespeichert. Da Polizeibeamte, die eine Verkehrsordnungswidrigkeit feststellen, die Halterdaten üblicherweise beim Zentralen Fahrzeugregister des Kraftfahrt-Bundesamtes abfragen, wurde die Anzeige über die Verkehrsordnungswidrigkeit mit den (falschen) Halterdaten an die Bußgeldstelle weitergeleitet. Die Mitteilung des Petenten, er sei nicht mehr Halter, hätte die Bußgeldstelle zu weiteren

Ermittlungen veranlassen müssen. Durch eine Anfrage bei der örtlichen Zulassungsstelle hätte sie den tatsächlichen Sachverhalt erfahren. Sodann hätte sie nach unserer Auffassung die Berichtigung der falschen Halterdaten in ZEVIS anstoßen müssen.

Wir haben deshalb die Bußgeldstelle darauf hingewiesen, daß sie verpflichtet ist, die Zulassungsstelle zu benachrichtigen, wenn sie davon erfährt, daß Halterdaten unrichtig sind. Es reicht keinesfalls aus, lediglich das Bußgeldverfahren einzustellen und ansonsten untätig zu bleiben. Im Fall des Petenten war dies um so weniger verständlich, als er die Berichtigung beantragt hatte. Die Bußgeldstelle kann sich nicht auf den Standpunkt zurückziehen, daß sie selbst nicht für die falschen Halterdaten verantwortlich ist, da die betroffenen Bürger die komplexen Informationswege kaum überschauen können, und die speichernden Stellen in der Regel nichts von der Unrichtigkeit erfahren. Da die Bußgeldstelle in großem Umfang Halterdaten nutzt, muß sie besondere Sorgfalt darauf verwenden, nur richtige Daten zu verwenden. Diese Einschätzung wird im Grundsatz auch von der Bußgeldstelle geteilt.

Bei dieser Gelegenheit haben wir erfahren, daß die Bußgeldstelle in vergleichbaren Fällen unrichtige Daten, die in ihrer Datei zur Verfolgung von Ordnungswidrigkeiten gespeichert sind, nicht löscht oder berichtigt, sondern lediglich eine Nebendatei mit den tatsächlich zutreffenden Daten anlegt, auf die immer dann verwiesen wird, wenn auf ein unrichtiges Datum zugegriffen wird. Diese Hilfskonstruktion ist bedenklich, da sie geeignet ist, den Anspruch der Betroffenen auf Löschung bzw. Berichtigung zu unterlaufen. Bei der geplanten Modernisierung des automatisierten Verfahrens zur Verfolgung von Verkehrsordnungswidrigkeiten ist auf jeden Fall sicherzustellen, daß die technischen Voraussetzungen für die erforderlichen Löschungen oder Berichtigungen geschaffen werden. Eine Stellungnahme der Behörde für Inneres lag uns bis zum Redaktionsschluß für diesen Bericht noch nicht vor.

4.11.2 Datenschutzrechtliche Kontrolle von ZEVIS

Im Zentralen Fahrzeugregister (ZEVIS) gespeicherte Fahrzeug- und Halterdaten dürfen nach § 36 des Straßenverkehrsgesetzes für die Erfüllung bestimmter Aufgaben an die Zulassungsstellen, an die Polizeien des Bundes und der Länder sowie an den Zoll und die Zollfahndungsdienststellen im automatisierten Verfahren (on-line) übermittelt werden. Nach dieser Vorschrift sind besondere Voraussetzungen zu erfüllen und Protokollierungsverpflichtungen einzuhalten. Die Kontrolle des Abrufverhaltens der genannten Stellen ist eine Aufgabe der Datenschutzbeauftragten des Bundes und der Länder. Daneben sind auch die zuständigen obersten Aufsichtsbehörden gehalten, im Rahmen ihrer Fachaufsicht auf die Rechtmäßigkeit und Erforderlichkeit der Abrufe für die Aufgabenerfüllung zu achten und auf eine einheitliche Abrufpraxis hinzuwirken.

Wir haben daher — in Abstimmung mit den anderen Datenschutzbeauftragten des Bundes und der Länder — die Behörde für Inneres aufgefordert, eine zentrale Ansprechstelle für die Einrichtung von ZEVIS-Anschlüssen jeweils für den Bereich der Polizei und der Zulassungsstellen zu benennen. Diese sollten untereinander möglichst engen Kontakt halten. Sie sollten Kriterien für eine einheitliche Vergabepraxis (z.B. Anzahl der Anschlüsse abhängig von den Aufgabenschwerpunkten) entwickeln und Kenntnis von der Kapazität und der tatsächlichen Zahl der geschalteten Anschlüsse haben. Ihnen würde auch die Aufgabe zufallen, Verbindung zu den übrigen koordinierenden Stellen des Bundes und der Länder zu halten und auf einheitliche Handhabung bei ZEVIS-Abrufen (eventuell durch Erarbeitung von Handlungsanweisungen) hinzuwirken. Die zentralen Ansprechstellen sollten ferner in regelmäßigen Zeitabständen die Abrufpraxis der abrufberechtigten Stellen kontrollieren und ihnen gegebenenfalls erforderliche Hinweise geben. Eine Antwort der Behörde steht bisher noch aus.

Mit den übrigen Datenschutzbeauftragten erarbeiten wir darüber hinaus ein Fahrzeugregister-Informationskonzept, um bundesweit den Informationsstand über die ZEVIS-Nutzung zu verbessern. Es soll Art und Umfang von Kontrollen bei abrufberechtigten Dienststellen und örtlichen Fahrzeugregistern regeln und einen vertieften Informationsaustausch zwischen den Datenschutzbeauftragten vorsehen.

4.11.3 On-line-Zugriff der Bußgeldstelle auf das örtliche Fahrzeugregister?

Zur Verbesserung ihrer Arbeit würde die Bußgeldstelle gern einen on-line-Zugriff auf das örtliche Fahrzeugregister einrichten. Das geltende Recht läßt dies jedoch nicht zu: Nach § 36 Abs. 2 Satz 2 Straßenverkehrsgesetz (StVG) ist eine on-line-Übermittlung von den örtlichen Fahrzeugregistern an die örtlich zuständigen Polizeidienststellen zur Verfolgung von Ordnungswidrigkeiten nach § 24 oder 24a zulässig. § 12 Abs. 1 Satz 2 Nr. 3 der Fahrzeugregister-Verordnung konkretisiert den Begriff der Polizeidienststellen auf die „Dienststellen des Polizeivollzugsdienstes". In der Begründung zu § 12 wird hierzu ausgeführt, daß die Bußgeldbehörden, die nach § 36 Abs. 1 Nr. 1 des Ordnungswidrigkeitengesetzes i. V. m. § 26 StVG zur Verfolgung und Ahndung von Verkehrsordnungswidrigkeiten zuständig sind, keine Aufgaben des Polizeivollzugsdienstes wahrnehmen. Die vorgesehene Möglichkeit, on-line zur Verfolgung von Ordnungswidrigkeiten nach §§ 24 und 24a StVG zuzugreifen, soll sich nur auf die Tätigkeit der Polizei im Rahmen der Verkehrsüberwachung im Straßenverkehr erstrecken. Ein entsprechender Gegenvorschlag des Bundesrates auf Einbeziehung der Bußgeldbehörden in den abrufberechtigten Empfängerkreis wurde vom Gesetzgeber nicht aufgegriffen. Auch eine organisatorische Anbindung der Bußgeldstelle an die Polizei würde hieran nichts ändern, da auch in diesem Fall die Bußgeldstelle keine Aufgaben des Polizeivollzugsdienstes wahrnehmen würde.

Somit können auch auf das örtliche Fahrzeugregister nur Polizeivollzugsdienststellen i. S. v. § 12 Abs. 1 Satz 2 Nr. 3 Fahrzeugregister-Verordnung on-line zugreifen. Nach den uns vorliegenden Informationen hält die Polizei selbst einen solchen Zugriff nicht für erforderlich.

4.11.4 Verfahren zur Erfassung und Erkennung von sogenannten „Mehrfachtätern" bei Verkehrsordnungswidrigkeiten

Angesichts des immer weiter zunehmenden Autoverkehrs in den Innenstädten und des begrenzten Parkraumes, stellen sogenannte „Mehrfachtäter" — etwa hartnäckige Falschparker — bei den Verkehrsordnungswidrigkeiten ein erhebliches Problem dar.

Die Bußgeldstelle ist daher daran interessiert, die Möglichkeit zu bekommen, Mehrfachspeicherungen — insbesondere aus abgeschlossenen Verfahren — zu einer Person im automatisierten Ordnungswidrigkeiten-Verfahren für die Erkennung und besondere Ahndung von Mehrfachtätern zu nutzen.

Die rechtliche Zulässigkeit eines solchen Verfahrens läßt sich zusammenfassend wie folgt beurteilen: Örtliche Dateien ohne gesetzliche Grundlage neben dem Verkehrszentralregister zur Speicherung und Auswertung von Entscheidungen bei Verkehrsordnungswidrigkeiten sind unzulässig. Sie unterlaufen das Verbot, Parallelspeicherungen zum Verkehrszentralregister vorzunehmen und sind daher abzulehnen. Dies gilt insbesondere auch für die Heranziehung von Daten, die nur noch zu Abrechnungs- und Dokumentationszwecken gespeichert werden.

Auf diese rechtliche Beurteilung hat sich auch der Bund-Länder-Fachausschuß für Straßenverkehrsordnungswidrigkeiten verständigt.

Anders wäre jedoch ein Vorhaben zu beurteilen, das die Zusammenfassung mehrerer laufender Verkehrsordnungswidrigkeitenverfahren aus rechtlichen Gründen — etwa weil der Täter in allen Fällen einen einheitlichen Vorsatz hatte — ermöglicht. Dann muß jedoch schon programmtechnisch sichergestellt werden, daß ein Zugriff auf die Daten abgeschlossener Verfahren ausgeschlossen ist. Abgeschlossen sind Fälle von Verkehrsordnungswidrigkeiten für die Behörde jedenfalls dann, wenn die Verhängung eines Verwarnungsgeldes wirksam (§ 56 Abs. 2 und 4 OWiG) oder ein Bußgeldbescheid rechtskräftig geworden ist oder das Gericht im Beschlußverfahren entscheidet, da auch in diesen Fällen eine nachträgliche Berücksichtigung von mehreren Taten zum Nachteil des Betroffenen ausgeschlossen ist (§ 72 Abs. 3 Satz 2 OWiG).

Sollen dagegen im Einzelfall auch die Daten aus abgeschlossenen Verfahren bei der Ahndung von Ordnungswidrigkeiten herangezogen werden, steht der Bußgeldstelle dafür das Verkehrszentralregister zur Verfügung. Die hier nicht erfaßten geringen Verstöße müssen unberücksichtigt bleiben. Entsprechende „schwarze Listen" die vor Jahren aus diesen Anlässen geführt worden sind, sind aus guten Gründen abgeschafft worden, sie sollten nicht in automatisierter Form wieder eingeführt werden.

4.12 Polizei

4.12.1 Entwurf für ein neues Polizeirecht in Hamburg

Über den Senatsentwurf für ein neues Polizeirecht haben wir in unserem letzten Tätigkeitsbericht (8. TB, 3.8.1., S. 51 ff) ausführlich berichtet. Seit Januar dieses Jahres liegt der Entwurf der Bürgerschaft zur Beratung vor. In zwei gemeinsamen Sitzungen des Innenausschusses und des Rechtsausschusses haben wir unsere wesentlichen Kritikpunkte am Senatsentwurf erläutert.

Ein Schwerpunkt der parlamentarischen Beratung betraf den Begriff der „Straftaten von erheblicher Bedeutung". Der gesetzlichen Definition dieser Straftaten kommt deshalb eine besondere Bedeutung zu, weil die neuen Befugnisse der Polizei zur Datenerhebung im präventiven Bereich, etwa zur längerfristigen Observation, zum verdeckten Einsatz technischer Mittel, zum Einsatz von verdeckten Ermittlern und V-Leuten hieran anknüpfen. Nach wie vor sind wir der Auffassung, daß die entsprechende Vorschrift (§ 1 Abs. 4 des Entwurfes eines Gesetzes über die Datenverarbeitung der Polizei — DVPolG-E —) zu weit gefaßt ist. So ist in dem Katalog der Straftaten von erheblicher Bedeutung immer noch § 129 StGB einbezogen. Nach dieser Vorschrift ist die Gründung einer Vereinigung, deren Zweck die Begehung von (beliebigen) Straftaten ist, mit Strafe bedroht. Auch die Unterstützung einer solchen Vereinigung oder die Beteiligung an ihr ist strafbar. Unsere Kritik richtet sich dagegen, daß mit der Nennung dieser Vorschrift in § 1 Absatz 4 DVPolG-E die Straftaten von erheblicher Bedeutung mit Bagatellstraftaten aufgefüllt werden, weil schwerwiegende Straftaten, zu deren Begehung eine Vereinigung gegründet wurde, schon vom übrigen Straftatenkatalog erfaßt sind. Wenn der Entwurf in der jetzt vorliegenden Fassung Gesetz werden sollte, wird es aber beispielsweise möglich sein, zur vorbeugenden Bekämpfung des verabredeten einfachen Ladendiebstahls einer Gruppe von drei Leuten verdeckte Ermittler oder Abhöranlagen einzusetzen.

Wir haben ferner darauf hingewiesen, daß auch die in § 138 StGB genannten Delikte im Rahmen des Katalogs von Straftaten erheblicher Bedeutung entbehrlich sind, da sie bis auf ganz wenige, praktisch bedeutungslose, Ausnahmen allesamt Verbrechen und als solche bereits erfaßt sind.

Schließlich haben wir dem Innen- und Rechtsausschuß vorgeschlagen, die Befugnisse zum verdeckten Einsatz technischer Mittel, zur Datenerhebung durch verdeckte Ermittler und V-Leute — mit einer Einschränkung — von den Voraussetzungen abhängig zu machen, unter denen auch eine Rasterfahndung zulässig sein soll. Nach § 23 des Entwurfs ist dies nur zur Abwehr einer unmittelbar bevorstehenden Gefahr für die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person zulässig. Allerdings sollte die „Leibesgefahr" durch „erhebliche Gefahren für die körperliche Unversehrtheit" ersetzt werden. Dann hätte man für den Einsatz der besonderen Erhebungsbefugnisse einen eindeutig begrenzten und besser handhabbaren Anknüpfungspunkt als den Katalog der Straftaten von erheblicher Bedeutung.

Andere Vorschriften des Gesetzesentwurfs sind in der bisherigen Diskussion noch zu kurz gekommen. Dies gilt insbesondere für die mangelnde Einhaltung des Zweckbindungsgebots und der Beschränkung des Löschungs- bzw. Vernichtungsgebots auf sogenannte „suchfähig gespeicherte Daten" (8. TB, 3.8.1.2.5.6, S. 55 f).

4.12.2 Entwürfe zum BKA- und BGS-Gesetz

4.12.2.1 BKA-Gesetz

Im 8. Tätigkeitsbericht (3.8.2, S. 61 ff) ist der Umfang der von den Länderpolizeien im Verbund mit dem Bundeskriminalamt (BKA) betriebenen Datenverarbeitung ausführlich dargestellt worden. Hieraus wird deutlich, daß die Datenverarbeitung der Länderpolizeien nur dann vollständig beurteilt werden kann, wenn auch die Praxis des Bundeskriminalamt mit in die Betrachtung einbezogen wird.

Das geltende Gesetz über das Bundeskriminalamt entspricht in keiner Weise den Anforderungen, die das Bundesverfassungsgericht zur Normenklarheit und Verhältnismäßigkeit aufgestellt hat. Der Bundesminister des Innern hat inzwischen einen neuen Referententwurf für ein BKA-Gesetz vorgelegt, der allerdings unzulänglich ist. In einer ausführlichen Stellungnahme haben wir die Behörde für Inneres aufgefordert, auf eine umfassende Änderung des Entwurfs hinzuwirken. An dieser Stelle soll lediglich auf den wesentlichen Kritikpunkt hingewiesen werden.

Während § 1 Absatz 1 des geltenden Gesetzes die Aufgaben des BKA auf die Bekämpfung von Straftätern, die sich international oder über das Gebiet eines Landes hinaus betätigen, begrenzt, weist der Entwurf dem BKA darüber hinaus auch Aufgaben bei der Bekämpfung von Straftaten „von sonst erheblicher Bedeutung" zu. Eine Definition dieses Begriffs enthält der Entwurf nicht. Wenn an einer Stelle in der Begründung ausgeführt wird, daß es sich bei Straftaten „von sonst erheblicher Bedeutung" um Fälle mittlerer Kriminalität handele, so muß daraus gefolgert werden, daß es Ziel des Entwurfs ist, die polizeiliche Datenverarbeitung generell außer in Fällen leichter Kriminalität beim Bundeskriminalamt zu zentralisieren. Diese Ausweitung der Zuständigkeiten des BKA widerspricht der förderativen Struktur der Bundesrepublik und dem Prinzip der funktionalen und informationellen Gewaltenteilung. Eine derart weite Aufgabenzuweisung an das Bundeskriminalamt kann auch nicht verhältnismäßig sein, da kein sachlicher Grund dafür ersichtlich ist, warum in allen Fällen von nicht nur leichter Kriminalität eine bundesweite Datenspeicherung, -nutzung und -übermittlung stattfinden soll.

Eine Zentralisierung polizeilicher Aufgaben auf den Gebieten der Strafverfolgung, der vorbeugenden Bekämpfung von Straftaten und der Gefahrenabwehr beim Bundeskriminalamt würde dazu führen, daß landesrechtliche Regelungen zur polizeilichen Datenverarbeitung von den Befugnissen des Bundeskriminalamtes überlagert würden. Da dem Entwurf ferner die Grundsätze der Normenklarheit und der Zweckbindung weitgehend fremd sind, würde der — unzureichende — Schutz, den das Landesrecht noch gegen unverhältnismäßige Eingriffe in das informationelle Selbstbestimmungsrecht bietet, weitestgehend ausgehöhlt. Das Ziel von bereichsspezifischen Vorschriften über die Datenverarbeitung der Polizeien in den Ländern, für die Anwender wie die betroffenen Bürger Klarheit über Art und Umfang der Erhebung und weiteren Verwendung von Daten zu schaffen, wird somit unerreichbar.

Hinzu kommt, daß der weitaus größte Bereich polizeilicher Datenerhebung mehrfach relevant ist: Einem Erhebungsvorgang ist nicht mehr ohne weiteres anzusehen, ob die weitere Verwendung der Daten zu Zwecken der Strafverfolgung, der Verhütung von Straftaten, der Vorsorge für künftige Strafverfolgung oder der Gefahrenabwehr erfolgen soll und ob diese Zwecke von der Staatsanwaltschaft, der Länderpolizei, dem Bundeskriminalamt oder ausländischen Behörden wahrgenommen werden. Damit entsteht in der Tat eine Situation, „in der Bürger nicht mehr wissen können, wer wann was und bei welcher Gelegenheit über sie weiß", die das Bundesverfassungsgericht im Volkszählungsurteil als unvereinbar mit dem Recht auf informationelle Selbstbestimmung und somit als grundrechtswidrig bezeichnet hat.

Eine wesentliche Forderung an bereichsspezifische Regelungen zur Datenverarbeitung von Sicherheitsbehörden ist daher die Verwirklichung einer funktionalen und informationellen Gewaltentrennung. Eine klare Abgrenzung zwischen den der Länder-

polizei regional zustehenden Befugnissen und den Fällen, in denen Befugnisse des BKA bis hin zum internationalen Informationsaustausch hinzutreten dürfen, ist insoweit zwingend.

Unter der Überschrift „Zentralstelle" werden im Entwurf verschiedene Aufgaben und Befugnisse zusammengefaßt, deren Qualität und Verhältnis zueinander unklar bleibt. Die Formulierung „Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen und für die Kriminalpolizei" ist Artikel 87 Absatz 1 Satz 2 Grundgesetz entnommen; als verfassungsrechtliche Kompetenznorm macht diese Vorschrift für sich gesehen nicht deutlich, welcher Natur die Aufgaben der Zentralstelle sind. Artikel 87 Absatz 1 Satz 2 setzt die Begriffe „Polizeiliches Auskunfts- und Nachrichtenwesen" sowie „Kriminalpolizei" voraus. Diese polizeilichen Tätigkeiten gehören jedoch grundsätzlich in die Verwaltungszuständigkeit der Länder. Die unterstützende Funktion einer Zentralstelle kann daher nur an der Länderzuständigkeit anknüpfen, jedoch keinen eigenen Zuständigkeitsbereich schaffen.

Diese subsidiäre Funktion des Bundeskriminalamtes, die allein das Ziel haben kann, die eigene Tätigkeit der Länderpolizeien zu unterstützen, und sie gegebenenfalls koordinieren soll, muß im Gesetz bei allen Vorschriften, die dem Bundeskriminalamt als Zentralstelle Aufgaben oder Befugnisse zuweisen, strikt beachtet und deutlich gemacht werden.

4.12.2.2 BGS-Gesetz

Bisher spielte das Gesetz über den Bundesgrenzschutz (BGS-Gesetz) im Bereich der Länder keine wesentliche Rolle, da auch in den Fällen, in denen die Landespolizei grenzpolizeiliche Aufgaben wahrgenommen hat, immer das jeweilige Landespolizeirecht anzuwenden war. Der Bund beabsichtigt jedoch, dies durch eine Novelle zum BGS-Gesetz zu ändern. Nach § 63 Absatz 3 des im Frühjahr vorgestellten Referentenentwurfs sollen der Polizei des Landes auch die Befugnisse nach dem BGS-Gesetz zustehen, soweit dieses über das Recht des Landes hinaus für die polizeiliche Kontrolle des grenzüberschreitenden Verkehrs besondere Befugnisse regelt. Diese Änderung hätte für Hamburg erhebliche Auswirkungen, da hier die Wasserschutzpolizei aufgrund einer Vereinbarung mit dem Bund grenzpolizeiliche Aufgaben wahrnimmt. Aus unserer Sicht ist dieser weitere Fall der Überlagerung des Landespolizeirechts durch Bundesrecht keinesfalls akzeptabel.

So sind etwa die tatbestandlichen Voraussetzungen nach dem Entwurf des BGS-Gesetzes weiter als nach dem Hamburger Entwurf für ein Gesetz über die Datenverarbeitung der Polizei. Die im BGSG-Entwurf für besondere Befugnisse vorausgesetzten grenzbezogenen „Straftaten von erheblicher Bedeutung" werden nicht in einem abschließenden Katalog aufgezählt. Daher besteht die Möglichkeit, Straftaten auch dann als „erheblich" einzustufen, wenn sie nicht im Katalog von § 1 Absatz 4 DVPolG-E enthalten sind.

Selbst wenn es gelänge, die Voraussetzungen für besondere Befugnisse nach dem BGS-Gesetz bruchlos an das Landesrecht anzupassen, würde es bei den einzelnen Befugnisnormen zu enormen Auslegungsschwierigkeiten darüber kommen, ob das Bundesrecht Befugnisse verleiht, die über die nach Landesrecht hinausgehen. Ein solcher „Wettlauf" um die jeweils weiteste Befugnisnorm würde weder dem Gebot der Normenklarheit noch den Bedürfnissen des Vollzugs gerecht werden. Wir haben daher die Behörde für Inneres aufgefordert, sich in den weiteren Beratungen für die ersatzlose Streichung dieser Regelung einzusetzen.

4.12.3 Internationaler Datenaustausch (Schengener Informationssystem)

Im Juni dieses Jahres wurde das Durchführungsübereinkommen zum Schengener Übereinkommen unterzeichnet. Es muß jedoch noch von den Gesetzgebungsorganen des Bundes ratifiziert werden. Darauf hinzuweisen ist, daß das Übereinkommen die Befugnisse zur Ausschreibung im sogenannten Schengener Informationssystem

(S.I.S.) etwa zur verdeckten Registrierung nach Artikel 99 von den Voraussetzungen des nationalen Rechts abhängig macht. Die erforderlichen Rechtsgrundlagen für die polizeiliche Datenverarbeitung sind im Bund allerdings überhaupt nicht, in den Ländern nur teilweise geschaffen worden und werden dem Recht auf informationelle Selbstbestimmung nur unvollkommen gerecht. Die datenschutzrechtliche Problematik des Informationsaustauschs zwischen den Schengener Vertragsstaaten ist daher in erster Linie im nationalen Recht begründet, wird allerdings durch die im Übereinkommen vorgesehenen Befugnisse verschärft.

Bedenklich ist ferner, daß die Zugriffsvoraussetzungen der verschiedenen Stellen zu unterschiedlichen Zwecken nach Artikel 101 des Übereinkommens nicht hinreichend präzise bestimmt sind. Es fehlen auch exakte Kriterien für die Durchbrechung der Zweckbindung z. B. zur Verhütung von Straftaten „von erheblicher Bedeutung" nach Artikel 102.

Auch in anderen Punkten werden die Forderungen der Konferenz der Datenschutzbeauftragten vom 26./27. Oktober 1989 (8. TB, 3.8.3.2, S. 70) nicht erfüllt. So ist zwar in Artikel 126 vorgesehen, daß jede Vertragspartei spätestens bis zum Inkrafttreten in ihrem nationalen Recht für die automatische Verarbeitung personenbezogener Daten, die nach dem Übereinkommen übermittelt werden, Maßnahmen zur Gewährleistung des Datenschutzes trifft, die dem Standard der Datenschutzkonvention des Europarates von 1981 entsprechen. Die im Übereinkommen vorgesehenen Übermittlungen dürfen erst dann beginnen, wenn diese Voraussetzungen erfüllt sind. Ein erheblicher Mangel besteht jedoch darin, daß diese Vorschrift für den wesentlichen Bereich des Informationsaustauschs über Asylbewerber nicht gelten soll. Die Überwachung der Einhaltung datenschutzrechtlicher Vorschriften des Übereinkommens durch die nationalen Kontrollinstanzen soll zwar bei der Speicherung von Daten über Asylbewerber nach Artikel 38 Absatz 12 gewährleistet sein, nicht jedoch bei Übermittlungen. Ein Grund für diese Regelungslücke ist nicht ersichtlich. Wir gehen daher davon aus, daß unsere Befugnis zur Kontrolle von Übermittlungen, die von den zuständigen Stellen in Hamburg an Schengener Vertragsstaaten vorgenommen werden, unberührt bleibt.

Als Fazit ist somit zwar das Bemühen der Vertragsstaaten festzustellen, im Schengener Durchführungsübereinkommen auch Sicherungen zum Schutz personenbezogener Daten vorzusehen. Dieser Schutz ist allerdings lückenhaft. Angesichts des Datenumfangs und der überaus komplizierten Regelungen des Vertragstexts wird für kaum einen Betroffenen noch nachvollziehbar sein, wo „seine Daten geblieben" sind, wenn sie erst einmal in das System der Übermittlungen und Speicherungen nach dem Übereinkommen geraten. Während das erste Schengener Übereinkommen von 1985 den völligen Wegfall der materiellen Grenzen zwischen den Vertragsstaaten zum Ziel hatte, errichtet das Durchführungsabkommen von 1990 neue Grenzen für die Rechte der Betroffenen auf Wahrung ihres informationellen Selbstbestimmungsrechts. Auch die Datenschutzkontrolle wird zahlreiche Hindernisse überwinden müssen, bevor sie den Gefährdungen, die sich aus den Vorschriften des Zusatzabkommens zur Datenverarbeitung ergeben, entgegentreten kann.

4.12.4 On-line-Zugriff der Polizei auf das Melderegister und die Mängel des POLAS-Systems

Der Senat hat im Juli die Verordnung über den automatisierten Abruf von Daten aus dem Melderegister durch die Polizei beschlossen. Entsprechend der Vorgabe in § 31 Absatz 4 HmbMG erhält die Polizei damit erstmalig den direkten Zugriff auf Vor-, Nach- und Geburtsnamen, Anschriften und Geburtsdaten aller Hamburger Einwohner. Es ist technisch ausgeschlossen, daß auch auf nicht zugelassene Daten zugegriffen wird, da für den on-line-Anschluß der Polizei ein besonderer separierter Datenbestand angelegt wird, der täglich entsprechend den Veränderungen im Melderegister aktualisiert wird. Die Verordnung sieht ferner ein abgestuftes Vorgehen bei der polizeilichen Abfrage vor, die Daten aller unter einer Adresse gemeldeten Personen (sogenannte Hausanfrage) dürfen nur sichtbar gemacht werden, wenn die Identität einer bestimmten Person nicht auf andere Weise festgestellt werden kann. Die beim Abruf verwandten Merkmale, Zeit-

punkt der Abfrage, Kennung des Endgeräts, Dienstnummer des abrufenden Polizeibeamten, Grunddaten der Person, deren Daten abgerufen wurden sowie bei der Hausanfrage auch der Anlaß des Abrufs werden automatisch protokolliert. Insgesamt stellt die Verordnung einen befriedigenden Kompromiß zwischen den Erfordernissen der polizeilichen Aufgabenerfüllung und den Belangen des Datenschutzes dar.

Doch die beste rechtliche Regelung taugt wenig, wenn die zur Datenverarbeitung eingesetzte Technik unzulänglich ist. Zur Melderegisterabfrage soll die Technik des polizeilichen Auskunfts- und Informationssystem (POLAS) benutzt werden. Dies wäre unproblematisch, wenn es für POLAS die erforderlichen Sicherungvorkehrungen gäbe, die eine unberechtigte Benutzung der Datenendgeräte ausschließt. Doch gerade dies ist nicht der Fall. Nach einer Verfügung des Polizeipräsidenten vom 15. Juli 1983 sollte spätestens 1984 jeder zugriffsberechtigte Mitarbeiter der Polizei eine Ausweislesekarte erhalten, die eine individuelle Zugriffsberechtigung enthält. Die Erschließung von Daten der automatisierten Informationssysteme sollte dann nur noch über die Ausweiskarte durch den Belegleser möglich sein.

Dieses Verfahren ist jedoch aus technischen Gründen bis heute nicht eingeführt, weil innerhalb der Polizei andere Prioritäten gesetzt wurden. Vielmehr ist der Zugang zu POLAS nach wie vor mittels einfacher Abfrage-Codes möglich; eine wirksame Zugriffskontrolle ist nicht gewährleistet.

Eine Nutzung von POLAS für das automatisierte Abrufverfahren aus dem Melderegister ohne weitere organisatorische Vorkehrungen hätte dazu geführt, daß die nach § 31 Absatz 4 Satz 4 HmbMG und der Vorordnung über den automatisierten Abruf aus dem Melderegister zwingend vorgesehenen technischen und organisatorischen Maßnahmen zur Sicherung gegen Mißbrauch unterlaufen worden wären. Die in der Verordnung geregelte Protokollierung von Abrufen aus dem Melderegister wäre nicht verwertbar gewesen, da die einzelnen Abrufe keinem bestimmten Bediensteten zuzuordnen gewesen wären. Auch die in § 8 Absatz 2 des Hamburgischen Datenschutzgesetz vorgeschriebenen Maßnahmen zur Datensicherung bei automatisierter Datenverarbeitung werden beim POLAS-Verfahren generell nicht eingehalten, obwohl es an 108 Terminals von tausenden von Polizeibeamten täglich genutzt wird.

Nachdem wir der Nutzung des POLAS-Systems für den Melderegisterabruf mit Nachdruck widersprochen hatten, teilte uns die Behörde für Inneres mit, daß sie zwar auch ein Interesse habe, möglichst schnell ein wirksames Verfahren zur Berechtigungsprüfung einzuführen, eine sofortige Umsetzung dieser Absicht sei jedoch nicht möglich. Grund hierfür sei der geplante Vollverbund des Hamburges POLAS-Systems mit dem bundesweiten INPOL-System, der zur Zeit noch nicht realisiert ist. Im Zuge der Installation des POLAS/INPOL-Vollverbunds („POLAS III") würden sehr viel differenziertere Zugriffsbefugnisse als bisher vergeben. Erst dann lägen auch die Voraussetzungen für eine rationelle Einführung des Magnetkartensystems vor. Als Alternative sei allenfalls denkbar, die bei der Polizei zur Verfügung stehende Programmierkapazität jetzt vorrangig zur Installation des Magnetkartenverfahrens einzusetzen, dies habe jedoch zur Folge, daß der Nutzen der Magnetkarten gering sei und sich die Einführung von „POLAS III" erheblich verzögere. Zur Zeit gehe man davon aus, daß der Vollverbund bis Ende 1991 realisiert werden könne.

Diese Aussagen haben wir akzeptiert. Um wenigstens für den on-line-Zugriff auf das Melderegister eine zuverlässige Identifizierung der einzelnen Abfragen zu ermöglichen, haben wir mit der Polizei vereinbart, daß für die Übergangszeit bei allen POLAS-Terminals ein Protokollbuch geführt wird. Hier sind Zeitpunkt und Anlaß der Abfrage aus dem Melderegister, Name und Dienstnummer des Abfragenden und die zur Abfrage verwendeten Daten in allen Fällen einzutragen, in denen der Zugriff nicht lediglich zur Bestätigung bereits bekannter Daten führt, oder die Abfrage mit unvollständigem Namen oder Geburtsdatum erfolgt.

Diese Übergangslösung kommt den in der Verordnung über den automatisierten Melderegisterabruf vorgesehenen Voraussetzungen nahe, für die übrigen Nutzungen von

POLAS zu polizeilichen Zwecken läßt sich dagegen keine vergleichbare Maßnahme zur Datensicherung realisieren. Wir sind uns mit der Polizei einig, daß dieser Zustand sowohl aus datenschutzrechtlicher wie aus polizeilicher Sicht dringend bereinigt werden muß. Wir werden strikt darauf achten, daß die feste Zusage, bis Ende 1991 ein wirksames Magnetkartensystem zur Überprüfung der Zugriffsberechtigung einzuführen, diesmal eingehalten wird. Weitere Verzögerungen — etwa im Hinblick auf neue Konzeptionen im INPOL-Verbund — könnten nicht hingenommen werden.

4.12.5 APIS

Die Speicherungspraxis der Staatsschutzabteilung des Landeskriminalamts in der Datei APIS war auch in diesem Jahr ein Schwerpunkt unserer Prüfungen bei der Polizei.

4.12.5.1 Polizeiinterne Untersuchung von APIS

Nachdem infolge unserer Prüfung im Jahr 1987 (6. TB, 4.11.3.1, S. 82 ff) eine große Zahl von Personendatensätzen gelöscht worden war, haben wir die Behörde für Inneres im Februar erneut um Stellungnahme zu den im 7. Tätigkeitsbericht (4.11.5, S. 91 f) aufgeführten Fragen gebeten. Daraufhin hat uns die Behörde für Inneres davon informiert, daß versucht werde, durch Schulung der zuständigen Mitarbeiter Wiederholungen der Fehler zu vermeiden, die zu den von uns beanstandeten Speicherungen geführt haben. Ferner erhielten wir den Bericht der polizeiinternen Arbeitsgruppe APIS, die anhand von 43 zwischen September 1988 und März 1989 gespeicherten Fällen mit 106 Personendatensätzen den tatsächlichen Nutzen der APIS-Speicherungen für die praktische Arbeit der Polizei intensiv untersucht hat. Die Arbeitsgruppe hat ihre Ergebnisse folgendermaßen zusammengefaßt:

„Der kriminalistische Nutzen in Form einer schnellen oder überhaupt möglichen Tataufklärung ist" (nach den Erkenntnisen der Untersuchung) „minimal. Das haben auch die praktischen Erfahrungen der letzten Jahre mit diesem System ergeben. Die Technik bietet komfortable Recherchierungsmöglichkeiten an. Diese sind jedoch kaum nutzbar, da die Arbeitsgrundlagen — nämlich die Straftaten (meist einfache Sachverhalte ohne besondere Arbeitsweisen bzw. mit meist fehlenden Aussagen zu Personen oder Sachen und fehlenden persönlichen Merkmalen der Tatverdächtigen) — für solche differenzierten und diffizilen technischen Möglichkeiten nichts hergeben. Dennoch ist APIS, das belegen die Zahlen der Untersuchung, als umfassendes, überregionales und vor allen Dingen schnelles Auskunftssystem im Bereich der Prävention nutzbringend und erforderlich. Zu gewinnende Erkenntnisse sind auch Elemente für Lagebeurteilungen, die es der Polizei ermöglichen, sich auf bevorstehende Ereignisse einzustellen. . ."

Weiter heißt es: „So muß man bei der Frage der Zukunft dieser Datei offen an die Tatsache herangehen, daß zunächst die Distanz zwischen den technisch hochentwickelten Unterstützungsmöglichkeiten und den tatsächlichen Erfordernissen in der Bewältigung der täglichen Staatsschutzkriminalität erkannt und gegebenenfalls reduziert werden muß. Praktisch kann das einen Verzicht auf Teilbereiche, Speicher- und Recherchiermöglichkeiten bedeuten, mit dem Vorteil, mit dem vorhandenen Material effektiver arbeiten zu können."

Damit hat Hamburg als bisher einziges Land den tatsächlichen — polizeilichen — Nutzen von APIS kritisch überprüft. Dies und insbesondere auch die selbstkritische Herangehensweise der Arbeitsgruppe wird von uns ausdrücklich begrüßt. Die Anregung Hamburgs, eine vergleichbare Untersuchung auch in einem Flächenstaat durchzuführen, ist allerdings nicht aufgegriffen worden. Vielmehr hat sich der Arbeitskreis II der Innenministerkonferenz — gegen das Votum Hamburgs — dafür ausgesprochen, an der Errichtungsanordnung unverändert festzuhalten.

4.12.5.2 Erneute Prüfung von Speicherungen in APIS

Wenn auch auf Bundesebene nur unbefriedigende Konsequenzen aus den bisherigen Erfahrungen bei der Überprüfung von Speicherungen in APIS gezogen wurden, so hat-

ten wir doch gehofft, daß sich die Hamburger Praxis grundlegend verbessert habe. Um ein Bild von der derzeitigen Situation zu erhalten, haben wir die innerhalb einer Woche im April von Hamburg vorgenommenen Speicherungen anhand der polizeilichen Akten überprüft. Dabei haben wir — in der großen Mehrzahl der herangezogenen Fälle — leider wiederum schwere Mängel festgestellt.

Trotz der inzwischen erfolgten Schulung lagen unerklärliche Fehlspeicherungen vor: Eine Gruppe, gegen deren Erfassung in APIS grundsätzlich keine Bedenken bestehen, da sie mit Hakenkreuzen und SS-Runen versehene Drohbriefe versandt hatte, war als linksextremistisch gespeichert. Über einen Demonstranten, der verdächtigt wird, Polizisten angegriffen zu haben, als eine Hausbesetzung beendet wurde, wurde im Freitext zur Speicherung ausgeführt, er habe sich als Besetzer im Haus befunden, obwohl die polizeilichen Feststellungen das Gegenteil ergeben hatten. Derartige grobe Versehen wecken erhebliche Zweifel daran, ob Speicherungen in APIS mit der erforderlichen Sorgfalt vorgenommen werden. Die Brauchbarkeit der Datei für die polizeiliche Praxis — insbesondere im Verbund — wird damit in Frage gestellt.

Besonders kritisch ist, wenn bei der Sachverhaltsschilderung ein durchaus differenziertes Bild polizeilicher Feststellungen zur Unkenntlichkeit verkürzt wird und Vorgänge, die in ihrer strafrechtlichen Qualität sowie räumlich und zeitlich nicht zusammengehören, einfach vermischt werden. So war eine Gruppe von Hausbesetzern gespeichert, der nach den polizeilichen Ermittlungsunterlagen zwar das Eindringen in ein leerstehendes Gebäude vorwerfbar war, die jedoch keinesfalls für einzelne Gewalttätigkeiten im Zusammenhang mit dem Polizeieinsatz verantwortlich gemacht werden konnten, da sie von der Gruppe der Demonstranten vor dem Haus immer räumlich getrennt war. Dementsprechend waren auch lediglich Strafbefehle mit jeweils geringen Geldstrafen wegen Hausfriedensbruchs ergangen. In APIS waren die betroffenen allerdings auch wegen Landfriedensbruchs erfaßt. Der Freitext zur Speicherung war so gefaßt, daß zwischen der Hausbesetzung und den Gewalttaten gegen Polizisten nicht unterschieden werden konnte. Aus der APIS-Speicherung mußte man folgern, daß die Besetzergruppe Polizeibeamte mit Knallkörpern und ähnlichen Gegenständen beworfen und zum Teil verletzt habe, obwohl die aktenmäßig polizeilichen Feststellungen hierfür nichts hergaben. Auch hinsichtlich des Verhaltens einzelner Teilnehmer an der Besetzung wurde nicht differenziert, obwohl die Feststellungen von Polizeibeamten vor Ort um derartige Differenzierungen durchaus bemüht waren.

Streitig ist zwischen uns und der Polizei derzeit, ob die APIS-Erfassung der Teilnehmer an der Hausbesetzung überhaupt von der Errichtungsanordnung gedeckt war, denn auch wenn sich die Betroffenen strafbar gemacht haben und hierbei ein politisches Motiv hatten, so ist zweifelhaft, ob aus einer demonstrativen Aktion gegen leerstehenden Wohnraum oder auch gegen die Wohnungspolitik generell eine gegen die verfassungsmäßige Ordnung gerichtete Zielsetzung hergeleitet werden kann.

Auch einzelne Korrekturen, die in Reaktion auf unsere letzte Überprüfung angekündigt worden sind, wurden nicht beachtet. So sollten zufällig Geschädigte — etwa Eigentümer von Häusern, an die Parolen oder Hakenkreuze gemalt werden — nicht mehr erfaßt werden, gleichwohl haben wir derartige Fälle festgestellt.

Für 19 von 22 der überprüften Personendatensätze haben wir die vollständige Löschung, bei mehreren institutions- oder gruppenbezogenen Feststellungen Berichtigungen gefordert. Dazu hat die Behörde für Inneres noch nicht Stellung genommen.

4.12.5.3 Schlußfolgerungen

Wenn APIS für die Aufklärung von Straftaten, also die vordringliche polizeiliche Aufgabe nach den Ergebnissen der polizeiinternen Untersuchung nur einen minimalen Nutzen hat, wird Argumenten, die bisher zur Rechtfertigung der Speicherpraxis angeführt worden sind, der Boden entzogen. Die Auffassung der Behörde für Inneres, daß APIS als „ermittlungsunterstützendes Recherchiersystem alle Informationen enthalten müsse, die Eingang in die Ermittlungsakte finden, auch wenn diese Informationen

noch nicht abschließend bewertet sind", kann somit nicht mehr hingenommen werden. Wir haben daher gefordert, daß zumindest in den Fällen von sogenannten anderen Straftaten, die keine eigentlichen Staatsschutzdelikte sind, Sachverhalte erst dann in APIS eingegeben werden, wenn nach Abschluß des Ermittlungsverfahrens die strafrechtliche Würdigung und die APIS-Relevanz auf einigermaßen gesicherter Grundlage beurteilt werden kann.

Auch wenn diese Verbesserung erfolgt, wird die generelle Skepsis gegenüber APIS voraussichtlich nicht ausgeräumt werden können. Alle Überprüfungen der Speicherungspraxis durch uns oder die Polizei selbst haben schwerwiegende Mängel aufgezeigt. Es spricht nichts für die Vermutung, daß dies immer nur „Zufallsfunde" waren, vielmehr dürften ganz erhebliche strukturelle Defizite die Ursache sein. Der Bericht der polizeiinternen Arbeitsgruppe spricht dies ebenfalls an, wenn gefordert wird, daß „die Distanz zwischen den technisch hochentwickelten Unterstützungsmöglichkeiten und den tatsächlichen Erfordernissen in der Bewältigung der täglichen Staatsschutzkriminalität erkannt und gegebenenfalls reduziert werden muß". Dieser „Erkenntnisprozeß" würde eigentlich eine dauernde externe wie interne Überprüfung der Speicherungspraxis erfordern, was schon allein angesichts der ständig wachsenden Zahl gespeicherter Personendatensätze unrealistisch ist. Solange die Polizeien in Bund und Länder nicht bereit sind, die Datei APIS durch eindeutige schriftliche Vorgaben auf ihren eigentlichen Zweck zurückzuführen, werden voraussichtlich auch weitere Stichprobenkontrollen zu dem Ergebnis führen, daß Speicherungen in APIS das informationelle Selbstbestimmungsrecht zahlreicher Betroffener unverhältnismäßig beeinträchtigen und der polizeiliche Nutzen der Daten insgesamt mehr als zweifelhaft ist.

4.12.6 Prüfung der Sexualtäterdatei

Im Berichtszeitraum haben wir die Sexualtäterdatei überprüft. Sie wird bei der für die Verfolgung von Straftaten gegen die sexuelle Selbstbestimmung zuständigen Dienststelle des Landeskriminalamts geführt und ist nach den Deliktstypen des dreizehnten Abschnitts des Strafgesetzbuchs (§§ 174 bis 184b) und einzelnen Begehungsformen aufgebaut. Innerhalb dieser Untergruppen ist sie nach den Geburtsjahren der gespeicherten Personen geordnet.

Maßgebend für diesen Aufbau ist zum einen der kriminologische Ansatz, daß Sexualstraftäter häufig Wiederholungstäter sind und ihre Taten nach einem verhältnismäßig konstanten Muster begehen. Zum anderen sind die Tatopfer fast immer in der Lage, Angaben über die Begehungsweise und das Alter des Täters zu machen. Somit kann unter einer begrenzten Anzahl von gespeicherten Personen gezielt nach bestimmten Tätern gesucht werden. Diesem Zweck dienen ferner verschiedenfarbige Reiter (z. B. für „gibt sich als Beamter aus"), mit denen einzelne Karteikarten in allen Deliktsgruppen versehen werden können.

Auf der Vorderseite der Karteikarten werden Identifizierungsdaten von Personen eingetragen, die bereits zuvor einschlägig in Erscheinung getreten sind. Auf der Rückseite befinden sich Kurzdarstellungen der Delikte. Das Ergebnis der Ermittlungs- oder Strafverfahrens wird nicht regelmäßig vermerkt. Den Karteikarten liegt mindestens ein Foto des Beschuldigten bei.

Häufig enthielten die Karteikarten Namen und Adressen von Eltern und/oder Ehepartnern der gespeicherten Person. Die Karteikartenvordrucke sehen diese Rubriken vor. In mehreren Fällen (insbesondere bei Straftaten gegen Kinder und sexuelle Nötigung oder Vergewaltigung) waren bei der Schilderung der Taten Namen von Opfern eingetragen. Nach der Auskunft der zuständigen polizeilichen Sachbearbeiter sind diese Angaben über Verwandte und Opfer in aller Regel nicht erforderlich. Wir konnten uns daher schnell mit der Polizei darüber verständigen, daß derart sensible Daten in Zukunft nicht mehr aufgenommen werden, und daß die vorhandenen Angaben über Verwandte und Opfer im Einzelfall gelöscht werden. Die prompte Bereitschaft der Polizei zur Korrektur der bisherigen Praxis wird von uns ausdrücklich begrüßt.

Bei der Durchsicht von Karteikarten aus allen größeren Rubriken haben wir keine Fälle festgestellt, in denen Speicherfristen überschritten waren, Sachverhalte aufgenommen waren, die nicht oder nicht mehr strafbar sind oder das Erreichen der Erheblichkeitsschwelle von § 184c StGB zweifelhaft war.

Unter diesen Voraussetzungen haben wir keine Bedenken gegen die Führung der Datei geltend gemacht.

4.12.7 Prüfung der Datei junger Gewalttäter

4.12.7.1 Problematik der Feststellungsanordnung

Bereits seit mehreren Jahren führt die Polizei eine Datei junger Gewalttäter. Im Januar dieses Jahres wurde endlich eine Feststellungsanordnung erlassen und eine spezielle polizeiliche Einsatzgruppe mit der Dateiführung beauftragt. Nach der Feststellungsanordnung sollen Personen zwischen 14 und 25 Jahren, die in einer Gruppe, einzeln im Schutz, aufgrund ihrer Verbindung oder unter dem Einfluß einer Gruppe mehrfach Straftaten mit Gewaltanwendung begehen und dabei Rohheit und Brutalität zeigen, in der Datei gespeichert werden. Allerdings sollen nicht nur Beschuldigte und Verdächtige Aufnahme finden, sondern auch sogenannte „andere Personen", wenn sie mit Straftaten junger Gewalttäter in Verbindung stehen und zureichende Anhaltspunkte die Annahme rechtfertigen, daß dies zur Aufklärung oder vorbeugenden Bekämpfung erheblicher Straftaten junger Gewalttäter, zur Ergreifung gesuchter Personen oder zur Gefahrenabwehr im Einzelfall erforderlich ist. Nach dem Wortlaut der Feststellungsanordnung sind hierunter insbesondere Gruppenmitglieder zu verstehen, denen eine direkte Beteiligung an Straftaten nicht nachgewiesen werden kann, die aber durch ihre Zugehörigkeit zur Gruppe oder Anwesenheit vor, bei oder nach Straftaten diese fördern oder ermöglichen.

Im Verfahren zur Abstimmung der Feststellungsanordnung haben wir immer wieder deutlich gemacht, daß die Gruppenzuordnung nach dem Wortlaut zu vage ist und insbesondere für die sogenannten anderen Personen keine zuverlässige Abgrenzung ermöglicht.

4.12.7.2 Überprüfung der Datei

Eine Überprüfung der Datei hat diese Bedenken im wesentlichen bestätigt.

Der Nutzen der Datei insgesamt soll nach der ausführlichen Darstellung durch die Vertreter der Polizei in erster Linie darin bestehen, Zeugen oder Geschädigten in Fällen der Strafverfolgung Lichtbilder zur Wiedererkennung von Tätern vorzulegen. Die Datei wird auch bei der Vorbereitung von Präventiveinsätzen, Einsätzen des Jugenschutzes sowie für die Erstellung von Lagebeurteilungen herangezogen. Diese Möglichkeiten zur Nutzung sind jedoch eher gering, da die auf jugendliche Gewalttäter spezialisierten Polizeibeamten in der Regel detaillierte Kenntnisse über den betroffenen Personenkreis haben, der Wiedererkennungswert für andere Polizisten im Einsatz aufgrund der Lichtbilder dagegen problematisch ist.

Unter der Voraussetzung, daß bereichsspezifische gesetzliche Grundlagen für die polizeiliche Datenverarbeitung geschaffen werden, haben wir keine grundsätzlichen Bedenken dagegen vorgebracht, die Datei als Lichtbildersammlungen über nachweisbar strafrechtlich in Erscheinung getretene Täter zu nutzen. Hierbei kann die Zugehörigkeit zu einer Gruppe wie Punker, Skinheads, Fußballrowdys, als Unterscheidungsmerkmal herangezogen werden, um Zeugen von vornherein nur Lichtbilder über den in Betracht kommenden Personenkreis vorzulegen.

Der von der Feststellungsanordnung erhobene Anspruch, wonach die Datei auch Erkenntnisse über Entwicklung und Zusammensetzung von Gruppen, Treffpunkte etc. und Hilfestellung bei Präventivmaßnahmen ermöglicht, kann dagegen in der Praxis kaum erfüllt werden. Vielmehr ist nach den Erläuterungen der Mitarbeiter der Einsatzgruppe Spezialkenntnis über die Gruppen und deren Angehörige Voraussetzung für

die Arbeit mit der Datei. Denkbar wäre allenfalls, daß die Datei bei klar abgrenzbaren Gruppen gewisse Rückschlüsse auf die Zahl krimineller Gruppenmitglieder in einem überschaubaren Zeitpunkt zuläßt. Voraussetzung hierfür wäre jedoch, daß eine sehr viel engere Eingrenzung der Gruppen vorgenommen würde. Keinesfalls erscheinen die bloßen Kriterien „Skins", „Punks", „Fußballfans" etc. geeignet, solche Erkenntnisse zu vermitteln.

Auch über die Intensität der strafbaren Betätigung von Gruppen und ihrer Mitglieder gibt die Datei keinerlei Auskunft, da — wenn überhaupt — Straftatbestände lediglich rudimentär erfaßt werden, jedoch keine Hinweise auf die Vorgehensweise.

Wer erkennen will, ob es sich bei einer gespeicherten Person um das Mitglied einer gefährlichen „Schlägerbande" oder jemand handelt, der ab und zu in alkoholisiertem Zustand unbedeutende Rangeleien begehen, wird ohne Hinzuziehung von Akten durch die Datei sehr schlecht bedient.

Im Unterschied zu dem sehr reduzierten aber durchaus vorhandenen Nutzen bei der Lichtbildvorlage erscheint uns die erheblich umfangreichere sogenannte „Obachtdatei" insgesamt fragwürdig zu sein. In der Mehrzahl der Fälle entfällt bei ihr der Vorgangsnachweis für Lichtbildvorlagen, da die dateiführende Stelle nur zu wenigen in der Obachtdatei gespeicherten Personen Lichtbilder vorhält. Sie dient vielmehr im wesentlichen als Nachweis von Erkenntnissen anderer Polizeidienststellen über jugendliche Gewalttäter.

Die Problematik der Obachtdatei spitzt sich bei den sogenannten anderen Personen weiter zu. Anhand der Eintragungen war in mehreren Fällen nur zu vermuten, daß es sich um andere Personen in diesem Sinne handelt. Wegen des eingeschränkten Nutzens der Datei würde es jedoch keinen Sinn machen, in den Karteikarten die Gründe für die Einordnung als andere Person zu vermerken. Da über andere Personen mangels Verdacht keine Lichtbilder auf Dauer aufbewahrt werden können, entfällt vielmehr grundsätzlich die Möglichkeit, Daten zu anderen Personen in der Datei junger Gewalttäter zu speichern und zu nutzen. Als äußerst problematisch ist bei der derzeitigen Praxis die Tatsache anzusehen, daß die Speichervoraussetzungen für die anderen Personen wesentlich geringer sind als für Beschuldigte und Verdächtige, da hier in der Regel mindestens zwei Straftaten vorliegen müssen. Bei anderen Personen reicht jedoch die einmalige Annahme der Kriterien der Feststellungsanordnung aus, und teilweise erfolgt die Speicherung aufgrund bloßer Anhaltemeldungen oder Ingewahrsamnahmen nach § 13 SOG.

4.12.7.3 Forderungen

Für die weitere Führung der Datei haben wir daher folgende Forderungen aufgestellt:

— Es sollte überprüft werden, ob ein Nachweis von Erkenntnissen anderer Polizeidienststellen zwingend erforderlich ist und wenn ja, ob POLAS hierfür ausreicht, auf die Obachtdatei somit verzichtet werden kann.

— Eine regelmäßige Speicherung von sogenannten anderen Personen muß ebenfalls unterbleiben. Nach eingehender Prüfung der vorhandenen Abgrenzungsmöglichkeiten für in Betracht kommende Gruppen könnte die Speicherung anderer Personen in Ausnahmefällen dann denkbar sein, wenn sich eine Förderung der Gewalttätigkeit abgrenzbarer Gruppen oder Gruppenzugehöriger tatsächlich feststellen läßt. Die hierfür notwendigen Feststellungen müssen den Voraussetzungen gleichkommen, die auch für Beschuldigte und Verdächtigte gelten (dauernde Zugehörigkeit zu einer ständig gewalttätigen Gruppe; Anwesenheit bei mindestens 2 Straftaten etc.).

— Die Feststellungsanordnung ist entsprechend neu zu fassen (entweder generelle Streichung der anderen Personen, oder erforderlichenfalls klare Begrenzung auf die Ausnahmefälle).

In einer ersten Stellungnahme hat es die Behörde für Inneres abgelehnt, die Feststellungsanordnung zum Kreis der sogenannten „anderen" Personen zu ändern, da hiervon eine Verbesserung der tatsächlichen Handhabung der Kartei nicht zu erwarten sei.

Allerdings soll zukünftig auf den Karteikarten vermerkt werden, daß es sich um eine „andere" Person handelt.

Zur Frage, ob eine bessere Zuordnung von gespeicherten Personen zu bestimmten Gruppen möglich ist, war bei Redaktionsschluß dieses Berichts die Meinungsbildung der Behörde für Inneres noch nicht abgeschlossen.

4.12.8 Bedenkliche Praxis bei der Löschung polizeilicher Daten

Wenn Bürger von ihren Rechten auf Auskunft, Berichtigung, Sperrung und Löschung ihrer Daten Gebrauch machen, entsteht hierüber wie in allen anderen Bereichen der Verwaltung auch zunächst einmal ein schriftlicher Vorgang: Die Betroffenen fragen unmittelbar oder im Wege einer Eingabe an den Hamburgischen Datenschutzbeauftragten schriftlich an, ob Daten über sie gespeichert sind, oder beantragen aufgrund einer Auskunft die Löschung. Auch unsere Stellungnahmen, die schriftlichen Antworten der Polizei und eventuelle Rechtsbehelfe gehören zu diesem besonderen polizeilichen Vorgang.

Aufgrund eines Einzelfalls haben wir festgestellt, daß derartige Vorgänge im Bereich der Polizeidienststelle mindestens noch drei Jahre lang aufbewahrt werden, die auch die Speicherung in der polizeilichen Datei veranlaßt hatte. Wenn Betroffene die Mitteilung erhalten, ihre Daten seien gelöscht, bekommen sie den Eindruck, daß die Polizei nunmehr nicht mehr über die gelöschten Informationen verfüge. Tatsächlich sind diese Informationen jedoch in unmittelbarer Nähe der Datei noch vorhanden, und alle Bediensteten, die vorher Zugang zur kriminalpolizeilichen Sammlung hatten, können nach wie vor ohne großen Aufwand nachschauen, was dort in einem Aktenordner oder einer sonstigen sorgfältig geführten namensalphabetisch geordneten Sammlung mit der Aufschrift „Anträge auf Auskunft, Sperrung, Löschung etc." noch vorrätig ist. Es hängt dann zwar vom Einzelfall ab, wie aussagekräftig diese Schriftstücke sind. Wenn die Betroffenen, der polizeiliche Sachbearbeiter oder ein Mitarbeiter des Hamburgischen Datenschutzbeauftragten sehr gründlich waren und die einzelnen zu löschenden oder gelöschten Daten genau bezeichnet haben, geht nicht einmal ein Bruchteil der bisherigen Informationen durch die Löschung verloren. Auch wenn einmal nicht so gewissenhaft gearbeitet wurde, ist die Tatsache, daß die Polizei früher über Daten zu einer bestimmten Person verfügte, immer noch von Interesse, vor allem wenn die jeweilige Dienststelle ganz besondere polizeiliche Aufgaben wahrnimmt (z. B. die Verfolgung von Staatsschutzdelikten). Der Informationswert vieler Dateien ist ohnehin nicht erheblich größer. Die Aufbewahrungsfrist hängt davon ab, ob vielleicht jemand nach einer gewissen Zeit noch mal nachgefragt hat, da die dreijährige Frist ordnungsgemäß erst ab dem letzten relevanten Vorgang zu laufen beginnt.

Dieser Praxis haben wir mit Nachdruck widersprochen. Sie ist geeignet, alle Speicherungsfristen, die für kriminalpolizeiliche Sammlungen gelten, zu unterlaufen, da immer dann, wenn die Betroffenen von ihren elementaren Rechten nach dem Datenschutzgesetz Gebrauch machen, eigene Vorgänge mit eigenen Speicherungsfristen entstehen und die ursprünglichen Speicherungen in polizeilichen Dateien ersetzen. Sie beeinträchtigt damit insgesamt die Wahrnehmung der Rechte auf Auskunft, Berichtigung, Sperrung und Löschung. Auskünfte über gespeicherte Daten und die vorgesehenen Löschungsfristen, die sich nicht auf diese Sekundärvorgänge beziehen, täuschen die Betroffenen und alle anderen am Verfahren Beteiligten über den wahren Sachverhalt, solange diese Praxis beibehalten wird.

Selbstverständlich kann in der Mehrzahl der Fälle nicht auf die schriftliche Erledigung derartiger Ersuchen verzichtet werden, und die Vorgänge sind auch eine zeitlang aufzubewahren. Aufbewahrungsort kann jedoch nicht die dateiführende Stelle selbst sein. Wir haben vorgeschlagen, derartige Vorgänge im Bereich der Rechtsabteilung der Landespolizeiverwaltung, die ohnehin bei allen Anträgen auf Auskunft etc. beteiligt wird, aber keine eigenen vollzugs- oder kriminalpolizeilichen Aufgaben wahrnimmt, zu zentralisieren. Ganz wesentlich ist jedoch, daß die Aufbewahrungsdauer dieser schriftlichen Vorgänge maximal auf die Speicherungsfrist in den kriminalpolizeilichen Samm-

lungen terminiert wird. Wird also die Auskunft erteilt, daß bestimmte Daten gespeichert sind und zu einem späteren Zeitpunkt nach den Richtlinien zur Führung kriminalpolizeilicher Sammlungen zu löschen sind, muß die Löschung auch diese schriftliche Auskunft selbst und alle weiteren Vorgänge im Zusammenhang mit dem Ersuchen umfassen.

Eine Stellungnahme der Polizei lag bis Redaktionsschluß zu diesem Bericht noch nicht vor.

4.12.9 Verfahren zur „Computerunterstützten Vorgangsbearbeitung" bei der Hamburger Polizei — COMVOR

Bereits 1988 ist eine Arbeitsgruppe gebildet worden, die die Aufgabe hat, ein umfassendes Verfahren zur Computerunterstützten Vorgangsbearbeitung (COMVOR) in allen Bereichen der Hamburger Polizei zu entwickeln und schrittweise einzuführen. Dieses äußerst ehrgeizige Projekt wird mit der Zielsetzung betrieben, eine einheitliche Struktur zur rechnerunterstützten Datenverarbeitung der Polizei zu schaffen, die die Bearbeitung und Verwaltung aller Arten polizeilicher Tätigkeiten ermöglicht und somit gleichermaßen die polizeiliche Tätigkeit effizienter machen, Stellen und Kosten einsparen soll. Mitarbeiter der Polizei sollen bei ihrer Arbeit von Anfang an durch Informations- und Kommunikationstechnik unterstützt werden. es soll in Zukunft nicht mehr erforderlich sein, auf verschiedene, getrennte Arbeitsmittel zurückzugreifen zu müssen. Voraussetzung hierfür ist die Integration aller bisher bestehenden Informationssysteme zu einem logisch einheitlichen Datenbestand, der das bisherige POLAS/INPOL-System ebenso umfaßt wie die polizeiliche Kriminalstatistik und die Vorgangsbearbeitung im Einzelfall. COMVOR würde somit gleichermaßen ein Textverarbeitungssystem enthalten wie die Kommunikation innerhalb der Polizei gewährleisten, sämtliche „Formblätter", die für die polizeiliche Sachbearbeitung erforderlich sind, zur Verfügung stellen, aber auch Anfragen bei allen polizeilichen Dateien und die Recherche mit mehreren verknüpfbaren Anfragekriterien ermöglichen.

Nach dem derzeitigen Sachstand sind dies Wunschvorstellungen der Polizei. Ob sie realistisch sind, muß als offen bezeichnet werden. Die technischen und organisatorischen Probleme, die sich bei wesentlich bescheideneren Neuerungen der IuK-Technik im Bereich der Polizei immer wieder ergeben, sprechen eher dagegen, daß COMVOR in einem überschaubaren Zeitrahmen eingeführt werden kann. Wir stehen mit der Arbeitsgruppe in ständigem und durchaus konstruktivem Meinungsaustausch, wobei allerdings bisher nur einige der Fragen, die aus datenschutzrechtlicher Sicht zu diesem Vorhaben zu stellen sind, angesprochen werden konnten.

Aus unserer Sicht liegt das Grundproblem darin, ob es überhaupt akzeptabel ist, sämtliche polizeilichen Daten in einem zentralen Datenpool zusammenzufassen und die Möglichkeit zu schaffen, sie ohne weiteres zu verknüpfen und auszuwerten, obwohl die Mehrzahl der Daten immer nur im Einzelfall lokal benötigt werden. Maßgeblich hierfür wird sein, welche Abschottungen nach Verarbeitungszwecken und Zugriffsberechtigungen erreicht werden und wie Zugriffe im Einzelfall kontrolliert werden können. Ungeklärt sind bisher auch die häufig auftretenden Fälle, daß Betroffene im Zuge polizeilicher Ermittlungen unterschiedliche Rollen einnehmen können (z. B. der Verdacht gegen den bisher Beschuldigten entfällt). Bleibt die Person als Zeuge oder Geschädigter im strukturierten Datenbestand gespeichert, welche Fristen und Zugriffsrechte sollen gelten? Wie erfolgt die Zuordnung eines neuen Vorgangs einer anderen Polizeidienststelle zum gleichen Sachverhalt, zur gleichen Person oder Objekt? Welche Informationen über den bereits bestehenden Vorgang erhalten die Sachbearbeiter der anderen Dienststellen? Soll die Aufbewahrung nach Abschluß des polizeilichen Verfahrens, die nur noch Dokumentationszwecken dienen kann, auch elektronisch erfolgen, welche Differenzierungen hinsichtlich der Zugriffsrechte sind hier erforderlich?

Von zentraler Bedeutung für das weitere Vorgehen der Arbeitsgruppe wird das Verhältnis der Polizei zur Staatsanwaltschaft im Strafermittlungsverfahren sein. Würde man die Staatsanwaltschaft für alle Daten, die im Strafvermittlungsverfahren anfallen, als

speichernde Stelle ansehen, da die Kriminalpolizei Hilfsorgan der Staatsanwaltschaft ist, läge die materielle und datenschutzrechtliche Verantwortung für diesen ganz wesentlichen Bereich von COMVOR bei ihr. Ist jedoch die Polizei auch im Strafermittlungsverfahren allein speichernde Stelle, stellt sich die Frage, ob der Staatsanwaltschaft eigene Zugriffsbefugnisse auf COMVOR eingeräumt werden müssen. Die Diskussion über diese Problemkreise hat erst begonnen, sie wird — auch unter Einbeziehung der Staatsanwaltschaft — weiter geführt werden müssen. Eine — auch nur vorläufige — Bewertung von COMVOR aus datenschutzrechtlicher Sicht wäre daher verfrüht.

4.13 Geheimdienste

4.13.1 Stand der Gesetzgebung

Entgegen der im letzten Tätigkeitsbericht (8. TB, 3.9.1, S. 76) geäußerten Befürchtung ist es kurz vor Fertigstellung dieses Berichts doch noch gelungen, im Rahmen eines Artikelgesetzes (vgl. 1.2) für die Geheimdienste des Bundes die lange geforderten gesetzlichen Grundlagen zu schaffen. Zeit für eine sorgfältige Analyse und Bewertung der — insbesondere vom Vermittlungsausschuß — noch bis zuletzt vorgenommenen Änderungen hatten wir bisher nicht.

Klar dürfte aber sein, daß jetzt — nachdem das Bundesverfassungsschutzgesetz novelliert ist — auch der Senat zügig einen Entwurf für ein Hamburgisches Verfassungsschutzgesetz vorlegen muß, damit auch das hamburgische Landesamt für Verfassungsschutz seine Arbeit auf gesetzliche Grundlagen stützen kann, die den verfassungsrechtlichen Vorgaben entsprechen. Umfassende Vorschläge dazu haben wir im letzten Tätigkeitsbericht (8. TB, 3.9.1.1 bis 3.9.1.9, S. 76 ff) gemacht. Wir würden es sehr begrüßen, wenn der Senat diese aufgreifen und in den Arbeiten für einen Gesetzesentwurf berücksichtigen würde.

4.13.2 Erfassung von Aus- und Übersiedlern — Datei „ADOS"

Ebenfalls im letzten Tätigkeitsbericht (8. TB, 3.9.2, S. 82 ff) hatten wir über unseren Widerstand gegen das begonnene Vorhaben der Verfassungsschutzbehörden berichtet, sämtliche Aus- und Übersiedler sowie die Asylbewerber aus den osteuropäischen Staaten über ihre Registriernummer zu erfassen und in der Datei „ADOS" zu speichern. Dies hätte zur — unzulässigen — Speicherung von vielen hunderttausend Menschen geführt. Nun können wir über die Stellungnahme des Senats zu unserem 8. Tätigkeitsbericht hinaus davon Kenntnis geben, daß das Vorhaben endgültig aufgegeben, die Datei ADOS aufgelöst und sämtliche Datensätze sowie die Protokollbänder zu ADOS gelöscht wurden. Sicher haben die politischen Veränderungen und nicht die Rechtsauffassung der Datenschutzbeauftragten diesen Erfolg bewirkt. Den Betroffenen dürfte dies gleichgültig sein.

4.14 Justiz

4.14.1 Stand der Gesetzgebung

4.14.1.1 Novellierung der Strafprozeßordnung

Im letzten Tätigkeitsbericht (8. TB, 3.10.1, S. 85 ff.) hatten wir ausführlich über die Bemühungen, den Strafverfolgungsbehörden rechtsstaatlich einwandfreie Grundlagen für ihre Arbeit zu schaffen, berichtet. Dies ist schon seit vielen Jahren eines der dringendsten Anliegen all jener, die befürchten, die Arbeit dieser Behörden könnte deshalb ins Zwielicht geraten, weil sich der Gesetzgeber verweigert. Im Hinblick auf die bis dahin geleistete Arbeit hatten wir gehofft, die Strafprozeßordnung könnte noch bis zum Ende der laufenden Legislaturperiode die parlamentarischen Hürden nehmen. Wir hatten nicht damit gerechnet, daß — wie nun geschehen — mit der Vorlage des Entwurfes des Strafverfahrensänderungsgesetzes 1989 im Juni des letzten Jahres sämtliche

Bemühungen eingestellt wurden, so daß Polizei, Staatsanwaltschaft und Gerichte voraussichtlich noch für längere Zeit mit leeren Händen dastehen werden.

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

Hinter diesem beeindruckenden Titel verbirgt sich u.a. der Versuch der Innenminister, über den Bundesrat an der stockenden Novellierung der Strafprozeßordnung (vgl. 4.14.1.1) vorbei doch noch die gesetzliche Absicherung für bestimmte geheime Ermittlungsmethoden wie den Einsatz verdeckter Ermittler, Abhörgeräte und Richtmikrofone, Rasterfahndung und heimliche Film- und Fotoaufnahmen zu erreichen.

Diese Methoden mögen für bestimmte Erscheinungsformen von Kriminalität zum Schutze der Bürger erforderlich sein. Darauf beschränkte sich der Entwurf jedoch nicht. Vielmehr sollten mit ihm diese tief in die Privatsphäre der Bürger eingreifenden Fahndungs- und Ermittlungsmethoden in das Strafverfahrensrecht allgemein eingeführt werden.

Der Entwurf forderte deshalb Kritik von vielen Seiten heraus. Auch die Datenschutzbeauftragten von Bund und Ländern trafen sich zu einer Sonderkonferenz, um ihre Bedenken zu formulieren. Insbesondere die folgenden Punkte hoben sie hervor:

— Die vorgesehenen Eingriffsbefugnisse der Strafverfolgungsbehörden werden an den konturenlosen Begriff „Straftaten von erheblicher Bedeutung" geknüpft. Damit dürfte nach der Begründung in der Praxis allenfalls die Kleinkriminalität ausscheiden. So soll z.B. auch die Rasterfahndung für eine Vielzahl von Delikten außerhalb organisierter Kriminalität zugelassen werden. Dies erscheint besonders bedenklich, weil gerade diese Form der Fahndung unbescholtene Bürger in großer Zahl unvermeidlich mit einbezieht und sie in der Folge Ziel weiterer Ermittlungen werden können.

— Tief in die Privatsphäre eindringende Ermittlungsmethoden werden nicht hinreichend präzisiert und sind großenteils unverhältnismäßig: So dürfen ohne Wissen des Betroffenen zur Aufklärung jeder Straftat — sogar in Wohnungen hinein — „Lichtbilder und Bildaufzeichnungen" aufgenommen sowie „besondere Sichthilfen" eingesetzt werden.

— Maßnahmen wie Einsatz von Peilsendern, Richtmikrofonen, Wanzen und sonstiger Überwachungstechniken können sich auch gegen dritte unverdächtige Personen richten, wenn „aufgrund bestimmter Tatsachen" anzunehmen ist, „daß sie mit dem Täter in Verbindung stehen oder eine solche Verbindung hergestellt wird". Es bleibt völlig offen, wie das Tatbestandsmerkmal der „Verbindung" eingegrenzt werden soll. Foto- und Filmaufnahmen von Unbeteiligten sind bereits zulässig, wenn sie für Ermittlungen „geeignet" sind. Damit kann kein Bürger vorhersehen, ob und wann er hiervon betroffen sein kann. Ohne Kenntnis der gegen ihn gerichteten Eingriffe kann er im Regelfall nicht einmal Rechtsschutz erlangen.

— Die Möglichkeiten der Telefonüberwachung werden über das vertretbare Maß hinaus ausgeweitet.

— Bedenken richten sich ferner dagegen, bei besonderen Ermittlungsmaßnahmen auf die vorherige richterliche Kontrolle zu verzichten und durch Eilkompetenzen die Entscheidung der diese Maßnahmen selbst durchführenden Polizei zu übertragen. Nicht einmal die nachträgliche richterliche Kontrolle ist in jedem Fall zwingend vorgesehen.

Im Gegensatz zu den erweiterten Befugnissen der Strafverfolgungsbehörden sind Regelungen zum Schutz oder im Interesse der Betroffenen nur unzureichend vorgesehen. Die mit besonderen Ermittlungsmethoden für besondere Strafverfolgungszwecke erhobenen Daten dürfen für zu weitgehende andere Zwecke verwendet werden. So sind z.B. die Begriffe „Zwecke der staatsanwaltschaftlichen Vorgangsverwaltung" und „Zwecke der Rechtspflege" zu unbestimmt. Es fehlen weiterhin ausreichende Bestimmungen zum Auskunftsrecht des Betroffenen und zur Löschung.

Selbst die Bundesregierung mußte in ihrer Stellungnahme zu dem Gesetzesentwurf des Bundesrates darauf hinweisen, „daß einzelne Vorschläge unter verfassungsrechtlichen und datenschutzrechtlichen Gesichtspunkten nicht unproblematisch erscheinen und näherer Prüfung bedürfen" (BT-Drucksache 11/7663, S. 52).

Dagegen hielten der Innen- und der Justizsenator, die vom Hamburgischen Datenschutzbeauftragten angeschrieben worden waren, weil mit dem Gesetzesentwurf auch der datenschutzrechtliche Standard des vom Senat beschlossenen Entwurfs zur Novellierung des Polizeirechts (vgl. 8. TB, 3.8.1, S. 51 ff.) unterboten wurde, die Regelungen für akzeptabel.

Aus Sicht des Datenschutzes kann nur begrüßt werden, wenn dieser Entwurf am Ende der Legistlaturperiode der Diskontinuität zum Opfer fällt. Die darin enthaltene Energie wäre besser in die rechtsstaatliche Ausgestaltung der Strafprozeßordnung investiert worden und es ist zu hoffen, daß die Arbeiten daran bald wieder aufgenommen werden.

4.14.1.3 Justizmitteilungsgesetz

Daß die Übermittlung unzähliger personenbezogener Daten aus den verschiedensten Verfahren der Zivil- und Strafgerichtsbarkeit nicht gesetzlich legitimiert ist, sondern auf der Grundlage einfacher Verwaltungsvorschriften erfolgt, obwohl solche Mitteilungen schwerwiegende Folgen für die Betroffenen haben können, wird von den Datenschutzbeauftragten schon seit vielen Jahren bemängelt. Eine Reihe von Betroffenen haben inzwischen beim Bundesverfassungsgericht Verfassungsbeschwerde gegen diese Praxis eingelegt, ohne daß bislang eine Entscheidung ergangen wäre.

Deshalb haben wir es begrüßt, daß der Bundesjustizminister nach einigen Jahren Pause die Arbeiten am Justizmitteilungsgesetz wieder aufgenommen hat und im Mai 1990 einen neuen Referentenentwurf zur Diskussion stellte. Leider wies auch dieser Entwurf wieder erhebliche Mängel auf:

— So begnügte er sich im wesentlichen mit weit gefaßten Rahmenvorschriften und Generalklauseln, die nach der Konzeption des Bundesjustizministers erst durch Verwaltungsvorschriften ausgefüllt und konkretisiert werden sollen. Damit verfehlt der Entwurf das Ziel der Normenklarheit. So kann der Bürger aus dem Gesetz nicht mehr erkennen, an wen bei welcher Gelegenheit personenbezogene Daten von ihm übermittelt werden. Dieses Defizit könnte bei Erhaltung einer gewissen Flexibilität dadurch behoben werden, daß der Gesetzgeber hinreichend konkretisierte Ermächtigungsgrundlagen schafft und auf der zweiten Stufe die Verwaltungsschriften durch Rechtsverordnungen ersetzt werden. Nur so wird er auch seiner Pflicht genügen können, das „Wesentliche" selbst zu regeln.

— Ein erheblicher Mangel des Entwurfs besteht darin, daß er fast durchgängig Datenübermittlungen schon dann vorsieht, wenn die Daten beim Empfänger für bestimmte Zwecke erforderlich sein können. Damit werden die datenübermittelnden Stellen auf seiten der Justiz praktisch von jeglicher Verantwortung freigezeichnet und großzügige Übermittlungsmöglichkeiten eröffnet. Dies ist auch deshalb bedenklich, weil Justizmitteilungen in der Regel Daten von hoher Sensibilität betreffen.

— Auch im weiteren zeichnet sich der Entwurf nicht dadurch aus, daß die Rechte des Betroffenen in ein ausgewogenes Verhältnis zu den Interessen der am Justizmitteilungsverfahren beteiligten Stellen gebracht werden. So wird die Verfolgung von Straftaten und Ordnungswidrigkeiten ebenso gleichgestellt wie die Abwehr erheblicher Nachteile für das Gemeinwohl mit sonst drohenden Gefahren für die öffentliche Sicherheit, obwohl eine Differenzierung nach dem jeweiligen Übermittlungszweck angebracht wäre.

— Besonders problematisch ist eine Übermittlung von Strafverfahrensdaten vor einer verfahrensbeendenden Entscheidung. Dies birgt die Gefahr in sich, daß die Betrof-

fenen erhebliche Nachteile hinnehmen müssen, obwohl sich im anschließenden Verfahren die zunächst erhobenen Vorwürfe nicht halten lassen. Eine Übermittlung vor rechtskräftiger Entscheidung muß deshalb die Ausnahme sein und auf solche Fälle beschränkt werden, in denen die frühzeitige Mitteilung zum Schutz der Allgemeinheit oder von Einzelpersonen zwingend geboten ist.

— Der Entwurf verzichtet auf Entscheidungsvorbehalte und Anordnungsbefugnisse, obwohl in einigen Fällen schwierige Abwägungsvorgänge zu bewältigen sind. Wir halten es z.B. für erforderlich, Mitteilungen in Jugendstrafsachen oder vor Verfahrensabschluß generell dem Richter vorzubehalten.

— Prinzipiell positiv ist die im Entwurf zum Ausdruck kommende Absicht, die Betroffenen grundsätzlich von der Tatsache der Übermittlung und ihrem Inhalt zu informieren, obwohl die Ausnahmevorschriften zu weit gefaßt sind.

— Auch die vorgesehenen Nachberichtspflichten sind zu begrüßen. Sie müssen jedoch durch die Pflicht ergänzt werden, Übermittlungen zu protokollieren, da nur dann die Nachberichtspflichten wirksam erfüllt und Betroffene ihre Berichtigungsansprüche nur so wirksam verfolgen können.

— Weiter muß der Entwurf ergänzt werden durch Bestimmungen, die festlegen, wann die Datenempfänger die übermittelten Daten zu löschen haben. Dies ist schon deshalb erforderlich, um eine Umgehung der Speicherfristen nach dem Bundeszentralregistergesetz zu verhindern.

4.14.1.4 Schuldnerverzeichnis

Die Bemühungen die Vorschriften über Auskünfte aus dem Schuldnerverzeichnis unter Beachtung der Rechtsprechung des Bundesverfassungsgerichtes zum informationellen Selbstbestimmungsrecht neu zu regeln, sind erfreulicherweise wieder aufgenommen worden. Es gibt jetzt einen Entwurf der Bundesregierung vom Mai 1990 sowie eine Stellungnahme des Bundesrates vom Juni 1990 (Bundesratsdrucksache 325/90). Damit ist das Stadium der Referentenentwürfe, über das man lange Zeit nicht hinausgekommen war, überwunden.

Da auch der Regierungsentwurf den aus datenschutzrechtlicher Sicht wichtigsten Kritikpunkt, nämlich die unkontrollierbar weite Streuung der Informationen aus dem Schuldnerverzeichnis in Listen, nicht beseitigt, müssen wir leider wieder auf die früheren Stellungnahmen (vgl. zuletzt 6. TB, 4.13.8, S. 99f) verweisen. Für besonders bedenklich halten wir, wenn — wie jetzt im Regierungsentwurf in Abweichung von früheren Referentenentwürfen vorgesehen — die Datenschutzaufsicht bei den privaten Empfängern von Abdrucken und Listen auf das Maß reduziert werden soll, das für alle privaten datenverarbeitenden Stellen gilt. Durch die ersatzlose Streichung des § 915 f Absatz 2 des Vorentwurfes ist nicht mehr die anlaßfreie Kontrolle der Listen- und Abdruckempfänger vorgesehen. Konsequenz des Fehlens einer speziellen Regelung ist die Geltung des allgemeinen Datenschutzrechtes, das für die private Datenverarbeitung nur eingeschränkte Kontrollmöglichkeiten eröffnet. Aus unserer Sicht wäre es als Gegengewicht für die ohnehin problematische listenmäßige Verteilung der Informationen aus dem Schuldnerverzeichnis an private Stellen unbedingt erforderlich, daß die Aufsichtsbehörde die korrekte Handhabung der Listen jederzeit und ohne äußeren Anlaß überprüfen kann.

Ein weiterer Mangel des Gesetzentwurfes ist das Fehlen einer ausdrücklichen Regelung darüber, ob private bundesweite Schuldnerverzeichnisse zulässig sind oder nicht. Wir halten es für wünschenswert, der Vermarktung von Informationen aus dem Schuldnerverzeichnis enge Grenzen zu setzen (vgl. 5.6.1), auch wenn damit die derzeit bestehende Praxis verändert werden müßte. Wie auch immer die Entscheidung des Gesetzgebers aussehen mag, er darf dieser praktisch außerordentlich bedeutsamen Streitfrage jedenfalls nicht ausweichen, sondern ist vielmehr von Verfassungs wegen gefordert, sie zu beantworten. Diesen Standpunkt teilt auch der Bundesrat, der in seiner Stellungnahme auf die Notwendigkeit einer eindeutigen Regelung im Gesetzestext hingewiesen hat.

Schließlich weist der Bundesrat auf ein weiteres Defizit des Gesetzentwurfes hin, daß nämlich der Regierungsentwurf die eindeutige Identifizierbarkeit der Person des Schuldners nicht sicherstellt. Er verlangt deshalb, im weiteren Gesetzgebungsverfahren zu prüfen, ob die Verpflichtung zur Aufnahme des Geburtsdatums der betroffenen Person in das Schuldnerverzeichnis normiert werden kann. Dies kann aus datenschutzrechtlicher Sicht nur nachhaltig unterstützt werden.

4.14.2 Austausch von Entscheidungen in Staatsschutzsachen

Von anderen Datenschutzbeauftragten sind wir darüber informiert worden, daß die Landesjustizverwaltungen vereinbart haben, dem Bundesminister der Justiz und allen Landesjustizverwaltungen Abschriften der wesentlichen Entscheidungen in Strafsachen, die nach § 120 GVG zur Zuständigkeit der Oberlandesgerichte gehören, zu übersenden, und zwar auch, wenn sie nicht rechtskräftig sind. Dieser Entscheidungsaustausch ist — so jedenfalls wohl die Praxis der überwiegenden Zahl der beteiligten Länder — in personenbezogener Form erfolgt. Dagegen soll das Land Nordrhein-Westfalen schon seit September 1985 im Rahmen dieses Austausches nur noch anonymisierte Fassungen der gerichtlichen Entscheidungen, d. h. solche Fassungen, in denen die personenbezogenen Daten aller Verfahrensbeteiligten unkenntlich gemacht worden sind, übersenden.

Zur Begründung hat der Justizminister dieses Bundeslandes darauf verwiesen, daß für die Übermittlung derart sensibler Daten eine bereichsspezifische gesetzliche Regelung nicht vorhanden und die personenbezogenen Mitteilungen auch nicht zur Erfüllung gesetzlicher Aufgaben der Empfänger erforderlich sind. Dieser Auffassung sind wir auch.

Wir haben die Justizbehörde deshalb gebeten, uns über die hamburgische Austauschpraxis zu berichten, und für den Fall, daß Hamburg personenbezogene Gerichtsentscheidungen versendet, zu begründen, warum eine solche Praxis entgegen der Auffassung des Landes Nordrhein-Westfalen erforderlich sein soll.

Darüber hinaus haben wir — wie auch schon in anderen Zusammenhängen — hervorgehoben, daß durch solche Urteilssammlungen keinesfalls die Speicherfristen und Auskunftsbeschränkungen des Bundeszentralregistergesetzes, die ausdrücklich auch zum Schutze der Betroffenen gesetzlich festgeschrieben wurden, unterlaufen werden dürfen.

Bislang liegt uns eine Stellungnahme der Justizbehörde nicht vor.

4.14.3 Veröffentlichung von Gerichtsentscheidungen

Mit einer Eingabe hatte sich ein Bürger an uns gewendet, der zuvor in einen Unterhaltsrechtsstreit mit seiner Tochter verwickelt war. Er hatte in einer juristischen Fachzeitschrift das Urteil entdeckt, das in diesem Rechtsstreit von einem Zivilsenat des Hanseatischen Oberlandesgerichts verkündet worden war. Er beklagte — aus unserer Sicht zu Recht —, daß der veröffentliche Abdruck des Urteils so deutliche personenbezogene Informationen enthielt, daß ein auch nur oberflächlich mit seinen persönlichen Verhältnissen vertrauter Leser ohne weiteres in der Lage gewesen wäre, ihn zu identifizieren. Dies wäre für ihn deshalb unangenehm gewesen, weil das Urteil ansonsten eine Reihe hochsensibler Daten aus der Privatsphäre sämtlicher Verfahrensbeteiligter enthielt, was in Familienrechtsstreiten nahezu unvermeidlich ist.

Der Präsident des Hanseatischen Oberlandesgerichts hielt zwar die veröffentlichten Daten für soweit neutralisiert, daß sie bei den in Hamburg herrschenden großstädtischen Verhältnissen noch ohne weiteres den Rückschluß auf bestimmte Personen zugelassen hätten; er hat den angesprochenen Fall aber gleichwohl zum Anlaß genommen, die Richter auf die bei der Veröffentlichung von gerichtlichen Entscheidungen möglicherweise entstehenden Datenschutzprobleme erneut anzusprechen. Da im Grundsatz zwischen dem Gerichtspräsidenten und dem Hamburgischen Datenschutzbeauftragten kein Dissens festzustellen war, haben wir trotz der unterschiedlichen Auffassungen in diesem Einzelfall keine Veranlassung zu einer weiteren Reaktion gesehen.

4.14.4 Richterauswahl durch Ausschüsse

Auf Grund einer Anfrage aus der Behörde für Arbeit, Gesundheit und Soziales hatten wir zu klären, welche Rechte den beratenden Ausschüssen nach § 18 Arbeitsgerichtsgesetz und § 11 Sozialgerichtsgesetz zustehen. Diese Gremien sind besetzt mit zwei Arbeitsrichtern/innen und je 2 Vertretern der Gewerkschaften und der Arbeitgeber bzw. mit 2 Sozialrichtern/innen, je 3 Vertretern der Versicherten und der Arbeitgeber sowie je 2 Personen für die Versorgungsberechtigten und die Kriegsopferversorgung. Nach § 18 ArbGG berät der Ausschuß die oberste Arbeitsbehörde des Landes beim Vorschlag der (hauptberuflichen) Kammervorsitzenden, nach § 11 SGG ist die Ausschußberatung bei der Ernennung der Berufsrichter auf Lebenszeit vorgesehen. In beiden Gerichtszweigen können Richter auf Probe und Richter kraft Auftrags verwendet werden.

In der Praxis wurde und wird der beratende Ausschuß der Sozialgerichtsbarkeit bei allen Personalentscheidungen über hauptamtliche Richter befaßt, so bei der Anstellung auf Probe oder kraft Auftrags und auch bei Beförderungen. Dabei beschränkt sich die Behörde für Arbeit, Gesundheit und Soziales in der Regel auf eine mündliche Darstellung der Bewerberlage — nicht zuletzt wegen Zweifeln an der vertraulichen Behandlung. Die Informationswünsche der Ausschußmitglieder gehen allerdings darüber hinaus bis zur uneingeschränkten Einsicht in die Personalakten.

Während in Niedersachsen ähnlich verfahren wird wie in Hamburg, beschränken die Gerichtsverwaltung Bayerns und Baden-Württembergs die Ausschußberatung auf die Ernennung von Richtern auf Lebenszeit. Informiert werden die Ausschußmitglieder durch eine formalisierte schriftliche Kurzdarstellung des beruflichen Werdeganges.

Gegen die Hamburger Praxis haben wir Bedenken geltend gemacht: Zwar liegt eine weitgehende Hinzuziehung des beratenden Ausschusses sowie eine intensive Unterrichtung der Ausschußmitglieder im Sinne des Zwecks der 1953 geschaffenen Mitbestimmungsgremien — sie sollen nämlich eine Vertrauensbasis zwischen Gerichtsbarkeit und betroffenen Interessenverbänden herstellen. 30 Jahre später stellte das Bundesverfassungsgericht im Volkszählungsurteil jedoch klar, daß jeder Eingriff in die informationelle Selbstbestimmung durch ein bereichsspezifisches, normenklares Gesetz legitimiert sein muß. Dies ist bei der Auslegung von § 18 ArbGG und § 11 SGG zu berücksichtigen: Wird die Hinzuziehung der beratenden Ausschüsse und ihre Befassung mit Richterpersonalien auf andere als im Gesetzeswortlaut festgelegte Anlässe ausgedehnt, fehlt es insoweit an der für die Personaldatennutzung erforderlichen Rechtsgrundlage. Darüber hinaus bedeutet nach heutigem Datenschutzrechtsverständnis eine bloße Aufgabenzuweisung — wie in § 18 ArbGG und § 11 SGG — noch keine Ermächtigung der beauftragten Stelle zur Verarbeitung personenbezogener Daten. Insoweit sind die genannten Gesetze also selbst für die ausdrücklich vorgesehenen Beteiligungsanlässe unvollständig. Nach Auffassung des Bundesverfassungsgerichts bewirkt dieser Mangel, daß bis zu einer bereichsspezifischen normenklaren gesetzlichen Regelung nur diejenigen Daten verarbeitet — also nur die Richterdaten offenbart — werden dürfen, die zur Erfüllung der Aufgaben der Ausschüsse unerläßlich sind. Die Einsicht in Personalakten scheidet damit von vornherein aus, weil sie viele für die Beratungsaufgabe nicht erforderliche Angaben enthalten.

Die Beschränkung auf die Offenbarung unerläßlicher Personaldaten ist nicht geboten, wenn der/die betroffene Richter/in in weitere Datenoffenbarungen einwilligt. Dies setzt allerdings Freiwilligkeit voraus. Angesichts der für die Richterlaufbahn vorgesehenen Lebenszeiternennung und der gesetzlich vorgeschriebenen Beratungsaufgabe des Ausschusses kann von einer freiwilligen Datenoffenbarung nur dann die Rede sein, wenn der/die Betroffene das vorgesehene Verfahren über die beschriebenen gesetzlichen Grenzen genau kennt und über den Umfang der an den Ausschuß weiterzugebenden Daten informiert ist. Davon kann bei der derzeitigen Praxis nicht ausgegangen werden.

Wir sind uns bewußt, daß hier modernes Datenschutzrecht und demokratische Mitbestimmung gesellschaftlicher Kräfte an staatlichen Entscheidungen in einem deutlichen

Spannungsverhältnis zueinander stehen. Eine rechtsstaatliche Lösung sehen wir allein in einer entsprechenden Ergänzung der genannten Vorschriften. Eine endgültige Entscheidung der Behörde für Arbeit, Gesundheit und Soziales über das weitere Verfahren der Ausschußberatungen ist uns bislang nicht bekannt geworden.

4.14.5 Ungelöste Probleme

Wir haben im letzten Tätigkeitsbericht verschiedene Probleme im Bereich der Justiz angesprochen, die weiterhin ungelöst sind. Weder bei der Frage der Kontrollkompetenz des Datenschutzbeauftragten bei den Gerichten und den Gerichtsvollziehern (vgl. 8. TB, 3.10.2 und 3.10.5) noch zur Frage der Bedingungen des Einsatzes von Personalcomputern an den Richterarbeitsplätzen (3.10.3) sind wir inhaltlich trotz der Gespräche, die wir mit Beteiligten geführt haben, vorangekommen. Bevor wir auf diese Fragen wieder zurückkommen, wollen wir die Beratungen im Rechtsausschuß der Bürgerschaft zu unserem 8. Tätigkeitsbericht und die Stellungnahme des Senats dazu abwarten.

4.15 Strafvollzug

4.15.1 Vorschläge zur Novellierung des Strafvollzugsgesetzes — Keine Reaktion

Auch das Strafvollzugsgesetz bedarf dringend datenschutzrechtlicher Ergänzungen, wie seit vielen Jahren anerkannt ist. Die Datenschutzbeauftragten in Bund und Ländern haben über ihre konkrete Mitarbeit bei der Beratung der verschiedenen Gesetzesentwürfe hinaus eine Arbeitsgruppe eingesetzt, die die wesentlichen Probleme aus ihrer Sicht einmal grundsätzlich aufgearbeitet hat. Das daraus entstandene Arbeitspapier, das nicht nur auf die verschiedenen Datenerhebungsmaßnahmen und Datenspeicherungen innerhalb der Strafvollzugsanstalten, sondern auch auf Fragen der Überwachung des Schriftwechsels, der Auskünfte an Behörden und Private und der sogenannte Häftlingsüberwachung eingeht und konkrete Regelungsanregungen gibt, haben wir im Juli des Berichtsjahres an die Justizbehörde mit der Bitte um Berücksichtigung bei den Beratungen zur Novellierung des Strafvollzugsgesetzes übersandt. Eine Reaktion darauf — und sei es nur in Form einer Eingangsbestätigung — haben wir nicht erhalten.

4.15.2 Erfassung von Besuchern der Strafgefangenen

Aus Anlaß von Eingaben haben wir schon Anfang 1989 ein Gespräch mit dem Strafvollzugsamt zu den Problemen der Erfassung von Besuchern der Strafgefangenen sowie der Speicherung und die Weitergabe der dabei anfallenden personenbezogenen Daten aufgenommen. Da für die Erfassung dieses Personenkreises eine bereichsspezifische Grundlage im Strafvollzugsgesetz nicht vorhanden ist, hatten wir dem Strafvollzugsamt vorgeschlagen, die Betroffenen zumindest aufzuklären, um wenigstens inhaltlich ihrem informationellen Selbstbestimmungsrecht (zu wissen, wer was wann zu welchem Zweck über sie in Erfahrung gebracht hat und was mit diesen Daten geschieht) näherzukommen.

Zu diesem Zweck sollte ein Hinweis- und Merkblatt zur Überwachung des Besuchsverkehrs erarbeitet und an die Gefangenen und die von ihnen benannten Besucher verteilt werden. In diesem Merkblatt sollte darauf hingewiesen werden, daß Name und Anschrift der Besucher, die nach Überprüfung durch die Anstalt zugelassen werden, sowie die Häufigkeit und Dauer der Besuche in einer Besucherkartei festgehalten werden. Außerdem sollten die Besucher darauf hingewiesen werden, daß Informationen aus der Besucherkartei unter den in § 34 StVollzG genannten Voraussetzungen von Amts wegen oder auf Anfrage an Strafverfolgungsbehörden (i.d.R. Polizei, Staatsanwaltschaft, ggf. Ausländerbehörde) weitergegeben werden können. Weiterhin sollten sie darauf aufmerksam gemacht werden, daß es bei der Verweigerung der Aufnahme in der Kartei unter Umständen zu einer Verweigerung der Besuchserlaubnis, jedenfalls aber zu Schwierigkeiten und Verzögerungen bei der Überprüfung der Besuchsberechtigung kommen kann. Dieses Merkblatt sollten die Besucher bei ihrem ersten Besuch

des Gefangenen unterschrieben mitbringen, um zu dokumentieren, daß sie den Besuch in voller Kenntnis der o.a. Umstände machen.

Das Strafvollzugsamt hatte der Verfahrensweise zugestimmt und mehrfach die Übersendung des nach unserer Kenntnis schon vorliegenden Merkblattes angekündigt, als die Justizbehörde plötzlich unter Hinweis auf — damals erst im Entwurf vorhandene — Regelungen zur Novellierung des Hamburgischen Datenschutzgesetzes eine Aufklärung der Betroffenen und Verfügungen bezüglich der Besucherkartei für entbehrlich erklärte.

Wir halten weder die nunmehr eingenommene rechtliche Position des Strafvollzugsamtes noch die Art und Weise der Abkehr von getroffenen Vereinbarungen für gerechtfertigt. Die Überwachung des Besucherverkehrs kann nur im Strafvollzugsgesetz geregelt werden. Ihm gebührt als lex speciales der Vorrang vor dem allgemeinen Datenschutzgesetz. Die Datenerhebungen, -speicherungen und -übermittlungen erfolgen derzeit ohne gesetzliche Grundlage. Die getroffene Vereinbarung war deshalb als Übergangsregelung gedacht, die wir nach wie vor für erforderlich halten. Wir haben deshalb das Strafvollzugsamt aufgefordert, die früheren Absprachen einzuhalten.

4.15.3 Datenschutzrechtliche Prüfung in der Justizvollzugsanstalt (JVA) Vierlande

Am 2. August 1990 haben wir in der JVA Vierlande eine datenschutzrechtliche Prüfung durchgeführt. Gegenstand der Prüfung war die DV-Unterstützung der Vollzugsgeschäftsstelle und die Sicherung der manuell geführten medizinischen Daten der Strafgefangenen.

In der Vollzugsanstalt kommt eine Zentraleinheit Siemens MX 500—20 mit 7 Bildschirmen zum Einsatz. Auf ihr werden ein Zahlstellenverfahren sowie ein Verfahren zur Verwaltung von Vollzugslockerungen abgewickelt.

Die Prüfung hat folgende Ergebnisse gebracht:

— Es war während der Prüfung möglich, unberechtigt in das System einzudringen und sogar Betriebssystem-Berechtigungen zu erschleichen. Damit war eine lückenlose Benutzer- sowie Zugriffskontrolle nicht gewährleistet.

— Unter den vorhandenen Disketten fanden sich auch ausgebrauchte Sicherungsdisketten mit altem Datenbestand. Die Datenträger waren nicht katalogisiert.

— Das Zahlstellenverfahren ist beim Hamburgischen Datenschutzbeauftragten nicht angemeldet worden; die gesetzlich vorgeschriebene Dateimeldung erfolgte bislang nicht.

— Die Krankenakten der Strafgefangenen werden in einem Raum mit mehreren Zugängen, von denen nur einer mit einem Sicherheitsschloß gesichert war, aufbewahrt. Auch der Schrank(-teil), in dem die Akten gelagert werden, war nicht durch ein Sicherheitsschloß gesichert.

Im einzelnen ergaben sich daraus folgende Bewertungen und Vorschläge:

— Die vorgefundene Möglichkeit, in das System einzudringen, stellt sich als Verstoß gegen § 8 Absatz 2 Nr. 4 und 5 HmbDSG n.F. dar. Sie muß durch die Veränderung der vorgegebenen Paßwörter verhindert werden.

  Es sollte sichergestellt werden, daß kein Benutzer ohne Betriebssystem-Berechtigung die Möglichkeit hat, mit dem Editor CED zu arbeiten, da er sich so diese Berechtigung erschleichen kann und dann in der Lage wäre, die Systemsicherheit zu gefährden. Systemprotokolle müssen ausgewertet und archiviert werden.

— Datenträger sind zu katalogisieren und auf die aktuellen Sicherungsdatenträger und Datenträger mit Systemprogrammen zu begrenzen. Ausgediente Sicherungsdatenträger müssen physikalisch gelöscht oder vernichtet werden. Sie dürfen nicht zusammen mit den anderen Datenträgern aufbewahrt werden, weil sonst eine effektive Datenträgerkontrolle erschwert oder unmöglich gemacht wird (vgl. § 8 Absatz 2 Nr. 2 HmbDSG n.F.).

— Das Unterlassen von Dateimeldungen für das Zahlstellenverfahren verstößt gegen § 24 Absatz 1 Satz 2 HmbDSG n.F. Sie sind unverzüglich nachzuholen.

Im übrigen konnte bisher nicht festgestellt werden, daß die beiden eingesetzten Verfahren freigegeben wurden, was im Rahmen einer datenschutzgerechten Organisation erforderlich ist (§ 8 Absatz 2 Nr. 10 HmbDSG n.F.).

— Die Krankenakten der Strafgefangenen, die sehr sensible Daten enthalten, müssen besser gesichert werden (vgl. § 8 Absatz 3 HmbDSG n.F.). Dazu ist zumindest erforderlich, daß die für die Lagerung dieser Akten eingesetzten Schränke oder Schrankteile mit Sicherheitsschlössern versehen werden.

Das Strafvollzugsamt hat in seiner Stellungnahme zugesichert, alle technischen und organisatorischen Mängel zu beseitigen, die fehlende Dateimeldung und die Freigabeerklärung für die Verfahren nachzuholen sowie in die Schränke für die Verwahrung der Krankenakten Sicherheitsschlösser einzubauen. Davon werden wir uns zu gegebener Zeit überzeugen.

4.16 Gesundheitswesen

4.16.1 Stand der Gesetzgebung

4.16.1.1 Hamburgisches Krankenhausgesetz

Ein Krankenhausgesetz mit Vorschriften zum Patientendatenschutz ist in Hamburg trotz langjähriger Bemühungen noch nicht in Kraft getreten, aber es gibt immerhin schon einen vom Senat beschlossenen Entwurf, der der Bürgerschaft zur Beratung zugeleitet wurde.

Leider sind in der nunmehr vorliegenden Fassung die Vorschläge und Stellungnahmen des Datenschutzbeauftragten nur teilweise berücksichtigt, so daß der datenschutzrechtliche Standard der Krankenhausgesetze anderer Bundesländer in einigen Punkten nicht erreicht wird. Verbesserungen im weiteren Gesetzgebungsverfahren sind dringend geboten.

Hauptschwachpunkt der Vorschriften zum Patientendatenschutz ist die Behandlung des Krankenhauses als funktionale Einheit: „Das Krankenhaus" erhebt, speichert und nutzt die Patientendaten und nicht etwa die Stelle, die die Daten zur Erfüllung ihrer Aufgaben benötigt. Selbst in einem Großbetrieb wie dem Universitätskrankenhaus Eppendorf mit einer Vielzahl weitgehend autonomer Fachkliniken findet nach dieser Sichtweise keine Übermittlung von Patientendaten statt, sondern nur eine aufgabenbezogene Nutzung. Das wäre weniger problematisch, wenn die berechtigten Geheimhaltungsbelange der Patienten durch Zweckbindungsvorschriften genauso gut geschützt werden könnten wie durch Übermittlungsregelungen. Davon kann jedoch nicht gesprochen werden.

So dürfen nach dem Entwurf Patientendaten genutzt werden, soweit dies für die Behandlung des Patienten erforderlich ist. Dagegen ist eine Übermittlung der Daten an Dritte zur Durchführung einer Mit-, Weiter- oder Nachbehandlung nur zulässig, wenn der Patient nach Hinweis auf die beabsichtigte Übermittlung nicht etwas anderes bestimmt. Für die Interessenlage des Patienten spielt es keine Rolle, ob eine erforderliche Mitbehandlung in einer anderen Fachklinik des gleichen Krankenhauses oder, falls dieses keine entsprechende Ausstattung hat, von der Abteilung eines anderen Krankenhauses durchgeführt wird. In beiden Fällen werden Patientendaten an Dritte, bisher nicht an der Behandlung beteiligte Personen offenbart und dem Patienten steht im Rahmen des Behandlungsvertrages das Recht zu, den Umfang der Behandlung und der Weitergabe von Daten zu beschränken.

Die Nutzung der Patientendaten „im Krankenhaus" soll dagegen offenbar unter erleichterten Voraussetzungen zulässig sein, denn nach der Begründung des Entwurfes würde die Anwendung der Übermittlungsregelungen die interdisziplinäre Zusammen-

arbeit der einzelnen Fachabteilungen unnötig erschweren, weil vor jeder Datenweitergabe zunächst deren Rechtmäßigkeit geprüft werden müßte. Das halten wir allerdings für selbstverständlich und zwar auch im Rahmen der Überlegungen zur Erforderlichkeit der Nutzung von Daten.

Besonders deutlich wird der Interessenkonflikt bei den Vorschriften über die Forschung mit Patientendaten. Nach dem Entwurf gibt es drei Abstufungen:

— Der behandelnde Arzt, der die Patientendaten bereits kennt, darf sie für eigene Forschungszwecke nutzen, wenn schutzwürdige Belange der Betroffenen dadurch nicht gefährdet werden.

— „Im Krankenhaus" dürfen die Daten zur Durchführung eines bestimmten wissenschaftlichen Forschungsvorhabens verarbeitet werden, wenn der Zweck der Forschung auf andere Weise nicht erreicht werden kann und schutzwürdige Belange der Betroffenen nicht gefährdet werden oder der Patient nach einer Unterrichtung über Art, Umfang und Zweck des Forschungsvorhabens der Verarbeitung nicht widersprochen hat.

— Eine Übermittlung von Patientendaten für ein bestimmtes wissenschaftliches Forschungsvorhaben ist grundsätzlich nur mit Einwilligung des Betroffenen zulässig. Eine Ausnahmeregelung besteht für den Fall, daß der Zweck der Forschung auf andere Weise nicht erreicht werden kann, die Einholung der Einwilligung nicht oder nur unter unverhältnismäßigem Aufwand möglich ist oder mit der Gefahr einer ernsten Gesundheitsverschlechterung für den Patienten verbunden wäre und das Interesse der Allgemeinheit an der Durchführung des Forschungsvorhabens das Geheimhaltungsinteresse des Betroffenen erheblich überwiegt.

Bei der Forschung mit Patientendaten ist es also von erheblicher Bedeutung, ob die Weitergabe von Patientendaten zwischen einzelnen Fachkliniken als Übermittlung oder als Nutzung angesehen wird. Nach dem vom Senat beschlossenen Gesetzentwurf ist es möglich, innerhalb einer Großklinik ohne Information des Betroffenen Behandlungsdaten von Patienten frei zu Forschungszwecken zu nutzen, wenn die forschenden Ärzte sich auf den Standpunkt stellen, schutzwürdige Belange des Betroffenen seien nicht berührt. Da der Patient nicht einmal über die Zweckentfremdung seiner für die Behandlung erhobenen Daten informiert wird und ihm nicht Gelegenheit gegeben wird, seine Betroffenheit zu artikulieren, erscheint diese Regelung nicht geeignet, einen angemessenen Interessenausgleich zwischen dem Forschungsinteresse und dem Persönlichkeitsrecht des Patienten herzustellen. In den Stellungnahmen zu den Referentenentwürfen hatten wir daher immer gefordert, die krankenhausinterne Forschung auf die Fachabteilungen zu begrenzen und dem Patienten ein Widerspruchsrecht einzuräumen. Die Weitergabe an andere Fachabteilungen bzw. -kliniken sollte dagegen als Datenübermittlung behandelt werden. Entsprechende Regelungen finden sich auch in den Krankenhausgesetzen anderer Bundesländer: In Bremen und Hessen ist festgelegt, daß die Weitergabe von Daten an andere Fachabteilungen eine Übermittlung darstellt, in Rheinland-Pfalz und im Saarland ist die krankenhausinterne Forschung auf Fachabteilungs- oder -klinikebene beschränkt, ohne daß über eine unzumutbare Beschränkung der interdisziplinären Forschung geklagt wird.

Soweit die Forschung mit Patientendaten durch behandelnde Ärzte und Facheinrichtungen an vereinfachte Bedingungen geknüpft wird, rechtfertigt sich dies aus ihrem engen Bezug zur Behandlung des Patienten: Im wesentlichen bereits bekannte Informationen werden zu einem anderen Zweck genutzt, was der Betroffene zumindest wissen sollte, damit er schutzwürdige Belange zur Geltung bringen kann. Bei zusätzlichen Offenbarungen ist die Anwendung der Übermittlungsregelungen und damit grundsätzlich die Einwilligung des Betroffenen erforderlich, sonst besteht die Gefahr, daß er unter Mißachtung seines Persönlichkeitsrechts zum Objekt der Forschung gemacht wird.

Ein weiterer Kritikpunkt am Gesetzentwurf ist die Regelung der Auftragsdatenverarbeitung. Aus datenschutzrechtlicher Sicht sollte sichergestellt werden, daß Patientendaten in der Regel im Krankenhaus und nur in Ausnahmefällen von externen Stellen ver-

arbeitet werden dürfen. Patientendaten, die die Verwaltung z.B. für die Leistungsabrechnung und für die Erstellung der Diagnosestatistik verarbeitet, müssen mindestens ebenso geschützt werden wie Sozialdaten durch die Regelung des § 80 SGB X, der eine Verarbeitung personenbezogener Daten durch nicht-öffentliche Stellen nur ausnahmsweise zuläßt. Für Daten aus dem ärztlichen Bereich sollten noch strengere Anforderungen gelten. Wünschenswert wäre, daß sie zum Schutz gegen unzulässige Verknüpfung in jeder Phase der Datenverarbeitung nicht nur logisch, sondern tatsächlich getrennt von anderen Dateien verarbeitet werden.

Verbesserungsbedürftig ist ferner die vorgeschlagene Regelung des § 7 Absatz 4, nach der die Geltung der Vorschriften über den Patientendatenschutz für die von Religionsgesellschaften betriebenen Krankenhäuser ausgeschlossen werden soll. Wenn grundsätzlich eine Regelungskompetenz für den Datenschutz auch in kirchlichen Krankenhäusern besteht, dürfen die staatlichen Regelungen nur dann zurücktreten, wenn die Religionsgesellschaften gleichwertige Regelungen erlassen haben.

Aus datenschutzrechtlicher Sicht ist zu hoffen, daß wenigstens diese Hauptkritikpunkte im weiteren Gesetzgebungsverfahren ausgeräumt werden können.

4.16.1.2 Änderung des Hamburgischen Ärztegesetzes

Im Zusammenhang mit dem Problem der Überwachung der ärztlichen Berufspflichten durch die Ärztekammer stellte sich wiederholt die entscheidende Frage: Ist der Arzt berechtigt oder sogar verpflichtet, der Ärztekammer personenbezogene Daten seiner Patienten zu offenbaren? Schwierig war eine Beantwortung dieser Frage vor allem deshalb, weil die Datenerhebungsbefugnisse der Ärztekammer und die korrespondierenden Offenbarungsbefugnisse der Ärzte im Falle eines Verdachts der Verletzung von Berufspflichten nicht ausreichend normenklar geregelt waren. Als Lösungsweg wurde eine Änderung des Hamburgischen Ärztegesetzes vorgeschlagen.

Die Ärztekammer hat zwar gemäß § 15 Absatz 1 Ziffer 1 des Hamburgischen Ärztegesetzes die Aufgabe, die Erfüllung der ärztlichen Berufspflichten zu überwachen und gemäß § 16 des Gesetzes über die Berufsgerichtsbarkeit der Heilberufe die erforderlichen Ermittlungen im Rahmen eines Vorverfahrens durchzuführen. Aus diesen Aufgaben der Ärztekammer folgt aber nicht zwangsläufig eine Offenbarungsbefugnis der Ärzte hinsichtlich der Daten des betroffenen Patienten. Zwar durfte der Arzt, gegen den der Verdacht eines Berufsvergehens geltend gemacht wurde, in Wahrnehmung berechtigter Interessen Patientendaten offenbaren, um sich gegen den Vorwurf zur Wehr zu setzen, er war dazu aber nicht verpflichtet. Noch problematischer waren die Ermittlungen der Ärztekammer, wenn sie von weiterbehandelnden Ärzten den Namen und Befund eines möglicherweise entgegen den Regeln der ärztlichen Kunst behandelten Patienten erfahren wollte. Die Kammer stellte sich regelmäßig auf den Standpunkt, daß die übergeordneten Interessen an einer Aufklärung von Berufspflichtverletzungen einen Eingriff in das Geheimhaltungsinteresse des Patienten erforderlich machten und daß die Ärzte unter dem Gesichtspunkt des rechtfertigenden Notstands zu einer Durchbrechung der Schweigepflicht befugt seien. In Anbetracht der engen Fassung der Voraussetzungen des rechtfertigenden Notstands, der eine akute Gefahr für eine höherwertiges Rechtsgut voraussetzt, war diese Argumentation nur in Ausnahmefällen geeignet, eine Offenbarungsbefugnis oder -pflicht des Arztes zu begründen.

Eine sowohl die Belange des betroffenen Patienten als auch die Ermittlungsinteressen der Ärztekammer befriedigende Lösung konnte im Rahmen der Änderung des Ärztegesetzes erzielt werden. Danach ist der Arzt befugt, soweit es zur Überwachung der Erfüllung der ärztlichen Berufspflichten erforderlich ist, Fragen der Ärztekammer über die Erfüllung seiner Berufspflichten zu beantworten und verpflichtet, ärztliche Aufzeichnungen und Unterlagen vorzulegen. Vor- und nachbehandelnde Ärzte sind, soweit erforderlich, der Ärztekammer zu Auskünften sowie zur Vorlage von ärztlichen Aufzeichnungen und Unterlagen über den Patienten verpflichtet, es sei denn, der Patient widerspricht ausdrücklich.

Erforderlich ist eine Offenbarung von personenbezogenen Daten des Patienten nur dann, wenn eine Aufklärung des Falls mit anonymisierten Daten nicht möglich ist. Vor- und nachbehandelnde Ärzte dürfen personenbezogene Daten nur offenbaren, wenn sie den Patienten zuvor über das Ersuchen der Ärztekammer aufgeklärt und ihm Gelegenheit gegeben haben, der Weitergabe von Informationen zu widersprechen.

4.16.2 Datenschutz im Krankenhaus

4.16.2.1 Weitergabe von Aufnahme- und Entlassungsanzeigen an die Krankenkassen

Nach der Neufassung des Rechts der gesetzlichen Krankenversicherung sind die Krankenhäuser seit dem 1. Januar 1990 verpflichtet, den Krankenkassen bei Aufnahme und Entlassung eines Patienten eine Mitteilung mit einem in § 301 SGB V festgelegten Inhalt (Versichertennummer, Aufnahme- und Entlassungsdiagnose, Aufnahme- und Entlassungsgrund, Aufnahme- und Entlassungstag des Patienten, Entgelte nach Bundespflegesatzverordnung) zuzuleiten. Zwischen den Krankenkassen und der Krankenhausgesellschaft, dem Verband der Krankenhausträger der Freien und Hansestadt Hamburg, ist umstritten, ob dieser Datensatz für die Abwicklung des Behandlungsverhältnisses ausreicht. Die Krankenhausgesellschaft ist an einer möglichst restriktiven Informationsweitergabe interessiert; sie hält daher den § 301 SGB V für eine abschließende Regelung. Die Krankenkassen legen die gesetzliche Verpflichtung der Krankenhäuser zu Datenübermittlung jedoch weiter aus: Sie verlangen von ihnen alle Informationen, die sie zur Aufgabenerfüllung für nötig halten.

Aus Anlaß der Beratungen zu dem Entwurf eines Vertrages über die allgemeinen Bedingungen der Krankenhausbehandlung, dessen Abschluß den Landesverbänden der Krankenkassen und den Krankenhausträgern gesetzlich vorgeschrieben ist, sind auch wir beteiligt worden.

Die rechtliche Problematik der Datenübermittlung zwischen Krankenhäusern und Krankenkassen haben wir im letzten Tätigkeitsbericht ausführlich dargestellt (8. TB, 3.1.1, S. 24ff). Auch nach unserer Auffassung ist § 301 SGB V als abschließende Regelung anzusehen. Dies bedeutet, daß die Übermittlungsbefugnisse der Krankenhäuser enger geregelt sind als die Datenerhebungsbefugnisse der Krankenkassen. Allerdings darf nicht verkannt werden, daß § 301 SGB V seinem Wortlaut nach noch nicht einmal die Weitergabe des Namens des Patienten, sondern nur seiner Versichertennummer zuläßt. Auch wenn aus datenschutzrechtlicher Sicht einer engen Auslegung der Übermittlungsbefugnisse der Vorzug zu geben ist, ist der Sinngehalt der Vorschrift dahingehend zu interpretieren, daß eine klare Identifizierung des Versicherten gewollt ist. Zulässig ist daher auch die Weitergabe von Name und Geburtsdatum, wenn die Versichertennummer nicht bekannt ist. Aus datenschutzrechtlicher Sicht ist es dringend erforderlich, daß der Gesetzgeber die Rechtslage durch eine Nachbesserung des SGB V klärt.

Datenschutzrechtliche Probleme gibt es nicht nur bei der Übermittlung von Versichertendaten an die Krankenkassen, sondern auch bei deren weiterer Auswertung und Verarbeitung. Schon vor Inkrafttreten der gesetzlichen Regelung erstellten die Krankenhäuser für die Krankenkassen Entlassungsanzeigen aufgrund einer Vereinbarung zwischen der Arbeitsgemeinschaft der Krankenkassenverbände und der Krankenhausgesellschaft. Diese Entlassungsanzeigen wurden der gemeinsamen Datenverarbeitungsstelle der Krankenversicherungen zur Auswertung überlassen und anschließend an die zuständigen Krankenkassen zur Abrechnung weitergeleitet. Aufgrund unserer datenschutzrechtlichen Bewertung akzeptierten die Krankenkassen, daß eine personenbezogene Speicherung von Versichertendaten bei der gemeinsamen Datenverarbeitungsstelle nur in Einzeldateien der jeweils zuständigen Krankenkassen zulässig ist. Dafür sollte ein Datensicherungskonzept erarbeitet werden, das uns aber bisher noch nicht zur Prüfung vorgelegt wurde. Deshalb gilt weiterhin die Vereinbarung, daß bei der gemeinsamen Datenverarbeitungsstelle nur solche Daten gespeichert werden dürfen, die keine Rückschlüsse auf eine Einzelperson zulassen. Der Vereinbarung über die

Weiterleitung von Entlassungsanzeigen an die gemeinsame Datenverarbeitungsstelle lag ein Datenkatalog zugrunde, der weiter gefaßt war als die gesetzliche Regelung des § 301 SGB V. Da die Vereinbarung der gesetzlichen Regelung angepaßt werden mußte und nur als Übergangsregelung bis zum Inkrafttreten einer vertraglichen Regelung konzipiert war, hat die Krankenhausgesellschaft die Vereinbarung gekündigt. Auch bei einer Reduzierung der Datenübermittlung auf den gesetzlich geregelten Umfang gelten die für die gemeinsame Datenverarbeitungsstelle getroffenen Regelungen weiter: Eine personenbezogene Speicherung ist nur in getrennten Einzeldateien zulässig. Dafür ist von den Krankenkassen ein Datensicherungskonzept vorzulegen.

4.16.2.2 UKE-Dienstanweisung

Aufgrund der Prüfung und Beanstandung der Patientendatenverarbeitung im Universitätskrankenhaus Eppendorf, über die wir im Vorjahr (8. TB, 3.13, S. 104 ff) berichteten, hat das Universitätskrankenhaus im März des Berichtsjahres den Entwurf einer Dienstanweisung über die Führung und Herausgabe von Krankenakten und Röntgenbildern, den Patientendatenschutz und die Forschung mit Patientendaten sowie den Einsatz dezentraler Kleinrechner vorgelegt. Nach diesem Entwurf wird es künftig verbindliche Vorschriften über die Dokumentationspflicht, die Beziehung und Aufbewahrung von Krankenunterlagen und ihre Weitergabe an Dritte geben. Der verantwortliche Personenkreis wird aufgabenbezogen festgelegt. Die Regelung des Patientendatenschutzes orientiert sich an den zu erwartenden Vorschriften im Hamburgischen Krankenhausgesetz.

Obwohl die Abstimmung zügig verlief und wir uns im Interesse einer baldigen Umsetzung auch damit einverstanden erklärten, daß für den Einsatz dezentraler Kleinrechner zunächst nur eine — ausfüllungsbedürftige — Rahmenregelung vorgesehen ist, hat es das UKE über 4 Monate nach Abschluß der Gespräche nicht geschafft, die Dienstanweisung in Kraft zu setzen.

4.16.2.3 Qualitätssicherung

Die Patientenversorgung im Krankenhaus kann verbessert werden, wenn gezielt Störfaktoren im Behandlungsgeschehen aufgespürt und ausgeschaltet werden. Bei der Ursachenermittlung sind Qualitätsvergleiche im Hinblick auf den Behandlungserfolg und die Komplikationsrate hilfreich, die innerhalb einer Krankenhausabteilung, aber auch abteilungs- oder krankenhausübergreifend durchgeführt werden können.

Qualitätssicherung ist den Krankenhäusern per Gesetz zur Aufgabe gemacht, das Krankenversicherungsrecht im SGB V enthält aber keine über die Zielvorgabe hinausgehenden konkreten Vorschriften über die Durchführung qualitätssichernder Maßnahmen. Im Entwurf des Hamburgischen Krankenhausgesetzes ist vorgesehen, daß der Senat durch Rechtsverordnung Maßnahmen zur Erkennung und Erfassung von Krankenhausinfektionen näher regeln und den Krankenhäusern vorschreiben kann, daß sie Aufstellungen in anonymisierter Form über die bei ihnen aufgetretenen Krankenhausinfektionen zu führen haben. Die Nutzung von Patientendaten zur Durchführung von qualitätssichernden Maßnahmen wird ausdrücklich zugelassen. Insofern ist eine bereichsspezifische Rechtsgrundlage für Eingriffe in das informationelle Selbstbestimmungsrecht des Patienten in Vorbereitung. Die abteilungsinterne Qualitätssicherung gehört auch zu den Sorgfaltspflichten des behandelnden Arztes und der behandelnden Fachabteilung und ist insofern vom Behandlungszweck gedeckt.

Im Rahmen unserer beratenden Tätigkeit haben wir zu Maßnahmen der internen und externen Qualitätssicherung Stellung genommen. Dabei ging es vor allem um das Problem, Daten über Krankenhausinfektionen, die im Rahmen der ärztlichen Dokumentation erhoben werden müssen, auch mittels elektronischer Datenverarbeitung zu erfassen und zu analysieren. In einem weiteren Schritt war geplant, mit anonymisierten Patientendaten eine vergleichende Infektionsstatistik zu erproben. Aus datenschutzrechtlicher Sicht bestehen gegen eine auf die Fachabteilung begrenzte personenbezogene Auswertung von Krankenhausinfektionen keine Bedenken, wenn sichergestellt

wird, daß nur die Daten genutzt werden, die zu Behandlungs- bzw. Dokumentationszwecken erhoben worden sind. Die Erfassung darüber hinausgehender, zusätzlicher Daten wäre nur mit Einwilligung der Patienten zulässig.

Wenn die zu Qualitätssicherungszwecken erfaßten Daten abteilungsübergreifend oder sogar krankenhausübergreifend gemeinsam ausgewertet werden sollen, müssen die Patientendaten anonymisiert werden. Dafür reicht nicht aus, daß der Name und der Geburtstag des Patienten weggelassen werden. Bei der Vielzahl der Einzelangaben, die für jeden Patienten gespeichert werden sollen, wäre eine Wiederherstellung des Personenbezugs mit Hilfe der Aufnahmenummer, des Aufnahme- und Entlassungsdatums und des OP-Datums ohne weiteres möglich, so daß jeder einzelne Datensatz personenbeziehbar bliebe. Es muß daher sichergestellt werden, daß diese Daten nicht an Dritte übermittelt werden, die an der Behandlung nicht beteiligt sind. Nur die behandelnde Fachabteilung darf in der Lage sein, die Identität des Patienten wiederherzustellen, wenn von der auswertenden Stelle Rückfragen zu einzelnen Datensätzen kommen. Sofern ein Klinikbeauftragter für Qualitätssicherung bestellt wird, kann er zwar Ansprechpartner für die Stellen außerhalb des Krankenhauses sein, die die Auswertungen durchzuführen haben, er darf aber keinen Zugriff auf personenbezogene Daten von Patienten haben. Verantwortlich für die Wahrung des Patientengeheimnisses bleibt der behandelnde Arzt. Er hat sicherzustellen, daß nicht unbefugt Patientendaten an Dritte offenbart werden.

Die Konzepte zur Durchführung interner und externer qualitätssichernder Maßnahmen werden von uns weiter begleitet.

4.16.2.4 Klinisches Tumorregister des Onkologischen Schwerpunktes Hamburg

Im Berichtsjahr hatten wir auch die Konzeption des Klinischen Tumorregisters des Onkologischen Schwerpunktes Hamburg datenschutzrechtlich zu beurteilen. Dieser Onkologische Schwerpunkt besteht aus den staatlichen Krankenhäusern AK St. Georg, AK Altona, AK Barmbek und AK Harburg. Die Zentrale befindet sich im AK St. Georg. Alle vier Krankenhäuser sind mit Rechenanlagen zur Erfassung der bei ihnen behandelten Krebspatienten ausgestattet. Geplant ist, Bestandteile der gespeicherten Datensätze aller Patienten anonymisiert im AK St. Georg zusammenzuführen.

Im Gegensatz zum epidemiologischen Krebsregister der Gesundheitsbehörde, dessen Daten auf der Grundlage des Hamburgischen Krebsregistergesetzes verarbeitet werden, wurde für klinische Krebsregister bisher eine gesetzliche Regelung nicht für erforderlich gehalten. Sie galten als Behandlungs- und Nachsorgeregister, woraus gefolgert wurde, daß die Speicherung und Nutzung der Daten vom Behandlungszweck gedeckt waren. Diese Einschätzung kann anbetrachts der Konzeption für das klinische Tumorregister des Onkologischen Schwerpunktes Hamburg nicht aufrecht erhalten werden. Zwar dienen die Register der vier beteiligten Kliniken weiterhin der Durchführung einer regelmäßigen Tumornachsorge und der Dokumentation von Behandlungsdaten, zu ihren Aufgaben soll aber darüber hinaus gehören, Aussagen über die Häufigkeit von Tumorerkrankungen und Auswertungen über Therapieergebnisse und Therapiefolgen zu ermöglichen. Diese Erkenntnisgewinnung soll zum einen die Qualitätskontrolle der Tumorbehandlung fördern, zum anderen klinische Studien über diagnostische bzw. therapeutische medizinische Maßnahmen unterstützen. Die klinischen Register dienen damit nicht nur der Behandlung des einzelnen Patienten, sondern auch Forschungszwecken. Die Abgrenzung zwischen Behandlung und Forschung ist im medizinischen Bereich oft schwierig. Vorsorgliche Auswertungen von Patientendaten zur Optimierung der Behandlung zukünftiger Patienten sind nach allgemeiner Auffassung der Forschung zuzuordnen.

Eine Nutzung von Behandlungsdaten zu Forschungszwecken oder ihre Übermittlung an einen bisher nicht an der Behandlung beteiligten Dritten bedarf einer gesonderten, über den Behandlungsvertrag hinausgehenden Rechtsgrundlage. Solange keine spezialgesetzliche Regelung für die Forschung mit Patientendaten in Kraft ist, ist die informierte Einwilligung des Patienten erforderlich. Das gilt gleichermaßen für die Verlaufs-

dokumentation, wenn Daten an und von weiterbehandelnden Ärzten bzw. Kliniken übermittelt werden, wie für Längsschnittuntersuchungen, wenn Daten zu Forschungszwecken ausgewertet werden, ohne daß noch ein Behandlungsbezug besteht. Wenn Daten gleichzeitig für das Hamburgische Krebsregister und für das klinische Register erhoben werden, ist der Patient darüber aufzuklären, daß die Daten in beiden Registern gespeichert werden sollen.

Nach dem Konzept sollen die Patientendaten aus den Einzelregistern in der Zentrale des Onkologischen Schwerpunktes im AK St. Georg zu einem gemeinsamen Register zusammengeführt werden. Sie werden dort unter einem Match-Code gespeichert sein, der der Zentrale eine Zuordnung zur übermittelnden Stelle, aber keine Identifizierung der Personen des Betroffenen ermöglicht. Eine Wiederherstellung des Personenbezugs ist nur dem übermittelnden Register möglich. Zugriff auf die Patientendaten haben nur die Fachabteilungen, die die Daten zum Register gemeldet haben. Gegen dieses Konzept bestehen keine grundsätzlichen datenschutzrechtlichen Bedenken. Im einzelnen wird aber noch in weiteren Gesprächen abgeklärt werden müssen, wie das Verhältnis der personenbezogenen geführten klinischen Register zu den meldenden Fachabteilungen zu regeln ist. Auch bei der Ausgestaltung des Informationsmaterials und der Einwilligungserklärung für die Datenspeicherung und -nutzung besteht noch Abstimmungsbedarf.

4.16.2.5 Projekt „Patientendatenbank"

Vom Landesbetrieb Krankenhäuser wurden wir gebeten, zu dem Projekt Patientendatenbank Stellung zu nehmen. Dabei geht es um folgendes: Ausgehend von der bestehenden datenverarbeitungstechnischen Struktur in den Krankenhäusern, die von wenigen zentralen Verfahren und einer Vielzahl unterschiedlicher dezentraler Verfahren in Funktionseinheiten geprägt ist, wurden Überlegungen angestellt, die Einzelanwendungen in einer zentralen Patientendatenbank zu integrieren und so ein umfassendes Krankenhauskommunikationssystem zu schaffen. Vorteile eines solchen Systems wären, die mehrmalige Erfassung von Patientenstammdaten zu vermeiden, einen verbindlichen Referenzdatenbestand zu schaffen, die zentrale Sicherung der Daten zu ermöglichen und Auskunfts-, Sperrungs- und Löschungsersuchen leichter bearbeiten zu können.

In Anbetracht der großen Unterschiede zwischen den bereits bestehenden Datenverarbeitungssystemen war von Anfang an klar, daß eine Umstellung auf einen gemeinsamen zentralen Datenbestand kurzfristig nicht zu erreichen war. Daher stellte sich die Frage, ob für einen längeren Zeitraum alle Daten parallel in den Einzelverfahren und zusätzlich zentral in der Patientendatenbank gespeichert werden könnten. Gegen ein solches Konzept bestanden gewichtige datenschutzrechtliche Bedenken. Wenn die Einzelanwendungen mit ihrem gesamten Datenbestand erhalten bleiben, besteht kein Bedürfnis für eine allumfassende Patientenzentraldatei, außer unter dem Gesichtspunkt der erleichterten Anfertigung von Sicherungskopien. Löschung bzw. Sperrung und Erfüllung von Auskunftsersuchen lassen sich auch durch eine Nachweisdatei erfüllen, die auf Patientenstammdaten und Hinweise auf dezentrale Verfahren beschränkt ist. Eine umfassende Speicherung aller Patientendaten ist dafür nicht erforderlich. Wenn dagegen geplant ist, die Datenbestände in den Subsystemen durch eine zentrale Patientendatenbank zu ersetzen, muß sichergestellt werden, daß die einzelnen Funktionsbereiche des Krankenhauses nur auf die Daten zugreifen können, die sie für ihre Aufgabenerfüllung benötigen. Flankiert von den erforderlichen zentralen Datensicherungsmaßnahmen wäre es dann durchaus möglich, den Schutz der Patientendaten besser sicherzustellen als bei einer Vielzahl von Einzelanwendungen.

Wegen der Schwierigkeiten der kurzfristigen Integration der Einzelanwendungen zu einer Patientendatenbank ist das ursprüngliche Konzept geändert worden. Nunmehr soll in einem ersten Schritt ein Datenmodell für die Krankenhäuser des Landesbetriebs entwickelt werden. Nach Vereinheitlichung der Datenstrukturen können integrationsfähige Datenverarbeitungsanwendungen zu einem Patientendatensystem zusammenge-

faßt werden, andere Anwendungen werden nach und nach angepaßt und in das System aufgenommen. Dadurch wird sichergestellt, daß die Patientendaten nicht parallel in Einzelanwendungen und in der zentralen Patientendatenbank gespeichert werden.

In welchem Zeitrahmen und in welcher Form das Projekt letztlich verwirklicht wird, ist noch nicht abzusehen.

4.16.2.6 Projekt „Neuplanung Betriebswirtschaft"

Nicht nur im medizinischen Bereich, sondern auch bei der Krankenhausverwaltung schreitet die Automation der Patientendatenverarbeitung weiter voran. Im Rahmen des Projekts „Neuplanung Betriebswirtschaft" werden Verbesserungen bei der Erfassung und Nutzung von Patientendaten zu Abrechnungszwecken angestrebt. Datenschutzrechtlich zu bewerten war die Einrichtung einer Nachweisdatei zur Unterstützung des Wiederauffindens von früheren Abrechnungsakten des Patienten, wenn die Kostenträgerschaft unklar ist. Für die Zulässigkeit einer solchen Nachweisdatei wurden einverständlich folgende Bedingungen festgelegt:

— Als Suchkriterium dient ein aus dem Namen und dem Geburtsdatum des Patienten gebildeter Match-Code;

— der Algorithmus für die Bildung des Match-Codes muß so beschaffen sein, daß eine Entschlüsselung (Ableitung des Namens und des Geburtsdatums aufgrund des Match-Codes) nicht möglich ist. Mit den Informationen dieser Nachweisdatei kann somit nicht auf die im Krankenhaus behandelten Patienten geschlossen werden;

— Die Nachweisfunktion der Nachweisdatei wird nur bei konkretem Anlaß benutzt, d.h. das Krankenhaus überprüft nur dann durch einen Dialogzugriff das Vorhandensein von Einträgen in der Nachweisdatei für einen Patienten, wenn die Kostenträgerschaft für diesen Patienten unklar ist;

— Zugriffe auf die Nachweisdateien anderer Krankenhäuser des Landesbetriebs sind unzulässig.

Das Vorhaben befindet sich noch in einem sehr frühen Planungsstadium. Die Klärung datenschutzrechtlicher Fragen diente der Vorbereitung des Ausschreibungsverfahrens, das gegen Ende des Jahres eingeleitet werden soll.

4.16.2.7 Zusammenarbeit zwischen Krankenhäusern und Polizei

Die Richtlinien des Landesbetriebs Krankenhäuser zur Zusammenarbeit zwischen Polizei und Krankenhäusern aus dem Jahre 1983 bedürfen unter datenschutzrechtlichen Gesichtspunkten dringend einer Überarbeitung. In ihnen ist u.a. festgelegt, in welchen Fällen und in welchem Umfang das Krankenhauspersonal befugt ist, ermittelnden Polizeibeamten Auskünfte über im Krankenhaus behandelte Patienten zu erteilen.

Nach den Abstimmungsgesprächen, an denen auch wir teilgenommen haben, hat der Landesbetrieb eine überarbeitete Fassung der Richtlinien vorgelegt, die Gesichtspunkte des Datenschutzes und der ärztlichen Schweigepflicht mit dem Ermittlungsinteresse der Polizei zu einem angemessenen Ausgleich bringt. Der aktuelle Entwurf geht zu Recht davon aus, daß grundsätzlich alle Umstände einer Krankenhausbehandlung einschließlich des dortigen Aufenthalts eines Patienten der ärztlichen Schweigepflicht unterliegen, die nicht nur für das ärztliche und pflegerische, sondern auch für das sonstige Krankenhauspersonal besteht. Dementsprechend soll festgelegt werden, wann das Ermittlungsinteresse der Polizei zur Straftatenverfolgung und zur Gefahrenabwehr die Offenbarung von Patientendaten für befugt erscheinen läßt. Dafür wurden folgende Grundsätze vorgeschlagen:

— Die eigene Auskunft des Patienten gegenüber der Polizei hat unbedingten Vorrang vor einer Information durch Krankenhausbedienstete.

— Die Schweigepflicht darf durchbrochen werden, wenn der Patient in die Erteilung der Auskünfte eingewilligt hat.

— Ist ein Patient, z. B. wegen Bewußtlosigkeit, nicht in der Lage, eine eigene Willensäußerung abzugeben, darf das Krankenhauspersonal im Falle einer nicht nur vorübergehenden Einwilligungsunfähigkeit dann Auskünfte erteilen, wenn eine mutmaßliche Einwilligung des Patienten unterstellt werden kann. Die Entscheidung darüber hat der behandelnde Arzt zu treffen. Bei der Annahme einer mutmaßlichen Einwilligung ist Zurückhaltung geboten.

— Eine Offenbarungsbefugnis kann sich ferner aus den Grundsätzen des rechtfertigenden Notstands ergeben, wenn die Weitergabe von Patientendaten zur Abwehr einer drohenden Gefahr für ein höherwertiges Rechtsgut erforderlich ist.

— Eine Auskunftspflicht besteht gemäß § 138 StGB für geplante bzw. noch nicht vollendete besonders schwere, enumerativ aufgeführte Straftaten.

— Zur Auskunft über medizinische Daten ist nur der Arzt befugt.

Unberührt von diesen Vorschlägen bleibt das Recht der Polizei auf Einsichtnahme in das vom Krankenhaus zu führende melderechtliche Verzeichnis.

Wir unterstützten den Entwurf, der geeignet ist, Unsicherheiten beim Krankenhauspersonal zu beseitigen.

Eine abschließende Stellungnahme der Polizei lag bis zum Redaktionsschluß für diesen Bericht allerdings noch nicht vor.

4.16.3 Prüfung des Bernhard-Nocht-Instituts

Die Nutzung der Vorteile der automatisierten Datenverarbeitung gerade in so sensiblen Bereichen wie dem Gesundheitswesen erfordert strenge Zulässigkeitsregelungen und Datensicherungsmaßnahmen, damit der Patientendatenschutz gewährleistet werden kann. Daß in diesem Bereich noch erhebliche Defizite bestehen, konnten wir bei einer datenschutzrechtlichen Prüfung der Verarbeitung personenbezogener Daten auf PC im Bernhard-Nocht-Institut feststellen.

Das Bernhard-Nocht-Institut ist ein Forschungsinstitut der Behörde für Arbeit, Gesundheit und Soziales mit angeschlossener klinischer Abteilung. Es führt Untersuchungsaufträge für Ärzte, Krankenhäuser und sonstige diagnostische Einrichtungen aus dem gesamten Bundesgebiet und zum Teil aus dem Ausland durch. Dabei fallen in einigen Abteilungen des Instituts hochsensible Patientendaten wie Diagnosen, Untersuchungsergebnisse — auch von HIV-Tests — an, die auf PC verarbeitet werden.

Mangels schriftlich fixierter Regelungen der zuständigen Behörde über die Zulässigkeit der automatisierten Verarbeitung von Patientendaten, über Zuständigkeiten, Zugriffsbefugnisse und zu treffende Sicherungsmaßnahmen, bleibt dem einzelnen Anwender die Entscheidung überlassen, welche Schutzvorkehrungen er für ausreichend hält. Es verwundert daher kaum, daß bei der Prüfung Gesetzesverstöße bzw. Mängel bei der Datenverarbeitung festgestellt wurden.

Als technisch-organisatorische Schwachstelle ist z. B. zu bemängeln, daß weder Benutzer- noch Systemverwalteraktivitäten protokolliert werden. Der Zugriffsschutz durch Paßworteingabe ist unzureichend, da zum Teil für mehrere Benutzer das gleiche Paßwort vergeben ist und die Paßworte unverschlüsselt auf der Festplatte gespeichert werden, so daß für geübte PC-Benutzer ein Direktzugriff dennoch möglich ist. Auch die Patientendaten sind weder auf der Festplatte noch auf den Archivdisketten verschlüsselt. Die Archivdisketten werden zum Teil unzureichend gesichert verwahrt.

An der Datenverarbeitung der klinischen Abteilung ist zu kritisieren, daß in ihrer Patientendatei nicht zwischen archivierten Fällen und aktuellen Behandlungsfällen differenziert wird. Ein Direktzugriff auf automatisiert gespeicherte personenbezogene medizinische Daten, dazu gehören auch Diagnosen und Verweildauern, ist nur bis zum

Abschluß des Behandlungsfalles vom Behandlungsvertrag gedeckt. Eine Nutzung dieser Daten zu anderen, etwa zu Forschungszwecken, bedarf einer zusätzlichen gesetzlichen Grundlage oder der informierten Einwilligung des Patienten. Auch hier fehlt eine Regelung für die Zulässigkeit der Datenverarbeitung und für die erforderlichen Datensicherungsmaßnahmen.

Zur Behebung der Mängel bei der automatisierten Datenverarbeitung haben wir der BAGS vorgeschlagen, verbindlich die Einhaltung der Datensicherungsmaßnahmen vorzuschreiben, wie sie in dem Datensicherungskonzept für Einzelplatz-PC (vgl. oben 2.2) beschrieben sind. Für Patientendaten gilt danach die Schutzstufe C, die insbesondere einen Paßwortschutz, Verbot des Betriebssystem-Zugriffs durch den Anwender, eine weitgehende Protokollierung und eine Verschlüsselung der Daten vorsieht.

Nicht nur bei der automatisierten Verarbeitung von Patientendaten, sondern auch bei dem herkömmlichen Umgang mit Untersuchungsaufträgen, Befundberichten, Testergebnissen und Krankenakten wurden Schwachstellen offenbar: So leiten die diagnostischen Abteilungen ihre Untersuchungsergebnisse, zum Teil zusammen mit der ärztlichen Bewertung, an die Abrechnungsabteilung zur Erstellung des Gebührenbescheides weiter. Dadurch erfolgt eine unzulässige Offenbarung von Patientendaten an die Verwaltungsabteilung, die für ihre Aufgabe allenfalls Informationen über die Art der durchgeführten Untersuchung, nicht aber über das Ergebnis benötigt. Hier muß durch organisatorische Maßnahmen sichergestellt werden, daß die ärztliche Schweigepflicht beachtet wird. Möglicherweise ist eine Abrechnung der durchgeführten Untersuchungen aufgrund des Auftrages ausreichend. Wünschenswert wäre eine generelle Codierung der Patientennamen durch die auftraggebende Stelle.

Festgestellt wurde im Rahmen der Prüfung auch, daß Patientendaten in einem über die Dokumentationspflicht hinausgehenden Maß oder länger als erforderlich aufbewahrt werden. Die Speicherung von Daten, die nicht mehr zur Aufgabenerfüllung, einschließlich der Dokumentation, benötigt werden, ist datenschutzrechtlich unzulässig. Die nicht mehr benötigten Patientenunterlagen und Krankenakten müssen ordnungsgemäß vernichtet werden.

Da wir unsere Verbesserungsvorschläge erst kurz vor Redaktionsschluß unterbreitet haben, liegt eine Stellungnahme der Behörde und des Instituts noch nicht vor.

5. Einzelne Probleme des Datenschutzes im nicht-öffentlichen Bereich

5.1 Versandhandel / interne Bonitätsprüfung

In unserem 6. Tätigkeitsbericht hatten wir mitgeteilt, daß erfreulicherweise ein Versandhandelsunternehmen nicht nur auf die SCHUFA-Anfrage über den Ehegatten des Bestellers verzichtet, sondern darüber hinaus SCHUFA-Anfragen generell nicht mehr durchführt (6. TB 5.1.1, S. 121). Im letzten Punkt müssen wir uns leider korrigieren.

Im Berichtszeitraum führten wir ein Gespräch mit Vertretern dieses Versandhauses, um uns über den neuesten Stand des Bonitätsprüfungsverfahrens zu informieren (vgl. dazu auch 6. TB a.a.O., 7. TB 5.1, S. 121). Dabei ergab sich, daß man sich mittlerweile für ein mehrstufiges Verfahren entschieden hat.

Die Bonität von Erstbestellern wird zunächst intern mittels eines Scoring-Verfahrens geprüft. Es basiert auf den gesammelten Erfahrungen des Versandhauses über das Kauf- und Zahlungsverhalten seiner Kreditkunden. Sie werden ständig statistisch ausgewertet. Zur Bonitätsprüfung benötigt das Versandhaus vom Kunden nur die Angaben auf dem Bestellschein. Als Ergebnis der Prüfung wird dem Kunden ein Parameter zugeordnet. Wenn er eine festgelegte Grenze unterschreitet, wird er auf den Kauf per Nachnahme verwiesen. Wird eine Obergrenze überschritten, wird ein Kundenkonto ohne weitere Prüfung eingerichtet. In einem Zwischenbereich, der bei ungefähr 50 % der Erstbesteller relevant ist, hängt die weitere Bonitätsprüfung von einer SCHUFA-Auskunft ab. Dies war für uns überraschend. Das Versandhaus hatte die SCHUFA-Anfrage zwischenzeitlich wieder eingeführt, aber die Aufsichtsbehörde über die Verfahrensänderung nicht informiert.

Die SCHUFA-Anfrage wird mit dem Merkmal „Versandhauskonto" vorgenommen. Dieses wird bei der SCHUFA ähnlich wie das Girokonto-Merkmal gespeichert und führt dazu, daß das Versandhauskonto für einen Zeitraum von drei Jahren „beobachtet" wird.

Das Versandhaus erhält — wenn der SCHUFA von dritter Seite negative Merkmale über den Kunden bekannt werden — ohne weitere Anforderung eine Nachmeldung. Eine Konsequenz derartiger Nachmeldungen kann sein, daß das Versandhaus bei einer erneuten Bestellung diesem Kunden keinen Ratenzahlungskredit mehr einräumt.

Wir sind der Auffassung, daß für die drei Jahre andauernde Beobachtung des Versandhandelskontos eine Einwilligung des Kunden eingeholt werden sollte. Denn andernfalls ist zweifelhaft, ob bei jeder Nachmeldung durch die SCHUFA das gemäß § 32 Absatz 2 Satz 1 BDSG erforderliche berechtigte Interesse des Empfängers vorliegt. Zumindest aber sollte dem Kunden die SCHUFA-Anfrage offengelegt werden.

Bedauerlicherweise konnten wir bislang mit diesen Anliegen nicht durchdringen. Die Vertreter des Versandhauses sind der Auffassung, daß derartige Informationen den Kunden eher verwirren, so daß erheblicher zusätzlicher Verwaltungsaufwand aufgrund von Nachfragen produziert werden würde. Daß mehr Transparenz, die wir schon im 6. Tätigkeitsbericht (6. TB, 5.1.2.2, S. 123) angefordert hatten, die Betroffenen verwirren soll, vermag uns nicht zu überzeugen. Vielmehr wird deren datenschutzrechtliche Position durch ein Verfahren, das weitgehend hinter ihrem Rücken abläuft, deutlich geschwächt.

5.2 SCHUFA/Kreditwirtschaft

5.2.1 SCHUFA

5.2.1.1 SCHUFA-Auslandskonzept

In unserem letzten Tätigkeitsbericht (vgl. 8. TB, 4.1, S. 113f.) haben wir ein Problem behandelt, das eine SCHUFA-Meldung über die Kreditaufnahme einer Person bei

einem österreichischen Bankhaus betraf. Erfreulich ist es jetzt, berichten zu können, daß über den Einzelfall hinaus eine generelle SCHUFA-Auslandskonzeption erarbeitet wurde.

Ausgangspunkt ist die Feststellung des Bundesgerichtshofes im Urteil vom 19. September 1985, daß die im Inland gebräuchliche SCHUFA-Klausel eine Einwilligung hinsichtlich positiver Kreditinformationen (z. B. Kreditaufnahme und vertragsgemäße Rückzahlung) bedeutet, hinsichtlich negativer Merkmale (z. B. Zwangsvollstreckung) aber nur eine Unterrichtung über die gesetzlichen Voraussetzungen für eine zulässige Übermittlung darstellt. Demgemäß sind auch die Übermittlungen negativer Daten durch die SCHUFA an eines der angeschlossenen Kreditinstitute nicht aufgrund einer Einwilligung statthaft, sondern nur unter den Bedingungen des § 32 Absatz 2 Satz 1 BDSG. Einer Übermittlung an ein ausländisches Kreditinstitut steht insoweit jedoch stets entgegen, daß nach unserer Auffassung das dortige Fehlen eines Datenschutzgesetzes die schutzwürdigen Belange des Betroffenen so stark beeinträchtigt, daß sie nach § 32 Absatz 2 Satz 1 BDSG nicht zulässig ist (vgl. Simitis in Simitis/Dammann/Mallmann/Reh, Kommentar zum Bundesdatenschutzgesetz 3. Auflage 1981 § 22 Rn. 54 f, § 32 Rn. 25).

Etwas anderes würde sich jedoch dann ergeben, wenn das Fehlen eines Datenschutzgesetzes durch vertragliche Regelungen zugunsten des Betroffenen kompensiert werden könnte.

An dieser Stelle setzt das Auslandsmodell der SCHUFA an. Das ausländische Kreditinstitut, das Vertragspartner der SCHUFA werden möchte, schließt mit der zuständigen SCHUFA-Gesellschaft in der Bundesrepublik einen Vertrag zugunsten Dritter (§ 328 BGB). Dadurch erhält ein zukünftiger Kunde des ausländischen Kreditinstitutes, dessen Bonität mit Hilfe einer SCHUFA-Anfrage geprüft werden soll, vertraglich einen Anspruch auf Auskunft über die zu seiner Person gespeicherten Daten. Ferner kann er Berichtigung unrichtiger Daten und Löschung unzulässig gespeicherter oder unzulässig übermittelter Daten verlangen. Beurteilungsmaßstab für die Zulässigkeit von Speicherung und Übermittlung ist das Bundesdatenschutzgesetz, da für das Vertragsverhältnis die Geltung deutschen Rechtes vereinbart wird. Der Kunde wird über seine Rechte durch die SCHUFA-Klausel auf seinem Kreditantrag informiert.

Ferner hat der Vertragspartner der SCHUFA einen sogenannten SCHUFA-Beauftragten zu bestellen. Er soll die Einhaltung der vertraglichen Pflichten überwachen und steht in regelmäßiger Verbindung zur SCHUFA. Außerdem verpflichtet sich der Vertragspartner der SCHUFA, die Einhaltung aller vertraglichen Pflichten in geeigneter Weise — gegebenenfalls bei einem Informationsbesuch der SCHUFA vor Ort — nachzuweisen sowie erkannte Mängel bei der Datenverarbeitung zu beseitigen.

Schließlich enthält der Rahmenvertrag noch eine allgemeine Verpflichtung des Vertragspartners, die Grundsätze des „Übereinkommens zum Schutze des Menschen bei der automatischen Verarbeitung personenbezogener Daten" des Europarates vom 28. Januar 1981 (DSK) einzuhalten. Soweit die bereits zitierten Vertragsbestimmungen nicht schon die Grundsätze der Konvention aufgreifen, wird dadurch ergänzend der Mindeststandard zur Datensicherung (Art. 7 DSK), der Zweckbindungsgrundsatz (Art. 5 Buchstabe b) und c) DSK), ein gesteigerter Schutz für besonders sensible Daten (Art. 6 DSK), der Grundsatz von Treu und Glauben (Art. 5 Buchstabe a) DSK) sowie der Grundsatz der Erforderlichkeit (Art. 5 Buchstabe e) DSK) festgeschrieben.

Das SCHUFA-Merkblatt, das Kunden auf Anfrage erhalten, wurde um die Information über die Rechte des Kunden bei ausländischen SCHUFA-Vertragspartnern erweitert.

Dieses Konzept soll unabhängig davon Anwendung finden, ob im Empfängerland ein Datenschutzgesetz existiert oder nicht. Falls der Gesetzgeber bereits tätig geworden ist, so ergänzen die vertraglichen Rechte die gesetzlichen Ansprüche. Möglicherweise hat dann darüber hinaus der Betroffene die zusätzliche Möglichkeit, eine fehlerhafte Verarbeitung seiner Daten bei einer unabhängigen Datenschutzkontrollinstitution zu rügen. In jedem Fall wäre das Vertragsmodell eine völlig unschädliche Ergänzung, so

daß eine mehr oder weniger unübersichtliche Differenzierung in Länder mit oder ohne Datenschutzgesetz, innerhalb oder außerhalb der Europäischen Gemeinschaft, mit oder ohne Ratifikation des „Übereinkommens zum Schutze des Menschen bei der automatischen Verarbeitung personenbezogener Daten" des Europarates vom 28. Januar 1981 unterbleiben kann (vgl. dazu 8. TB, 4.5.5 S. 130 f).

Wir sind der Auffassung, daß dieses Modell geeignet ist, Bedenken gegen eine Datenübermittlung ins Ausland, auch wenn im Ausland kein Datenschutzgesetz existiert, weitgehend auszuräumen. Ausschlaggebend dafür ist die Überlegung, daß ein qualitativer Unterschied zwischen vertraglichen und gesetzlichen Ansprüchen nicht besteht, wenn und soweit in jedem Fall sichergestellt ist, daß der Betroffene seine Rechte kennt oder zumindest kennen kann. Dies ist hier dadurch gewährleistet, daß alle Betroffenen eine SCHUFA-Klausel unterzeichnen, die ihnen eine erste Aufklärung bietet. Näheres kann jeder Interessierte dann entweder dem SCHUFA-Merkblatt entnehmen oder durch eine mündliche Nachfrage klären. Wir meinen darüber hinaus, daß der schwächste Punkt der „Vertragslösung", nämlich die Unmöglichkeit, vertraglich eine unabhängige Datenschutzkontrollinstanz zu installieren, durch das Kontrollrecht der SCHUFA „vor Ort" gemildert wird. Denn die SCHUFA ist der hiesigen Aufsichtsbehörde gegenüber verantwortlich und hat ihr gegenüber dafür einzustehen, daß ihre Datenübermittlungen und -speicherungen zulässig sind. Dies ist aber nur dann der Fall, wenn das Auslandskonzept in der Praxis vollständig und richtig realisiert wird. Insofern bauen die Aufsichtsbehörden auf das Eigeninteresse der SCHUFA, beim Vertragspartner für vertragsgemäße Zustände zu sorgen.

Wir räumen allerdings ein, daß sich dieses Konzept nun in der Praxis bewähren muß, bevor es gelobt werden kann. Darüber hinaus wäre ein einheitlicher — möglichst hoher — Datenschutzstandard in Europa allemal wünschenswerter als der hier unternommene Versuch, die Niveauunterschiede mit Vertragsmodellen auszugleichen.

5.2.1.2 Mutmaßliche Einwilligung in eine SCHUFA-Anfrage

Im Berichtszeitraum beschwerte sich ein Petent darüber, daß sein kontoführendes Kreditinstitut ohne seine Einwilligung über ihn eine SCHUFA-Auskunft eingeholt hatte. Der Beschwerdeführer unterhielt ein Girokonto, für das kein Überziehungskredit vereinbart war. Dementsprechend hatte er auch nicht die übliche SCHUFA-Klausel unterzeichnet. Damit hätte er in den Austausch positiver oder wertneutraler Kreditinformationen über seine Person eingewilligt und wäre über die gesetzlichen Voraussetzungen der Übermittlung negativer Merkmale unterrichtet worden. Als er sein Konto mehrere Wochen ungenehmigt überzog, prüfte die Bank, ob sie ihrem Kunden einen Überziehungskredit einräumen sollte, und fragte zu diesem Zweck bei der SCHUFA unter dem Merkmal „Kredit beantragt" an. Das Kreditinstitut unterstellte dabei eine mutmaßliche Einwilligung, da der Kunde tatsächlich Kredit in Anspruch genommen habe. Die SCHUFA erteilte die Auskunft.

Wir halten den Informationsaustausch zwischen Kreditinstitut und SCHUFA unter diesen Voraussetzungen nicht für zulässig.

Für eine mutmaßliche Einwilligung ist solange kein Raum, wie der Betroffene — wie hier — unmittelbar befragt werden kann. Dieser allgemeine Rechtsgrundsatz gilt nicht nur im Straf- und im Zivilrecht, sondern auch im Datenschutzrecht. Dort findet er sogar eine noch striktere Ausprägung, weil § 3 Satz 2 BDSG grundsätzlich die Schriftform für die Einwilligung verlangt.

Ferner kann sich das Kreditinstitut nicht auf einen gesetzlichen Erlaubnistatbestand stützen. Nach § 24 Absatz 1 Satz 1 3. Alt. BDSG sind die schutzwürdigen Belange des Betroffenen gegen das berechtigte Interesse des Empfängers abzuwägen. Dies setzt voraus, daß der Betroffene seine Belange vorbringen kann. Daran mangelt es aber, wenn ohne sein Wissen Informationen über ihn ausgetauscht werden. Für ein solches Vorgehen besteht insbesondere dann keinerlei Rechtfertigung, wenn der Betroffene ohne Schwierigkeit hätte befragt werden können.

Gleichwohl nahm auch die SCHUFA zu diesem Vorfall dahingehend Stellung, daß sie ebenfalls die tatsächliche Kontoüberziehung für ausreichend erachte, um eine Auskunft zu erteilen und darüber hinaus die bei dieser Anfrageart üblichen Nachmeldungen über das Kreditverhalten des Kunden während der Dauer des Bestehens des Girokontos durchzuführen. Denn die tatsächliche Kontoüberziehung müsse einem Kreditantrag gleichgestellt werden.

Dabei wird unseres Erachtens übersehen, daß bei einem Kreditantrag die SCHUFA-Klausel vorgelegt und unterzeichnet wird, bevor es zu Datenübermittlungen kommt. Derjenige, der unter diesen Umständen von einer Kreditaufnahme absehen will, erhält dazu die Gelegenheit. Es gibt keinen Grund, bei einer tatsächlichen Kontoüberziehung anders zu verfahren. Denn jedes Kreditinstitut ist in der Lage, ungenehmigte Kontoüberziehungen zu unterbinden. Das Kreditinstitut hat daher die Möglichkeit, vor der faktischen Kontoüberziehung dem Betroffenen die übliche SCHUFA-Klausel zu unterbreiten und sich vorzubehalten, die Kontoüberziehung abzulehnen, wenn ihr Kunde am SCHUFA-Verfahren nicht teilnehmen will.

Unter diesen Umständen kann die Datenübermittlung auch nicht auf § 32 Absatz 2 BDSG gestützt werden, denn die Kreditinstitute können ohne die Einwilligung ihrer Kunden das nach dieser Vorschrift geforderte „berechtigte Interesse" grundsätzlich nicht glaubhaft machen.

Wir werden uns in weiteren Gesprächen darum bemühen, die Beteiligten davon zu überzeugen, daß auf die — tatsächlich mögliche — Unterzeichnung der SCHUFA-Klausel nicht unter Berufung auf mutmaßliche Einwilligung verzichtet werden darf.

5.2.2 Datenschutzrechtliche Ergänzungen im Entwurf eines Verbraucherkreditgesetzes

Die Bundesregierung hat einen Entwurf für ein Gesetz zur Regelung von Verbraucherkrediten vorgelegt. Er verfolgt das Ziel, einen angemessenen Verbraucherschutz bei Kreditverträgen zwischen gewerblichen Kreditgebern und Verbrauchern sicherzustellen. Im Vordergrund steht die umfassende Unterrichtung des Verbrauchers über seine mit der Kreditaufnahme verbundenen Verpflichtungen, insbesondere über die Kreditkosten. Außerdem sollen Kreditnehmer vor Vertragsbedingungen geschützt werden, die sie unangemessen benachteiligen. Der Anwendungsbereich des Gesetzes ist weit gefaßt und bezieht nicht nur herkömmliche Darlehen ein, sondern auch Überziehungskredite und andere kontokorrentähnliche Kredite sowie Kreditgewährungen vermittels einer Kreditkarte. Darüber hinaus erfaßt das Gesetz grundsätzlich jeden entgeltlichen Zahlungsaufschub bei Liefergeschäften und Dienstleistungen, somit auch Abzahlungsgeschäfte.

Wir sind der Auffassung, daß ein Verbraucherschutzgesetz unvollständig bleiben wird, wenn nicht auch die Datenverarbeitung in Kreditinformationssystemen, also jenen Institutionen, die Informationen über das Kreditverhalten von Verbrauchern sammeln und weitergeben, eine bereichsspezifische Regelung erfährt. In der Kreditwirtschaft werden in großem Umfang Informationen über die Kreditwürdigkeit nahezu der gesamten erwerbstätigen Bevölkerung gesammelt und weitergegeben. Nicht nur Kreditaufnahmen, sondern bereits die Einrichtung eines Girokontos oder die Ausgabe einer Kreditkarte ziehen eine ständige automationsgestützte Bonitätsbeobachtung der Verbraucher nach sich. Zwar haben die Datenschutzaufsichtsbehörden in der Vergangenheit eine Reihe von Absprachen mit der Schutzgemeinschaft für allgemeine Kreditsicherung — SCHUFA — getroffen. Jedoch können diese Absprachen keine gesetzliche Regelung ersetzen. Es gibt immer wieder Unklarheiten (siehe 5.2.1.2) und es ist bis heute nicht gelungen, bestimmte Nutzer von Kreditinformationssystemen, wie zum Beispiel den Handel und den Versandhandel, zur Offenlegung ihrer Teilnahme am SCHUFA-Verfahren zu bewegen.

Daher sollte die Gelegenheit genutzt werden, die folgenden — wünschenswerten — Regelungen im Gesetz zu verankern:

— Kreditinformationsdienste sollten einer strikten Zweckbindung unterworfen werden. Danach dürften Daten von Kreditnehmern nur erfaßt und genutzt werden, soweit dies zur Beurteilung der Kreditwürdigkeit und zur Bonitätskontrolle erforderlich ist. Eine Verwendung für andere Zwecke, etwa zur Personaleinstellung, zum Abschluß von Mietverträgen oder zu Werbezwecken, wäre unzulässig. Die Empfänger von Kreditinformationen dürfen die Daten ebenfalls nur im Rahmen der Zweckbindung verwenden.

— Festzulegen wäre, welche Merkmale über nicht vertragsgemäßes Verhalten und welche sonstigen Angaben über Zahlungsunfähigkeit oder -unwilligkeit (Negativmerkmale) in Kreditinformationssystemen verarbeitet werden dürfen.

— Vor der Übermittlung bestimmter Negativmerkmale, bei denen Fehlentscheidungen über die Zahlungsunfähigkeit oder -unwilligkeit nicht auszuschließen sind (z. B. Verdacht des Scheckkartenmißbrauchs), müßte dem Kreditnehmer Gelegenheit zur Stellungnahme gegeben werden.

— Durch Verpflichtungen zu fortwährender Aktualisierung wäre sicherzustellen, daß der Datenbestand des Kreditinformationsdienstes zu jeder Zeit ein zutreffendes Bild über die Bonität der Kreditnehmer vermittelte.

— Nur mit schriftlicher Einwilligung dürften sogenannte positive oder neutrale Merkmale über den Kunden verarbeitet werden.

— Personenverwechslungen, die in der Praxis häufig auftreten und zu schwerwiegenden Nachteilen für die Betroffenen führen können, müßten wirksam ausgeschlossen werden.

— Es wären Löschungsfristen festzulegen, die der besonderen Schutzbedürftigkeit der Kreditdaten Rechnung trügen.

— Kreditnehmer müßten schon dann benachrichtigt werden, wenn Daten zu ihrer Person erstmals im Kreditinformationssystem gespeichert werden; es sei denn, es stünde fest, daß sie auf andere Weise hiervon Kenntnis erlangt hätten.

— Das Auskunftsrecht der Kreditnehmer müßte sich auch auf die Herkunft und die Empfänger der Daten erstrecken.

— Soweit Kreditgeber am Kreditinformationsverfahren teilnehmen, wären sie der anlaßfreien Überwachung durch die Aufsichtsbehörde zu unterstellen.

— Bei mathematisch-statistischen Verfahren zur Bewertung der Bonität von Verbrauchern (Kreditscoring) müßte den Kreditnehmern auf Antrag über die Bewertungsgrundlagen und -kriterien sowie über errechnete Teil- und Gesamtwerte kostenlos Auskunft erteilt werden.

Auf Initiative des Bundesbeauftragten für den Datenschutz hat über dieses Anliegen zwischen Vertretern des Bundesministeriums für Justiz, dem Bundesbeauftragten für den Datenschutz und einigen Datenschutzaufsichtsbehörden ein Gespräch stattgefunden. Es bleibt abzuwarten, ob entsprechende Regelungen in das weitere Gesetzgebungsverfahren eingebracht werden.

5.2.3 Datenübermittlung durch Gläubigerbanken an Makler im Zwangsvollstreckungsverfahren

Durch die Eingabe eines Petenten erlangten wir vom folgenden Sachverhalt Kenntnis: Eine Bank beantragte die Zwangsversteigerung eines Grundstücks, wogegen der Schuldner Rechtsmittel einlegte. Bevor über die Rechtsmittel entschieden worden war und bevor das Vollstreckungsgericht einen Versteigerungstermin bestimmt hatte, beauftragte die Bank ohne Einverständnis des Schuldners unter Hinweis auf die geplante Zwangsversteigerung einen Makler, die Immobilie interessierten Käufern anzubieten. Daraufhin suchten mehrfach Kaufinteressenten das betreffende Grundstück zur Besichtigung auf und wollten vom dort wohnenden Eigentümer, dem Schuld-

ner der Bank, nähere Einzelheiten wissen. Letztendlich erledigte sich das Zwangsversteigerungsverfahren durch einen Vergleich, und zwar bevor über die Rechtsmittel entschieden wurde und bevor ein Versteigerungstermin bestimmt worden war.

Der Petent wandte sich mit der Bitte an uns, das Vorgehen der Bank rechtlich zu bewerten. Wir teilten mit: Nach unserer Rechtsauffassung stellt das Verhalten der Bank einen rechtswidrigen Eingriff in das allgemeine Persönlichkeitsrecht des Schuldners dar, der unter Umständen gemäß § 823 Absatz 1 BGB i.V.m. Artikel 1 Absatz 1, Artikel 2 Absatz 1 GG zum Schadensersatz verpflichten kann.

§ 823 Absatz 1 BGB schützt das allgemeine Persönlichkeitsrecht und als dessen Bestandteil auch die Geheimhaltung der persönlichen und wirtschaftlichen Verhältnisse einer Person. In diese Sphäre hat die Bank durch die Weitergabe der Informationen über die Immobilie und über die eingeleitete Zwangsversteigerung eingegriffen.

Der Eingriff war — zu diesem Zeitpunkt — auch rechtswidrig, weil das Interesse des Schuldners, auch im Zwangsversteigerungsverfahren möglichst schonend behandelt zu werden und nicht unnötigen Unannehmlichkeiten ausgesetzt zu sein, gegenüber dem Interesse der Bank, das Grundstück optimal zu verwerten, überwog.

Für die Bewertung war für uns die Überlegung maßgeblich, daß im Zwangsversteigerungsverfahren zwei Verfahrensabschnitte unterschieden werden müssen, in denen die Interessen der Betroffenen unterschiedlich zu gewichten sind.

Im ersten Verfahrensabschnitt prüft das Vollstreckungsgericht die formellen und materiellen Voraussetzungen der beantragten Zwangsversteigerung, entscheidet über einstweilige Einstellungen nach § 30a ZVG und hat nach Lösungsmöglichkeiten zu suchen, um die Zwangsversteigerung zu vermeiden (so Steiner-Teufel, Zwangsversteigerung und Zwangsverwaltung, Vorbem. zu §§ 35 ff ZVG Rn. 3). Im Interesse des Schuldners ist das Verfahren während dieses Verfahrensstandes nicht öffentlich.

Diese Sachlage ändert sich, wenn Alternativen zur Zwangsversteigerung nicht existieren oder nicht realisierbar sind und die Zwangsversteigerung nicht mehr abwendbar ist. Ab diesem Zeitpunkt tritt das Interesse des Gläubigers an der Verwertung des Grundstücks in den Vordergrund. Das Geheimhaltungsinteresse des Schuldners bezüglich seiner persönlichen wirtschaftlichen Verhältnisse tritt zurück und das Verfahren wird öffentlich (ebenso Steiner-Teufel, a.a.O. Rn. 6, § 42 Rn. 7, 11).

Diese differenzierte Gestaltung des Verfahrens kann die beabsichtigten Schutzwirkungen nur entfalten, wenn die Beteiligten die unterschiedlichen Interessen beachten. Deshalb entnehmen wir den Vorschriften des Zwangsvollstreckungsgesetzes, die sich direkt nur an das Vollstreckungsgericht wenden, den allgemeinen Rechtsgedanken, daß Informationen über die Zwangsversteigerung an Personen, die nicht am Verfahren beteiligt sind, erst nach der Festsetzung des Versteigerungstermins weitergeleitet werden dürfen. Diesen Grundsatz hat auch der betreibende Gläubiger zu beachten. Er darf vor der Bestimmung des Versteigerungstermins die persönlichen und wirtschaftlichen Verhältnisse des Schuldners nicht offenlegen, um das vermeintliche Zwangsversteigerungsobjekt optimal zu verwerten.

5.3 Versicherungswirtschaft

5.3.1 Zentrale Warn- und Hinweissysteme

Die zentralen Warn- und Hinweissysteme in der Versicherungswirtschaft sind aufgrund ihrer Vielzahl und ihrer datenschutzrechtlichen Problematik regelmäßig Gegenstand unserer Berichterstattung (vgl. zuletzt 8. TB, 4.2.1, S. 114 ff).

5.3.1.1 Einordnung der Tätigkeit der Verbände bei Verwendung des phonetischen Strukturcodeverfahrens

Wenn und soweit die Daten in solchen Systemen uncodiert oder in Matchcodes verarbeitet werden, neigen wir dazu, die Tätigkeit der Verbände, die sie unterhalten, als Aus-

kunftei betrieb im Sinne von § 31 Absatz 1 Nr. 1 BDSG a.F. einzuordnen, während die Versicherungswirtschaft sie als Datenverarbeitung für eigene Zwecke nach dem 3. Abschnitt des BDSG qualifiziert. Bislang konnte lediglich Einvernehmen darüber hergestellt werden, daß bei Verwendung des phonetischen Strukturcodeverfahrens die Versicherungsunternehmen für die Datenverarbeitung in den Warn- und Hinweisdateien nach dem 3. Abschnitt des Bundesdatenschutzgesetzes die Verantwortung tragen und die Datenverarbeitung im Sinne von § 31 Absatz 1 Nr. 3 BDSG a.F. anzusehen ist.

Ausschlaggebend dafür sind die folgenden Überlegungen: Mit Einführung des Strukturcodeverfahrens erreicht die Chiffrierung eine Qualität, die mit den herkömmlichen Matchcodes nicht mehr zu vergleichen ist. Es ist der Tatsache Rechnung zu tragen, daß die Verbände, z. B. im Falle eines an sie gerichteten Auskunftsverlangens, nur noch mit sehr großem Aufwand in der Lage wären festzustellen, ob die Daten einer Person gespeichert sind oder nicht. Das Strukturcodeverfahren verwandelt nämlich Name und Adresse in eine Ziffernfolge, die aus sich heraus nicht mehr deanonymisiert werden kann (Einwegcodierung). Eine Reidentifizierung ist nur dadurch möglich, daß bei dem einmeldenden Versicherungsunternehmen die Identität der Person erfragt wird. Dies geschieht durch das im Datensatz uncodiert beigefügte Aktenzeichen, mit dem der Sachbearbeiter den Originalvorgang auffinden kann. Bei Verwendung des Strukturcodeverfahrens könnte also der Verband dem Auskunftsersuchen einer Person nur dadurch nachkommen, daß er seinerseits Name und Adresse chiffriert, mit der codierten Warndatei abgleicht, eine unter Umständen sehr große Zahl von Treffern erhält, die jeweiligen Identitäten durch Nachfrage bei den Versicherungsunternehmen feststellt, um anhand der dann entstehenden Liste entscheiden zu können, ob die anfragende Person dabei ist oder nicht. Dies wäre ein unverhältnismäßiger Aufwand.

Daraus folgt, daß der Verband nicht mehr als eine selbständige datenverarbeitende Stelle im Sinne des Bundesdatenschutzgesetzes aufzufassen ist, da er keine personenbeziehbaren — und damit keine personenbezogenen — Daten verarbeitet. Ob chiffrierte Daten personenbeziehbar (und damit personenbezogen) sind, bestimmt sich auch nach der Interessenlage desjenigen, der mit den chiffrierten Informationen in einer bestimmten Situation umgeht. Haben die Informationen für ihn einen so großen Wert, daß damit zu rechnen ist, daß er den zur Deanonymisierung erforderlichen Aufwand auch tatsächlich — und sei es nur im Einzelfall — betreiben wird, so ist die Personenbeziehbarkeit zu bejahen (vgl. dazu Dammann in Simitis/Dammann/Mallmann/Reh, Kommentar zum Bundesdatenschutzgesetz 3. Auflage 1981 § 2 Rn. 34 ff, besonders Rn. 36). Diese Situation ist bei den Verbänden zur Zeit nicht erkennbar. Denn sie dürften an den Erkenntnissen aus den Warndateien nicht oder jedenfalls nicht in dem Maße interessiert sein, daß sie die Reidentifizierungsprozedur aus eigenem Antrieb auf sich nehmen würden.

Deshalb halten wir diese Tätigkeit der Verbände bei Verwendung des Strukturcodeverfahrens für Auftragsdatenverarbeitung. Unschädlich für diese Einordnung ist, daß der Auftragnehmer die Daten „blind" verarbeitet (ebenso Dammann in Simitis/Dammann/Mallmann/Reh, Kommentar zum Bundesdatenschutzgesetz 3. Aufl. 1981 § 8 Rn. 4). Es ist auch kein logischer Widerspruch, daß eine Verarbeitung von nicht chiffrierten Daten nach § 31 Absatz 1 Nr. 1 BDSG a.F. (nach anderer Ansicht nach § 23 ff BDSG a.F.) und die gleiche Verarbeitung im chiffrierten Zustand nach § 31 Absatz 1 Nr. 3 BDSG a.F. zu beurteilen ist. Verändert sich eine wesentliche Verarbeitungsmodalität, so kann sich selbstverständlich auch die rechtliche Einordnung verändern.

Die Datenschutzkommission des Gesamtverbandes der Versicherungswirtschaft schloß sich nunmehr unserer Auffassung an, den Verband dann als Auftragsdatenverarbeiter im Sinne des § 31 Absatz 1 Nr. 3 BDSG a.F. einzuordnen, wenn und soweit das phonetische Strukturcodeverfahren angewandt wird. Nun müssen jedoch die Auftragsbeziehungen zwischen Versicherungsunternehmen und Verband ausgestaltet werden.

5.3.1.2 Benachrichtigung der „Dritten" im Sachversicherer-Informationssystem

In unserem letzten Tätigkeitsbericht hatten wir berichtet, mit den Verbänden der Versicherungswirtschaft habe Einigkeit darüber erzielt werden können, daß die Personen, die nicht auf andere Art und Weise von der Aufnahme ihrer Daten in das Sachversicherer-Informationssystem (SAVIS) Kenntnis erlangen konnten (sog. Dritte), qualifiziert zu benachrichtigen seien (8. TB 4.2.1.2., S. 116 f). Unter einer qualifizierten Benachrichtigung verstehen wir eine Information, die zumindest das enthält, was ein Versicherungsnehmer bei Antragstellung der (neuen) Einwilligungsklausel nach dem BDSG und dem Merkblatt zur Datenverarbeitung in der Versicherungswirtschaft entnehmen kann. Leider stellte sich zwischenzeitlich heraus, daß nach wie vor kein Konsens über den notwendigen Inhalt einer Unterrichtung besteht.

Der Gesamtverband der Versicherungswirtschaft (GDV) schlägt vor, den „Dritten" die folgende Information zukommen zu lassen:

> „. . . unser Versicherungsnehmer meldete uns den obigen Schaden.
>
> Im Rahmen der Bearbeitung dieses Schadens wurden die Daten der beteiligten Personen (Name, Anschrift, Geschlecht und — soweit vorhanden — das Geburtsdatum) in unserem Hause gespeichert sowie in anonymisierter Form an den Verband der Sachversicherer e.V. weitergegeben.
>
> Wir geben Ihnen von der Speicherung gemäß § 26 Bundesdatenschutzgesetz Kenntnis . . ."

Der GDV ist der Ansicht, mit dieser Benachrichtigung seinen gesetzlichen Pflichten zu genügen. § 26 Absatz 1 BDSG verlange nur eine Benachrichtigung über die Tatsache der Speicherung, und im übrigen habe der Betroffene auch keinen Auskunftsanspruch über die Tatsache einer Übermittlung und ihren Adressaten. Dann aber könne auch nicht verlangt werden, den Betroffenen über die Weitergabe seiner Daten an alle Versicherer der Sparte zu unterrichten.

Nach unserer Auffassung folgt die Pflicht zur qualifizierten Unterrichtung nicht aus § 26 BDSG a.F., sondern aus der Erwägung, daß die Versicherungsunternehmen sich nur eines solchen Verfahrens bedienen dürfen, in dem sichergestellt ist, daß die Übermittlungen der personenbezogenen Daten von einem (dem speichernden) Versicherungsunternehmen zum anderen (dem anfragenden) Versicherungsunternehmen zulässig sind. Sofern eine Einwilligung nicht vorliegt, kommt als Erlaubnistatbestand nur die 3. Alternative des § 24 Absatz 1 S. 1 BDSG a.F. in Betracht, denn die Übermittlung zum Zwecke der Warnung anderer Unternehmen ist in keinem Fall von einem Versicherungsvertrag gedeckt — dies gilt erst recht, wenn der Betroffene gar nicht Versicherungsnehmer ist. § 24 Absatz 1 BDSG a.F. aber verlangt in jedem Einzelfall eine Abwägung zwischen den berechtigten Interessen der Versicherungswirtschaft und den schutzwürdigen Belangen des Betroffenen. Dies kann in der Praxis nur dann verwirklicht werden, wenn ein Betroffener Gelegenheit erhält, seine Belange dem Versicherungsunternehmen, das ihn in ein Warnsystem einmelden will, zu unterbreiten. Dazu muß er wissen, welche Konsequenzen eine Aufnahme seiner Daten in SAVIS nach sich zieht.

Dementsprechend haben wir vorgeschlagen, folgendermaßen zu unterrichten:

> „Im Rahmen der Bearbeitung dieses Schadens wurden die Daten der beteiligten Personen (Name, Anschrift, Geschlecht und — soweit vorhanden — das Geburtsdatum) in unserem Hause gespeichert sowie an den Verband der Sachversicherer e.V. weitergegeben, der in unserem Auftrag die Daten an solche Versicherungsunternehmen weiterleitet, mit denen Sie anläßlich eines Versicherungsantrages oder zur Abwicklung eines Schadensfalles in Verbindung treten. Zweck dieser zentralen Registrierung ist es, Hinweise auf ein eventuell erhöhtes Betrugsrisiko zu geben."

Diese Formulierung wurde nicht akzeptiert. Allerdings hat der Gesamtverband der Deutschen Versicherungswirtschaft inzwischen seine weitere Gesprächsbereitschaft

signalisiert. Dies nehmen wir gerne auf, müssen jedoch darauf hinweisen, daß die Zustimmung zum Gesamtverfahren für uns von einer befriedigenden Lösung dieses Problems abhängt. Diese Position hatten wir zuletzt in unserem 8. Tätigkeitsbericht klar zum Ausdruck gebracht (4.2.1.2, S. 116 m.w.Nw.).

5.3.1.3 Das Meldeverfahren der Kfz-Versicherer

In unserem 7. Tätigkeitsbericht nahm das Warnsystem der Kfz-Versicherer einen breiten Raum ein (7. TB, 5.4.1.3, S. 136 ff). Der beim HUK-Verband installierte Auskunftsbetrieb dient dem Zweck, dem Versicherungsbetrug zu begegnen. Im Gegensatz zu allen anderen Warn- und Hinweissystemen in der Versicherungswirtschaft übermittelt der HUK-Verband auf Einzelnachfrage Informationen aus seinen K-Dateien. Dieses Warn- und Hinweissystem unterscheidet sich daher nicht von einem herkömmlichen Auskunfteibetrieb und muß deshalb nach den dafür geltenden Vorschriften des 4. Abschnittes des Bundesdatenschutzgesetzes beurteilt werden.

Die im 7. Tätigkeitsbericht dargestellte datenschutzrechtliche Bewertung ergab, daß das Verfahren in seiner jetzigen Form nicht akzeptiert werden kann. Im letzten Tätigkeitsbericht konnten wir uns auf den Hinweis der geplanten grundsätzlichen Neukonzeption in naher Zukunft beschränken (8. TB, 4.2.1.5, S. 119). Obwohl diese Neukonzeption erfreulicherweise inzwischen in Teilen vorgelegt wurde (siehe unter 5.3.1.3.2), müssen wir aus gegebenem Anlaß noch einmal auf den Ist-Zustand eingehen.

5.3.1.3.1 Ist-Zustand

Im Berichtszeitraum erreichte uns eine Beschwerde, die die Schwächen des Kfz-Meldeverfahrens noch einmal deutlich macht.

Das jetzige Verfahren beruht auf folgendem Prinzip:

Jede Anfrage eines Versicherungsunternehmens beim HUK-Verband darüber, ob über eine bestimmte Person „Erkenntnisse" vorliegen, führt zwangsläufig dazu, daß diese Person in die Datei A oder B gemeldet wird, mit der Folge, daß bei allen späteren Anfragen die früheren Nachfragen als „Meldungen" übermittelt werden.

Auch über den Petenten, der eine Autovermietung betreibt, wurden auf diese Art und Weise diverse Eintragungen zur Datei „A" vorgenommen und an andere Versicherer übermittelt. So entstand sukzessive der Eindruck, man habe es mit einer Person mit einem langen „Sündenregister" zu tun. Dies führte nach Angaben des Beschwerdeführers dazu, daß nach einer Weile die Sachbearbeiter der Versicherungsunternehmen, bei denen er Schadensansprüche anmeldete, die Regulierungen mit dem Hinweis ablehnten, an ihn werde nicht mehr freiwillig, sondern nur noch aufgrund eines Gerichtsurteils gezahlt.

Der Petent wandte sich an uns und an den HUK-Verband mit der Bitte um Löschung. Der HUK-Verband war zunächst zur Löschung nur dann bereit, wenn von den einmeldenden Versicherungsunternehmen „Löschungsbewilligungen" erteilt würden. Einige der Unternehmen stimmten zu, weil seinerzeit offensichtlich nur eine Nachfrage, nicht aber eine Einspeicherung der Daten bezweckt worden war. Als wir uns später über die zur Person gespeicherten Daten informierten, stellten wir jedoch fest, daß auch die „bewilligten" Löschungen nicht durchgeführt waren. Hierzu erklärte man uns: Aus DV-technischen Gründen könne eine Löschung nur im Rahmen eines Reorganisationslaufes des gesamten Datenbestandes durchgeführt werden. Dieser Lauf finde nur zweimal monatlich statt. Das gleiche gelte für Berichtigungen. In besonderen Fällen sei man aber bereit, die sofortige Löschung im Rahmen einer Daten-Reorganisation vorzunehmen.

Der Petent beharrte darauf, daß sämtliche Eintragungen unverzüglich gelöscht werden sollen. Er behauptete, sein Verhalten habe nie Anhalt für den Verdacht betrügerischer Manipulationen gegeben. Bei den Meldungen handele es sich vielmehr um Racheakte einzelner Sachbearbeiter. Der HUK-Verband war zur Aufklärung des Sachverhaltes

nicht in der Lage und mußte die einmeldenden Versicherungsunternehmen um Darlegung der Hintergründe bitten. Dies beanspruchte naturgemäß Zeit und wäre auch nicht zu beanstanden, wenn in der Zwischenzeit eine Sperrung der Daten erfolgt wäre. Es stellte sich bei unserer Prüfung jedoch heraus: Eine Sperrung ist technisch überhaupt nicht realisierbar. Bestrittene Angaben müssen entweder gelöscht werden oder sie bleiben unverändert im System; mit der Folge, daß sie bei einer Anfrage automatisch wieder herausgegeben werden.

Unter diesen Umständen haben wir eine sofortige Löschung aller Daten gefordert, die der HUK-Verband dann auch durchführte.

Nachzutragen ist noch, daß ein Hamburger Versicherungsunternehmen darlegte, es sei Usus, eine Abrechnung auf fiktiver Grundlage dem HUK-Verband zur Warndatei zu melden.

Dazu ist zu bemerken, daß die Abrechnung laut Gutachten oder Kostenvoranschlag nach unseren Informationen, die ausführlich im 7. TB dargestellt und vom HUK-Verband als sachlich richtig befunden wurden, keineswegs für eine Meldung ausreichen soll. Auch nach der Neukonzeption ist dieser Umstand für sich allein grundsätzlich nicht ausreichend, um den Verdacht betrügerischer Manipulationen zu rechtfertigen.

Wir haben mit Rücksicht auf die beabsichtigte Neukonzeption darauf verzichtet, eine Liste der Datenschutzverstöße anzufertigen und sie dem Verband als unsere Stellungnahme zu überreichen. Insbesondere vertieften wir nicht das Problem, welche Konsequenzen aus einem Verstoß gegen die Benachrichtigungspflicht nach § 34 Absatz 1 BDSG zu ziehen wären. Wir haben allerdings darum gebeten, das neue Konzept zügig zu realisieren. Inzwischen wurde uns signalisiert, daß das jetzige Verfahren noch im Jahre 1991 durch ein neues abgelöst werden soll.

5.3.1.3.2 Neukonzeption

Im Februar dieses Jahres stellte uns der HUK-Verband seine neue Konzeption für seine zentrale Registrierstelle Kfz-Versicherungen vor. Danach soll nur noch eine statt der bisherigen fünf Dateien aufgebaut und gepflegt werden. Der Verband wird nicht mehr wie bisher Auskünfte auf Einzelnachfrage erteilen, sondern die von den Versicherungsunternehmen gemeldeten Daten verdächtiger Personen sammeln, codieren und an alle angeschlossenen Versicherungsunternehmen regelmäßig verschicken.

Im übrigen wurden Kriterien entwickelt, anhand derer (unter weitestgehender Einschränkung subjektiver Bewertungsspielräume) entschieden werden soll, ob eine Meldung erfolgen darf und muß. Grundidee ist, daß bei einem Schadensfall für das Vorliegen bestimmter Verdachtsmomente Punktzahlen vergeben werden. Summieren sich bei einem Schadensfall die Verdachtsmomente und demzufolge die Punktzahlen bis zu einer Obergrenze, dann soll dieser Schadensfall gemeldet werden.

Wir sind zwar der Meinung, daß eine Einzelauskunft aufgrund einer konkreten Nachfrage gegenüber dem neuen Verfahren, allen Versicherungsunternehmen alle Datensätze — sei es in codierter oder in nicht codierter Form — zur Verfügung zu stellen, vorzuziehen wäre. Insofern hat das jetzige System auch eine gute Seite. Wir meinen jedoch, daß das neue Konzept einen Fortschritt darstellt, weil es einen datenschutzrechtlich unvertretbaren Zustand beendet und plausibel und kalkulierbar die Voraussetzungen der Speicherung in der Warndatei beschreibt. Wir sind allerdings der Ansicht, daß noch nicht alle Probleme gelöst sind. So ist noch zu klären, welche Personen bei einem meldepflichtigen Schaden in die Datei aufgenommen werden sollen. Wir sind mit dem Gesamtverband der Ansicht, daß es wenig überzeugend wäre, wenn beispielsweise jeder Zeuge eines meldepflichtigen Schadensfalles — unabhängig davon, wie stark die Verdachtsmomente in Hinblick auf seine Person sind — erfaßt werden würde. Darüber hinaus ist offen, ob und gegebenenfalls wie der von den Übermittlungen betroffene Personenkreis, der nicht als Versicherungsnehmer oder auf andere Art und Weise von der Aufnahme der Daten in das Warnsystem hat Kenntnis nehmen können, unterrichtet wird.

Es besteht Einigkeit darüber, daß noch weitere Gespräche erforderlich sind. Wir gehen davon aus, daß das Meldeverfahren für die Kfz-Versicherer auch für die Zukunft einen Aufgabenschwerpunkt der Aufsichtsbehörde darstellen wird.

5.3.1.4 Transfer der Datensammlungen aus den Warn- und Hinweissystemen in Mitgliedsländer der EG

Der Europäische Binnenmarkt wird sicherlich zu verstärkten Aktivitäten ausländischer Versicherer auf dem deutschen Markt führen. War bislang erforderlich, daß ein ausländisches Versicherungsunternehmen eine deutsche Niederlassung gründete, um sich deutsche Marktanteile zu erschließen, so dürfte diese Voraussetzung demnächst entfallen und zwar nicht nur bei den Großrisiken, sondern auch im sogenannten Massengeschäft. Dem hiesigen Verbraucher stünde dann verstärkt die Möglichkeit offen, seine Versicherungsverträge bei in Deutschland nicht niedergelassenen Versicherern abzuschließen.

Damit dürften auch diese Versicherer ein erhebliches Interesse daran entwickeln, mit Hilfe der hiesigen zentralen Warn- und Hinweissysteme „ungünstige Risiken" auszusortieren. Dies aber bedeutete, daß ausländischen Versicherungsunternehmen riesige Datenbestände zur Verfügung gestellt werden müßten und zwar auch dann, wenn sie ihren Geschäftsbetrieb in Ländern unterhalten, die kein Datenschutzgesetz kennen. Dies ist — innerhalb der EG — etwa in Spanien und Belgien der Fall.

Datenschutzrechtlich stellt sich unter anderem (vgl. ansonsten 8. TB, 4.5.5, S. 130 f) die Frage, ob die Übermittlung der Datensammlungen aus den zentralen Warn- und Hinweissystemen an Versicherungsunternehmen im EG-Ausland nach § 24 Absatz 1 Satz 1 3. Alt. BDSG a.F. zulässig wäre. Nach unserer Auffassung beeinträchtigt eine Übermittlung in ein datenschutzfreies Ausland, also z.B. nach Spanien oder Belgien, die schutzwürdigen Belange der Betroffenen so gravierend, daß sie in der Regel unzulässig ist. Dies gilt zwar nicht für eine Übermittlung, für die eine rechtswirksame Einwilligung des Betroffenen vorliegt. Jedoch willigen bei weitem nicht alle Personen, deren Daten in Warnsysteme der Versicherungswirtschaft aufgenommen werden, darin ein. Etliche sind darüber nicht einmal informiert (siehe oben 5.3.1.2).

Eine andere Beurteilung käme nur dann in Betracht, wenn die Beeinträchtigung der schutzwürdigen Belange der Betroffenen anderweitig verhindert werden könnte. Eine denkbare Kompensationsmöglichkeit besteht darin, nach dem Vorbild der SCHUFA-Auslandskonzeption dem Betroffenen vertragliche Datenschutzrechte einzuräumen. Möglichkeiten und Grenzen einer solchen Vertragslösung unter Berücksichtigung der besonderen Verhältnisse in der Versicherungswirtschaft werden die Aufsichtsbehörden für den Datenschutz in Zukunft ausloten müssen. Dem wollen wir hier nicht vorgreifen. An dieser Stelle ist lediglich anzumerken, daß im Gegensatz zum Auskunftssystem der SCHUFA die Verfahren in der Versicherungswirtschaft — zumindest für einige der von einer Speicherung betroffenen Personen — nicht transparent sind (vgl. oben 5.3.1.2). Ist aber den Betroffenen schon die Aufnahme ihrer Daten in ein Warnsystem nicht bewußt, so können sie (erst recht) nicht von Berichtigungs-, Sperrungs- oder Löschungsansprüchen profitieren, die ihnen ohne ihr Wissen möglicherweise vertraglich eingeräumt wurden.

5.3.2 Fakultative Gruppenversicherungsverträge

Bereits mehrfach haben wir über fakultative Gruppenversicherungsverträge (vgl. zuletzt 5. TB 6.5.5, S. 125 f) berichtet. Dies sind Rahmenverträge zwischen Vereinen und Versicherungsunternehmen, die es Vereinsmitgliedern ermöglichen, Einzelversicherungsverträge zu günstigeren als den üblichen Konditionen abzuschließen. Zu diesem Zweck übermittelt der Verein die Daten seiner Mitglieder an das Versicherungsunternehmen, mit dem er die vertragliche Rahmenbeziehung unterhält. Im Jahre 1986 konnte nach langen Verhandlungen erreicht werden, daß die Übermittlungen grundsätzlich nur aufgrund einer Einwilligung des betroffenen Vereinsmitgliedes erfolgen. Den Personen, die einem Verein beitreten (Neumitglieder), wird mit der Beitrittserklä-

rung zugleich eine Einwilligungserklärung zur Datenübermittlung vorgelegt, die sie unterschreiben können, aber nicht müssen. Die Erklärung lautet z.B.:

„. . . Der Verein hat für seine Mitglieder einen günstigen Gruppenversicherungsvertrag abgeschlossen. Um die Vergünstigungen des Gruppenversicherungsvertrages zu erhalten, bin ich damit einverstanden, daß hierfür mein Name und meine Anschrift an den Versicherer weitergegeben werden."

Die Personen, die zum Zeitpunkt des Abschlusses eines Rahmenvertrages bereits Vereinsmitglieder waren (Altmitglieder), erhalten ein sogenanntes Avisschreiben, mit dem der Besuch eines Versicherungsvertreters angekündigt wird. Sind sie mit dem Besuch nicht einverstanden, können sie dem widersprechen. Dann werden auch keine Daten an die Versicherungsgesellschaft übermittelt. Bei fehlendem Widerspruch sind die Übermittlungen gemäß § 24 Absatz 1 Satz 1 3. Alt. BDSG a.F. zulässig, da keine schutzwürdigen Belange des Betroffenen entgegenstehen.

Im Jahre 1989 erhielten wir verschiedene Eingaben, aus denen hervorging, daß diese Vereinbarungen nicht in jedem Fall eingehalten werden. So rügte etwa ein Beschwerdeführer, kein Avisschreiben bekommen zu haben, sondern unvorbereitet von Versicherungsvertretern aufgesucht worden zu sein. Diese sollen sich darüber hinaus nicht als Versicherungs- sondern als Vereinsvertreter ausgegeben haben.

Wir haben daraufhin das betroffene Hamburger Versicherungsunternehmen gebeten, seinen Versicherungsaußendienst noch einmal über die Absprachen mit den Aufsichtsbehörden zu instruieren, um solche „Pannen" in Zukunft zu vermeiden. Die Gesellschaft versicherte, die Absprachen würden genau eingehalten. Im konkreten Einzelfall müßte es sich um ein Mißverständnis handeln. Dieser Vorgang hat seine Erledigung dadurch gefunden, daß der beteiligte Verein keine Gruppenversicherungsverträge mehr offeriert.

Datenschutzrechtlich bedeutsamer war ein für die Aufsichtsbehörde bislang unbekannter Sachverhalt, den uns ein anwaltlich vertretener Petent mitteilte. Danach wird denjenigen Vereinsmitgliedern, die einen Versicherungsvertrag abgeschlossen haben, bei dieser Gelegenheit noch eine weitere Erklärung vorgelegt. Sie lautet:

„. . . Bis auf meinen jederzeit möglichen Widerruf spende ich dem Verein laufend Beträge in Höhe der jeweils anfallenden Risikoanteile aus der Überschußbeteiligung. . ."

Durch Unterschrift unter diese Erklärung tritt das Vereinsmitglied seinen Anspruch auf Rückerstattung von Prämienanteilen (den Risikoanteilen aus der Überschußbeteiligung) schenkungsweise an den Verein ab. Solche Rückerstattungen gibt es beispielsweise in der Sterbegeldversicherung. Die Gesamtsumme der so gespendeten Beträge variiert je nach Höhe der Versicherungssumme, dem Alter des Versicherungsnehmers bei Vertragsabschluß und dem Zeitpunkt des Versicherungsfalles und steht in ihrer endgültigen Größenordnung zum Zeitpunkt der Abtretung naturgemäß noch nicht fest. Sie kann aber bei einer langen Laufzeit und einer Versicherungssumme von etwa 10 000,— DM auch nach Angaben des Versicherungsunternehmens durchaus mehr als 1000,— DM betragen. Bei einer so großzügigen Schenkung muß die Frage gestellt werden, ob der Schenker sich über die Tragweite seiner Erklärung bewußt ist. Da die meisten Vereine von den gespendeten Überschußanteilen wirtschaftlich im starken Maße abhängig sind (so die Aussage des Schatzmeisters eines namhaften Verbandes), ist das Interesse an der Aufrechterhaltung dieser Praxis sehr groß.

Wir haben mit den übrigen obersten Aufsichtsbehörden für den Datenschutz die Frage diskutiert, ob die Tatsache, daß die Vereine die Daten ihrer Mitglieder nicht nur zu dem Zweck des Abschlusses von Versicherungsverträgen, sondern offensichtlich auch mit dem Ziel übermitteln, die Zuwendung von Forderungen zu erreichen, eine datenschutzrechtliche Neubewertung der Datenübermittlungen erfordert. Wir sind übereinstimmend zur folgenden Ansicht gelangt: Eine Einwilligung ist nur dann rechtsgültig, wenn der Einwilligende sie in Kenntnis aller mit der Übermittlung verfolgten Zwecke

abgegeben hat. Eine Einwilligung kann die Datenübermittlung deshalb nur dann abdecken, wenn der Verein seine Mitglieder auch über den zusätzlichen Zweck aufklärt, damit eine Zuwendung zu seinen Gunsten erreichen zu wollen.

Ohne Einwilligung wäre die Übermittlung nach § 24 Absatz 1 Satz 1 3. Alt. BDSG a. F. nur zulässig, wenn eine Interessenabwägung im Einzelfall ergäbe, daß schutzwürdige Belange des Betroffenen nicht überwiegen. Es ist naheliegend, daß vor allem ältere Menschen die überraschende Konfrontation mit einer Abtretungserklärung als verwirrend und darüber hinaus auch als zudringlich empfinden können. Sofern sie den Inhalt der Erklärung während des Vertreterbesuches überhaupt erfassen, sehen sie sich möglicherweise auch einem „sozialen Druck" ausgesetzt und wollen gegenüber „ihrem" Verein/Verband nicht kleinlich sein. Wir meinen daher, daß die Datenübermittlung, wenn und soweit damit die Vorlage einer Abtretungserklärung als Nebenzweck verbunden ist, geeignet ist, schutzwürdige Belange zu beeinträchtigen.

Eine umfassende Erklärung halten wir auch bei den Altmitgliedern für erforderlich. Ihnen müßte das Avisschreiben darüber Auskunft geben, daß nicht nur ein Versicherungsvertrag abgeschlossen werden soll, sondern zugleich eine Zuwendungserklärung erstrebt wird. Andernfalls kann nicht davon ausgegangen werden, daß bei fehlendem Widerspruch des Betroffenen keine seiner schutzwürdigen Belange beeinträchtigt sind.

Da die Zuwendungserklärungen im Rahmen fakultativer Gruppenversicherungsverträge nicht nur datenschutz- sondern auch verbraucherschutz- und versicherungsaufsichtsrechtliche Fragen aufwerfen, haben wir uns sowohl mit dem Verbraucherschutzverein in Berlin als auch mit dem Bundesaufsichtsamt für das Versicherungswesen in Verbindung gesetzt, unseren Standpunkt erläutert und um Stellungnahmen gebeten. Nach Meinung des Verbraucherschutzvereines ist zwar eine größere Transparenz in den verschiedenen Erklärungen zu begrüßen, noch besser wäre es jedoch, diese Art der Spendenerhebung würde gänzlich unterbleiben. Das Bundesaufsichtsamt teilt ebenfalls unsere datenschutzrechtlichen Bedenken, zumal früher der Beitritt zum Gruppenversicherungsvertrag und die Abtretung der Überschußanteile an den Verein in einer Urkunde, also mit einer Unterschrift, erklärt worden seien. Es sieht sich jedoch nicht in der Lage, aufsichtsrechtliche Maßnahmen zu ergreifen, da die Zuwendungserklärung dem Rechtsverhältnis zwischen dem Verein und seinem Mitglied zuzuordnen sei.

Die Vertreter eines Hamburger Versicherungsunternehmens, das einen großen Anteil am Markt der Gruppenversicherungsverträge hat, sind dagegen der Auffassung, daß datenschutzrechtliche Belange gar nicht betroffen seien. Die Datenübermittlungen hätten lediglich den Zweck, den Abschluß von Versicherungsverträgen zu ermöglichen. Die Abtretung der Risikoanteile sei ein weiteres Rechtsgeschäft, das damit nicht gekoppelt sei. Der Betroffene werde darüber beim Besuch des Vertreters aufgeklärt. Schließlich sei die Abtretung auch frei widerruflich.

Trotz der unterschiedlichen Auffassungen konnte ein Kompromiß erzielt werden. In die Avisschreiben der Verbände wird ein zusätzlicher Passus aufgenommen, mit dem auf die Möglichkeit der Zuwendung von Prämienrückerstattungsansprüchen an den Verband hingewiesen und zugleich dargelegt wird, daß der Abschluß einer Sterbegeldversicherung von der Abgabe einer solchen Zuwendungserklärung nicht abhängig ist. Es wird allerdings ein gutes Jahr in Anspruch nehmen, bis alle Vereine — es sind ca. dreihundert — die geänderten Avisschreiben verwenden werden.

Das Unternehmen sah sich jedoch außerstande, auf die Vereine hinsichtlich einer Ergänzung der Einwilligungserklärungen für Neumitglieder einzuwirken. Insoweit bleibt es bei den Einwilligungstexten, die keine Information auch über das Abtretungsgeschäft enthalten. Dieser Mangel kann jedoch dadurch behoben werden, daß auch die Neumitglieder die Avisschreiben erhalten. Wenn und soweit dadurch eine vollständige Information sichergestellt ist, kann eine rechtswirksame Einwilligung angenommen werden. Andernfalls müssen die Aufsichtsbehörden die Zulässigkeit der Daten-

übermittlung am Maßstab des § 24 Absatz 1 Satz 1 3. Alt. BDSG a. F. prüfen, der — wie oben ausgeführt — den Vereinen keine sichere Rechtsgrundlage bietet.

5.3.3 Schweigepflichtentbindungsklauseln im Schadensfall

In der Vergangenheit haben die Erklärungen zur Entbindung von der ärztlichen Schweigepflicht, die ein Versicherungsnehmer bei Abschluß eines Versicherungsvertrages abgeben soll, eine wichtige Rolle in der Arbeit der Aufsichtsbehörde gespielt (vgl. 7. TB, 5.4.3 S. 151 f, 6. TB, 5.4.3 S. 140 ff.). Sie konnte mit der bundesaufsichtsamtlichen Veröffentlichung zu einem Abschluß gebracht werden (siehe VerBAV Nov. 1989). Da damit aber nicht alle Sparten abgedeckt sind, in denen Schweigepflichtentbindungserklärungen eine Rolle spielen, und da die veröffentlichten Texte zum Teil nur die Erklärungen betreffen, die bei einem Antrag auf Abschluß eines Versicherungsvertrages verlangt werden, nicht aber jene, die bei Eintritt des Schadensfalles zu unterzeichnen sind, sind die Probleme um die Schweigepflichtentbindung noch nicht restlos beseitigt.

Im Berichtszeitraum haben sich die Datenschutzaufsichtsbehörden und das Bundesaufsichtsamt für das Versicherungswesen auf Formulierungen für Schweigepflichtentbindungserklärungen bei einem Antrag zu einer Berufsunfähigkeits-, Pflegerenten- und Reisekostenrücktrittsversicherung geeinigt. Auch die Versicherungswirtschaft hat Zustimmung signalisiert, so daß wir mit einem baldigem erfolgreichen Abschluß rechnen.

Eine Reihe von Eingaben zeigte uns, daß — vor allem in Haftpflichtfällen — die Versicherungsunternehmen dem Geschädigten Erklärungen vorlegen, die weit über das Erforderliche hinausgehen.

Um hier Verbesserungen zu erreichen, haben wir einen Textvorschlag zur Schweigepflichtentbindungserklärung für die

— Haftpflichtversicherung und die

— allgemeine Unfallversicherung

mit dem BAV und den Verbänden der Versicherungswirtschaft erörtert.

Ein Ergebnis konnte bislang nur in der allgemeinen Unfallversicherung erzielt werden. Der Text, der hier einem Versicherungsnehmer im Schadenfall unterbreitet werden soll, lautet:

> „Mir ist bekannt, daß der Versicherer zur Beurteilung seiner Leistungspflicht die Angaben überprüft, die ich hier zur Begründung der Ansprüche mache oder die sich aus den von mir eingereichten Unterlagen (z. B. Bescheinigungen, Atteste) oder von mir veranlaßten Mitteilungen eines Krankenhauses oder von Angehörigen eines Heilberufes ergeben. Zu diesem Zweck befreie ich hiermit die Angehörigen von Heilberufen oder Krankenanstalten, die in den vorgelegten Unterlagen genannt sind oder die an der Heilbehandlung beteiligt waren, von ihrer Schweigepflicht. Ebenso entbinde ich von der Schweigepflicht zur Prüfung von Leistungsansprüchen im Falle meines Todes.
>
> Diese Schweigepflicht-Entbindung gilt auch für Behörden — mit Ausnahme von Sozialversicherungsträgern —; ferner für die Angehörigen von anderen Unfall- sowie von Kranken- oder Lebensversicherern, die nach dort bestehenden Versicherungen befragt werden dürfen.
>
> Diese Erklärung gebe ich für die/den von mir gesetzlich vertretene(n) ... ab, die/der die Bedeutung dieser Erklärung nicht selbst beurteilen kann."

Das BAV teilte mit, daß Unfall-Schadenanzeigen mit einer anderslautenden Schweigepflichtentbindungserklärung nur noch für eine Übergangszeit bis zum Ende des Jahres 1990 Verwendung finden dürfen.

5.3.4 Auskunftsstelle über den Versicherungsaußendienst e.V. (AVAD)/Auskünfte über Ehegatten

Aufgrund einer Eingabe erhielten wir davon Kenntnis, daß die AVAD bei einer Anfrage über eine weibliche Person unverlangt die — recht negative — Auskunft über eine männliche Person gleichen Nachnamens und gleicher Anschrift herausgegeben hatte. Sie vermutete — zu recht — daß es sich um den Ehemann handeln müsse. Dieser beschwerte sich bei uns.

Wir hielten dieses Verfahren für unvereinbar mit § 32 Absatz 2 Satz 1 BDSG. Denn das anfragende Versicherungsunternehmen hatte zu dem Ehemann kein berechtigtes Informationsinteresse glaubhaft gemacht. Gleichwohl ist einzusehen, daß es Fälle geben kann, in denen erst die Auskunft über den Ehegatten ein zutreffendes Bild vermittelt. Gelegentlich kommt es nämlich vor, daß einschlägig vorbelastete ehemalige Versicherungsaußendienstler ihre Ehegatten vorschieben, um weiterhin zweifelhafte Geschäfte betreiben zu können. In einem solchen Fall wäre der Zweck der AVAD-Auskunft, nämlich Verbraucher vor unseriösen Versicherungsaußendienstmitarbeitern oder -maklern zu schützen, nicht erreichbar, würde man sich auf die Auskunft beschränken, daß keine Eintragung vorhanden ist.

Inzwischen konnte mit der AVAD ein Verfahren verabredet werden, das die unterschiedlichen Interessen zu einem angemessenen Ausgleich bringt: Bei Nachnamens- und Adressenübereinstimmung zu einer Person, über die eine Auskunft vorhanden ist, weist die AVAD das anfragende Versicherungsunternehmen auf die Existenz einer solchen Information hin. Es liegt dann beim Anfragenden aufzuklären, wer von den beiden Personen tatsächlich das Vermittlungsgeschäft betreibt. Stellt sich heraus, daß eine Person die andere als Strohmann/Strohfrau benutzt, so kann das anfragende Unternehmen das ursprüngliche Ersuchen auf Auskunft über den Ehegatten erweitern. Erst dann übermittelt die AVAD die Daten auch über den Ehegatten.

5.4 Handels- und Wirtschaftsauskunfteien

5.4.1 Probleme bei der Kontrolle der Zulässigkeit und Ordnungsmäßigkeit der Datenverarbeitung

Eine Petentin beschwerte sich darüber, daß bei einer namhaften Handels- und Wirtschaftsauskunftei über ihre Person unrichtige Daten gespeichert seien. Im Zuge der Sachaufklärung stellte sich heraus, daß eine große in Hamburg ansässige Versicherungsgesellschaft bei der Auskunftei zu einer GmbH angefragt hatte, die den Namen der Petentin trug und unter ihrer Adresse den Geschäftsbetrieb unterhalten sollte.

Da eine solche Gesellschaft zu keiner Zeit bestanden hatte und auch eine Gründung von der Petentin nicht beabsichtigt war, versuchten wir aufzuklären, worin das berechtigte Interesse des Empfängers an der Auskunft bestanden haben könnte. Damit aber hatten wir keinen Erfolg. Nach intensiven Recherchen ließ sich lediglich rekonstruieren, daß die Auskunft zur Prüfung einer angeblichen Kreditanfrage in Höhe von 30 000 DM angefordert worden war. Ein Sachbearbeiter oder zumindest die Abteilung, die die Auskunft angefordert hatte, ließen sich nicht ermitteln. Die Versicherungsgesellschaft war anhand der von ihr bei der Online-Anfrage eingegebenen Merkmale, die die Auskunftei gespeichert hatte, nicht in der Lage nachzuvollziehen, warum und von welchem Mitarbeiter die Auskunft eingeholt worden war. Dies ist aber kein Einzelfall, sondern ist als generelle Schwäche des Verfahrens anzusehen. Deshalb muß geprüft werden, ob es seinen Zweck — den Anforderungen des § 32 Absatz 2 BDSG in der Praxis zu genügen — noch erfüllt.

Gemäß § 32 Absatz 2 BDSG ist die Übermittlung von personenbezogenen Daten nur zulässig, wenn der Empfänger ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat. Die Gründe für das Vorliegen eines berechtigten Interesses und die Mittel für ihre glaubhafte Darlegung sind aufzuzeichnen. Sinn und Zweck der Aufzeichnungspflicht ist, die nachträgliche Kontrolle zu ermöglichen.

In der Praxis soll dem § 32 Absatz 2 BDSG dadurch Rechnung getragen werden, daß der Datenempfänger auf einem vorgedruckten Formular allgemeine Kriterien wie Bonitätsprüfung, Geschäftsanbahnung, Forderung, u.ä. angibt und gegebenenfalls bei Online-Verfahren der Auskunftei übermittelt. Möglich ist auch, die Rubrik „Sonstiges" anzukreuzen. Die Auskunftei zeichnet diese vorformulierten Angaben auf und notiert das Datum und den Empfänger der Auskunft. Mehr als die Firmenangabe wird aber häufig nicht vermerkt und zwar auch dann nicht, wenn der Empfänger ein Großunternehmen mit vielen tausend Mitarbeitern ist. Nur eine einzige Auskunftei verlangt in ihrem Vordruck die Angabe eines Aktenzeichens. Eine andere Auskunftei sieht weder Aktenzeichen noch Unterschrift vor. Auf Initiative der Aufsichtsbehörden wurde vor einigen Jahren dieses — nach unserer Ansicht nicht ausreichende — Vorgehen durch ein Stichprobenverfahren ergänzt. Damit soll nachträglich bei 1 ‰ der Anfragen von den Auskunfteien geprüft werden, ob der Empfänger ein berechtigtes Interesse an der Auskunft gehabt hat. Dies geschieht zumeist dadurch, daß der betriebliche Datenschutzbeauftragte der Auskunftei beim Empfänger der Auskunft formularmäßig anfragt, aus welchen Gründen die Auskunft angefordert worden war.

Es bestehen erhebliche Zweifel, ob dieses Verfahren noch mit § 32 Absatz 2 BDSG zu vereinbaren ist. Zwar verlangt das Gesetz nicht, daß die Auskunftei sich vor der Übermittlung positiv von einem berechtigten Interesse des Übermittlungsempfängers überzeugen muß. Es genügt vielmehr eine glaubhafte Darlegung. Eine Darlegung ist unseres Erachtens aber nur dann glaubhaft, wenn sie so detailliert erfolgt, daß eine nachträgliche Überprüfung zumindest möglich ist. Dazu gehören Angaben, die eine Individualisierung der Person ermöglichen, die die Anfrage initiiert hat und dafür die Verantwortung trägt. Andernfalls ist die Mißbrauchsgefahr unübersehbar. Auch die nachträglichen Stichprobenkontrollen können dem nicht wirksam entgegenwirken, zumal berücksichtigt werden muß, daß die „Kontrolleure" bei fehlerhaften Anfragen in Interessenkonflikte geraten können. Schließlich sind die zu Kontrollierenden in erster Linie Geschäftspartner.

Wir beabsichtigen, diesen Problemkreis nochmals im Kreise der obersten Aufsichtsbehörden mit dem Ziel zu erörtern, eine Verbesserung des Verfahrens zu erreichen.

5.4.2 Grenzüberschreitender Datenverkehr

Auch im Geschäftsbereich der Handels- und Wirtschaftsauskunfteien ist zu konstatieren, daß der Datentransfer ins Ausland in dem Maße zunimmt, in dem sich der Europäische Binnenmarkt seiner Vollendung nähert. Schon jetzt gibt es mit INTERNET einen Zusammenschluß europäischer Handelsauskunfteien, der eine Standardisierung von Auskunftsinhalten vorbereitet, was den grenzüberschreitenden Datenverkehr ohne Zweifel erleichtern wird. Ebenfalls schon heute werden ausländischen Partnerorganisationen Daten aus dem Bestand inländischer Auskunfteien zur Verfügung gestellt.

Aus diesem Grund haben die obersten Aufsichtsbehörden für den Datenschutz einen Vorstoß unternommen, um mit den Handels- und Wirtschaftsauskunfteien Lösungsmöglichkeiten für das Problem zu erörtern, das aus dem unterschiedlichen Datenschutzniveau innerhalb der Europäischen Gemeinschaft resultiert. Nach dem Vorbild des SCHUFA-Auslandskonzeptes (vgl. oben 5.2.1) wären auch hier Vertragsmodelle zumindest in Betracht gekommen.

Eine Diskussion über Risiken und Lösungskonzepte ist allerdings bislang nicht in Gang gekommen, weil die Handels- und Wirtschaftsauskunfteien über ihren Verband Rechtsansichten vortragen lassen, die dies bereits im Vorfeld blockieren.

— So wird vorgetragen, daß nach § 32 Absatz 2 BDSG eine Übermittlung schon dann zulässig sei, wenn der Empfänger ein Informationsinteresse darlege. Auf eventuell entgegenstehende schutzwürdige Belange des Betroffenen käme es nicht an. Seine Belange seien unerheblich. Deswegen sei auch unbeachtlich, ob sie durch das Fehlen eines Datenschutzgesetzes im Empfängerland beeinträchtigt sein könnten.

Diese Interpretation des § 32 Absatz 2 Satz BDSG steht im Widerspruch zur einhellig vertretenen Meinung, daß ein Informationsinteresse des Übermittlungsempfängers nur dann ein „berechtigtes" im Sinne der Vorschrift ist, wenn keine überwiegenden schutzwürdigen Belange des Betroffenen entgegenstehen.

— Weiter wird die Auffassung vertreten, daß eine Datenexportrestriktion in bestimmte EG-Länder eine versteckte Ausländerdiskriminierung und damit ein Verstoß gegen Artikel 7 EWG-Vertrag sei.

Daran ist richtig, daß nach Artikel 7 Absatz 1 EWG-Vertrag jede Diskriminierung aus Gründen der Staatsangehörigkeit verboten ist. Die Vorschrift untersagt sowohl die offene als auch die versteckte Diskriminierung von Ausländern. Bei einer offenen Diskriminierung wird direkt an die Ausländereigenschaft angeknüpft. Da die §§ 24 Absatz 1 und 32 Absatz 2 BDSG die Übermittlungsvoraussetzungen für Inländer wie für Ausländer gleichermaßen festlegen, ist eine offene Diskriminierung ausgeschlossen. Eine versteckte Diskriminierung liegt vor, wenn eine Vorschrift zwar nicht ausdrücklich auf die Ausländer- oder Inländereigenschaft abstellt, ihre Voraussetzungen aber typischerweise nur Ausländer oder nur Inländer treffen. Artikel 7 EWG-Vertrag gebietet hingegen nicht, Marktbürger eines anderen Mitgliedstaates von allen rechtlichen Restriktionen zu befreien, die in ihrem Heimatstaat nicht existieren. Eine Ungleichbehandlung, die sich ohne Rücksicht auf die Staatsangehörigkeit allein daraus ergibt, daß die verschiedenen nationalen Rechtsordnungen unterschiedlich streng sind, stellt keine Diskriminierung aus Gründen der Staatsangehörigkeit dar (ausführlich EuGH Rs 126/82 „Smit Transport" AS 1983, 72; Grabitz in: Grabitz, EWG-Vertrag, Art. 7 Rn. 7).

— Darüber hinaus wird die Meinung geäußert, jede Restriktion des freien Datenverkehrs innerhalb der EG würde gegen die Gewährleistung des freien Warenverkehrs nach Artikel 30, 34 EWG-Vertrag und/oder die des freien Dienstleistungsverkehrs nach Artikel 59 EWG-Vertrag verstoßen.

Der Geschäftsbetrieb von Handels- und Wirtschaftsauskunfteien ist gemäß Artikel 60 EWG-Vertrag dem Dienstleistungsverkehr zuzuordnen. Richtig ist, daß die Gewährleistung der Dienstleistungsfreiheit in Artikel 59 EWG-Vertrag unmittelbare Wirkung für den Marktbürger entfaltet. Sowohl Privatunternehmen als auch Privatpersonen können aus dieser Norm ein subjektives öffentliches Recht ableiten. Daraus folgt jedoch keineswegs, daß unter Mißachtung nationaler Rechtsvorschriften ein Recht auf ungehinderten Datenexport bestünde. Nationale Rechtsvorschriften sind vielmehr zu beachten, solange ihnen keine diskriminierende Wirkung zukommt (Randelzhofer in: Grabitz, EWG-Vertrag, Artikel 59 Rn. 11). Dies aber ist — wie oben festgestellt — nicht der Fall.

— Dann wird das Argument vertreten, soweit ein Datenexport in ein Land in Rede stehe, das die Datenschutzkonvention des Europarates ratifiziert habe, sei ein Verbot oder eine Restriktion ein Verstoß gegen Artikel 12 Absatz 2 der Konvention, wonach die Aufsichtsbehörden gehindert seien, den grenzüberschreitenden Verkehr personenbezogener Daten in das Hoheitsgebiet einer anderen Vertragspartei zu verbieten oder von besonderen Voraussetzungen abhängig zu machen.

Zutreffend ist, daß Artikel 12 der Datenschutzkonvention des Europarates als eine „self-executing-Norm" mit der Ratifikation der Konvention durch die Bundesrepublik Bestandteil unserer innerstaatlichen Rechtsordnung geworden ist, ohne daß es eines weiteren Rechtsetzungsaktes bedarf. Dementsprechend bindet Artikel 12 Absatz 2 der Datenschutzkonvention die Gerichte und die Verwaltung und somit auch die Aufsichtsbehörden als Verwaltungsbestandteil, für die demgemäß ein Verbot besteht, den grenzüberschreitenden Datenverkehr in das Hoheitsgebiet eines anderen Vertragsstaates zu verhindern oder von besonderen Voraussetzungen abhängig zu machen.

Für den Datenverkehr der Handels- und Wirtschaftsauskunfteien ist jedoch nicht Absatz 2 sondern Absatz 3 der Konvention maßgeblich. Danach kann jeder Ver-

tragsstaat von Absatz 2 abweichen, wenn das innerstaatliche Recht für bestimmte Arten von personenbezogenen Daten oder automatisierten Dateien besondere Vorschriften enthält, es sei denn, die Vorschriften des anderen Vertragsstaates sehen einen gleichwertigen Schutz vor. Die §§ 32 bis 35 BDSG enthalten für Auskunfteien derartige besondere Bestimmungen. Zu nennen sind die Aufzeichnungspflicht, die Sperrfrist und die besonderen Löschungspflichten für sensitive Daten. Somit sind die Aufsichtsbehörden schon aus diesem Grund befugt, den Datenexport in solche Empfängerländer besonderen Voraussetzungen zu unterwerfen, die keine gleichwertigen Schutzvorschriften vorhalten.

— Schließlich wird sogar vorgetragen, die Vertragslösung sei eine völkerrechtswidrige Einmischung in die inneren Angelegenheiten zumindest der Staaten, die eine Datenschutzregelung in ihrem innerstaatlichen Recht erlassen haben. Aber sie stieße auch bei Staaten ohne Datenschutzgesetz auf Bedenken, wenn und soweit das Fehlen von gesetzlichen Vorschriften auf ein bewußtes Unterlassen des nationalen Gesetzgebers zurückzuführen wäre.

Diese Auffassung entbehrt schon deshalb weitgehend einer Grundlage, weil mit der Entschließung des Europäischen Parlamentes zum Schutz der Rechte des einzelnen angesichts der fortschreitenden technischen Entwicklung auf dem Gebiet der Datenverarbeitung (Bundestags-Drucksache 8/2928) mindestens seit 1979 von einem übereinstimmenden Willen der Mitglieder der Europäischen Gemeinschaft auszugehen ist, innerhalb der Gemeinschaft Datenschutzgesetze zu schaffen, die dem Standard der Datenschutzkonvention des Europarates entsprechen. Damit läßt sich jedenfalls innerhalb der EG das Fehlen von Datenschutzgesetzen nicht mehr mit einem ausdrücklichen gesetzgeberischen Willen begründen. Darüber hinaus weisen die neuesten Bemühungen der EG-Kommission für eine Datenschutzrichtlinie ebenfalls in eine völlig andere Richtung. Auch außerhalb der EG bemühen sich nationale Gesetzgeber darum, Datenschutzoasen zu beseitigen, wie Initiativen in Ungarn und Polen zeigen.

5.5 Informations- und Kommunikationsdienstleistungen

5.5.1 Mailboxen

Bereits im letzten Tätigkeitsbericht (8. TB, 4.4, S. 123 ff) hatten wir eine datenschutzrechtliche Einordnung der Dienstleistungen eines Mailboxbetreibers vorgenommen. Wir erzielten das Ergebnis, daß die Dienstleistung „elektronische Kommunikation" als Auftragsdatenverarbeitung zu qualifizieren ist. Dem haben sich die obersten Datenschutzaufsichtsbehörden der übrigen Bundesländer (Düsseldorfer Kreis) angeschlossen. Im übrigen stand stets außer Zweifel, daß die Verarbeitung der Kundendaten zum Zwecke der Gebührenabrechnung Datenverarbeitung für eigene Zwecke des Mailboxbetreibers ist, mithin dem 3. Abschnitt des Bundesdatenschutzgesetzes unterfällt.

Im Berichtszeitraum haben wir uns abermals mit dem Mailboxbetreiber in Verbindung gesetzt. Ziel war es, in den Allgemeinen Geschäftsbedingungen des Unternehmens

— eine Klarstellung der datenschutzrechtlichen Einordnung,

— eine Einwilligung des Kunden für die Aufnahme in das Teilnehmerverzeichnis,

— eine Selbstbindung des Betreibers an die mit dem Teilnehmervertrag verbundenen Zwecke sowie

— die Einhaltung von Löschungsfristen

zu erreichen.

Dabei hatten wir nur teilweise Erfolg. So wurde vereinbart, daß das Unternehmen in seine Allgemeinen Geschäftsbedingungen sinngemäß folgende Klauseln aufnehmen wird:

1. Das Unternehmen verarbeitet die elektronischen Nachrichten im Auftrag der Teilnehmer. Zulässigkeit und Umfang der Datenverarbeitung richten sich gemäß §§ 31 Absatz 1 Nr. 3, 37 BDSG a. F. insoweit nach den Weisungen des Teilnehmers.
2. Der Mailbox-Betreiber steht dafür ein, daß alle Personen, die mit der Durchführung dieses Vertrages befaßt sind, das Bundesdatenschutzgesetz kennen und beachten, insbesondere vor Aufnahme ihrer Tätigkeit nach § 5 BDSG zur Wahrung des Datengeheimnisses verpflichtet werden.
3. Der Teilnehmer erhält die Möglichkeit, in das Teilnehmerverzeichnis des Unternehmens aufgenommen zu werden. Die Eintragung ist nur auf Grund einer schriftlichen, frei widerruflichen Einwilligungserklärung des Teilnehmers zulässig. Der Widerruf ist bei der nächstfolgenden, redaktionell noch nicht abgeschlossenen Ausgabe des Verzeichnisses zu berücksichtigen.

Nicht durchdringen konnten wir mit unserem Anliegen, das Unternehmen möge sich auf freiwilliger Basis (über das Bundesdatenschutzgesetz hinausgehend) einem strikten Zweckbindungsgrundsatz verpflichten. Wir hatten sinngemäß etwa die folgende Regelung zur Diskussion gestellt: „Das Unternehmen verwendet die Daten seiner Teilnehmer nur zur Durchführung dieses Vertrages, es sei denn, der Teilnehmer stimmt einer anderweitigen Verwendung, etwa einer Übermittlung an Dritte, ausdrücklich zu. Insbesondere speichert das Unternehmen außerhalb des Auftragsverhältnisses personenbezogene Daten der Teilnehmer nur zu dem Zweck, ordnungsgemäße Abrechnungen zu erstellen. Die Abrechnungsdaten werden nach Eingang der Zahlung gesperrt und mit Ablauf der Aufbewahrungsfristen nach dem Handelsgesetzbuch gelöscht."

Obwohl in der Sache grundsätzlich keine Einwände bestanden, wurde entgegengehalten, das Unternehmen könne sich eine datenschutzrechtliche „Vorreiterrolle" gegenüber der Konkurrenz nicht erlauben. Bleibt zu hoffen, daß sich langfristig die Erkenntnis durchsetzt, daß vorbildlicher Datenschutz (ebenso wie vorbildlicher Umweltschutz) ein attraktiver Werbeträger sein kann, der in Kreisen aufgeklärter Verbraucher Wettbewerbsvorteile verschafft.

5.5.2 Private Netzanbieter

Im Berichtszeitraum haben wir uns mit einer weiteren Form der privaten Kommunikationsdienstleistungen beschäftigt, die durch die Poststrukturreform möglich geworden ist. Dazu besuchten wir ein Hamburger Unternehmen, das in sein Dienstleistungsangebot einen sogenannten „Netzwerkservice" aufgenommen hat.

Der Netzwerkbetreiber offeriert den Datentransport für zumeist größere Unternehmen, die zu ihren Filialen Verbindung halten wollen. Zu diesem Zweck hat er von der Deutschen Bundespost-Telekom Standleitungen (Hauptanschlüsse für Direktleitungen, kurz: HfD) angemietet, die zur Zeit 13 auf das Bundesgebiet verteilte Netzknoten verbinden. Von den Netzknoten gehen wiederum fest angemietete Standleitungen zum Kunden. Es ist geplant, den Zugang zum Netz auch über Wählleitungen zuzulassen. Ferner soll über einen Knotenrechner in Frankfurt, den ein amerikanisches Unternehmen betreibt, eine weltweite Verbindung (zu 85 Ländern mit zum Teil mehreren Netzknoten) erreicht werden.

Der Kunde des Netzwerkbetreibers sendet seine Daten in Paketen zu 128 Bytes zuzüglich der Steuerdaten zum nächstgelegenen Netzknoten. In jedem Netzknoten werden die Pakete verschiedener Kunden miteinander vermischt. Der Netzknotenrechner ermittelt für jedes Paket den günstigsten Weg zum Empfänger, das dann auf diese Weise von Netzknoten zu Netzknoten transportiert wird. Um Übertragungsausfälle zu vermeiden, bleiben die Paket-gebündelten Daten in jedem Netzknoten solange gespeichert, bis der Empfängerknoten eine Empfangsbestätigung an den Absenderknoten übermittelt hat. Danach werden die Daten gelöscht. So werden maximal sieben Pakete gleichzeitig für einen Zeitraum zwischengespeichert, der sich im Millisekundenbereich bewegt.

In jedem Netzknoten wird die Anzahl der Bytes notiert, die ein Kunde pro Tag gesendet hat. Diese Information wird an das Rechenzentrum des Betreibers übermittelt, um die Abrechnung für den Kunden zu erstellen. Sie bleibt nach Rechnungserstellung noch drei Monate gespeichert, um Reklamationen bearbeiten zu können.

Die datenschutzrechtliche Einordnung dieser neuen Dienstleistungen nach den Kategorien des Bundesdatenschutzgesetzes aus dem Jahre 1977 ist nicht unproblematisch. Da die Kundendaten — bis auf die Abrechnungsdaten — nur für eine extrem kurze Zeit (Millisekundenbereich) in den Netzknoten zwischengespeichert werden, ist zweifelhaft, ob eine Speicherung im Sinne von § 2 Absatz 2 Nr. 1 BDSG vorliegt. Denn durch die Art des Verfahrens bedingte technische Übergangsstadien innerhalb eines Verarbeitungsvorganges sind nach herkömmlicher Ansicht nicht vom Speicherungsbegriff des Bundesdatenschutzgesetzes umfaßt (vgl. § 3 der Begründung zum Regierungsentwurf, Bundestags-Drucksache 7/1027; Damann in: Simitis/Damann/Mallmann/Reh, Kommentar zum Bundesdatenschutzgesetz, 3. Aufl. 1981 § 2 Rn. 87). Da die Daten auch nicht verändert oder gelöscht und durch den Netzwerkbetreiber wohl auch nicht übermittelt werden — vgl. § 2 Absatz 2 Nr. 2 BDSG, der die Weitergabe durch die speichernde Stelle verlangt, — neigen wir dazu, die Leistung als Datenübermittlung im Auftrag des Kunden zu qualifizieren.

Bei der Datenübermittlung im Auftrag ist der Absender die speichernde Stelle, die sich zu der von ihr gewünschten Weitergabe an Dritte (Übermittlung nach § 2 Abs. 2 Nr. 2 BDSG) der Transportleistung des Netzwerkbetreibers bedient. Insoweit könnte man auf die Idee kommen, den Netzwerkbetreiber mit einem Transportunternehmen für Datenträger zu vergleichen. Deren Dienstleistungen werden höchst unterschiedlich bewertet. So heißt es beispielsweise in den „Allgemeinen Verwaltungsvorschriften der Länder, Teil I, Hinweise zur Anwendung des BDSG", unter 3.2.2.3 „Ausnahmen zur geschäftsmäßigen Datenverarbeitung im Auftrag": „Auch wenn eine Auftragsdatenverarbeitung die in § 31 Absatz 1 Nr. 3 BDSG genannten Voraussetzungen erfüllt, sind Fälle denkbar, in denen die Anwendung aller Vorschriften des vierten Abschnittes zu vom Gesetz nicht beabsichtigten Ergebnissen führen würde. Dies ist insbesondere der Fall bei . . . Transport von Datenträgern, wenn hierdurch der Tatbestand der Übermittlung erfüllt wird (z. B. bei Transportunternehmen). Der Geschäftszweck des Auftraggebers ist hier meist nicht auf die Datenverarbeitung, sondern auf eine andere Tätigkeit gerichtet, die lediglich gelegentlich den Tatbestand der Datenverarbeitung erfüllen kann. In diesen Fällen finden die Vorschriften über die Meldepflicht (§ 39 BDSG), über die Bestellung des Datenschutzbeauftragten (§ 38 BDSG) und die Vorschriften über die Verpflichtung auf das Datengeheimnis (§ 5 Abs. 2 BDSG) keine Anwendung. Die Pflichten zur Datensicherung und zur Beachtung der Weisungen des Auftraggebers bleiben jedoch unberührt."

Wir haben uns nicht von diesem Verständnis leiten lassen, sondern sind der Auffassung, daß jede Tätigkeit, die eine Unterstützung bei einer der Phasen der Datenverarbeitung darstellt, als Auftragsdatenverarbeitung zu qualifizieren ist (ebenso Dammann in: Simitis/Dammann/Mallmann/Reh, Kommendar zum Bundesdatenschutzgesetz, 3. Aufl. 1981 § 8 Rn. 4). Wir halten dieses Ergebnis auch deshalb für zutreffend, weil gegenüber dem physischen Transport von Datenträgern ein Netzwerkservice ein größeres Datenschutzrisiko darstellt, das es rechtfertigt, nicht nur die Weisungsgebundenheit und die Gebote der Datensicherheit verbindlich zu machen, sondern darüber hinaus mit

- der Meldepflicht nach § 39 BDSG den Aufsichtsbehörden eine Marktübersicht zu bieten,
- der Verpflichtung auf das Datengeheimnis ein höheres Maß an Vertraulichkeit zu gewährleisten und
- der Bestellung eines betrieblichen Datenschutzbeauftragten eine innerbetriebliche Datenschutzkontrolle zu etablieren.

Damit können allerdings die spezifischen Probleme bei privaten Kommunikationsdienstleistungen keineswegs als „gelöst" angesehen werden. So ist eine von vielen offenen Fragen, ob der Gesetzgeber bewußt und gewollt private Anbieter von Kommunikationsdienstleistungen von der Übermittlung von Sozialdaten hat ausschließen wollen. § 81 Absatz 2 SGB X gestattet die Übermittlung nur jenen Unternehmen, auf die der zweite Abschnitt des Bundesdatenschutzgesetzes Anwendung findet. Dies aber ist lediglich die Deutsche Bundespost-Telekom. In diesem Zusammenhang könnte auch die weitere Frage aufgeworfen werden, ob nicht die Privilegierung der Deutschen Bundespost-Telekom verfassungsrechtlich problematisch ist.

5.6 Private bundesweite Schuldnerverzeichnisse

Gegenwärtig drängen in Konkurrenz zu den großen Handels- und Wirtschaftsauskunfteien sowie zur SCHUFA kleinere Unternehmen an verschiedenen Orten der Bundesrepublik auf den Dienstleistungsmarkt mit dem Angebot, Auskünfte aus allen Schuldnerverzeichnissen der Bundesrepublik zu liefern. So ist auch die Hamburger Aufsichtsbehörde von der Absicht eines hiesigen Unternehmens informiert worden, ein bundesweites privates Schuldnerverzeichnis (sogenanntes Bonitäts-Terminal) aufzubauen und seinen Kunden daraus im online-Betrieb Auskünfte zu erteilen.

5.6.1 Zur Zulässigkeit nach geltendem Recht

Dies war für uns Anlaß, die datenschutzrechtliche Zulässigkeit eines privaten bundesweiten Schuldnerverzeichnisses erneut und grundsätzlich zu überprüfen.

Rechtsgrundlage für die Schuldnerverzeichnisse ist § 915 ZPO. Nach Absatz 1 der Vorschrift führen die Amtsgerichte ein Schuldnerverzeichnis für den jeweiligen Amtsgerichtsbezirk, in das alle Personen eingetragen werden, welche die eidesstattliche Versicherung (e.V.) abgegeben haben, gegen die zur Erzwingung der Abgabe der e.V. ein Haftbefehl erlassen wurde oder gegen die eine solche Haft von mindestens sechs Monaten Dauer vollstreckt worden ist.

Nach § 915 Absatz 4 ZPO dürfen Abschriften aus dem Verzeichnis nur erteilt und entnommen werden, sofern die Einhaltung von Löschungsfristen gesichert erscheint. Die Veröffentlichung in jedermann zugänglichen Druckerzeugnissen ist verboten. Im übrigen enthält die Vorschrift eine Ermächtigung für den Bundesminister der Justiz zum Erlangen der konkretisierenden Vorschriften. Dem ist jener im Jahre 1955 durch Erlaß einer „Allgemeinen Vorschrift zur Erteilung und Entnahme von Abschriften oder Auszügen aus den Schuldnerverzeichnissen" (kurz: AV) nachgekommen.

Die AV gestattet nach ihrem § 1 die Erteilung von Abschriften und Auszügen an bestimmte Berufsvertretungen und andere vertrauenswürdige Körperschaften, Personen und Unternehmen. Sie dürfen daraus im Einzelfall vertraulich Auskünfte erteilen. Außerdem erlaubt § 4 AV den Berufsvertretungen, die Informationen als Druckerzeugnisse (Listen) an ihre Mitglieder weiterzugeben. Diese wiederum dürfen daraus im Einzelfall vertrauliche Auskünfte erteilen. Daraus ist zum Teil geschlossen worden, daß privaten Institutionen das Führen zentraler Schuldnerverzeichnisse zum Zwecke der Auskunftserteilung nach dem Wortlaut der AV — unter bestimmten Restriktionen — durchaus erlaubt sei.

Auch die Aufsichtsbehörden haben bislang nicht gerügt, daß alle namhaften Auskunfteien ebenso wie die SCHUFA ihren Informationsbedarf entweder durch den Bezug der Listen von den Industrie- und Handelskammern — so in Hamburg — oder dadurch befriedigen, daß die Amtsgerichte ihnen die Abschriften aus den Verzeichnissen direkt zukommen lassen — so bislang in Schleswig-Holstein.

Es bestehen jedoch erhebliche Zweifel, ob die Allgemeinen Vorschriften verfassungsrechtlichen Bedenken standhalten können. Unklar ist bereits, ob die AV als Allgemeine Verwaltungsvorschrift oder als Rechtsverordnung anzusehen ist. Sie bezeichnet sich selbst als Anordnung und benennt keine Verordnungsermächtigung.

Qualifiziert man die AV als Allgemeine Verwaltungsvorschrift, so liegt auf der Hand, daß für die Verbreitung der Informationen aus den Schuldnerverzeichnissen keine ausreichende Rechtsgrundlage vorhanden ist, die jedoch nach der Rechtsprechung des Bundesverfassungsgerichts zum informationellen Selbstbestimmungsrecht erforderlich ist.

Als Rechtsverordnung wäre die AV an Artikel 80 Absatz 1 Satz 2 GG zu messen. Danach muß das zur Verordnung ermächtigende Gesetz selbst Inhalt, Zweck und Ausmaß der erteilten Ermächtigung bestimmen. Die wesentlichen Verarbeitungsmodalitäten hat der Gesetzgeber — so das Bundesverfassungsgericht im Volkszählungsurteil — selbst zu bestimmen. Diesen Anforderungen genügt § 915 Absatz 4 Satz 3 ZPO auch dann nicht, wenn man es für ausreichend erachtet, daß sich Inhalt, Zweck und Ausmaß aus dem Sinnzusammenhang der Norm ermitteln lassen. Insoweit ließe sich allenfalls erschließen, daß die Abschriften aus dem Schuldnerverzeichnis zu denselben Zwecken verwendet werden dürfen wie das Schuldnerverzeichnis selbst. Ob es allerdings darüber hinaus weitere zulässige Zwecke gibt, die ein Abschriftenempfänger verfolgen darf, ob es weiterhin zulässig ist, aus den Abschriften Listen zu erstellen, zu welchen Zwecken derartige Listen gegebenenfalls verteilt werden dürfen und an wen, läßt sich dem § 915 ZPO auch bei großzügiger Auslegung nicht entnehmen.

Die verfassungsrechtlichen Mängel der Regelungen des § 915 ZPO und der AV können schließlich nicht durch einen Rückgriff auf die Vorschriften des 4. Abschnittes des Bundesdatenschutzgesetzes aufgefangen werden, da deren Zweck nicht die Behebung verfassungsrechtlicher Mängel an sich vorhandener bereichsspezifischer Rechtsgrundlagen ist.

Zusammenfassend war daher festzustellen, daß die gegenwärtige Praxis, Informationen aus den Schuldnerverzeichnissen privaten Auskunfteien einschließlich der SCHUFA entweder von den Amtsgerichten durch Direktbelieferung oder über den Umweg der Verzeichnisse der Industrie- und Handelskammern zur Verfügung zu stellen, einer gültigen Rechtsgrundlage entbehrt. Dies dürfte auch die Auffassung des Bundesjustizministers sein, denn er bemüht sich seit langem, den § 915 ZPO den verfassungsrechtlichen Vorgaben anzupassen (vgl. 4.14.1.4 dieses Berichts).

Diese verfassungsrechtlichen Bedenken mußten wir auch dem betroffenen Hamburger Unternehmen mitteilen. Dies ist jedoch nicht bereit, sein Vorhaben aufzugeben, sondern hat den Betrieb nunmehr aufgenommen. Es beruft sich unter anderem auch darauf, daß die bisherige Praxis zu einer Selbstbindung geführt habe, die es aus Gründen des Gleichbehandlungsgebotes nicht gestatte, einzelne Unternehmen von dem Bezug von Listen von der IHK oder von Abschriften direkt von den Amtsgerichten auszuschließen.

Um zu einer möglichst einheitlichen Haltung in dieser Frage zu gelangen, haben wir uns mit dem Amtsgericht Hamburg und auch mit der Justizbehörde in Verbindung gesetzt. Letztere bestätigte, daß auch die Hamburgische Justizverwaltung die Auffassung aller Landesjustizminister teilt, daß private bundesweite Schuldnerverzeichnisse de lege lata unzulässig sind. Das Amtsgericht hat gleichwohl die hiesige Praxis, der IHK Abschriften zukommen zu lassen und die Verteilung der Listen der IHK zu überlassen, bislang nicht revidiert. Der Justizminister in Schleswig-Holstein hat dagegen bereits entsprechende Schritte eingeleitet, um die Vermarktung der Schuldnerdaten auf der gegenwärtig mangelhaften Rechtsgrundlage zu unterbinden.

5.6.2 Zur Identitätsverwechslung

Im 7. Tätigkeitsbericht hatten wir im Zusammenhang mit der SCHUFA ausführlich über das Problem der Identitätsverwechslungen bei Daten aus dem Schuldnerverzeichnis berichtet (7. TB, 5.2.3, S. 123 f). Die im Schuldnerverzeichnis gespeicherten personenbezogenen Angaben enthalten oftmals lediglich den Namen und eine Adresse des Schuldners, nicht jedoch sein Geburtsdatum. In derartigen Fällen kommt es vor, daß irrtümlicherweise eine unbeteiligte Person für diejenige gehalten wird, über die eine

Eintragung im Schuldnerverzeichnis vorhanden ist. Die zu Unrecht mit der Eintragung in Verbindung gebrachte Person kann dann erhebliche Schwierigkeiten bekommen, z. B. bei der Beantragung eines Kredites oder sogar bei der Anmietung einer Wohnung. Diese Probleme treten umso häufiger auf, je größer der Verbreitungsgrad von Informationen aus dem Schuldnerverzeichnis ist.

Im Rahmen unserer Beratung des bereits oben schon erwähnten Hamburger Unternehmens, das kürzlich einen Auskunfteibetrieb mit Informationen aus dem Schuldnerverzeichnis aufgenommen hat, haben wir nachdrücklich auf die Verwechslungsproblematik hingewiesen. Erfreulicherweise hat sich dieses Unternehmen entschlossen, ein mathematisches Verfahren in seine Datenbank zu integrieren, das Personenverwechslungen weitgehend auszuschließen in der Lage ist.

Anhand einer statistischen Auswertung von über 2 Millionen Adreßdaten (Name, Anschrift) wurde analysiert, mit welcher Wahrscheinlichkeit zwei verschiedene Personen gleichen Namens unter der gleichen Adresse gemeldet waren. Dies kommt bei Personen mit häufigen Namen eher vor als bei Personen mit sehr seltenen Namen. Ferner wurde ausgewertet, mit welcher Wahrscheinlichkeit verschiedene Personen gleichen Namens und gleichen Geburtsdatums unter der gleichen Adresse gemeldet waren. Danach war es möglich, dem Adreßdatensatz einen Parameter zuzuordnen, der angibt, mit welcher Wahrscheinlichkeit eine Personenverwechslung auftreten kann. Die Auskunftei gibt die Information nur dann heraus, wenn diese Wahrscheinlichkeit kleiner als 1:100 Millionen ist.

Ungeachtet der oben dargestellten grundsätzlich Bedenken gegen die Vermarktung der Schuldnerverzeichnisdaten muß eingeräumt werden, daß hier ein Weg beschritten wurde, der geeignet ist, die Gefährdung unbeteiligter Dritter praktisch auszuschließen.

5.7 Arbeitnehmerdatenschutz

5.7.1 Beschäftigten-Daten für die Verbandsstatistik

Bereits Mitte letzten Jahres hatte sich der Gesamtpersonalrat eines Versicherungsunternehmens an uns gewandt, um die Weitergabe detaillierter Mitarbeiterdaten durch die Geschäftsleitung an den Arbeitgeberverband überprüfen zu lassen. Die Daten sollen der Erstellung einer Verbandsstatistik dienen und enthalten Angaben zu Alter und Geschlecht, Schul- und Berufsausbildung, zu Betriebszugehörigkeit, Funktion, Status, Arbeitszeit und insbesondere zur Gehaltseinstufung einschließlich der ausgezahlten Zulagen. Der Name wird allerdings nicht erhoben.

Anhand eines früheren Ausdrucks der „flexiblen Personalstatistik" des Verbandes haben wir festgestellt, daß für einzelne Personen eine Anonymität der Statistik nicht gewährleistet ist: Bereits die Auswertungsliste für die gesamte Versicherungswirtschaft enthält bei mehreren Merkmalen die Personenzahl „1". So ist der Aufstellung zum Beispiel zu entnehmen, daß Frau X, 36 Jahre alt, seit 13,4 Jahren im Betrieb teilzeitbeschäftigte Sachverständige im Innendienst, 6350,— DM verdient. Herr Y, 45,3 Jahre alt, 15,2 Jahre im Betrieb, verdient als teilzeitbeschäftigter Sachverständiger im Außendienst 4380,— DM (Einzelangaben zur Anonymisierung jeweils verändert). Die Identität von Frau X und Herrn Y und weiterer Einzelpersonen vom Auszubildenden bis zur Führungsebene ist sicherlich von vielen Empfängern der statistischen Listen (Geschäftsleitungen der Mitgliedsunternehmen) unschwer herauszufinden. Jedenfalls bedarf es zur Erlangung des nötigen Zusatzwissens keines besonderen großen Aufwandes. Die Auswertungen werden jedoch nicht nur für die gesamte Versicherungswirtschaft vorgenommen, sondern jeweils auch für die einzelnen Versicherungssparten (Schadens-, Lebens-, Kranken-, Rückversicherung). Je kleiner diese Sparten sind, desto häufiger werden Einzelpersonen in der Statistik auftauchen und desto leichter werden diese zu identifizieren sein.

Es handelt sich somit — jedenfalls teilweise — um die Übermittlung personenbeziehbarer Daten. Die von § 24 Absatz 1 Satz 1 1. Alternative BDSG a. F. aufgestellte Forde-

rung, die Übermittlung müsse sich „im Rahmen der Zweckbestimmung eines Vertragsverhältnisses" — hier: des Arbeitsvertrages — halten, ist bei der Weitergabe an den Verband nicht erfüllt. Aber selbst wenn man — trotz Vorliegens eines Vertragsverhältnisses zwischen Übermittler und Betroffenen — die zweite Zulässigkeits-Alternative („berechtigte Interessen") in Betracht zöge, stünden der Übermittlung nach unserer Auffassung schutzwürdige Belange der Betroffenen entgegen: Die Personalstatistik hat ausdrücklich auch den Zweck, dem Arbeitgeberverband eine Grundlage für die tarifpolitische Strategie gegenüber den Gewerkschaften an die Hand zu geben. Den Arbeitnehmervertretungen wird die Statistik jedoch nicht zur Verfügung gestellt. Nur in den Tarifverhandlungen selbst findet ein Informationsaustausch über die Erhebungsergebnisse für den gesamten Wirtschaftszweig statt.

Im Anschluß an unsere Beratung weigerte sich der Betriebsrat, der Übermittlung der Beschäftigtendaten an den Arbeitgeberverband in der gewünschten Form zuzustimmen. Eine neue Betriebsvereinbarung zur Anwendung eines Personalabrechnungssystems enthält die Ermittlung und Weitergabe von Personaldaten für die flexible Personalstatistik nicht.

Unmittelbar vor Redaktionsschluß dieses Berichts teilte uns der Arbeitgeberverband nunmehr mit, daß er das mit der Statistikerstellung beauftragte EDV-Service-Unternehmen angewiesen habe, „künftig alle Auswertungspositionen automatisch zu unterdrücken, bei der nur eine Person in der Liste erscheinen würde". Dies ist im Interesse der Betroffenen zu begrüßen.

5.7.2 Namenskürzel beim Nachrichtendienst einer Presseagentur

Der Betriebsrat einer Presseagentur bat uns, zum Entwurf einer Betriebsvereinbarung Stellung zu nehmen, die die Datenverarbeitung bei der Herausgabe des täglichen Nachrichtendienstes regelt. Es ging im wesentlichen um folgendes Problem: Der Nachrichtendienst wird über eine Nachrichtendatenbank elektronisch erstellt und den Empfängern entweder in Papierform geschickt oder elektronisch übermittelt. Jede Meldung weist durch ein Kürzel von 2 Zeichen den Redakteur oder Bearbeiter aus. Einige Mitarbeiter der Presseagentur befürchteten, daß bestimmte Bezieher des Nachrichtendienstes — Medienunternehmen, Regierungsstellen, Parteien — anhand der Kürzel und mit Hilfe der EDV langfristig ein politisches Profil der einzelnen Redakteure erstellen könnten. Sie strebten deswegen folgende Klausel in der Betriebsvereinbarung an: Die Nachrichtenbank wird so eingerichtet, daß Dritte Kürzel nicht recherchieren können bzw. daß beim Abruf durch Dritte Kürzel unterdrückt werden. Diese Regelung sollte dann in Kraft treten, „wenn sie das Amt des Datenschutzbeauftragten der Freien und Hansestadt Hamburg für geboten erachtet".

In unserer Stellungnahme teilten wir dem Betriebsrat mit, daß wir die beabsichtigte Klausel für zulässig, aber nicht für datenschutzrechtlich geboten halten. Dabei kann dahingestellt bleiben, ob und bis zu welchem Umfang der dargestellte Sachverhalt dem Medienprivileg des § 1 Absatz 3 BDSG unterfällt, das Datenschutzgesetz also nicht gilt. Denn es bestehen bereits erhebliche Zweifel, ob es sich bei den Namenskürzeln bezogen auf die Empfänger überhaupt um personenbezogene Daten handelt: Die Kürzel werden von den Bearbeitern bzw. Redakteuren selbst ausgewählt. Dabei sind sie an keine Regel gebunden. Ein Egon Schmidt kann sich „nt" (die letzten Buchstaben von Vor- und Zuname) aussuchen. Wer sich jeweils hinter den Namenskürzel verbirgt, wird Beziehern nicht offenbart. Entsprechende Anfragen werden nicht beantwortet. Die Bearbeiter haben auch die Möglichkeit, ihre Kürzel nach einer bestimmten Zeit wieder zu ändern. Schließlich kann vom Kürzel unter einer Meldung nicht auf die politische Einstellung des Kürzel-Inhabers geschlossen werden: Je nachdem woher die Meldung stammt, können die zwei Buchstaben den Autoren oder aber auch nur den Redakteur bzw. Bearbeiter, der die Meldung in den Nachrichtendienst aufgenommen hat, bezeichnen. Die Kürzel sind deshalb zur Identifikation einer bestimmten politischen Einstellung des Betroffenen gar nicht geeignet.

Schließlich haben wir darauf hingewiesen, daß das Schutzinteresse der Kürzelinhaber nicht besonders gewichtig sein dürfte: Beiträge und Meldungen für eine Presseagentur sind grundsätzlich für die Öffentlichkeit bestimmt; selbst die angenommene Möglichkeit Dritter, Meldungen bestimmten Redakteuren zuzuordnen, wäre deswegen nach unserer Ansicht kein unzulässiger Eingriff in das informationelle Selbstbestimmungsrecht des Betroffenen.

Der Betriebsrat hat unserer Auffassung nicht widersprochen und inzwischen eine Betriebsvereinbarung ohne die erwähnte Klausel abgeschlossen.

5.7.3 Bewerbung bei einem Wach- und Sicherheitsunternehmen

Folgender Sachverhalt war Gegenstand einer Eingabe: Ein Petent bewarb sich bei einem Sicherheitsunternehmen als Aushilfskraft. Dafür hatte er einen umfangreichen Bewerberbogen auszufüllen und ein Führungszeugnis zu beschaffen. Der Arbeitgeber beantragte beim zuständigen Wirtschafts- und Ordnungsamt einen Waffenschein für den Bewerber. Der Petent wurde zwei Tage in dem Betrieb eingesetzt. Dann fragte ihn der Geschäftsleiter eindringlich nach Vorstrafen und hielt ihm schließlich eine alte Jugendstrafe vor — nach Angaben des Petenten unter Hinweis auf gute Kontakte zur Polizei. Das beantragte Führungszeugnis lag zu diesem Zeitpunkt noch nicht vor.

Unsere Recherchen ergaben, daß die Daten tatsächlich nur von der Polizei stammen konnten: In der Datei POLAS/KA sind zwei Jugendstrafermittlungsverfahren gegen den Petenten aus den Jahren 1981 und 1983 gespeichert, das Führungszeugnis enthält dagegen keine Eintragung. (Einen Verstoß der Speicherung dieser Daten gegen die Richtlinien zur Führung Kriminalpolizeilicher personenbezogener Sammlungen (KpS) konnten wir nicht feststellen.) Diese Erkenntnisse müssen jedoch nicht von der Polizei selbst, sondern können auch durch das Wirtschafts- und Ordnungsamt an den Arbeitgeber gelangt sein. Denn in der Regel ermächtigen die Bewerber das Wirtschafts- und Ordnungsamt durch Unterzeichnung einer vorformulierten Erklärung, Informationen einzuholen und an den Arbeitgeber weiterzugeben. Zur Zuverlässigkeitsüberprüfung fragt das Wirtschafts- und Ordnungsamt beim Bundeszentralregister (unbeschränkte Auskunft), beim Gesundheitsamt des zuständigen Bezirks, sowie beim Landeskriminalamt an, ob nachteilige Informationen bekannt sind. Ist dies der Fall, teilt es dem Arbeitgeber diese mit der Aufforderung mit, die Meldung zurückzuziehen. Die Folge ist in den meisten Fällen eine Kündigung ohne nähere Begründung.

Gegen dieses Verfahren haben wir verschiedene Bedenken geltend gemacht: Da es an einer gesetzlichen Grundlage für die Übermittlung der Daten vom Landeskriminalamt zum Wirtschafts- und Ordnungsamt und weiter zum Arbeitgeber fehlt, wäre die Datenübermittlung allenfalls mit Einwilligung der Betroffenen möglich. Die Einwilligung beruht nach unserer Auffassung jedoch nicht auf einer freien Entscheidung: Zum einen hat der Arbeitnehmer nur die Wahl einzuwilligen oder auf den Arbeitsplatz zu verzichten. Zum anderen ist es fraglich, ob dem Arbeitnehmer bewußt ist, welchen Umfang die erteilte Einwilligung hat bzw. von welchen persönlichen Daten der Arbeitgeber Kenntnis erlangen kann. Über die Angaben im abgeforderten Führungszeugnis, selbst über die der unbeschränkten Auskunft aus dem Bundeszentralregister gehen die übermittelten polizeilichen Erkenntnisse oft hinaus. Auch im vorliegenden Fall enthielt das Führungszeugnis des Petenten keine Eintragung.

Ferner ist zu bemängeln, daß der Arbeitnehmer nicht erfährt, welche Informationen das Wirtschafts- und Ordnungsamt erlangt und an den Arbeitgeber weitergegeben hat. Hier wird ein Verfahren praktiziert, das dem Arbeitnehmer von vornherein die Möglichkeit nimmt, sich gegen die Vorwürfe zu wehren, die durch die Weitergabe der Daten an den Arbeitgeber entstanden sind und meist zur — problemlosen — Kündigung noch in der Probezeit führen.

Es wird von uns nicht in Frage gestellt, daß die Sicherheitsunternehmen ihre Bewerber auf deren Zuverlässigkeit überprüfen müssen. Es muß aber sichergestellt werden, daß dies auf normenklarer Rechtsgrundlage geschieht und daß das Verfahren für die

Bewerber transparent gemacht wird. Mit diesem Ziel haben wir uns sowohl an die Behörde für Wirtschaft, Verkehr und Landwirtschaft als auch an den Bundesverband Deutscher Wach- und Sicherheitsunternehmen e.V. gewandt.

Zudem müßte aus unserer Sicht der eingesetzte Bewerbungsbogen überprüft werden. Er enthält zur Zeit etwa 75 Fragen, die zum Teil nicht für die Bewerberauswahl, sondern erst für die Vergütungsabrechnung erforderlich, zu einem anderen Teil unter Zugrundelegung der einschlägigen Rechtsprechung überhaupt unzulässig sind: So etwa die Fragen nach der Gewerkschafts-Mitgliedschaft, dem Arbeitgeber des Ehegatten, einer Schwangerschaft, nach Hobbies oder früheren Schulden. Dies bietet die Möglichkeit, daß Wach- und Sicherheitsunternehmen umfassende Persönlichkeitsprofile ihrer Arbeitnehmer erstellen, die nicht mehr vom Zweck des Arbeitsverhältnisses und damit von dem von der Rechtsprechung begrenzten Fragerecht des Arbeitgebers gedeckt sind. Schließlich ist in diesem Zusammenhang auch zu kritisieren, daß Sicherheitsunternehmen von ihren Arbeitnehmern in regelmäßigen Abständen die Vorlage einer SCHUFA-Selbstauskunft verlangen. Nachdem Arbeitgeber keine Auskünfte mehr von der SCHUFA bekommen, erfahren sie über die abgeforderte Selbstauskunft, die eigentlich dem Datenschutz des Betroffenen dienen soll, heute sogar mehr als durch die ihnen nicht mehr zugängliche sogenannte B-Auskunft der SCHUFA, die nur „Negativmerkmale" enthielt.

5.8 Sonstige Probleme aus dem nicht-öffentlichen Bereich

5.8.1 Datenübermittlung von den Hamburger Wasserwerken zur Deutschen Bundespost-Telekom

Die Hamburger Wasserwerke (HWW) baten im Berichtszeitraum um eine datenschutzrechtliche Stellungnahme zu dem Vorhaben, Namen und Adressen ihrer Rechnungsempfänger sowie jeweils eine Kennzeichnung der Grundstücke, für die die Wasserrechnungen ausgestellt werden, an die Deutsche Bundespost-Telekom zu übermitteln.

Die Deutsche Bundespost-Telekom war an diesen Daten aus zweierlei Gründen interessiert. Zum einen ist sie nach der Poststrukturreform aufgrund von § 9 Fernmeldeanlagengesetz verpflichtet, mit allen Nutzern von Fernmeldeanlagen privatrechtliche Verträge zu schließen, nach denen sie insbesondere das Recht erhält, Leitungen auf deren Grundstücken zu verlegen. Diese Verträge sind unabhängig von den bisherigen Nutzungsberechtigungen der Deutschen Bundespost erforderlich. Sie sind auch mit jenen Personen zu schließen, die als Eigentümer eines Mietshauses auf ihrem Grundstück die fernmeldetechnische Grundausstattung für die Telefonanschlüsse der Mieter dulden. Die Ansprechpartner für derartige Verträge sind deshalb nicht mit den Inhabern der Telefonanschlüsse identisch. Vielmehr besitzt die Deutsche Bundespost-Telekom insoweit nur „Grundeigentümererklärungen", die beim erstmaligen Verlegen der Telefonleitungen abgegeben worden waren, alle Rechtsnachfolger des Eigentümers banden und zum Teil veraltet sind.

Zum anderen wollte die Deutsche Bundespost mit den von den HWW erlangten Daten ihr Marketing für Dienste und Anschlüsse verbessern.

Wir haben zunächst — in Übereinstimmung mit den HWW — die Auffassung vertreten, die Datenübermittlungen seien datenschutzrechtlich vertretbar, wenn die Betroffenen zuvor informiert werden und widersprechen können. Durch den Widerspruch sollten sie Gelegenheit erhalten, entgegenstehende Belange vorzubringen, um den HWW die nach § 24 Absatz 1 Satz 1 3. Alt. BDSG a. F. erforderliche Einzelfallabwägung zu ermöglichen. Nach summarischer Prüfung waren wir der Ansicht, daß bei Ausbleiben eines Widerspruches die berechtigten Interessen der Telekom die schutzwürdigen Belange der Betroffenen überwiegen.

Auch aufgrund der zahlreichen Widersprüche und Beschwerden, die bei den HWW und auch bei uns eingingen, haben wir unsere Rechtsauffassung noch einmal über-

prüft und sind zu dem Ergebnis gekommen, daß mit dem geplanten Verfahren keinesfalls die Grundbuchordnung (GBO) unterlaufen werden dürfe. Zwar sind die Daten der Rechnungsempfänger der HWW (Name, Anschrift des Rechnungsempfängers und Grundstücksbezeichnung) häufig nicht mit den Grundeigentümerdaten aus dem Grundbuch identisch. Der Eigentümer muß nämlich nicht zugleich der Rechnungsempfänger sein, so etwa nicht bei den Grundstücken, die von einer dritten Person verwaltet werden. Es wird jedoch auch Fälle geben, in denen Rechnungsempfänger und Eigentümer identisch sind. Dann ist die Grundbuchordnung zumindest berührt und daher nach unserer Auffassung von vornherein zu beachten. Nach § 12 GBO ist Einsicht in das Grundbuch nur demjenigen zu gestatten, der ein berechtigtes Interesse daran hat. Die Notwendigkeit der Vertragsabschlüsse ist als berechtigtes Interesse in diesem Sinne anzunehmen. Die Verbesserung des Marketings hingegen dürfte dafür nicht ausreichen.

Mit den Hamburger Wasserwerken war erfreulicherweise schnell Konsens darüber hergestellt, das in Aussicht genommene Verfahren so nicht durchzuführen. Es sind in keinem Fall Daten an die Deutsche Bundespost-Telekom übermittelt worden. Statt dessen soll ein Weg gefunden werden, der die geschilderten Bedenken ausräumt. Die frühzeitige Beteiligung der Aufsichtsbehörde ist uns zugesagt worden.

5.8.2 Kundenprofile in computergestützten Reisereservierungssystemen

Im Rahmen unserer Beratungstätigkeit haben wir uns mit computergestützten Reisereservierungssystemen auseinandergesetzt. Dabei haben wir eine neue Variante der automatisierten Persönlichkeitserfassung — diesmal in der Touristikbranche — kennengelernt.

Im einzelnen geht es um Folgendes: In bundesdeutschen Reisebüros werden zunehmend EDV-gestützte Reservierungssysteme eingesetzt. Mit ihnen können Vorgangsverwaltungssysteme kombiniert werden. Damit ausgerüstete Reisebüros bauen sukzessive umfassende Kundenprofile auf. Neben Namen, Nationalität, Adresse und Geburtsdatum „weiß" ein solches System nach einiger Zeit z. B., daß der Kunde am liebsten mit einer bestimmten Gesellschaft fliegt und vegetarische Kost bevorzugt. Der Expedient wird auch darauf aufmerksam gemacht, daß der Kunde bei seinen letzten New-York-Aufenthalten im X-Hotel gewohnt hat. Daneben werden bei Privatkunden auch Angaben über seine Hobbies gespeichert (z. B. Abenteuerurlaub im Kajak o. ä.). Wird per Kreditkarte gezahlt, merkt sich das System automatisch die Kartennummer.

Diese Profile können — sofern die notwendige technische Infrastruktur vorhanden ist — weltweit mit den jeweiligen Kooperationspartnern der Reisebüros ausgetauscht werden. Sie können unter Umständen auch in einem Rechenzentrum abgelegt und bei Bedarf von anderen Interessenten abgerufen werden.

Wir haben Zweifel, ob den meisten Kunden die Tragweite eines solchen Systems bewußt ist. Soweit ersichtlich, wird ihnen in der Regel nur die Erklärung dahingehend abverlangt, ob sie mit der Verarbeitung ihrer Daten einverstanden sind. Dies dürfte aber für eine derartig umfassende Speicherung personenbezogener Daten nicht ausreichen. Kundendaten, die nicht unmittelbar für die Abwicklung eines aktuellen Reisevertrages benötigt werden, dürfen nach unserer Auffassung nämlich nur mit — informierter — Einwilligung des Betroffenen verarbeitet werden. Zu einer wirksamen Einwilligung gehört dann das Wissen des Kunden, daß mit seinen bei Buchungen anfallenden Daten ein Kundenprofil über ihn angelegt werden soll.

Wir werden uns deshalb darum bemühen, in Zusammenarbeit mit den übrigen Aufsichtsbehörden darauf hinzuwirken, daß die Reiseagenturen ihre Kunden umfassend aufklären, wenn sie deren Daten für den Aufbau von Kundenprofilen nutzen wollen. Sie müssen darauf verzichten, wenn der Kunde seine Einwilligung verweigert.

prüft und sind zu dem Ergebnis gekommen, daß mit dem geplanten Verfahren keinesfalls die Grundbuchordnung (GBO) unterlaufen werden dürfe. Zwar sind die Daten der Rechnungsempfänger der HWW (Name, Anschrift des Rechnungsempfängers und Grundstücksbezeichnung) häufig nicht mit den Grundeigentümerdaten aus dem Grundbuch identisch. Der Eigentümer muß nämlich nicht zugleich der Rechnungsempfänger sein, so etwa nicht bei den Grundstücken, die von einer dritten Person verwaltet werden. Es wird jedoch auch Fälle geben, in denen Rechnungsempfänger und Eigentümer identisch sind. Dann ist die Grundbuchordnung zumindest berührt und daher nach unserer Auffassung von vornherein zu beachten. Nach § 12 GBO ist Einsicht in das Grundbuch nur demjenigen zu gestatten, der ein berechtigtes Interesse daran hat. Die Notwendigkeit der Vertragsabschlüsse ist als berechtigtes Interesse in diesem Sinne anzunehmen. Die Verbesserung des Marketings hingegen dürfte dafür nicht ausreichen.

Mit den Hamburger Wasserwerken war erfreulicherweise schnell Konsens darüber hergestellt, das in Aussicht genommene Verfahren so nicht durchzuführen. Es sind in keinem Fall Daten an die Deutsche Bundespost-Telekom übermittelt worden. Statt dessen soll ein Weg gefunden werden, der die geschilderten Bedenken ausräumt. Die frühzeitige Beteiligung der Aufsichtsbehörde ist uns zugesagt worden.

5.8.2 Kundenprofile in computergestützten Reisereservierungssystemen

Im Rahmen unserer Beratungstätigkeit haben wir uns mit computergestützten Reisereservierungssystemen auseinandergesetzt. Dabei haben wir eine neue Variante der automatisierten Persönlichkeitserfassung — diesmal in der Touristikbranche — kennengelernt.

Im einzelnen geht es um Folgendes: In bundesdeutschen Reisebüros werden zunehmend EDV-gestützte Reservierungssysteme eingesetzt. Mit ihnen können Vorgangsverwaltungssysteme kombiniert werden. Damit ausgerüstete Reisebüros bauen sukzessive umfassende Kundenprofile auf. Neben Namen, Nationalität, Adresse und Geburtsdatum „weiß" ein solches System nach einiger Zeit z.B., daß der Kunde am liebsten mit einer bestimmten Gesellschaft fliegt und vegetarische Kost bevorzugt. Der Expedient wird auch darauf aufmerksam gemacht, daß der Kunde bei seinen letzten New-York-Aufenthalten im X-Hotel gewohnt hat. Daneben werden bei Privatkunden auch Angaben über seine Hobbies gespeichert (z.B. Abenteuerurlaub im Kajak o.ä.). Wird per Kreditkarte gezahlt, merkt sich das System automatisch die Kartennummer.

Diese Profile können — sofern die notwendige technische Infrastruktur vorhanden ist — weltweit mit den jeweiligen Kooperationspartnern der Reisebüros ausgetauscht werden. Sie können unter Umständen auch in einem Rechenzentrum abgelegt und bei Bedarf von anderen Interessenten abgerufen werden.

Wir haben Zweifel, ob den meisten Kunden die Tragweite eines solchen Systems bewußt ist. Soweit ersichtlich, wird ihnen in der Regel nur die Erklärung dahingehend abverlangt, ob sie mit der Verarbeitung ihrer Daten einverstanden sind. Dies dürfte aber für eine derartig umfassende Speicherung personenbezogener Daten nicht ausreichen. Kundendaten, die nicht unmittelbar für die Abwicklung eines aktuellen Reisevertrages benötigt werden, dürfen nach unserer Auffassung nämlich nur mit — informierter — Einwilligung des Betroffenen verarbeitet werden. Zu einer wirksamen Einwilligung gehört dann das Wissen des Kunden, daß mit seinen bei Buchungen anfallenden Daten ein Kundenprofil über ihn angelegt werden soll.

Wir werden uns deshalb darum bemühen, in Zusammenarbeit mit den übrigen Aufsichtsbehörden darauf hinzuwirken, daß die Reiseagenturen ihre Kunden umfassend aufklären, wenn sie deren Daten für den Aufbau von Kundenprofilen nutzen wollen. Sie müssen darauf verzichten, wenn der Kunde seine Einwilligung verweigert.