BÜRGERSCHAFT
DER FREIEN UND HANSESTADT HAMBURG
14. Wahlperiode

Drucksache 14/3432
18. 01. 93

Der Hamburgische Datenschutzbeauftragte

An die
Frau Präsidentin der Bürgerschaft

Betr.: 11. Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten

Gemäß § 23 Hamburgisches Datenschutzgesetz übersende ich der Bürgerschaft den 11. Tätigkeitsbericht*

Dem Senat leite ich den Tätigkeitsbericht gleichzeitig zu

Dr. Schrader

* Verteilt nur an die Abgeordneten der Bürgerschaft

Bürgerschaftsdrucksachen — außer Senatsvorlagen — sind — gedruckt auf chlorfrei gebleichtem Papier — zu beziehen bei:
Druckerei Wattenberg & Schrie GmbH Theodorstraße 41 a 2000 Hamburg 50 Telefon 89 39 48

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

vorgelegt im Januar 1993
(Redaktionsschluß: 2. Dezember 1992)

Dr. Hans-Hermann Schrader

Herausgegeben vom Hamburgischen Datenschutzbeauftragten
Baumwall 7 · 2000 Hamburg 11 · Tel.: 35 04 20 47
Auflage: 2500 Exemplare

Druck: Lütcke & Wulff, Hamburg 1

INHALTSVERZEICHNIS

		Seite
1.	**Zur Lage des Datenschutzes**	1
1.1	Schwerpunkt vorgezogener Datenschutz	1
1.2	Weitere Schwerpunkte	3
1.3	Grundrecht auf Datenschutz	4
1.4	Hamburgisches Datenschutzgesetz	6
1.4.1	Anwendungsbereich	6
1.4.2	Datenschutz für Jugendliche	7
1.4.3	Verhältnis zur Bürgerschaft	7
1.5	Neuere hamburgische Gesetze	8
1.5.1	Anwendung des Hamburgischen Archivgesetzes	8
1.5.2	Gesetzentwürfe	8
1.6	Bundesdatenschutzgesetz	9
1.6.1	Fehlender Datenschutz bei Akten	9
1.6.2	Aufsicht im nicht-öffentlichen Bereich	10
1.7	EG-Richtlinienentwurf zum Datenschutz	11
1.8	Verhältnis zum Bürger	12
1.8.1	Eingaben	13
1.8.2	Öffentlichkeitsarbeit	13
1.9	Zusammenarbeit mit Verwaltung und Justiz	14
1.9.1	Datenschutz-Jahrestreffen	15
1.9.2	Unterausschuß Datenschutz	15
1.9.3	Richtlinie zur Beteiligung des Hamburgischen Datenschutzbeauftragten	15
1.9.4	Zusammenarbeit mit den Personalräten	16
1.9.5	Bürgerschaftliche Anfragen und Eingaben	16
1.9.6	Große Automationsvorhaben	16
1.9.7	Beanstandungen	17
1.9.8	Datenschutz bei den Gerichten	17
2.	**Entwicklung der Dienststelle**	17
3.	**Automatisierte Datenverarbeitung**	18
3.1	Ausbau der IuK-Infrastruktur	18
3.1.1	IuK-Drucksache	18
3.1.2	Infrastrukturansatz und Datenschutz	19

3.1.3 Rechtliche Voraussetzungen für die Einführung von Kommunikationsnetzen ... 21
3.2 Neuordnung der Zuständigkeiten in der Hamburger Verwaltung ... 23
3.2.1 Landesamt für Informationstechnik (LIT) ... 23
3.2.2 Senatsamt für den Verwaltungsdienst ... 23
3.2.3 Fachbehörden ... 23
3.3 Datensicherungsmaßnahmen bei Fernwartung ... 24
3.4 Fernsteuerungs- und Netzwerkkontrolliprogramme ... 26
3.5 Empfehlungen zur Benutzerverwaltung in IuK-Systemen ... 29
3.5.1 Administration von Benutzerkennungen ... 30
3.5.2 Vorgaben zur Paßwortverwaltung ... 31
3.6 Löschung und Entsorgung von Festplatten ... 31
3.7 Überblick über Privat-PC ... 33
3.8 Prüfung der Datenverarbeitungszentrale (DVZ) ... 33
3.9 Prüfung von UNIX-Anlagen im Senatsamt für den Verwaltungsdienst ... 34
3.9.1 Prüfungsinhalte ... 34
3.9.2 Datenschutzrechtliche Bewertung ... 35
3.9.3 Forderungen zur Verbesserung der Datensicherheit ... 36

Einzelne Probleme des Datenschutzes im öffentlichen Bereich

4. Telekommunikation und Neue Medien ... 38
4.1 Fangschaltungs-Beschluß des Bundesverfassungsgerichts ... 38
4.2 Prüfung der Telekommunikationsanlage des Fachbereichs Informatik der Universität Hamburg ... 39
4.3 Digitalisierung des Behördennetzes ... 41
4.4 Einführung eines Datenübertragungsdienstes in der Hamburger Verwaltung ... 43
4.5 Risiken von Sprachinformationssystemen ... 43
4.6 Datenschutzrechtliche Einordnung Neuer Medien ... 44
4.6.1 Mailbox-Systeme ... 44
4.6.2 Videodat ... 46
5. Umweltschutz ... 47
5.1 EG-Richtlinie über den freien Zugang zu Informationen über die Umwelt ... 47
5.2 Referentenentwurf eines Umweltinformationsgesetzes des Bundes ... 47
5.2.1 Gesetzgebungskompetenz ... 48
5.2.2 Informationsanspruch ... 48
5.2.3 Beschränkungen des Informationsanspruchs ... 48
5.2.4 Unterrichtung der Öffentlichkeit ... 49
5.3 Hamburgisches Abwassergesetz ... 49
5.4 Referentenentwurf für ein Hamburgisches Bodenschutzgesetz ... 50
5.5 Automationsvorhaben abfallwirtschaftliche Planung ... 50
5.6 Nachtrag zur Prüfung der Stadtreinigung ... 51
6. Sozialwesen ... 51
6.1 Entwurf des Zweiten SGB-Änderungsgesetzes ... 51
6.2 Projekt Sozialhilfe-Automation (PROSA) ... 53
6.3 Projekt Jugendamts-Automation (PROJUGA) ... 53
6.4 Fachliche Weisung zum Sozialdatenschutz ... 55
6.5 Basisuntersuchung beim Landesbetrieb Pflegen & Wohnen ... 55
6.6 Schweigepflicht-Entbindungserklärung des Versorgungsamtes ... 57
6.7 Offenbarung von Jugendhilfedaten ... 58
6.7.1 Akteneinsicht in Jugendhilfeakten ... 58
6.7.2 Verwendung von Jugendhilfedaten in öffentlichen Bürgerschaftsdebatten ... 60
6.8 Kontrollzuständigkeit bei der Vereinigung Städtischer Kinder- und Jugendheime ... 60
6.9 Verfolgung von Mietpreisüberhöhungen ... 62
6.10 Unzulässige Datenerhebung der Sozialämter ... 63
7. Personalwesen ... 64
7.1 Automationsvorhaben Projekt Personalwesen (PROPERS) ... 64
7.2 Neues Personalaktenrecht ... 65
7.3 Personalärztlicher Dienst ... 67
7.4 Bewerbungen aus den neuen Bundesländern ... 69
7.5 Weitergabe von Personaldaten an private Versicherungsgesellschaften ... 70
7.6 Mitarbeiterdaten im Hamburg Handbuch ... 71
7.7 HVV-Großkundenabonnement ... 72

Erhebung von Gesundheitsdaten bei Bewerbern ... 72
Personaldatenschutz bei Zuwendungsempfängern ... 73
Statistik ... 74
Landesstatistiken ohne Auskunftspflicht ... 74
1 Abgrenzung von Planung, Forschung und Statistik ... 74
2 Umsetzungsprobleme ... 75
Umstellung der Prüfungsstatistik auf das neue Hochschulstatistikgesetz des Bundes ... 76
Schulwesen ... 77
Schulgesetzentwurf ... 77
Regelung zur Verwendung privater PC durch Lehrer ... 79
Betriebspraktika von Schülern ... 81
Steuerwesen ... 82
Keine Änderung der Abgabenordnung (AO) ... 82
Private PC im Betriebsprüfungsdienst ... 84
Zeichnungsvorbehalt der Finanzamtsvorsteher ... 84
Zugriff der Steuerfahndung auf Patientendaten ... 85
Wissenschaft und Forschung ... 86
Datenerhebung durch die Hochschulen ... 86
1 Hochschuldatenverordnung ... 86
2 Fragebogen der Hochschule für bildende Künste ... 86
Forschungsvorhaben ... 87
Bauwesen ... 88
Entwurf eines Hamburgischen Vermessungsgesetzes ... 88
Fehlbelegungsabgabe-Verfahren ... 89
.1 Änderung des Verfahrens ... 89
.2 Novellierung des Hamburgischen Gesetzes über den Abbau der Fehlsubventionierung im Wohnungswesen ... 90
Hamburger Mietenspiegel ... 91
Projekt Bauaufsicht mit Computerunterstützung (BACom) ... 92
Parlamentarischer Untersuchungsausschuß SAGA ... 93
Meldewesen ... 95
Verwechslungen im Melderegister ... 95
Wachsende Unzuverlässigkeit des Melderegisters ... 96
Standesamt ... 97

15. Ausländerbehörde ... 99
15.1 Automation der Ausländerverwaltung ... 99
15.1.1 Registriernummern ... 99
15.1.2 Warnmeldungen ... 100
15.2 INPOL-Ausschreibung von Ausländern ... 100
16. Personalausweisregister ... 102
16.1 Zugriff der Polizei auf Paßfotos ... 102
16.2 Paßfotos in Ermittlungsakten ... 103
17. Polizei ... 104
17.1 Projekt Computerunterstützte Vorgangsbearbeitung bei der Polizei (COMVOR) ... 104
17.1.1 Neue Konzeption für das Projekt ... 104
17.1.2 Datenschutzkonzept ... 105
17.2 Probleme des bundesweiten Informationssystems der Polizei (INPOL) ... 106
17.2.1 Datenschutzrechtliche Anforderungen an Regelungen für das INPOL-System im Gesetz über das Bundeskriminalamt ... 106
17.2.2 Übermittlung von Kfz-Sachfahndungsdaten durch das Bundeskriminalamt an Hersteller und den HUK-Verband ... 109
17.2.3 Verlängerung der Speicherfristen für die Arbeitsdatei Innere Sicherheit (APIS) ... 110
17.2.4 Personenbezogene Hinweise ... 111
17.3 Zugriffssicherung für das polizeiliche Auskunftssystem (POLAS) ... 112
17.4 Prüfung von Kriminalakten über Kinder ... 113
17.4.1 Speicherung auch von Kindern ... 113
17.4.2 Rechtliche Ausgangsposition ... 114
17.4.3 Einzelne Fallgruppen ... 115
17.4.4 Zusammenfassende Bewertung ... 117
17.5 Datei über Zuhälter- und Milieukriminalität ... 118
17.6 Akten über politische Organisationen beim polizeilichen Staatsschutz ... 118
17.7 Einsatz besonderer Befugnisse zur Datenerhebung durch die Polizei ... 120
17.8 Videoaufnahmen von Versammlungen ... 122
18. Verfassungsschutz ... 124
18.1 Entwurf des Hamburgischen Verfassungsschutzgesetzes ... 124

18.2 [illegible]überprüfung von Beschäftigten ... 126
18.3 [illegible]erung der Referatsarbeitskartei (RAK) ... 126
18. [illegible] ... 127
18.1 [illegible] zur Bekämpfung der organisierten Kriminalität und Lauschangriff ... 127
19.2 [illegible] des Justizmitteilungsgesetzes ... 129
19.3 [illegible]zuständigkeit bei den Gerichten ... 130
19.4 Prüfung des Schuldnerverzeichnisses ... 131
19.5 Private und dienstliche PC bei der Staatsanwaltschaft ... 131
20. Strafvollzug und Postkontrolle ... 133
21. Gesundheitswesen ... 134
21.1 Verstärkte Automation in den Krankenhäusern ... 134
21.2 Gesundheits-Strukturgesetz ... 135
21.3 Dienstanweisungen zum Datenschutz in den Krankenhäusern 137
21.3.1 Überblick ... 137
21.3.2 Dienstanweisung Datenschutz für IuK-Anwendungen im Landesbetrieb Krankenhäuser ... 138
21.4 Gesundheitsberichterstattung ... 140
21.5 Qualitätssicherung im Krankenhaus ... 141
21.5.1 Projekt Qualitätssicherung in der Chirurgie (Quasic) ... 141
21.5.2 Projekt Qualitätssicherung Geburtshilfe ... 142
21.5.3 Externe Qualitätssicherung ... 143
21.6 Übermittlungen vom Krankenhaus an Krankenkassen ... 143
21.7 Mitteilungen der Krankenhäuser an Sozialämter ... 144
21.8 Neue Berufsordnung für Hamburger Ärzte ... 145
21.9 Mitgliedsbeiträge der Ärzte zur Ärztekammer ... 146
21.10 Schutz von Patientendaten bei Auflösung und Verkauf von Arztpraxen ... 146
21.11 Übermittlung von Patientendaten an Verrechnungsstellen ... 149

Einzelne Probleme des Datenschutzes im nicht-öffentlichen Bereich

22. Werbewirtschaft ... 151
22.1 Neue Regelung für unadressierte Postwurfsendung ... 151
22.2 Interessentenwerbung durch Umfrage ... 151
23. Schufa ... 152
23.1 Anfrageberechtigung bei telefonischer Anfrage ... 152
23.2 Auskunft aufgrund mutmaßlicher Einwilligung ... 153
23.3 Auslandsvertragsmodell ... 153
24. Private bundesweite Schuldnerverzeichnisse ... 153
24.1 Rechtslage ... 153
24.2 Kreditschutz-Vereinigung (KSV) ... 154
25. Versicherungswirtschaft ... 154
25.1 Automationsentwicklung ... 154
25.2 Zentrale Registrierstelle Rechtsschutz ... 155
25.3 Allfinanz-Konzepte ... 156
25.4 Schweigepflicht-Entbindungsklauseln ... 157
25.4.1 Reise-Rücktrittskosten-Versicherung ... 157
25.4.2 Kfz-Haftpflichtversicherung ... 158
25.4.3 Altverträge in der Lebens-, Unfall- und Krankenversicherung 158
25.4.4 Information der Ärzte über Neufassungen ... 159
25.5 Gruppenversicherungsverträge ... 159
25.6 Datenübermittlungen in das Ausland ... 160
26. Handels- und Wirtschaftsauskunfteien ... 161
26.1 Kein Vertragsmodell ... 161
26.2 Keine Erhöhung der Stichproben ... 162
27. Kartengestützte Zahlungsverfahren ... 162
27.1 Electronic-cash ... 163
27.2 Lastschriftverfahren ... 164
27.3 Rechte der Betroffenen ... 166
28. Meldepflicht nach § 32 BDSG ... 167
29. Arbeitnehmerdatenschutz ... 167
29.1 Psycho-Tests bei Bewerberauswahl ... 167
29.2 Personaldatenschutz von Auszubildenden ... 168
30. Sonstige Probleme aus dem nicht-öffentlichen Bereich .. 169
30.1 Datenverarbeitung bei der Scientology Kirche Hamburg e.V. ... 169
30.2 Mieterdatenschutz und Selbstauskunft ... 171
30.3 Einsichtnahme in Mitgliederlisten von Parteien ... 172
Geschäftsverteilung ... 174
Stichwortverzeichnis ... 178

1. Zur Lage des Datenschutzes

Der Datenschutz befindet sich in einer schwierigen Phase. Nachdem mit den neueren Landesdatenschutzgesetzen und dem neuen Bundesdatenschutzgesetz deutliche Fortschritte erreicht worden waren, sind nun in der Gesetzgebung insbesondere im Bereich der inneren Sicherheit, aber auch auf anderen Gebieten unverkennbar Einschränkungen des Persönlichkeitsrechts und damit des Datenschutzes feststellbar.

Für diese Entwicklung ist die Frage kennzeichnend: Wieviel Freiheit können wir uns leisten? Als Antwort darauf werden zunehmend weitreichende Eingriffe befürwortet, die bis zum Abhören von Wohnungen reichen. Damit wird der Kernbereich des informationellen Selbstbestimmungsrechts für jeden Bürger in einer Weise berührt, die nicht mehr hinnehmbar ist.

Als Rechtfertigung wird dabei geltend gemacht, daß mit einer eindeutigen Gesetzgebung normenklare Regelungen der Einschränkungen im Interesse der Allgemeinheit getroffen würden. Dies entspricht jedoch nur formal den vom Bundesverfassungsgericht aufgestellten Grundsätzen.

Danach hat der Gesetzgeber bei seinen Regelungen vor allem den Grundsatz der Verhältnismäßigkeit zu beachten. Dies bedeutet in den Worten des Bundesverfassungsgerichts, daß die gesetzlichen Einschränkungen „nicht weiter gehen dürfen, als es zum Schutz öffentlicher Interessen unerläßlich ist."

Das Bundesverfassungsgericht hat erfreulicherweise seine Rechtsprechung zum Schutz der Grundrechte mit dem Fangschaltungs-Beschluß vom 25. März 1992 fortgeführt (siehe dazu auch 4.1). Es hat dort betont, daß „staatliche Maßnahmen gegenüber grundrechtsgeschütztem Verhalten Eingriffe" sind und deshalb einer gesetzlichen Grundlage mit den besonderen Anforderungen nach dem Verhältnismäßigkeitsprinzip bedürfen. Dagegen ist es laut Bundesverfassungsgericht nicht möglich, die grundrechtlichen Schutzbereiche einfach „nach Eingriffsnotwendigkeiten zuzuschneiden", indem man sich auf immanente Schranken des Grundrechts beruft. Sonst „könnte das Grundrecht den Einzelnen auch nicht mehr vor fehlerhafter, mißbräuchlicher oder exzessiver Verwertung von Kommunikationsdaten" schützen.

Gemäß diesen Grundsätzen wird bei der weiteren Gesetzgebung sehr sorgfältig darauf zu achten sein, daß nicht nur normenklare, sondern vor allem verhältnismäßige Regelungen getroffen werden, die das informationelle Selbstbestimmungsrecht nicht ständig als nachrangig behandeln.

1.1 Schwerpunkt vorgezogener Datenschutz

Eine weitere aktuelle Gefährdung des Datenschutzes ergibt sich daraus, daß die Ausweitung der automatisierten Datenverarbeitung bis hin zu flächendeckenden Anwendungen zügig fortgesetzt wird. Diesen Herausforderungen kann nur ein vorgezogener Datenschutz effektiv begegnen, der bereits bei der

Vorbereitung von Automationsvorhaben wirksam wird. Nachträgliche Kontrollen genügen allein nicht mehr.

Die Datenschutzkonzeption, die im 10. TB eingehend beschrieben worden ist (1.1 und 3.), muß daher konsequent weiterverfolgt werden. Daraus ergeben sich konkrete Schlußfolgerungen für unsere Beteiligung bei der Planung von Automationsvorhaben und für die Lösung der Probleme bei der zunehmenden Vernetzung (siehe dazu 3.1).

Die bisherige Regelung in § 23 Abs. 4 des Hamburgischen Datenschutzgesetzes (HmbDSG), wonach der Hamburgische Datenschutzbeauftragte über Planungen neuer IuK-Anwendungen mit einer Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten ist, reicht offensichtlich nicht mehr aus. Wir sind im Jahr 1992 – anders als bei den bisherigen großen Vorhaben wie PROSA und PROPERS (siehe 1.9.6) – wiederholt von neuen Automationsvorhaben vor allem im Gesundheitsbereich mit besonders sensiblen Daten (z.B. 3.3 und 21.1) erst unterrichtet worden, als die Planung bereits weit fortgeschritten war. Teilweise wurde sogar behauptet, daß die späte Unterrichtung noch rechtzeitig im Sinne der erwähnten gesetzlichen Regelung sei (21.1).

Unbestritten muß es der Verwaltung freistehen, zu Beginn ihrer Projektplanungen vorläufige Konzepte zu entwickeln und auch wieder ganz oder teilweise aufzugeben. Eine verbindliche Planung, die dem Hamburgischen Datenschutzbeauftragten mitzuteilen ist, liegt aber vor dem Abschluß des endgültigen Konzepts vor. Mit dem Beginn konkreter Planungen einschließlich der Beteiligung Dritter und spätestens vor Beginn der Realisierung einschließlich der Beauftragung Dritter hat die Unterrichtung zu erfolgen.

Zur Klarstellung gegenüber der Verwaltung ist es hilfreich, daß das Senatsamt für den Verwaltungsdienst mit der neuen Richtlinie die maßgeblichen Zeitpunkte für eine Beteiligung des Hamburgischen Datenschutzbeauftragten konkretisiert hat (siehe 1.9.3). Dem – vom Bundesverfassungsgericht wiederholt bekräftigten – Grundrechtsschutz durch Verfahren würde es entsprechen, daß diese Aussagen nicht nur in Verwaltungsvorschriften enthalten sind, sondern die Grundsätze in den Text des § 23 Abs. 4 HmbDSG aufgenommen werden. Zugleich würden sie damit eindeutig auch für die öffentlichen Unternehmen nach § 2 Abs. 2 HmbDSG gelten.

Die gesetzliche Regelung für die Planung von Automationsvorhaben ist darüber hinaus in mehreren Punkten ergänzungsbedürftig. Die im 10. TB erwähnten Lösungsansätze für einen wirksamen Datenschutz bei Automationsvorhaben (insbesondere 3.3) sind inzwischen in der Stellungnahme des Senats und in den bürgerschaftlichen Ausschußberatungen behandelt worden. Im Sinne des Grundrechtsschutzes durch Verfahren ist es angebracht, in das Hamburgische Datenschutzgesetz grundsätzliche Aussagen über

— Risikoanalysen vor der Entscheidung über den Einsatz oder die wesentliche Änderung eines automatisierten Verfahrens

— Freigabeverfahren für den erstmaligen Einsatz oder die wesentliche Änderung eines automatisierten Verfahrens

— erweiterte Anforderungen an Online-Verfahren und gemeinsame Dateien

— Prüfung der Sozialverträglichkeit bei der Einführung von neuen Datenverarbeitungstechniken

jeweils mit Beteiligung des Hamburgischen Datenschutzbeauftragten aufzunehmen. Gemäß dem Vorschlag des Unterausschusses Datenschutz hat der Rechtsausschuß am 16. November 1992 der Bürgerschaft als Ersuchen an den Senat empfohlen, die Lösungsansätze im 10. TB für datenschutzrechtliche Regelungen zur automatisierten Datenverarbeitung in die Überlegungen zur bevorstehenden Novellierung des Hamburgischen Datenschutzgesetzes einzubeziehen. Die Bürgerschaft wird darüber voraussichtlich am 13. Januar 1993 beschließen.

Die Rechtsprechung des Bundesverfassungsgerichts verpflichtet den Gesetzgeber, im Bereich der Grundrechtsausübung alle wesentlichen Entscheidungen selbst zu treffen. Dazu gehören allerdings nur die Grundaussagen und nicht weitere Einzelregelungen, die Verwaltungsvorschriften überlassen werden können. Demgemäß habe ich eine begrenzte Zahl von Regelungsvorschlägen für die Novellierung des Hamburgischen Datenschutzgesetzes der Justizbehörde zugeleitet.

Bei den Vorschlägen ist auch berücksichtigt worden, daß eine zu starke Einbindung des Datenschutzbeauftragten in die fachliche Verantwortung für die Automationsvorhaben vermieden werden muß. Zustimmungs- oder sogar Vetorechte des Datenschutzbeauftragten sind schon deshalb nicht angebracht, weil die Unabhängigkeit des Datenschutzbeauftragten unberührt und eine klare Trennung von den eigenständigen Aufgaben der Verwaltung erhalten bleiben muß.

Insgesamt halte ich diese Datenschutzkonzeption auch im Interesse der Verwaltung für sachgerecht, um eine für beide Seiten rechtzeitige „Prävention im Dialog" (Prof. Simitis) zu erreichen. Eine verspätete Beteiligung ist dagegen gerade für die Verwaltung selbst nachteilig, weil sie zu erheblichem Zeit- und Kostenaufwand wegen nachträglich erforderlicher Änderungen führen kann.

Die Lösungsvorschläge sind teilweise bereits in anderen Landesdatenschutzgesetzen enthalten. In der vorgesehenen Kombination von inhaltlichen und verfahrensmäßigen Verbesserungen würde eine derartige Ergänzung des Hamburgischen Datenschutzgesetzes erheblich zu einem effektiven Datenschutz beitragen, ohne die Belange der Verwaltung zu beeinträchtigen. Es würde Hamburg gut anstehen, mit einem wirksamen vorgezogenen Datenschutz Maßstäbe für die Datenschutzgesetzgebung zu setzen.

1.2 Weitere Schwerpunkte

Wie im 10. TB erwähnt (1.1), liegt mir besonders an einem wirkungsvollen Schutz der Gesundheitsdaten und der Personaldaten, die von besonderer Sen-

sibilität für die Betroffenen sind. Deshalb wird auf diese Schwerpunkte im vorliegenden Tätigkeitsbericht beim Personalwesen (7.) und Arbeitnehmerdatenschutz (29.) sowie beim Gesundheitswesen (21.) wieder näher eingegangen.

Wegen der Risiken für den Datenschutz ist es ferner wichtig, sachgerechte Regelungen und Verfahrensweisen für die Datenverarbeitung auf Privat-PC sicherzustellen. Nach einem Überblick in dem Abschnitt über Automatisierte Datenverarbeitung (3.7) wird dieses Thema in den jeweiligen Abschnitten, z. B. beim Schulwesen (9.2) und bei der Staatsanwaltschaft (19.5), behandelt.

Hervorzuheben ist schließlich aus dem Bereich der automatisierten Datenverarbeitung die zunehmende Fernwartung, die datenschutzrechtlich in verschiedener Hinsicht problematisch ist (3.3). Wenn sie sogar in den USA – mit dem dortigen unzureichenden Datenschutz – durchgeführt wird, sind die Schwierigkeiten offenkundig.

Die Anwendung neuerer hamburgischer Gesetze mit erheblichen Auswirkungen auf den Datenschutz ist von uns sorgfältig verfolgt worden, z.B. hinsichtlich der Datenerhebung mit besonderen Methoden nach dem Gesetz über die Datenverarbeitung der Polizei (17.7).

Im nicht-öffentlichen Bereich sind die weitreichenden neuen Allfinanz-Konzepte erstmals dargestellt worden, die zu einer Datenübermittlung zwischen verschiedenen Branchen, wie z.B. Banken und Versicherungen, zunächst innerhalb einer Unternehmensgruppe führen (25.3).

1.3 Grundrecht auf Datenschutz

Die Beratungen der Kommission Verfassungsreform des Bundesrates und – seit Anfang 1992 – der Gemeinsamen Verfassungskommission von Bundesrat und Bundestag haben die Datenschutzbeauftragten des Bundes und der Länder veranlaßt, sich für die Aufnahme eines Grundrechts auf Datenschutz in das Grundgesetz auszusprechen. Mit der Entschließung vom 28. April 1992 haben die Datenschutzbeauftragten dazu folgende Fassung empfohlen:

„Jeder hat das Recht, über die Preisgabe und Verwendung seiner persönlichen Daten selbst zu bestimmen. Dazu gehört das Recht auf Auskunft und Einsicht in amtliche Unterlagen. Dieses Recht darf nur durch Gesetz oder aufgrund eines Gesetzes eingeschränkt werden, soweit überwiegende Interessen der Allgemeinheit es erfordern."

Zur Begründung haben die Datenschutzbeauftragten darauf verwiesen, mit der Aufnahme eines Grundrechts auf Datenschutz in das Grundgesetz würde „für die Bürger deutlicher erkennbar, daß unsere Verfassung ihr Recht auf Datenschutz in gleicher Weise garantiert wie die traditionellen Grundrechte".

Als weitere Gründe nannten sie die wachsende Bedeutung des Datenschutzes für das Funktionieren der freiheitlichen Demokratie und eine Reaktion auf die negativen Erfahrungen der DDR-Geschichte sowie eine Anpassung des

Grundrechtskatalogs an den technischen Wandel. Schließlich könnten auf diese Weise die Konsequenzen aus den politischen Erfahrungen gezogen werden, die in mehreren Bundesländern und im Ausland mit ähnlichen Verfassungsbestimmungen gemacht wurden.

Für die weitere Diskussion ist es in der Tat von Bedeutung, daß in immer mehr Landesverfassungen ein Grundrecht auf Datenschutz eingefügt worden ist oder werden soll. Angesichts dieser Verfassungsbestimmungen in den Ländern wäre es nicht verständlich, wenn eine solche Regelung für das Grundgesetz nicht auch mehrheitsfähig würde. Ohne Regelung im Grundgesetz würde das Grundrecht auf Datenschutz nur in den Ländern gelten, deren Verfassungen es vorsehen. Bürger in Ländern wie Hamburg, deren Verfassungen keinen Grundrechtsteil haben, wären dann schlechter gestellt.

Die Kommission Verfassungsreform des Bundesrates hatte am 14. Mai 1992 mit einfacher Mehrheit befürwortet, daß Bestimmungen über den Datenschutz in das Grundgesetz eingefügt werden. Die Gemeinsame Verfassungskommission von Bundesrat und Bundestag hat die Thematik ebenfalls näher behandelt, ohne allerdings eine zustimmende Tendenz erkennen zu lassen. Mit einem abschließenden Votum wird noch im Dezember 1992 oder sonst Anfang 1993 gerechnet.

Die Datenschutzbeauftragten des Bundes und der Länder haben mit ihrer Entschließung vom 28. April 1992 weitere Empfehlungen für die Verfassungsdiskussion gegeben. Sie halten es für erforderlich, eine Stärkung der Grundrechte aus Art. 10 (Fernmeldegeheimnis) und 13 GG (Unverletzlichkeit der Wohnung) im Hinblick auf neue Überwachungstechniken sowie Instrumente zur Technikfolgenabschätzung vorzusehen.

Darüber hinaus haben sich die Datenschutzbeauftragten für die nähere Prüfung eines „Rechts auf Zugang zu den Daten der Verwaltung (Aktenöffentlichkeit, Informationsfreiheit)" ausgesprochen. Damit wird eine Ergänzung zum Datenschutz durch einen freien Datenzugang erstmals von den Datenschutzbeauftragten thematisiert. Die Verfassung des Landes Brandenburg enthält nun – erstmals als generelle Aussage in einer Landesverfassung – in Art. 21 Abs. 4 als „Recht auf politische Mitgestaltung" folgende Regelung:

„Jeder hat das Recht auf Einsicht in Akten und sonstige amtliche Unterlagen der Behörden und Verwaltungseinrichtungen des Landes und der Kommunen, soweit nicht überwiegende öffentliche oder private Interessen entgegenstehen."

Damit sind Ansätze, die bereits seit einiger Zeit im Umweltbereich als Informationszugangsrechte behandelt werden (siehe 5.1 und 5.2), zu einem allgemeinen Bürgerrecht mit Verfassungsrang weiterentwickelt worden. Die Ausgestaltung von Informationsrechten des Bürgers soll zwischen den Datenschutzbeauftragten noch näher erörtert werden. Darauf wird im 12. TB weiter eingegangen werden.

1.4 Hamburgisches Datenschutzgesetz

Zur beabsichtigten Novellierung des Hamburgischen Datenschutzgesetzes war im 10. TB (1.2.1) bereits auf den wesentlichen Änderungsbedarf hingewiesen worden. Als wichtiger Teilbereich ist oben der vorgezogene Datenschutz genannt worden (1.1). Unsere Änderungsvorschläge habe ich inzwischen noch einmal zusammengefaßt und der Justizbehörde zugeleitet. Es ist zu erwarten, daß daraufhin die Justizbehörde demnächst eine Senatsvorlage erarbeitet. Besonders zu erwähnen sind folgende Punkte:

1.4.1 Anwendungsbereich

Über zehn Jahre nach dem ersten Hamburgischen Datenschutzgesetz von 1981 ist der Anwendungsbereich des Gesetzes erstaunlicherweise keineswegs eindeutig geregelt. Infolgedessen gibt es wiederholt Unklarheiten und Meinungsverschiedenheiten, ob und wie insbesondere für die hamburgischen öffentlichen Unternehmen – also die privatrechtlich organisierten Unternehmen, die Aufgaben der hamburgischen öffentlichen Verwaltung wahrnehmen – das Hamburgische Datenschutzgesetz oder das Bundesdatenschutzgesetz gilt.

Zur Abgrenzung zwischen öffentlichem und nicht-öffentlichem Bereich teile ich die Auffassung des Bundesinnenministeriums, daß folgende Kriterien für die Zuordnung einer privatrechtlich organisierten Vereinigung als öffentliche Stelle genannt hat:

— beherrschender Einfluß des Bundes oder der Länder, insbesondere mit Stimmen- oder Anteilsmehrheit,

— Wahrnehmung öffentlicher Aufgaben der Verwaltung, einschließlich Aufgaben der Daseinsvorsorge,

— Einbeziehung auch der Vereinigungen, die nur einen Gesellschafter haben,

— Behandlung der Vereinigung als öffentlich-rechtliches Wettbewerbsunternehmen, soweit sie am Wettbewerb teilnimmt.

Dabei geht es nicht nur um die formale Frage, welche Regelungen anzuwenden sind. Entscheidend ist vielmehr, daß bei unveränderter öffentlicher Aufgabenerfüllung datenschutzrechtlich eine „Flucht ins Privatrecht" verhindert werden soll. Es ist gerade auch für den Datenschutz des Bürgers nicht nachvollziehbar, daß nur wegen einer Änderung der Rechtsform die geringeren Anforderungen des Bundesdatenschutzgesetzes – insbesondere ohne Einbeziehung der Datenverarbeitung in Akten und mit eingeschränkten Aufsichtsmöglichkeiten – gelten sollen.

Die Erörterung dieser grundsätzlichen Thematik dauert zwischen den Datenschutzbeauftragten und den Aufsichtsbehörden noch an. Danach ist die Regelung im Hamburgischen Datenschutzgesetz zu treffen, das zu den Vereinigungen bisher keine Aussage enthält.

1.4.2 Datenschutz für Jugendliche

Regelungsbedürftig ist die Frage, ob und ab wann Minderjährige ihre Datenschutzrechte selbst wahrnehmen können oder ob dies den gesetzlichen Vertretern vorbehalten bleiben soll. Die Minderjährigen sind unstreitig bereits Träger des Grundrechts auf Datenschutz; sie haben aber ohne ausdrückliche Regelung nicht die Handlungsfähigkeit im Verwaltungsverfahren, jedenfalls neben den gesetzlichen Vertretern ihre Rechte als Betroffene selbst wahrzunehmen. Andererseits sind sie als Jugendliche bereits bedingt strafmündig und noch vor der Volljährigkeit in verschiedenen Bereichen selbständig entscheidungsfähig.

Deshalb bietet es sich an, den Jugendlichen – d.h. ab Vollendung des 14. Lebensjahres – die datenschutzrechtliche Handlungsfähigkeit einzuräumen. Wer von Gesetzes wegen für seine Straftaten verantwortlich ist, sollte auch das Recht haben, Auskunft über die ihn betreffenden Daten in amtlichen Unterlagen zu erhalten und z.B. eine Berichtigung oder Löschung zu verlangen. Deshalb habe ich vorgeschlagen, in das Hamburgische Datenschutzgesetz – und damit erstmals in ein Datenschutzgesetz – das Recht zur Ausübung der Datenschutzrechte durch die Jugendlichen aufzunehmen.

1.4.3 Verhältnis zur Bürgerschaft

Dringend ergänzungsbedürftig sind die Regelungen über das Verhältnis zwischen dem Hamburgischen Datenschutzbeauftragten und der Bürgerschaft. Nach dem jetzigen § 23 HmbDSG erhält die Bürgerschaft lediglich den jährlichen Tätigkeitsbericht und kann mit einem Viertel der Abgeordneten vom Hamburgischen Datenschutzbeauftragten Gutachten und Berichte verlangen. Der Hamburgische Datenschutzbeauftragte kann sich – außer mit dem Tätigkeitsbericht – nicht ohne weiteres an die Bürgerschaft wenden, sondern ihr nur Empfehlungen zur Verbesserung in ihren eigenen Datenschutzangelegenheiten geben. Damit bleibt die hamburgische Regelung deutlich hinter den anderen Datenschutzgesetzen zurück.

Für die Stellung der Bürgerschaft gegenüber dem von ihr gewählten Datenschutzbeauftragten wäre es angebracht, daß sie und ihre Ausschüsse ebenso wie der Senat vom Hamburgischen Datenschutzbeauftragten verlangen können, Hinweisen auf Angelegenheiten und Vorgänge des Datenschutzes bei den öffentlichen Stellen nachzugehen. Zugleich wäre zu regeln, daß der Hamburgische Datenschutzbeauftragte sich jederzeit an den Senat und die Bürgerschaft wenden kann und im letzteren Falle gleichzeitig den Senat unterrichtet.

Wie ähnliche Regelungen in vielen Datenschutzgesetzen ohne vorherige Verfassungsänderung zeigen, handelt es sich dabei nicht um ein Problem der Gewaltenteilung mit der Folge, daß es dazu erst einer Verfassungsänderung oder einer Gesetzesänderung mit verfassungsändernder Mehrheit bedarf. Bei einem unmittelbaren Verkehr zwischen Bürgerschaft und Hamburgischem

Datenschutzbeauftragten erfolgt verfassungsrechtlich keine Gewaltenverschiebung, weil dem Datenschutzbeauftragten keine Exekutivbefugnisse, sondern lediglich Beratung, Empfehlung und allenfalls Beanstandung ohne unmittelbare Rechtswirkung zustehen. Die Verantwortung des Senats für die Exekutive, der der Hamburgische Datenschutzbeauftragte zugeordnet ist, wird deshalb nicht beeinträchtigt; dies gilt jedenfalls dann, wenn der Senat jeweils gleichzeitig unterrichtet wird.

1.5 Neuere hamburgische Gesetze

Im 10. TB waren die verschiedenen hamburgischen Gesetze mit Datenschutzvorschriften genannt worden, die im Jahre 1991 von der Bürgerschaft verabschiedet worden waren (1.2.2). Zu weiteren Gesetzesvorlagen des Senats an die Bürgerschaft ist es bisher im Jahre 1992 nicht gekommen, obwohl seit dem Volkszählungsurteil des Bundesverfassungsgerichts von 1983 mit dessen Aussagen über die gebotenen gesetzlichen Regelungen fast 10 Jahre vergangen sind. Ich habe deshalb bereits Anfang 1992 betont, daß selbst bei großzügiger Verfahrensweise der sog. Übergangsbonus mit Ende der jetzigen Legislaturperiode der Bürgerschaft abgelaufen sein wird. Die Vorlage der verschiedenen noch ausstehenden Gesetzesentwürfe wird daher zunehmend eilbedürftig.

1.5.1 Anwendung des Hamburgischen Archivgesetzes

Zu diesem neuen Gesetz vom 21. Januar 1991 gab es Schwierigkeiten bei der Frage, in welchen Fällen die Behörden Unterlagen abzuliefern haben oder selbst vernichten dürfen (siehe auch 17.6). Vielfach verlangen wir von den Behörden, Daten gemäß den gesetzlichen Regelungen zu löschen. Zugleich ist aber die Regelung im Hamburgischen Archivgesetz zu beachten, daß Unterlagen auch dann anzubieten sind, wenn sie nach einer Rechtsvorschrift gelöscht werden müßten oder könnten.

Die Anbietungspflicht entfällt datenschutzrechtlich nur, wenn die Speicherung personenbezogener Daten von Anfang an unzulässig war. In diesen Fällen soll eine unzulässige Speicherung auch nicht im Staatsarchiv zu einer weiteren Aufbewahrung führen.

Das Staatsarchiv hat wegen dieser Auslegungsfragen ein Rundschreiben an alle Behörden gerichtet. Mit dem Staatsarchiv stimmen wir überein, daß jede Behörde sorgfältig zu prüfen hat, ob im Einzelfall Unterlagen dem Staatsarchiv anzubieten sind oder nicht.

1.5.2 Gesetzentwürfe

Die Bürgerschaft hatte mit Ersuchen vom 8./9. April 1992 den Senat aufgefordert, über die Vorlage überfälliger Gesetzentwürfe mit Regelungen zum Datenschutz im Schulwesen, Vermessungswesen, Meldewesen und beim Verfassungsschutz zu berichten. Die Vorlage und Erörterung von Referentenentwür-

fen zu diesen Themen ist daraufhin – mit Ausnahme des Meldegesetzes – deutlich beschleunigt worden. Der Senat hat angekündigt, daß er die Gesetzentwürfe in sämtlichen Fällen bis Ende 1992 beraten will.

Auf den Stand der Gesetzgebung wird in den jeweiligen Abschnitten dieses Tätigkeitsberichts eingegangen (Schulgesetz 9.1, Vermessungsgesetz 12.1, Verfassungssschutzgesetz 18.1). Nach wie vor ist offen, ob und wann das Gesundheitswesen insbesondere in den Bezirksämtern eine zeitgemäße gesetzliche Grundlage erhält, die datenschutzrechtlichen Anforderungen genügt.

1.6 Bundesdatenschutzgesetz

Nachdem das neue Bundesdatenschutzgesetz (BDSG) am 1. Juni 1991 in Kraft getreten war, mußten inzwischen zahlreiche Auslegungsfragen geklärt werden. Beispiele sind dafür die geringeren Voraussetzungen für eine Datei im Vergleich zum bisherigen Datenschutzgesetz – mit Konsequenzen z. B. für die rechtliche Einordnung der Textverarbeitung –, die erweiterten Handlungsmöglichkeiten als Aufsichtsbehörde und die neuen Regelungen für die betrieblichen Datenschutzbeauftragten. Die bewährte Kooperation mit den betrieblichen Datenschutzbeauftragten insbesondere in verschiedenen Gesprächskreisen förderte dabei eine sachgerechte Anwendung des neuen Gesetzes.

Im 10. TB (1.3) war ferner die problematische Regelung in § 24 Abs. 6 BDSG erwähnt worden, mit der in die Kontrollbefugnisse der Landesdatenschutzbeauftragten eingegriffen wird. Die Bürgerschaft hatte danach mit Ersuchen vom 8./9. April 1992 den Senat aufgefordert, über die weitere Vorgehensweise zu berichten. Dieses Problem ist inzwischen aufgrund der Stellungnahmen der Justizbehörde – auch bei den bürgerschaftlichen Ausschußberatungen zum 10. TB – zufriedenstellend geklärt; demnach kommt § 24 Abs. 6 BDSG bei der Kontrolle der Datenverarbeitung der hamburgischen Behörden nicht zur Anwendung, weil der Datenschutz insoweit abschließend durch das Hamburgische Datenschutzgesetz geregelt ist.

1.6.1 Fehlender Datenschutz bei Akten

Als gravierender Mangel des Bundesdatenschutzgesetzes hat sich herausgestellt, daß das Gesetz bei den nicht-öffentlichen Stellen und damit in der gesamten Wirtschaft grundsätzlich nur für Dateien, aber nicht für die Verarbeitung personenbezogener Daten in Akten gilt. Dies hat zur Folge, daß die Betroffenen bei Daten in Akten ihre sonst bei automatisierter Datenverarbeitung bestehenden Rechte nicht geltend machen können und auch wir als Aufsichtsbehörde nicht eingreifen können.

In letzter Zeit sind uns wiederholt Fälle bekanntgeworden, in denen Unternehmen und Organisationen die Auskunft gegenüber dem Betroffenen gerade bei sensiblen Daten mit dem Hinweis abgelehnt haben, daß sie die personenbezo-

genen Daten nur in Akten führen oder nur in nichtautomatisierten internen Dateien. Problematisch ist dies zum Beispiel bei

— Organisationen mit umfassenden Fragebögen und Tests über Mitglieder und Interessenten sowie sonstigen Unterlagen über weitere Personen (siehe 30.1)

— Arbeitgebern und Personalberatungsfirmen mit intensiven Persönlichkeitsangaben über Bewerber (siehe 29.1)

— Großvermietern oder -maklern mit eingehenden Unterlagen über Mieter und Interessenten (siehe 30.2).

Das Bundesverfassungsgericht hatte bereits im Volkszählungsurteil von 1983 erklärt, mit dem Recht auf informationelle Selbstbestimmung sei eine Rechtsordnung nicht vereinbar, „in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß." Dieser Grundgedanke gilt auch für den nicht-öffentlichen Bereich, wie das Bundesverfassungsgericht in einem Beschluß von 1991 ausgeführt hat. Danach ist das Persönlichkeitsrecht nicht nur vor direkten staatlichen Eingriffen geschützt, sondern wirkt sich auch auf die Auslegung und Anwendung privatrechtlicher Vorschriften aus.

Da Akten vielfach alphabetisch abgelegt werden oder sogar mit Namenskennzeichnung der Betroffenen genau so leicht zugänglich sind wie Dateien, ist der Ausschluß des Datenschutzrechts bei Akten im nicht-öffentlichen Bereich verfassungsrechtlich nicht mehr nachvollziehbar. Ich halte deshalb die Regelung im Bundesdatenschutzgesetz mit dem Ausschluß der Rechte der Betroffenen und der Aufsichtsbehörden für verfassungswidrig. Wenn es insoweit nicht bald zu einer Gesetzesänderung – etwa im Zusammenhang mit der bevorstehenden Umsetzung des neuen EG-Richtlinienentwurfs zum Datenschutz (siehe 1.7) – zu Gunsten der Betroffenen kommt, kann nur eine Entscheidung des Bundesverfassungsgerichts die Rechtslage klären. Zumindest müßte erreicht werden, daß den Betroffenen ein Selbstinformationsrecht als Grundlage aller übrigen Datenschutzrechte eingeräumt wird; sonst sind sie allein auf eine freiwillig gestattete Akteneinsicht angewiesen (siehe 30.1).

1.6.2 Aufsicht im nicht-öffentlichen Bereich

Auch wenn für uns als Aufsichtsbehörde die Beratungsfunktion im Vordergrund steht, kann auf die Kontrolltätigkeit nach § 38 BDSG nicht verzichtet werden. Die verbesserten Möglichkeiten der Anlaßaufsicht (siehe 10. TB, 1.3) und die regelmäßige Überwachung aller meldepflichtigen Firmen sind von uns wahrzunehmen.

Ohne eine entsprechende Stellenausstattung ist dies jedoch nicht leistbar. Deshalb war in den letzten Jahren diese Kontrolltätigkeit fast ganz unterblieben. Nach der eingehenden Erläuterung unseres Stellenbedarfs (siehe 10. TB, 2.3) hat die Bürgerschaft inzwischen eine neue Stelle für den Stellenplan 1992 bewilligt. Offen ist noch eine dringend erforderliche Stelle für einen Informatiker, da nur mit derartiger technischer Sachkunde die künftig vorgesehenen Firmenprüfungen durchführbar sind.

1.7 EG-Richtlinienentwurf zum Datenschutz

Die Kommission der Europäischen Gemeinschaften hat am 15. Oktober 1992 einen überarbeiteten Entwurf für einen „Vorschlag für eine Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten" vorgelegt. Eine Überarbeitung war notwendig, nachdem das Europäische Parlament am 10. Februar 1992 umfassende Änderungsvorschläge zum ersten Entwurf der Datenschutzrichtlinie beschlossen hatte.

Der Ministerrat muß nun den gemeinsamen Standpunkt annehmen. Danach erfolgt eine 2. Lesung des Entwurfs mit Abstimmung im Europäischen Parlament und im Ministerrat. Der Zeitpunkt für den endgültigen Beschluß der Richtlinie ist noch ungewiß.

Der nunmehr vorliegende Entwurf enthält wesentliche Änderungen des ursprünglichen Vorschlags, die eine Novellierung des BDSG unumgänglich machen werden. Der Entwurf verzichtet auf eine formelle Unterscheidung zwischen den für den öffentlichen und den privaten Bereich geltenden Regeln. Die Richtlinie betrifft die Datenverarbeitung öffentlicher Stellen – soweit die EG hierfür die Rechtsetzungsbefugnis besitzt – und privatwirtschaftlicher Organisationen ohne Differenzierung.

Der Anwendungsbereich der Richtlinie beschränkt sich auf personenbezogene Daten, die in Dateien enthalten oder dazu bestimmt sind, in Dateien aufgenommen zu werden. Unklar bleibt nach dem geänderten Entwurf, ob der nationale Gesetzgeber stärkeren Datenschutz einführen kann. Zwar haben Kommissionsbeamte den Datenschutzbeauftragten zugesichert, daß ein strengeres nationales Datenschutzniveau möglich sei. Eine entsprechende Klarstellung in Art. 5 des Entwurfs wäre aber wünschenswert.

Nicht voll berücksichtigt wurde die vom Europäischen Parlament geforderte strikte Zweckbindung für die Verarbeitung personenbezogener Daten. Auch der abgeänderte Entwurf sieht lediglich die bloße Vereinbarkeit der Zwecke der Erhebung und Verwendung vor.

Die in Art. 18 geregelte Meldepflicht geht von dem Grundsatz aus, daß jede Verarbeitung, sofern sie teilweise oder vollständig automatisiert ist, der Kontrollbehörde zu melden ist. Hervorzuheben ist, daß nach Abs. 4 der Vorschrift die Kontrollbehörde die Verarbeitungen prüfen muß, die in Hinsicht der Rechte und Freiheiten von Personen besondere Risiken aufweisen. Die Prüfung ist innerhalb einer Frist von 15 Tagen nach dem Tag der Meldung der Datenverarbeitung vorzunehmen. Daraus würde sich ein kaum realistischer Zeitdruck für eine angemessene Prüfung ergeben.

Nach Art. 19 können die Mitgliedstaaten eine Vereinfachung und Befreiung von der Meldepflicht für bestimmte Kategorien von Verarbeitungen vorsehen, die die Rechte und Freiheiten der betroffenen Personen nicht beeinträchtigen.

Art. 30 regelt die Befugnisse der Kontrollbehörde, die nach Inkrafttreten der Richtlinie und der Umsetzung in nationales Recht im privaten Bereich gelten werden. Danach verfügt die Kontrollbehörde neben Untersuchungsbefugnissen auch über effektive Eingriffsbefugnisse, wie die Anordnung der Sperrung oder Löschung von Daten, das Verbot einer Verarbeitung, die Anordnung der Vernichtung eines Datenträgers oder die sog. Verwarnung.

Nach Art. 30 wird es auch möglich sein, daß jeder Mitgliedstaat mehrere unabhängige Kontrollbehörden benennen kann. Es besteht daher kein Anlaß für eine Änderung der in Deutschland bewährten Praxis, wo gemäß dem BDSG und den Landesdatenschutzgesetzen bereits mehrere Kontrollbehörden bestehen. Allerdings ist eine weisungsunabhängige Kontrollbehörde im privaten Bereich nach dem deutschen Rechtssystem wegen des Prinzips der parlamentarischen Verantwortung für die Eingriffsverwaltung nicht möglich.

In Art. 33 wird die Rechtsetzungsbefugnis der EG-Kommission geregelt. Unklar bleibt, ob die Kommission ohne ein Gesetzgebungsverfahren die Kompetenz erhalten soll, datenschutzrechtliche Regelungen zu treffen. Eine derartige Generalermächtigung wäre abzulehnen, da die Kommission sonst außerhalb des Anwendungsbereichs der Richtlinie umfassend in alle Datenbereiche der Mitgliedstaaten eingreifen könnte.

Art. 35 des Entwurfs sieht vor, daß die Mitgliedstaaten bis zum 1. Juli 1994 die Richtlinie durch die erforderlichen Rechts- und Verwaltungsvorschriften umsetzen. Angesichts der schwierigen Sachfragen erscheint diese Frist für die Novellierung der deutschen Datenschutzgesetze sehr knapp.

1.8 Verhältnis zum Bürger

Die gesamte Arbeit der Datenschutzbehörden soll dazu dienen, den Anliegen der Bürger gerecht zu werden. Dies ist allerdings nicht immer leicht zu realisieren, weil auf Seiten der Bürger ganz unterschiedliche Erwartungen und Vorstellungen über den Datenschutz bestehen.

Viele Bürger meinen, daß wir den Zugriff auf alle Daten haben und einen Datenschutz in ihrem Sinne anordnen können. Enttäuschungen bleiben dann nicht aus, wenn wir ihnen nur Hilfe zur Selbsthilfe geben können. Andererseits wird unser Angebot vielfach gern aufgegriffen, den Bürgern die Klärung ihrer Datenschutzprobleme mit der Verwaltung und Wirtschaft soweit wie möglich abzunehmen.

Die Reaktion der Bürger fällt naturgemäß ganz unterschiedlich aus, wenn sie einerseits den Datenschutz als Behinderung bei der Durchsetzung eigener Interessen wahrnehmen oder wenn sie andererseits selbst Betroffene sind,

dabei allerdings manchmal den Datenschutz als Vorwand oder letzten Ausweg gegenüber berechtigten Belangen geltend machen wollen (siehe z.B. 21.9). Bei diesen unterschiedlichen Interessenlagen bemühen wir uns, den Grundgedanken des Datenschutzes verständlich zu machen, daß jeder selbst über die Verwendung seiner Daten bestimmen kann, soweit nicht überwiegende Interessen der Allgemeinheit oder eines Dritten entgegenstehen.

1.8.1 Eingaben

Die Bürger wenden sich weiterhin täglich mit schriftlichen Eingaben, telefonischen Anfragen und persönlichen Besuchen an die Dienststelle des Hamburgischen Datenschutzbeauftragten. Wir achten besonders darauf, daß die Eingaben in möglichst kurzer Zeit beantwortet werden. Bis Ende November 1992 gingen 308 schriftliche Eingaben zu folgenden Themen ein:

Öffentlicher Bereich	169	Nicht-öffentlicher Bereich	139
davon Sicherheitsbereich	51	davon Versandhandel	4
Gesundheits- und Sozialbereich	47	Versicherungswirtschaft	15
übrige Bereiche	71	Kreditwirtschaft	8
		Werbung	5
		Arbeitnehmer-Datenschutz	10
		SCHUFA und Auskunfteien	22
		Gesundheitswesen	23
		sonstige	52

Wie im 10. TB (1.4.2) erwähnt, werden im zweimonatigen Abstand Bürgersprechstunden zu Datenschutzfragen ohne Themenvorgabe durchgeführt. Dieses Angebot besteht zusätzlich zu der ständigen Möglichkeit, sich unmittelbar an uns zu wenden, da wir die Behandlung der Anliegen der Bürger nicht auf bestimmte Sprechtage oder Sprechzeiten beschränken. Die Bürgersprechstunden, deren Termin vorher über die Medien bekanntgegeben wird, wurden insbesondere von denjenigen Bürgern genutzt, denen es nicht um Eingaben zu akuten Problemen, sondern mehr um allgemeine Fragen zum Datenschutz geht.

1.8.2 Öffentlichkeitsarbeit

Zum Kontakt mit den Bürgern haben wir auch mit einer Reihe von Vorträgen und Referaten zu Datenschutzfragen beigetragen. Vor der Abgeordnetenversammlung des Zentralausschusses Hamburgischer Bürgervereine habe ich über „Datenschutz für die Bürger in Verwaltung und Wirtschaft – Rechte und Pflichten des Einzelnen – " gesprochen. Diese Verbindung wird u.a. dadurch fortgesetzt, daß die Einladungen zu den Bürgersprechstunden jeweils vom Zentralausschuß an die Bürgervereine zur Bekanntmachung weitergegeben werden.

In der öffentlichen Vortragsreihe über Datenschutzfragen setzte sich Prof. Brunnstein am 4. Juni 1992 mit den „Auswirkungen der aktuellen Rechnersicherheitsprobleme auf den Datenschutz" auseinander. Für den nächsten Vortrag in dieser Reihe hat erfreulicherweise Bundesverfassungsrichter Prof. Grimm bereits zugesagt.

Die vierteljährlichen Gespräche in der Dienststelle mit Vertretern von Presse und Rundfunk über aktuelle Datenschutzprobleme fanden erhebliche Resonanz in der Öffentlichkeit. Zusätzlich wurden bürgerrelevante Themen in Presse-Erklärungen behandelt, z.B. zum Datenschutz für SAGA-Mieter.

Die Broschüre „Das neue Datenschutzrecht" als Informationsschrift über das neue Hamburgische Datenschutzgesetz und das neue Bundesdatenschutzgesetz ist nach großer Nachfrage inzwischen vergriffen. Nach der Novellierung des Hamburgischen Datenschutzgesetzes soll eine neu gefaßte Broschüre herausgegeben werden; eine Broschüre über das Bundesdatenschutzgesetz wird weiterhin verteilt. Die Informationsschrift „Datenschutzkonzept für PC" hat so großen Anklang gefunden, daß mit einer 2. Auflage inzwischen insgesamt über 10 000 Exemplare verteilt worden sind.

Zu dem Entwurf einer Broschüre, die der Bundesbeauftragte federführend für die Datenschutzbehörden herausgibt, haben wir mehrere Beiträge insbesondere für Justiz und innere Sicherheit geliefert. Die neue Ausgabe dieser Broschüre „Der Bürger und seine Daten" soll 1993 erscheinen.

Zur Unterrichtung über die Rechte, die das Bundesdatenschutzgesetz den Betroffenen bei den nicht-öffentlichen Stellen gewährt, erarbeiten wir derzeit mit den anderen Aufsichtsbehörden ein einheitliches Informationsblatt zum Datenschutz im wirtschaftlichen Bereich. Mit einer allgemein verständlichen Darstellung sollen dort die bürgerrelevanten Themen besonders berücksichtigt werden.

In der Stellungnahme zum 10. TB hatte der Senat bemerkt, „daß das Datenschutzgesetz dem Hamburgischen Datenschutzbeauftragten nicht die Aufgabe zuweist, administrative Kompetenzen der Fachbehörden und Ämter wahrzunehmen". Anlaß für diese Sorge war ein zu diesem Zeitpunkt lediglich im Entwurf vorliegendes Merkblatt zum Sozialdatenschutz, das mit den betroffenen Behörden noch inhaltlich abgestimmt werden sollte.

Der Hinweis des Senates war überraschend, denn bereits in ihren Geleitworten zu unserer Broschüre „Wegweiser zum Datenschutz" hatten sowohl der damalige Präsident der Bürgerschaft als auch der Präses der Justizbehörde ausdrücklich darauf hingewiesen, daß es zu unseren Aufgaben gehört, die Bürger über ihre Rechte gegenüber dem Staat und über den Datenschutz aufzuklären.

1.9 Zusammenarbeit mit Verwaltung und Justiz

Die Behörden und auch die Gerichte befinden sich uns gegenüber oft in der Situation, ihre Verfahrensweisen zu rechtfertigen. Darunter kann das Verständnis dafür leiden, daß Verwaltung und Justiz in erster Linie selbst für die Einhaltung und Förderung des Datenschutzes verantwortlich sind. Derartigen Tendenzen kann am besten durch eine aufgeschlossene Zusammenarbeit begegnet werden, gerade auch mit einer frühzeitigen gemeinsamen Erörterung von Datenschutzfragen im Sinne eines vorgezogenen Datenschutzes (siehe dazu 1.9).

1.9.1 Datenschutz-Jahrestreffen

Zu einem offenen Meinungsaustausch soll beitragen, daß jeweils im Februar ein Datenschutz-Jahrestreffen in der Dienststelle des Hamburgischen Datenschutzbeauftragten mit den Vertretern von Bürgerschaft, Verwaltung, Justiz, Kammern, Gewerkschaften und Bürgervereinen stattfindet. Bei dem ersten Jahrestreffen am 27. Februar 1992 sprach Frau Senatorin Dr. Peschel-Gutzeit über aktuelle Datenschutzfragen wie die Beratungen zum Grundrecht auf Datenschutz.

1.9.2 Unterausschuß Datenschutz

Nachdem der 10. TB Mitte Januar 1992 veröffentlicht worden war, wurde seine weitere Behandlung erfreulich beschleunigt und konzentriert. Der Senat gab seine Stellungnahme bereits nach drei Monaten Mitte April 1992 ab, wie dies im übrigen etwa im Berliner Datenschutzgesetz als regelmäßige Frist vorgesehen ist.

Die bürgerschaftliche Beratung erfolgt nunmehr im neuen Unterausschuß Datenschutz des Rechtsausschusses. Damit können die Datenschutzfragen sinnvollerweise in einem eigenen Unterausschuß behandelt werden. Nach eingehender Erörterung wurde noch im September 1992 die Beratung abgeschlossen. Daraufhin kann die Bürgerschaft den Bericht im Plenum behandeln, bevor der folgende Tätigkeitsbericht vorgelegt wird.

Im übrigen hat sich gezeigt, daß auch die Termine der Unterausschußsitzungen erheblich zur Beschleunigung beitragen. So wurden zur Ausschußsitzung Anfang September 1992 von verschiedenen Behörden insgesamt vier seit langem erwartete Richtlinien-Entwürfe vorgelegt. Dies spricht ebenfalls für die Einrichtung des neuen Unterausschusses.

1.9.3 Richtlinie zur Beteiligung des Hamburgischen Datenschutzbeauftragten

Zur generellen Klärung hinsichtlich der Zusammenarbeit der Verwaltung mit dem Hamburgischen Datenschutzbeauftragten soll die Richtlinie des Senatsamts für den Verwaltungsdienst vom 12. November 1992 beitragen. Nachdem vorab klargestellt worden war, daß die Richtlinie nicht den Hamburgischen Datenschutzbeauftragten bindet, habe ich das Vorhaben durchaus begrüßt, gerade auch im Hinblick auf die bereits erwähnten Unklarheiten bei der Planung neuer Automationsvorhaben.

Darüber hinaus ist eine Zusammenfassung sämtlicher Beteiligungsfälle einschließlich Gesetzgebungsvorhaben, Vorbereitung von Verwaltungsvorschriften usw. hilfreich für alle Beteiligten. Ein gemeinsamer vorgezogener Datenschutz kann davon besonders profitieren. Die Richtlinie zur Beteiligung des Hamburgischen Datenschutzbeauftragten tritt am 2. Januar 1993 in Kraft.

1.9.4 Zusammenarbeit mit den Personalräten

Gelöst werden konnte ferner das Problem der Zusammenarbeit des Hamburgischen Datenschutzbeauftragten mit den Personalräten. Nach anfänglichen Meinungsverschiedenheiten habe ich schließlich im gegenseitigen Einvernehmen festgestellt, daß wir weiterhin Anfragen von Personalräten in Angelegenheiten des Datenschutzes grundsätzlich beantworten und die Leiter der Dienststellen durch Übersendung von Ausfertigungen der Antworten regelmäßig unterrichten werden.

Außerdem gehe ich zusammen mit dem Senatsamt für den Verwaltungsdienst davon aus, daß es im allgemeinen nicht unsere Aufgabe sein kann, der Frage einer etwaigen Überschreitung der Befugnisse durch Personalräte insbesondere in dienststellenintern noch nicht abschließend behandelten Angelegenheiten nachzugehen. Die Entwicklung der weiteren Praxis werden wir beobachten.

1.9.5 Bürgerschaftliche Anfragen und Eingaben

Schwierigkeiten gab es ferner wiederholt durch die Praxis des Senats, bei Antworten auf bürgerschaftliche Anfragen nicht näher auf einzelne Punkte einzugehen, „weil der Datenschutz berührt werden würde". Solche pauschalen Antworten dürfen nicht dazu führen, daß der Datenschutz als Vorwand bei der Beantwortung verwendet wird. Deshalb habe ich in einem Rundschreiben darauf hingewiesen, daß bürgerschaftliche Anfragen datenschutzrechtlich grundsätzlich selbst dann zu beantworten sind, wenn es um Berufs- oder besondere Amtsgeheimnisse geht und nicht überwiegende schutzwürdige Interessen eines Betroffenen entgegenstehen. Abweichende bundesrechtliche Regelungen – z.B. nach dem Sozialgesetzbuch – bleiben davon unberührt und gehen dem Hamburgischen Datenschutzgesetz vor.

Die Einhaltung des Datenschutzes bei der Bearbeitung von bürgerschaftlichen Anfragen und auch von Eingaben soll nun ebenfalls durch eine – mit uns abgestimmte – Durchführungsbestimmung des Senatsamtes für den Verwaltungsdienst sichergestellt werden. Der inzwischen überarbeitetete Entwurf soll nach Abschluß der Behördenbeteiligung umgehend in Kraft gesetzt werden.

1.9.6 Große Automationsvorhaben

Die wichtige Zusammenarbeit bei großen Automationsprojekten wie dem Projekt Sozialhilfe-Automation (PROSA) und dem Projekt Personalwesen (PROPERS) verlief weiterhin sehr positiv. Der Fortgang der Beratungen im Projekt Computerunterstützte Vorgangsbearbeitung bei der Polizei (COMVOR) wurde gleichfalls einvernehmlich erörtert (siehe dazu näher 17.1). Auf die Probleme bei neueren Automationsprojekten habe ich oben hingewiesen (siehe 1.1).

1.9.7 Beanstandungen

Gemäß meiner Ankündigung im 10. TB (1.4.1) konnte erfreulicherweise vermieden werden, daß es zu förmlichen Beanstandungen wegen nur formaler Versäumnisse bei der Behandlung von Datenschutzthemen kam. Derartige Verzögerungen konnten jeweils noch rechtzeitig ausgeräumt werden.

In diesem Zusammenhang ist zu erwähnen, daß das Bundesverwaltungsgericht im Februar 1992 entschieden hat, daß die Beanstandung durch einen Landesdatenschutzbeauftragten kein Verwaltungsakt ist. Zur Begründung hat das Gericht angeführt, daß mit der Beanstandung keine rechtliche Regelung verbunden ist. Infolgedessen ist gegen eine Beanstandung keine Klage vor dem Verwaltungsgericht möglich. Das Bundesverwaltungsgericht hat damit das vorangegangene Urteil des Schleswig-Holsteinischen Oberverwaltungsgerichts in dieser Sache bestätigt, das im übrigen bemerkt hatte: „Von den vorstehenden Ausführungen unberührt bleibt die Frage, ob die beanstandete Behörde gut beraten ist, der – häufig mit einer nicht unbedeutenden Öffentlichkeitswirkung ausgestatteten – datenschutzrechtlichen Beanstandung und den darin enthaltenen Empfehlungen nicht zu folgen."

1.9.8 Datenschutz bei den Gerichten

Überaus zögerlich verläuft leider die Klärung der Datenschutzkontrolle bei den Gerichten. Die Bürgerschaft hatte bereits mit Ersuchen vom 13./14. März 1991 zum 8. TB den Senat aufgefordert, dieses Thema zum Abschluß zu bringen. Dies ist jedoch auch in der Zwischenzeit trotz unserer erheblichen Vorarbeiten nicht gelungen, weil sich die Gerichte der erforderlichen Mithilfe weitgehend entzogen haben. Auf Vorschlag des Unterausschusses Datenschutz hat daraufhin der Rechtsausschuß am 16. November 1992 der Bürgerschaft ein erneutes Ersuchen an den Senat empfohlen, endlich die Kontrollzuständigkeit des Hamburgischen Datenschutzbeauftragten bei den Gerichten hinsichtlich der Verwaltungsangelegenheiten zu klären. Die Vorbereitungen in der Justizbehörde sind dazu vorangebracht worden. Die Reaktion der Gerichte bleibt abzuwarten.

In dieser Situation war es außerordentlich mühsam, eine Überwachung des Datenschutzes im Bereich der Gerichte überhaupt vorzunehmen. Schließlich ist es mit Unterstützung der Justizbehörde aber doch gelungen, jedenfalls die Verfahrensweise bei der Führung des Schuldnerverzeichnisses des Amtsgerichts Hamburg zu prüfen und datenschutzrechtlich zu bewerten (siehe 19.4).

2. Entwicklung der Dienststelle

Im Berichtsjahr hat sich die personelle Ausstattung der Dienststelle positiv entwickelt. Bereits weiter oben (1.6.2) habe ich über die verbesserte Personalsituation bei der Aufsicht im nicht-öffentlichen Bereich berichtet. Außerdem hat die Bürgerschaft eine zusätzliche Angestelltenstelle bewilligt.

Nach den personellen Veränderungen im Jahre 1991 hat es im Berichtsjahr vergleichsweise geringe Bewegungen im Personalbestand gegeben. Zu erwähnen

ist die Versetzung eines langjährigen Mitarbeiters der Aufsichtsbehörde nach Mecklenburg-Vorpommern.

Das seit Jahren anhängige Problem, die Position des Stellvertreters des Hamburgischen Datenschutzbeauftragten angemessen zu bewerten, sollte nun endlich gelöst werden. Mit einem Ländervergleich habe ich belegt, daß Hamburg gegenüber der Bewertung in allen anderen vergleichbaren Ländern deutlich benachteiligt ist.

Für den Vertretungsfall, bei dem der Stellvertreter gegebenenfalls unvorhergesehen über längere Zeit (siehe auch 10. TB, 2.1), aber auch bei normalem Ablauf in jedem Jahr mindestens mehrere Wochen die volle Verantwortung gegenüber den Mitarbeitern, den Behörden und der Wirtschaft, dem Senat und der Bürgerschaft sowie der Öffentlichkeit zu tragen hat, ist eine herausgehobene Bewertung gegenüber den anderen Referatsleitern angebracht. Dieses sonst in der Verwaltung unbestrittene Prinzip ist hier bisher nicht beachtet worden.

Für die Bewertung sind auch die 1992 bei der Stellvertretung erfolgten Änderungen zu berücksichtigen. Die Stellvertretung liegt nun bei dem Leiter des größten Referats. Zugleich wurden seine eigenen Aufgaben um die Bereiche Umweltschutz und neue Datenverarbeitungstechniken in der Wirtschaft (z.B. Electronic-cash) erweitert.

Die personellen Veränderungen machten eine Aktualisierung der Geschäftsverteilung erforderlich, die am Ende dieses Tätigkeitsberichtes abgedruckt ist. Bemerkenswert ist zum einen, daß der Anteil der Teilzeitbeschäftigten mit einem Drittel der Mitarbeiter weiterhin hoch ist. Zum anderen ist der Frauenanteil mit ca. 40 % der Gesamtzahl der Mitarbeiter unverändert groß; eines der Referate wird durch zwei teilzeitbeschäftigte Frauen im höheren Dienst geleitet.

3. Automatisierte Datenverarbeitung

3.1 Ausbau der IuK-Infrastruktur

3.1.1 IuK-Drucksache

Mit der Bürgerschaftsdrucksache 14/2148 vom 24. Juni 1992 hat der Senat die Grundlinien seiner IuK-Politik erläutert. Nach wie vor werden mit dem verstärkten Einsatz von Informations- und Datenverarbeitungstechnik Rationalisierungseffekte angestrebt. Im Vergleich mit der IuK-Drucksache aus dem Jahr 1986 (vgl. 4. TB, 3.1) legt der Senat mit seiner aktuellen Vorlage jedoch stärkeres Gewicht auf Modernisierungsaspekte, die sich nicht unmittelbar in Kosteneinsparungen bzw. rechnerisch nachvollziehbaren Leistungsverbesserungen ausdrücken lassen.

Zu dieser Umorientierung mögen auch die Erfahrungen der letzten Jahre beigetragen haben, in denen sich Einsparungserwartungen jedenfalls nicht durchgängig realisieren ließen und zugleich die Orientierung an Rationalisierungskriterien zu wenig Spielraum für fachliche und politische Schwerpunktsetzungen beließ.

In Zukunft soll die Hamburger Verwaltung mit einer einheitlich geplanten, behördenübergreifenden IuK-Infrastruktur ausgestattet werden. Soweit dies zur Aufgabenerfüllung erforderlich ist, sollen dann von jedem beliebigen mit IuK-Technik ausgestatteten Arbeitsplatz

- mit jedem anderen angeschlossenen Arbeitsplatz Nachrichten ausgetauscht werden können,
- unter Beachtung des Datenschutzes und der Datensicherheit auf jede IuK-Anwendung zugegriffen werden können, unabhängig davon, auf welchem Rechner sie zur Verfügung gestellt wird,
- externe Datenbanken und Kommunikationsdienste genutzt werden können.

Ein derartiges Konzept setzt neben der Bereitstellung von arbeitsplatzbezogener IuK-Technik auch die gegenseitige Vernetzung von Rechnern und Anwendungen in einem landesweiten Kommunikationsnetz (vgl. auch 4.3) voraus.

3.1.2 Infrastrukturansatz und Datenschutz

Der Senat betont wiederholt, daß bei dem beabsichtigten Ausbau der IuK-Infrastruktur der Datenschutz gewahrt werden soll. Gleichwohl möchten wir an dieser Stelle auf Probleme hinweisen, die im Zusammenhang mit dem beschriebenen Infrastrukturansatz stehen:

Mit dem zügigen Ausbau der Ausstattung der Arbeitsplätze mit IuK-Technik und ihrer gegenseitigen Vernetzung verringern sich die technischen und finanziellen Hemmschwellen für den Einsatz moderner DV-Technik. Am Arbeitsplatz verfügbare Rechnerleistung, verbunden mit auch für den Sachbearbeiter verhältnismäßig leicht zu handhabenden Entwicklungssystemen, lassen datenverarbeitungstechnische „Lösungen" für Probleme attraktiv erscheinen, obwohl im Grunde andere Maßnahmen angemessener wären.

Wenn sich z.B. bestimmte Verwaltungsabläufe so umständlich und aufwendig gestalten, daß sie nur noch mit Computerunterstützung bewältigt werden können, wäre es angebracht, die Ursachen für diese Schwierigkeiten zu beseitigen, anstatt vorschnell zur Computertechnik zu greifen. Dabei ist zu berücksichtigen, daß sich die Erwartungen hinsichtlich des Aufwandes bei der Verfahrensentwicklung und -pflege und hinsichtlich der Funktionalität geplanter ADV-Verfahren nicht immer realisieren lassen (vgl. z.B. 13.2). Zum Teil werden sehr zeit- und kostenaufwendige Nachbesserungen erforderlich, so daß der Technikeinsatz im Ergebnis kontraproduktiv sein kann.

Die Zielvorstellung einer umfassend mit vernetzter DV-Technik ausgestatteten Verwaltung ist auch alles andere als datenschutzfreundlich. Das Grundrecht auf informationelle Selbstbestimmung verlangt, daß bei DV-Verfahren nur die personenbezogenen Daten verarbeitet werden, die für die jeweilige Aufgabenerfüllung erforderlich sind. Die informationelle Trennung zwischen den verschiedenen Aufgaben und den dazu erforderlichen personenbezogenen Daten

wird bei einem behördenübergreifenden Netz mit einheitlichen Schnittstellen zumindest hardwaremäßig aufgehoben.

Die Verwaltung soll tendenziell zu einem informatorischen Ganzen zusammenwachsen, wobei an einem Arbeitsplatz Daten aus den verschiedensten Aufgabenbereichen verfügbar werden. Dabei wird übersehen, daß die Verwaltung keinen einheitlichen „Dienstleistungsbetrieb" darstellt, sondern sich aus informationell gegeneinander abzuschottenden Einheiten zusammensetzt. Technische Schnittstellen zwischen verschiedenen Automationsverfahren sind nur dann gerechtfertigt, wenn die wahrzunehmenden Aufgaben einen entsprechenden Informationsfluß erfordern.

Der Infrastrukturansatz wird auch mit dem Argument gerechtfertigt, nur so lasse sich mehr „Bürgernähe" erreichen, z.B. durch Konzentration verschiedener fachlicher Aufgaben bei wenigen Stellen („Bürgeramt"). Diese vermeintliche Bürgerfreundlichkeit ist mit entscheidenden Nachteilen für die Wahrung des Persönlichkeitsrechts verbunden: Wenn die Möglichkeit zum Zugriff auf alle Daten aus verschiedenen Funktionsbereichen besteht, können diese auch zum Nachteil des Bürgers zusammengeführt und verdichtet werden. Die informationelle Gewaltenteilung zwischen den verschiedenen Verwaltungseinheiten und damit das vom Bundesverfassungsgericht in seinem Volkszählungsurteil betonte Zweckbindungsgebot werden gefährdet.

Daten, die für eine bestimmte Fachaufgabe benötigt werden, dürfen grundsätzlich nicht für andere Fachaufgaben genutzt werden (Zweckbindung). Dem muß auch die IuK-Infrastruktur Rechnung tragen.

Der schnelle Ausbau der IuK-Technik bewirkt noch weitere Gefahren: Da es – insbesondere beim PC-Einsatz – keiner umständlichen Abstimmung mit anderen Stellen (ADV-Referat, Rechenzentrum) mehr bedarf, können mittlerweile auch sehr umfangreiche Datenbestände kurzfristig gespeichert und ausgewertet werden. Die Regularien des Datenschutzrechts (z.B. Meldepflicht zum Dateiregister gem. § 24 HmbDSG) und der verwaltungsinternen Richtlinien zur Gewährleistung der Ordnungsmäßigkeit der Datenverarbeitung (z.B. Freigaberichtlinie), die auf die formalisierten Abläufe in der Groß-ADV abgestellt sind, werden dabei nicht immer beachtet (vgl. z.B. 14. – Automation im Standesamt).

Noch problematischer ist es, wenn – sofern Rechner und Netze erst einmal vorhanden sind – auch größere Verfahren außerhalb der regulären und einigermaßen transparenten Abläufe der IuK-Planung implementiert werden und dabei Datenschutzaspekte nicht in ausreichendem Maße berücksichtigt werden.

Da – zumindest beim heutigen Stand der in der Verwaltung eingesetzten Technik – die auf gemeinsamer Hardwarebasis betriebenen Anwendungen nicht vollständig voneinander abgeschottet werden können, gefährdet jede technische Erweiterung, Veränderung oder Ergänzung eines für sich genommen sicheren Systems, z.B. der Anschluß zusätzlicher Rechner oder die Einrichtung neuer Schnittstellen, die Datensicherheit. Um so wichtiger sind präventive Risikoanalysen, die das Gesamtspektrum der auf einer Hardwarebasis betriebenen Anwendungen berücksichtigen (vgl. 10. TB, 3.3).

Wenn z.B. ein bislang als Arbeitsplatzrechner autonom betriebener Computer für die Teilnahme an einem elektronischen Postsystem mit einem Kommunikationsnetz verbunden wird, muß untersucht werden, welche Auswirkungen dies auf die Sicherheit aller bisher auf dem Rechner betriebenen Verfahren einschließlich der Textverarbeitung hat. Während im autonomen Betrieb Unbefugten der Zugriff auf Ressourcen einschließlich gespeicherter Daten durch Mittel der Zugangskontrolle (z.B. Unterbringung des Rechners in gesicherten Räumen) verwehrt werden konnte, müssen nun ergänzende Maßnahmen getroffen werden, um einen Zugriff über die Kommunikationsschnittstelle zu verhindern. Auch muß gewährleistet werden, daß berechtigte Benutzer des elektronischen Postsystems nur innerhalb desselben arbeiten können, ohne auf die übrigen Daten zuzugreifen. Ferner muß nachvollzogen werden können, welche Daten wann an wen übermittelt wurden (Übermittlungskontrolle gem. § 8 Abs. 2 Nr. 6 HmbDSG).

Dieser Zusammenhang macht deutlich, daß mit der zunehmenden Vernetzung ein wichtiges Argument für die Dezentralisierung von Datenverarbeitung wieder in Frage gestellt wird. Die Tatsache, daß autonom betriebene Rechner einen Mißbrauch von Daten unmöglich machen, die an zentraler Stelle gespeichert sind, wurde von den PC-Befürwortern häufig ins Feld geführt. Mit der Integration von PC in Netze werden dezentral gespeicherte Daten netzweit verfügbar und könnten prinzipiell auch mißbraucht werden. Dies gilt insbesondere angesichts der Tatsache, daß die für Netze verfügbaren Datenschutzmechanismen mit ihrer zunehmenden sonstigen Funktionalität bisher nicht schritthalten konnten.

3.1.3 Rechtliche Voraussetzungen für die Einführung von Kommunikationsnetzen

Obwohl behördenübergreifende Netze mit erheblichen Risiken für das informationelle Selbstbestimmungsrecht verbunden sind, enthält das geltende Datenschutzgesetz keine ausdrücklichen Regelungen darüber, unter welchen Voraussetzungen sie eingerichtet werden dürfen.

§ 11 HmbDSG enthält Regelungen über automatisierte Abrufverfahren, bei denen genau definierte Partner nach abstrakten Kriterien bestimmte Daten zur Erfüllung einer bestimmten Aufgabe austauschen. Wegen der besonderen Risiken ist die Einrichtung derartiger Abrufmöglichkeiten nur dann zulässig, wenn sie aufgrund einer für jedes Abrufverfahren zu erlassenden Rechtsverordnung erfolgen.

Die „Einrichtung" eines Abrufverfahrens ist als Prozeß zu verstehen, der sich aus der Herstellung der hardwaremäßigen Voraussetzungen und der Bereitstellung der für den Datenaustausch erforderlichen Software zusammensetzt, welche auch den Umfang der auszutauschenden Daten festlegt.

§ 11 HmbDSG ist für behördenübergreifende Netze, denn derartige Netze sind nicht an einzelne Verfahren gebunden, vielmehr die technischen Voraussetzungen für einen beliebigen Partner geschaffen, wobei die im Netz verfügbare Software die Übertragung jedweder Information ermöglicht.

Von einem automatisierten Abrufverfahren unterscheidet sich die berechtigte Infrastruktur auch dadurch, daß sie prinzipiell keine Kenntnis über Partner und der transportierten Daten kennt.

Legt man die § 11 HmbDSG zugrunde liegende Wertung des Gesetzgebers, daß automatisierte Informationsübermittlungen durch Einrichtung eines direkten Zugriffs auf die Daten einer anderen Stelle besonders sensible Risiken für das Grundrecht auf informationelle Selbstbestimmung begründen, auf die vorgesehene Infrastruktur an und berücksichtigt man außerdem die verfassungsgerichtlichen Vorgaben an einen auch präventiv ausgestalteten Datenschutz, so ergibt sich, daß die vorgesehene Einrichtung des Netzes einer gesetzlichen Ermächtigung bedarf.

Die potentiellen, gegenüber dem Abrufverfahren gesteigerten Risiken durch die potentielle Aufhebung der Begrenzung der beteiligten Stellen und der übermittelten Informationen gebieten im Sinne der Wesentlichkeitstheorie des BVerfG, daß ein solches Netz nur durch oder aufgrund einer ausdrücklichen gesetzlichen Ermächtigung geschaffen werden darf.

Die zu schaffende gesetzliche Regelung muß den datenschutzrechtlichen Anforderungen nicht nur in formaler Hinsicht genügen, sondern ihnen auch inhaltlich durch Beachtung des Verhältnismäßigkeitsgrundsatzes (vgl. 3.1.2) Rechnung tragen. Dies bedeutet, daß eine Vernetzung von Stellen, die personenbezogene Daten verarbeiten, nur dann zulässig ist, wenn dies von der jeweiligen Fachaufgabe her angemessen ist.

Der Anschluß an ein behördenübergreifendes Kommunikationsnetz kann ferner nur dann in Frage kommen, wenn die schutzwürdigen Belange der Betroffenen berücksichtigt werden. Rechner, auf denen besonders schutzwürdige Daten verarbeitet werden (hierzu gehören insbesondere solche Daten, die besonderen Amts- oder Dienstgeheimnissen unterliegen), dürfen nicht ohne weiteres in ein allgemeines behördenübergreifendes Kommunikationssystem einbezogen werden. Vor dem Anschluß derartiger Rechner ist durch verbindliche Vorgaben und entsprechende Maßnahmen auf den in das Netz integrierten Rechnern die Sicherheit vor unberechtigtem Zugriff zu gewährleisten (vgl. 3.1.1). Dies gilt insbesondere dann, wenn das Netz Kommunikationsschnittstellen zu öffentlichen Netzen (z.B. Datex-P) aufweist (vgl. 4.3 und 4.4).

3.2 Neuordnung der Zuständigkeiten in der Hamburger Verwaltung

Bereits Ende 1991 hat der Senat die Grundsatzentscheidung gefällt, die bislang auf verschiedene Behörden verteilten Zuständigkeiten für zentral bereitgestellte IuK-Ressourcen der Hamburger Verwaltung in einem Landesamt für Informationstechnik zusammenzuführen (zur bisherigen Zuständigkeitsverteilung vgl. 10. TB, 3.6.1).

3.2.1 Landesamt für Informationstechnik (LIT)

Das LIT soll als „übergreifendes Kompetenz- und Servicezentrum" die bisher bei der Finanzbehörde angesiedelte Datenverarbeitungszentrale (DVZ), die Abteilung Fernmeldetechnik der Baubehörde und Teile des Senatsamtes für den Verwaltungsdienst umfassen, die betriebliche Durchführungsaufgaben im IuK-Bereich wahrnehmen.

Ferner soll das LIT – zusätzlich zu den bislang von den zusammengeführten Stellen wahrgenommenen Aufgaben – unter anderem auch für die Behörden Planungs- und Beratungsaufgaben z.B. auf dem Gebiet der Technikfolgenabschätzung und des Datenschutzes wahrnehmen (vgl. 10. TB, 3.3.2).

Die Zusammenfassung der betrieblichen IuK-Aufgaben im LIT bietet die Chance, Reibungsverluste und Koordinationsprobleme zu vermeiden, die in der Vergangenheit die Erkennung und Lösung datenschutzrechtlicher Probleme – z.B. bei der Digitalisierung des behördlichen Telekommunikationsnetzes (vgl. 4.3 und 9. TB, 3.5.1) – erschwert hat. Es ist zu begrüßen, daß Datenschutzberatung und Technikfolgenabschätzung in den Aufgabenkatalog des LIT aufgenommen wurden. Es ist allerdings darauf hinzuweisen, daß die effektive Wahrnehmung der neuen Aufgaben auch personell gewährleistet werden muß. Da bisher lediglich die bei verschiedenen Behörden angesiedelten Stellen bei unverändertem Gesamtbestand zusammengefaßt werden, müssen entweder die entsprechenden Personalkapazitäten durch Umorganisation freigesetzt oder – falls dies nicht möglich ist – zusätzliche Stellen für diesen Aufgabenbereich eingerichtet werden.

3.2.2 Senatsamt für den Verwaltungsdienst

Das Senatsamt für den Verwaltungsdienst – Organisationsamt – ist weiterhin für die ministeriellen Aufgaben im IuK-Bereich auch im Bereich des Datenschutzes zuständig. Das Senatsamt wird ferner weiterhin Grundsatzaufgaben des IuK-Bereichs einschließlich der mit der Planung von IuK-Netzen zusammenhängenden Fragen wahrnehmen und die behördenübergreifende IuK-Gesamtplanung koordinieren.

3.2.3 Fachbehörden

Die Fachbehörden werden wie bisher für die Anwendungsentwicklung zuständig sein, sollen jedoch auch bei dieser Aufgabe vom LIT durch entsprechende Service-Angebote unterstützt werden.

Bedeutsam ist auch, daß die Behörden hinsichtlich der betrieblichen Durchführungsaufgaben in Zukunft von einem noch festzulegenden Zeitpunkt an nicht mehr einem Benutzungszwang des LIT unterliegen sollen. Dies hätte zur Konsequenz, daß sich Behörden prinzipiell auch bei der Durchführung ihrer Datenverarbeitung privater Auftragnehmer (z.B. kommerzieller Rechenzentren) bedienen können, diese jedoch gem. § 3 Abs. 1 HmbDSG unter besonderer Berücksichtigung der Eignung der getroffenen Datensicherungsmaßnahmen auszuwählen haben.

Ferner wird zu beobachten sein, wie sich die Öffnung des LIT als Serviceunternehmen auch für nicht-öffentliche Auftragnehmer auf die Datensicherheit auswirken wird. Neben der auch bisher schon vorzunehmenden Abschottung der Behördenverfahren untereinander muß dann auch gewährleistet werden, daß die behördliche Datenverarbeitung in besonderer Weise gegen die Datenverarbeitung für private Stellen abgeschottet ist.

3.3 Datensicherungsmaßnahmen bei Fernwartung

Zunehmende Systemkomplexität und Spezialisierung haben mittlerweile dazu geführt, daß immer mehr EDV-Anwender ihre Systeme nicht mehr selbst warten. Die regelmäßige Überwachung der Betriebsabläufe, das Einspielen neuer Programmversionen, Fehlerdiagnosen sowie deren Beseitigung erfolgen statt dessen durch externe Wartungstechniker. Um Anfahrtskosten zu vermeiden, wird die Wartung zudem in vielen Fällen nicht mehr vor Ort durchgeführt, sondern per Fernwartung. Statt im Rechnerraum zu arbeiten, ist der Wartungstechniker über Kommunikationsnetze (z.B. Telefon) an den zu wartenden Computer angeschlossen. Im Universitätskrankenhaus Eppendorf wird die Fernwartung demnächst sogar per Satellit aus den USA abgewickelt.

Die Auslagerung von regelmäßigen Wartungsarbeiten auf externe Systemspezialisten hat vielseitige Auswirkungen. Sie verstärkt nicht nur die Abhängigkeit von externen Spezialisten und gefährdet so die Ordnungsmäßigkeit der Datenverarbeitung gemäß § 10 HmbDSG, sondern bringt auch direkte datensicherungstechnische Probleme mit sich. Dies gilt insbesondere für Fernwartung: Zum einen kann der Anwender nur schwer nachvollziehen, welche Person überhaupt am anderen Ende der Telefonleitung die Fernwartung durchführt. Zum anderen kann der Wartungstechniker Daten auf externe Datenträger kopieren, auf die er im Rahmen der Wartung zugreift, ohne daß davon der Anwender überhaupt Kenntnis erhält.

Falls auf den zu wartenden Systemen personenbezogene Daten verarbeitet werden, muß diesen Risiken durch technisch-organisatorische Maßnahmen entgegengewirkt werden. Insbesondere sollte ein Zugriff auf personenbezogene Daten, deren Mißbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann (Stufe B und C des Schutzstufenkonzepts des Hamburgischen Datenschutzbeauftragten; vgl. 9. TB, 3.2.2.1), im Rahmen der Fernwartung verhindert werden.

Hierzu sind folgende Maßnahmen umzusetzen:

1. Um eine Nutzung der Fernwartungsleitung durch Unbefugte auszuschließen, sollte die Dialogverbindung nur durch die Systemexperten des zu wartenden Rechners aufgebaut werden. Der Aufbau der Verbindung sollte im Normalfall automatisch über festgelegte Rufnummern erfolgen, die im Rechner hinterlegt sind. Der Wartungstechniker muß sich darüber hinaus bei jedem Wartungsvorgang erneut durch ein vereinbartes Paßwort autorisieren.
2. Fernwartungsaktivitäten sollten lokal mitverfolgt und ggf. unterbrochen werden können. Hierzu sollte bei der verantwortlichen Stelle vor Ort ein Systemexperte vorhanden sein.
3. Der Zugriff auf personenbezogene Daten kann dadurch ausgeschlossen werden, daß Daten nur auf Verzeichnissen oder Datenträgern gespeichert werden, die während des Wartungsvorgangs nicht verfügbar sind. Werden Test- und Service-Programme des Herstellers auf der Anlage gespeichert, sind diese unter einer besonderen Kennung abzuspeichern.
4. Der Wartungstechniker sollte keinen Systemverwalterstatus erlangen können. Sofern eine physikalische Abkopplung der Dateien mit personenbezogenen Daten nicht möglich ist, ist das Einspielen von Änderungen ins Betriebssystem und in systemnahe Software durch die Fernwartungszentrale abzulehnen und ausschließlich vor Ort durchzuführen. Die Übernahme der Änderungen ist erst nach Freigabe der speichernden Stelle vorzunehmen. Anwendungsprogramme sollten nicht durch Fernwartung aktiviert werden können.
5. Sämtliche Fernwartungsaktivitäten sind revisionssicher aufzuzeichnen. Die Protokolle müssen durch entsprechende Programme ausgewertet werden können und vor Manipulation geschützt sein.
6. Der Personenbezug der gespeicherten Daten kann durch eine geeignete Anonymisierung aufgehoben werden. Hierzu sollten Namen und weitere, die Person unmittelbar identifizierende Daten von anderen anwendungsspezifischen Daten getrennt gespeichert werden. Während der Fernwartungstechniker lediglich Zugriff auf die anonymisierten Daten hat, ist die Verknüpfung der Dateien zu Anwendungszwecken nur dem berechtigten Fachpersonal erlaubt.

Darüber hinaus sind organisatorische Maßnahmen zu treffen, die weitgehend auch für traditionelle Wartung gelten. Im Wartungsvertrag sind klare Regelungen hinsichtlich der Abgrenzung der Kompetenzen und Pflichten zwischen Wartungspersonal und Personal der verantwortlichen Stelle festzuschreiben. Insbesondere sind Art und Umfang der Wartung schriftlich festzulegen. Grundsätzlich sollte das Wartungspersonal auf das Datengeheimnis verpflichtet werden. Falls personenbezogene Daten geringer Sensibilität bei der Fernwartung

übertragen werden, ist ihre Nutzung für andere Zwecke untersagen. Die Daten sind ausschließlich für Zwecke der Wartung zu verwenden. Nach Abschluß der Arbeiten sind diese Daten beim Hersteller unverzüglich zu löschen.

Sofern Fernwartung durch ausländische Stellen durchgeführt werden soll, sind stets die jeweiligen Regelungen über die Übermittlung von personenbezogenen Daten an Stellen außerhalb der Bundesrepublik Deutschland (z.B. § 17 HmbDSG, § 17 BDSG) anzuwenden. Die Fernwartungsstelle darf die Daten von sich aus nicht an Firmen weiter übermitteln, weil sonst unzulässigerweise der öffentliche Bereich endgültig im Abrufverfahren verlassen würde (§ 11 Abs. 4 HmbDSG).

Die aufgeführten Maßnahmen bilden insgesamt ein wirksames Instrumentarium, einerseits die Offenbarung von personenbezogenen Daten an außerhalb arbeitendes Personal soweit wie möglich zu vermeiden und andererseits potentielle Datenmißbräuche von vornherein einzuschränken. Dies gilt insbesondere für die in Nummer 6 beschriebene Anonymisierung von Daten. Beispielsweise wurde es im Falle des anfangs angesprochenen Universitätskrankenhauses Eppendorf gerade durch die Realisierung dieser Anforderung ermöglicht, ein datenschutzrechtlich noch vertretbares Fernwartungskonzept umzusetzen.

3.4 Fernsteuerungs- und Netzwerkkontrollprogramme

Seit geraumer Zeit sind auf dem Markt verschiedene Kommunikationsprogramme erhältlich, die der Analyse und der Fernsteuerung von Netzwerken dienen. Während sich ein Teil dieser Programme ausschließlich auf die Unterstützung des Systemverwalters bei der Konfiguration und technischen Kontrolle eines Netzwerkes beschränkt, lassen andere auch den direkten Zugriff auf die Bildschirminhalte der Benutzerstationen und sogar auf die im Leitungsnetz übertragenen Daten zu. Sie berühren damit direkt Belange des Datenschutzes und der Datensicherheit.

Diese Kontrollprogramme lassen sich aufgrund des Leistungsumfanges und ihrer Zielrichtung in drei Arten unterteilen:

— Netzwerkdiagnoseprogramme,

— Fernsteuerungsprogramme (Remote-Control-Software),

— Netzwerkanalyseprogramme.

Netzwerkdiagnoseprogramme liefern dem Systemverwalter detaillierte Informationen über alle eingeschalteten Rechner sowie die Netzwerkauslastung und führen Fehlerstatistiken. Der Systembetreuer kann von seiner Station aus die Kommunikation zwischen zwei verschiedenen Rechnern im Netzwerk testen, eventuelle Übertragungsfehler werden ihm dabei angezeigt. Die Leistungsfähigkeit dieser Programme unterscheidet sich sowohl im Umfang der ermittelbaren Kontrollinformationen als auch in deren grafischer Aufbereitung. Ein Zugriff auf den Inhalt der im Netz verwendeten Daten besteht hierbei jedoch nicht.

Fernsteuerungsprogramme gehen weit über die Leistung der reinen Diagnoseprogramme hinaus. Mit ihnen lassen sich alle Rechner im Netz fernsteuern, d.h. sowohl von einer einzigen Station innerhalb als auch über Modem/Telefonnetz von einem außerhalb des betreffenden Netzwerkes zugeschalteten Rechner bedienen.

Solche Programme funktionieren in etwa nach dem gleichem Prinzip. Auf dem für die Ausübung der Fernsteuerung vorgesehenen Rechner wird die Remote-Software installiert, auf den dem Zugriff unterliegenden Stationen wird ein einzelnes, zum Lieferumfang gehörendes Programm speicherresident geladen. Über ein SETUP-Menü legt man unter anderem fest, welcher Benutzer auf welche Station zugreifen kann. Dabei kann unterschieden werden, ob der Betrachter den Bildschirm der anderen Station nur sehen kann oder auch Eingaben vornehmen darf, also mit diesem Rechner wie mit seinem eigenen arbeiten kann. Schaltet man sich mit Hilfe der Fernsteuerungssoftware in eine Station ein, wird über das dort vorgehaltene Programm die Verbindung hergestellt.

Der aktuelle Bildschirminhalt der Station wird über die serielle Schnittstelle gesendet und am entfernten Arbeitsplatz des Betrachters komplett wieder aufgebaut. Dies geschieht im Hintergrund durch das Mitspeichern einer unsichtbaren Kopie des Bildschirmspeichers. Die am entfernten PC getätigten Tastatureingaben werden an das Netz zurückübermittelt, als ob sie von der ursprünglichen Station erfolgt wären.

Der Betrachter kann sich auch den Bildschirminhalt mehrerer Benutzer gleichzeitig ansehen, indem er sich auf seinem Schirm mehrere Fenster einrichtet. Ein Programm erlaubt auch standardmäßig den umgekehrten Fall, nämlich bis zu sechzehn Betrachter für einen Benutzerbildschirm.

Einige Programme bieten die Möglichkeit des Dateitransfers. Sie können eine Bildschirmabbildung festhalten und in eine Datei umwandeln, die sich speichern und weiterverarbeiten läßt. Ebenso ist es möglich, einzelnen Benutzern Eingaben über die Tastatur zu verwehren, damit der Betrachter den alleinigen Zugriff auf die Stationen erhält.

Reine Netzwerkanalyseprogramme bieten neben der Fülle von Informationen über die Netzwerkauslastung und -aktivitäten auch technische Unterstützung zur Lokalisierung physischer Kabelfehler. Derartige Programme können jedes einzelne Element eines beliebigen, im Netzwerk übertragenen Datenpaketes lesbar machen. Ein Programm wurde in erster Linie für den Einsatz auf tragbaren PC mit entsprechender Schnittstelle zum jederzeitigen Anschluß in ein Netzwerk, auch von außerhalb über Modem, konzipiert.

Von den Herstellern werden dem Kunden allein die Vorteile solcher Software offeriert:

— Administrationserleichterung für den Systemverwalter, z.B. Bedienung aller Stationen im Netz, ohne dafür vom Schreibtisch aufstehen zu müssen,

— perfekte Hotline zwischen Softwarehaus und Anwender (z.B. daß der Kundenberater von seinem PC aus jederzeit helfen kann und die Programmpflege auch nachts von außerhalb möglich ist),

— Arbeit von zu Hause aus am eigenen PC auf den Rechnern im Unternehmen,

— Einwahlmöglichkeit für Außendienstmitarbeiter direkt in ein entferntes Netzwerk mit Datenzugriff,

— Darstellung zu Schulungszwecken auf einem Bildschirm für mehrere Betrachter gleichzeitig.

Daß solche Programme nicht nur ein reibungsloses Funktionieren der Netze unterstützen, sondern auch die Überwachung der Benutzer und den Zugriff auf im Netz übertragene Daten ermöglichen, wird von den Herstellern in der Regel verschwiegen.

Nur wenige Fernsteuerungsprogramme bieten die Möglichkeit, es für den Benutzer erkennbar zu machen, wenn er von einem entfernten Betrachter bei seiner Bildschirmtätigkeit beobachtet wird.

Ein Programm kann beispielsweise so eingestellt werden, daß der Benutzer am Zielsystem entweder gefragt wird, ob er die Aufschaltung genehmigt, oder der Betrachter muß ein spezielles Paßwort kennen. Andere Produkte bieten die Möglichkeit, dem Benutzer die Aufschaltung an seinem Bildschirm durch ein entsprechendes Symbol anzuzeigen.

Da diese Sicherungen des Benutzers konfigurationsabhängig sind, liegt die Nutzung der Schutzmechanismen allein in der Hand des Systemverwalters. Standardmäßig ist der Schutz des Benutzers nicht vorgegeben. Für den Arbeitnehmer/Mitarbeiter ist also nicht unbedingt erkennbar, ob der Arbeitgeber/Vorgesetzte ihn bei seiner Arbeit kontrolliert.

Besondere Sicherungsmaßnahmen wegen der Risiken für die im Netzwerk enthaltenen Daten bzw. die einzelnen Benutzer sind bei solchen Produkten geboten, die nicht nur die Überwachung der zwischen zwei Stationen übertragenen Daten gestatten, sondern darüber hinaus die Kontrolle der Zugriffsrechte bei der Anmeldung von Benutzern ermöglichen. Auf diese Weise können Benutzernamen und Kennworte auf dem Weg zwischen einer Station und dem Server aufgezeichnet und lesbar gemacht werden, sofern sie nicht verschlüsselt worden sind. Der Betrachter kann sie anschließend für eigene Zwecke verwenden.

Die Pflege und Kontrolle umfangreicher Netzwerke ist häufig ohne den Einsatz von Analyse- und Steuerungsprogrammen für die Systemadministration nicht mehr leistbar. Dem Mißbrauch der beschriebenen Programme muß durch entsprechende Sicherungsmaßnahmen vorgebeugt werden. Insbesondere muß

der unbefugte Anschluß fremder Rechner mit Analyseprogrammen in das Netz über frei zugängliche Schnittstellen und Datenleitungen verhindert werden.

Da die beschriebenen Programme zur Verhaltens- und Leistungskontrolle geeignet sind, ist ihr Einsatz mitbestimmungspflichtig. Personal- und Betriebsräte sind vor der Installation solcher Produkte zu informieren, ihre Nutzung sollte streng über Betriebs- und Dienstvereinbarungen reglementiert werden.

Es ist jederzeit nachvollziehbar zu protokollieren, wer wann welche Bildschirminhalte und Daten zur Kenntnis genommen oder verarbeitet hat.

Der Benutzer muß nicht nur erkennen können, wann und wie lange eine andere Person sich auf seinen Bildschirm aufschaltet und den Inhalt zur Kenntnis nimmt, sondern er muß selbst diese Aufschaltung freigeben können.

Bei Nutzung von Fernsteuerungsprogrammen im eigenen Netzwerk müssen die vorhandenen Zugriffssicherungen wie Paßwortschutz und Rückrufautomatik unbedingt eingesetzt werden.

Fernsteuerungs- und Netzwerkanalysprogramme bieten die Möglichkeit, den „gläsernen Mitarbeiter" zu schaffen. Sie sind eine große Gefahr für den Arbeitnehmerdatenschutz. Darüber muß sich jeder, der diese Produkte einsetzen will, bewußt werden.

Mit Hilfe dieser Programme ist ein Unterlaufen der Maßnahmen zur Datensicherung gemäß § 8 HmbDSG bzw. § 9 BDSG, insbesondere der Zugriffs-, Benutzer- und Speicherkontrolle möglich, da der entfernte Betrachter bei der Aufschaltung auf eine beliebige Station im Netz und der direkten Eingabe von seinem eigenen Bildschirm aus die gleichen Zugriffsrechte erhält wie der tatsächlich angemeldete Benutzer. Auch hinsichtlich der Eingabekontrolle dürfte kaum zu gewährleisten sein, daß nachträglich überprüft und festgestellt werden kann, ob Daten zu einer bestimmten Zeit von einem angemeldeten Benutzer oder einer Person, die sich über ein Fernsteuerungsprogramm auf seinen Bildschirm aufgeschaltet hat, eingegeben worden sind.

3.5 Empfehlungen zur Benutzerverwaltung in IuK-Systemen

§ 8 HmbDSG bzw. § 9 BDSG verpflichten alle öffentlichen und nicht-öffentlichen Stellen, die personenbezogene Daten automatisiert verarbeiten, die erforderlichen technischen und organisatorischen Maßnahmen zur Sicherstellung des Datenschutzes zu treffen.

Von entscheidender Bedeutung, insbesondere für die Speicher-, Benutzer- und Zugriffskontrolle, ist dabei die Identifikation und Authentisierung der zugriffsberechtigten Personen. Dies erfolgt in der Regel über ein Paßwort, dessen Gestaltung daher besonderen Anforderungen unterliegen sollte.

Da wir bei Prüfungen von automatisierten Verfahren immer wieder auf Schwachstellen im Umgang mit Benutzerkennungen und Paßwörtern stoßen,

sollten die nachfolgend dargestellten Anforderungen zur Administration und Gestaltung erfüllt sein.

3.5.1 Administration von Benutzerkennungen

Jede zur Systembenutzung berechtigte Person muß eine eigene Benutzerkennung (User-Id) erhalten, damit die Systemaktivitäten immer zweifelsfrei und nachvollziehbar auf ihren Urheber und ihre Urheberin zurückgeführt werden können. Es dürfen keine gemeinsamen Kennungen für mehrere Personen eingerichtet werden.

Benutzerkennungen dürfen auf Dauer grundsätzlich nur für Bedienstete der datenverarbeitenden Stelle eingerichtet werden. Fremdpersonal, z.B. in Wartungsfällen, darf keinen unkontrollierten und uneingeschränkten Zugriff zum Rechner erhalten.

Benutzerkennungen dürfen nur eingerichtet werden für den Zeitraum, in dem sie tatsächlich verwendet werden. Nicht mehr benötigte Kennungen, z.B. bei Ausscheiden von Mitarbeitern, sind unverzüglich zu löschen. Sie sind zu sperren, wenn sie vorübergehend für einen längeren Zeitraum nicht benötigt werden.

Dateien, in denen Benutzerkennungen und Paßwörter verwaltet werden, sind gegen unbefugten Zugriff besonders zu schützen. Paßwörter dürfen nicht lesbar sein; sie sind verschlüsselt zu speichern.

Bei jeder Anmeldung sollte dem Benutzer angezeigt werden, wann seine Kennung zuletzt verwendet worden ist (Tag, Uhrzeit, Terminal).

Die Zugangsberechtigung über Paßwörter zum Rechner sollte systemintern auf die Tageszeiten begrenzt werden, zu denen üblicherweise autorisierte Benutzer den Zugriff benötigen.

Es sollte systemintern verhindert werden, daß die Eingabe von Kennwörtern über die Belegung von Funktionstasten erfolgen kann.

Bei längerer Nichtbenutzung des Bildschirmarbeitsplatzes unter einer noch aktiven Benutzerkennung sollte systemseitig sichergestellt werden, daß automatisch eine Abmeldung („Auto-Log-Off") oder zumindest eine Sperrung der Tastatur erfolgt (z. B. Weiterarbeiten erst nach erneuter Paßworteingabe).

Wird der Rechner mit dem öffentlichen Wählnetz verbunden, sind darüber hinaus bei der Anmeldung von Benutzern zusätzliche Sicherungsmaßnahmen zu treffen (z. B. Rückrufautomatik).

Fehlversuche bei der Eingabe von Paßwörtern sind zu protokollieren. Es muß sichergestellt sein, daß die Protokolle regelmäßig auf unberechtigte Zugriffsversuche kontrolliert werden.

Die Zahl der Anmeldeversuche ist systemseitig zu begrenzen. Nach einer entsprechenden Anzahl von Fehlversuchen muß die Benutzerkennung gesperrt

werden. Versuche, über ein Paßwort die dazugehörige Benutzerkennung zu ermitteln, lassen sich ferner durch exponentiell ansteigende Verzögerung nach erfolgter falscher Paßworteingabe verhindern.

3.5.2 Vorgaben zur Paßwortverwaltung

Paßwörter dürfen nur dem Benutzer bekannt sein, nicht schriftlich hinterlegt und keiner anderen Person mitgeteilt werden.

Der Benutzer muß das ihm bei der Ersteinrichtung vom Systemverwalter zugewiesene Paßwort durch ein neues ersetzen.

Sämtliche vom Hersteller bei Auslieferung des Rechners oder der Software vorgegebenen Standardpaßworte sind von der Systemadministration umgehend zu ändern oder zu sperren.

Die Mindestlänge eines Paßwortes sollte grundsätzlich sechs Stellen betragen. Bei Benutzern, die Zugriff auf die Betriebssystemebene oder besonders schützenswerte Daten erhalten, sollte das Paßwort mindestens acht Stellen lang sein.

Das Paßwort für die Systemadministration ist für den Vertretungsfall an einem sicheren Ort in einem verschlossenem Umschlag zu hinterlegen.

Für Paßwörter dürfen keine leicht zu erratenden Zeichenfolgen, wie Vor- oder Familiennamen, Zahlen und Daten aus dem Lebens- oder Aufgabenbereich des Benutzers, einfache Zeichenkombinationen (z.B. 4711) oder nebeneinanderliegende Tasten verwendet werden. Trivialpaßwörter sollten, wenn möglich, automatisch vom System abgewiesen werden.

Das Paßwort ist grundsätzlich aus dem gesamten verfügbaren Zeichenvorrat zu bilden. Es sollte stets alphanumerisch gestaltet werden, d.h. aus Buchstaben und Zahlen oder Sonderzeichen bestehen. Nebeneinander verwendete Groß- und Kleinschreibung erhöhen zusätzlich die Sicherheit.

Das Paßwort sollte in regelmäßigen Abständen, spätestens nach sechs Wochen, geändert werden. Der Benutzer sollte automatisch vom System zur Änderung des Paßwortes aufgefordert werden.

Es sollte systemseitig automatisch verhindert werden, daß aus Bequemlichkeit als neues Paßwort wieder ein altes gewählt wird.

3.6 Löschung und Entsorgung von Festplatten

Bei der Löschung und Entsorgung von nicht mehr benötigten magnetischen Datenträgern ist grundsätzlich zu verhindern, daß möglicherweise noch gespeicherte personenbezogene Daten Unbefugten zugänglich gemacht werden. Die gespeicherten Informationen sind derart unkenntlich zu machen, daß eine Rekonstruktion ausgeschlossen ist.

Problematisch wird diese unwiderrufliche Datenvernichtung eigentlich erst dann, wenn das Speichermedium defekt ist und sich auf die übliche Art und Weise im Rechnersystem nicht mehr ansprechen läßt. Die Formatierung des Datenträgers oder die physikalische Löschung der Daten ist nicht mehr möglich.

Als sicherste Lösung erscheint neben der gewaltsamen Zerstörung des Speichermediums in unauswertbare Partikel, z. B. Shreddern von Disketten und Magnetbändern, die Führung durch ein hinreichend starkes Magnetfeld. Letzteres ist bei Festplatten in Winchestertechnologie sehr aufwendig, da physikalisch gesehen der durch das geschlossene Gehäuse entstehende „Faraday-Käfig" überwunden werden muß. Dabei erfolgt häufig nicht nur eine unregelmäßige und unzureichende Datenlöschung, es werden vor allem die Schreib-/Leseköpfe beschädigt.

Die Magnetisierung von Festplatten kann deshalb auch nicht vom Benutzer wahrgenommen werden, wenn dieser an Garantie- oder Wartungsverträge gebunden ist. Der Auftragnehmer verweist in diesen Fällen darauf, daß der Ausbau von Festplatten aus einem Rechner zum Entfall von Reparaturansprüchen und Serviceleistungen führt.

Lassen sich technische Defekte an Festplatten vor Ort beim Kunden nicht beheben, tauscht das autorisierte Fachpersonal des Lieferanten den Datenträger aus. Die für den Kunden nicht mehr verwendbare Festplatte geht in den Besitz des Lieferanten über – mit allen darauf gespeicherten (personenbezogenen) Daten.

Defekte Festplatten lassen sich allerdings durchaus wieder reparieren und weiterverwenden oder der Inhalt läßt sich mit einigem Aufwand rekonstruieren. Es ist also keinesfalls ausgeschlossen, daß auf die gespeicherten Daten wieder zugegriffen werden kann.

Diese Problematik wird mit der voraussichtlich ab 1994 bundesweit in Kraft tretenden Elektronikschrottverordnung erheblich verstärkt. Zur Vermeidung, Verringerung und Verwertung von Abfällen gebrauchter elektrischer und elektronischer Geräte sieht der Entwurf dieser Verordnung eine Rücknahmeverpflichtung für Alt-Geräte von Handel und Herstellern vor.

Im Interesse der Sicherheit vor mißbräuchlicher Nutzung gespeicherter personenbezogener Daten ist deshalb dem Umgang mit defekten bzw. nicht mehr benötigten Speichermedien, die personenbezogene Daten enthalten, besondere Beachtung zu widmen.

Für den Fall, daß die Datenträger nicht selbst innerhalb der speichernden Stelle unwiderruflich unkenntlich gemacht werden können (z.B. aufgrund vertraglicher Bindungen), ist unter Berücksichtigung von § 11 BDSG bzw. § 3 HmbDSG ein entsprechender schriftlicher Auftrag an den Auftragnehmer zu erteilen. Die Verantwortung für die ordnungsgemäße Datenverarbeitung verbleibt beim Auftraggeber. Er sollte den Vorgang der Datenlöschung überwachen und sich vom Ergebnis überzeugen können.

In allen anderen Fällen hat vor der Weitergabe der Datenträger an den Hersteller oder ein zur Entsorgung verpflichtetes Unternehmen eine unwiderrufliche Löschung vor Ort zu erfolgen. Dies kann entweder durch vollständige Zerstörung (Disketten, Magnetbänder) geschehen oder durch Verfahren mit Einwirkung entsprechend abgestimmter Magnetfelder.

Hier bietet sich der Kauf eigens dafür konzipierter Löschgeräte an, die die Anforderungen der Datenschutzgesetze und der DIN 32757 ohne Materialvernichtung erfüllen. Sie werden inzwischen nicht mehr nur für Disketten, Magnetbänder und Magnetplatten, sondern auch für gekapselte Festplatteneinheiten angeboten. In speichernden Stellen, die über eine entsprechende Anzahl von Datenträgern verfügen, kann dabei der finanzielle Aufwand für die Beschaffung von Löschgeräten durchaus in einem angemessenen Verhältnis zur Schutzwürdigkeit der Daten stehen.

3.7 Überblick über Privat-PC

Wie wir bereits früher beschrieben haben (vgl.10. TB, 3.8), sind mit dem Einsatz von privaten PC datenschutzrechtliche Probleme verbunden. Obwohl aufgrund dieser Risiken in fast allen Behörden die Nutzung von Privatgeräten nur in Ausnahmefällen gestattet ist, sind dennoch weiterhin zahlreiche Privat-PC im Einsatz. Dies gilt insbesondere für Betriebsprüfer in den Finanzämtern, Lehrer und Staatanwälte: Während die Betriebsprüfer private Geräte bisher nur deshalb eingesetzt haben, weil entsprechende Mittel zur Beschaffung dientlicher PC nicht zur Verfügung standen, wird im Schulbereich und bei den Gerichten ein überwiegender Teil der Arbeitszeit in häuslicher Umgebung und somit auch mit privaten Arbeitsmitteln durchgeführt.

Der Diskrepanz zwischen Verbotsregelungen einerseits und zahlreichem Einsatz von Privat-PC andererseits haben wir durch praxisgerechte Lösungen entgegenzuwirken versucht. So hat die Finanzbehörde die Anschaffung dienstlicher Geräte zugesagt (vgl. 10.2). Für den Schulbereich wurde eine Regelung erlassen, die für Privat-PC zumindest einen mit dienstlichen Geräten vergleichbaren Sicherheitsstandard vorschreibt (vgl. 9.2). Für den Bereich der Staatsanwaltschaft liegt eine Regelung vor, die aber leider wiederholt nicht eingehalten wurde (vgl. 19.5).

3.8 Prüfung der Datenverarbeitungszentrale (DVZ)

Im 10. TB (3.6) hatten wir ausführlich über die Prüfung der Sicherheit der Datenverarbeitung in der DVZ berichtet. Unsere Feststellungen hatten verschiedene Sicherheitsmängel ergeben, die seitens des Organisationsamtes im wesentlichen anerkannt worden sind. Inzwischen sind – soweit technisch zur Zeit möglich – unsere Vorschläge und Forderungen aufgegriffen und überwiegend auch bereits erfüllt worden. Hierzu zählt auch die am 1. Januar 1993 in Kraft tretende Richtlinie zur Datensicherung für den Dialogbetrieb auf Zentralrechnern.

Da die Paßwortsicherung das zentrale Sicherungsinstrument gegen eine mißbräuchliche Benutzung der Datenverarbeitungszentrale und vor allem gegen einen unberechtigten Zugriff auf die dort gespeicherten Daten ist, kommt ihr eine herausragende Bedeutung für die Gesamtsicherheit der eingesetzten Systeme zu. Trotz der Zusage des Senatsamtes für den Verwaltungsdienst im April 1991, eine zwingend erforderliche Regelung zur Verwaltung von Paßwörtern zu erarbeiten, unterliegen die Benutzer der DV-Anlagen in der DVZ zur Zeit immer noch keinen ausreichenden Beschränkungen bei der Paßwortvergabe.

Wir haben deshalb das Senatsamt erneut aufgefordert, diesen Sicherheitsmangel umgehend zu beseitigen. Daraufhin wurde nunmehr der Entwurf einer Paßwortrichtlinie erstellt und den Behörden zur Stellungnahme vorgelegt. Es wird angestrebt, die Richtlinie am 1. Januar 1993 in Kraft zu setzen.

Die in ihr enthaltenen Regelungen werden allein die Paßwortverwaltung im Rahmen der Nutzung der Zentralrechner in der DVZ sowie der hieran angeschlossenen Arbeitsplatz- und Abteilungsrechner betreffen.

Auch wenn unsere Forderungen zum Paßwortmanagement sich im Rahmen der Prüfung nur auf die Nutzung der Rechner in der DVZ bezogen haben, sind wir der Auffassung, daß entsprechende Regelungen für alle anderen in den Behörden autonom eingesetzten Arbeitsplatz- und Abteilungsrechner gelten müssen.

3.9 Prüfung von UNIX-Anlagen im Senatsamt für den Verwaltungsdienst

3.9.1 Prüfungsinhalte

Im Jahr 1992 haben wir verschiedene in der Hamburger Verwaltung eingesetzte Abteilungsrechner geprüft. Darunter befanden sich auch die im Senatsamt für den Verwaltungsdienst unter der UNIX-Betriebssystemvariante SINIX betriebenen Rechner. Prüfungsgegenstand war hauptsächlich die Gewährleistung der technischen und organisatorischen Maßnahmen gemäß § 8 Hamburgisches Datenschutzgesetz.

Da das Senatsamt für den Verwaltungsdienst für die Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme in den Behörden und sonstigen öffentlichen Stellen der Freien und Hansestadt Hamburg zuständig ist und aufgrund seiner Richtlinienkompetenz einen Vorbildcharakter gegenüber anderen hamburgischen Behörden und Ämtern hat, wird im folgenden ausführlicher über die hier durchgeführte Prüfung berichtet.

Das Organisationsamt und das Personalamt benutzen gemeinsam zwei miteinander in einem lokalen Netzwerk über Ethernet-Karten verbundene Rechner, die zudem jeweils an die Zentralrechner der Datenverarbeitungszentrale (DVZ) angeschlossen sind. Aufgrund des DVZ-Anschlusses haben Benutzer mit entsprechender Zugriffsberechtigung die Möglichkeit, über Terminals der Abteilungsrechner auf DVZ-Anwendungen zuzugreifen. Über Ethernet ist auch ein im Organisationsamt installiertes Entwicklungssystem unter der UNIX-Variante AIX in das lokale Netzwerk eingebunden. An die beiden SINIX-Rechner sind insgesamt 102 Bildschirmgeräte, 21 Drucker sowie ein Personal Computer angeschlossen.

Die zentrale Administration der beiden SINIX-Rechner obliegt der Verwaltung (Referat –V–) des Senatsamtes. Hier sind drei Mitarbeiter gleichberechtigt für die Aufgaben der Systembetreuung zuständig. Es wurden im wesentlichen nur in folgenden Verfahren personenbezogene Daten verarbeitet:

— Verzeichnis der Verpflichtungsermächtigten,

— Handbuch „Mit Hamburg verbunden",

— Datenbank für die zentrale IuK-Schulung.

Darüber hinaus wurden z. T. sehr sensible personenbezogene Daten in Texten gespeichert. Dazu gehören vor allem Widerspruchsverfahren gegen Personalentscheidungen, die Bestandteil der Personalakte sind.

3.9.2 Datenschutzrechtliche Bewertung

Die Bewertung der Systemsicherheit geschah gemäß § 8 HmbDSG in Abhängigkeit von der Sensibilität der personenbezogenen Daten. Die Schutzwürdigkeit der vom Senatsamt für den Verwaltungsdienst gespeicherten Daten war sehr unterschiedlich: Zwar waren die aufgeführten Datenbank-Anwendungen als wenig sensibel einzuschätzen; gleichzeitig wurden aber im Einzelfall auf beiden Rechnern sehr sensible Texte gespeichert. Unabhängig von der Diskussion, ob Texte Dateien im Sinne des § 4 Abs. 5 HmbDSG sind, gelten die zur Sicherstellung des Datenschutzes erforderlichen technischen und organisatorischen Maßnahmen gemäß § 8 Abs. 1 HmbDSG für sämtliche in der Verwaltung verarbeiteten personenbezogenen Daten. Die in § 8 Abs. 2 HmbDSG vorgeschriebenen Kontrollen sind bei automatisierter Datenverarbeitung zu gewährleisten, auch sofern sie außerhalb von Dateien erfolgt.

Angesichts der Sensibilität der gespeicherten Daten wurde der festgestellte Sicherheitsstandard insgesamt als nicht ausreichend angesehen. Im einzelnen waren die nachfolgend dargestellten Punkte zu bemängeln:

Grundsätzlich sollten unter UNIX die Benutzer – außer dem Systemverwalter – keinen Zugang zur Betriebssystemebene (shell) erhalten. Während es Menüsteuerungen oder Anwendungsprogramme erlauben, dem Benutzer nur die Eingaben am Bildschirm zu gestatten, für die er auch berechtigt ist, unterliegt der shell-berechtigte Benutzer nur den Zugriffsbeschränkungen, die UNIX standardmäßig bietet. Eine Kontrolle der auf Betriebssystemebene verwendeten Befehle findet nicht statt.

Durch die hohe Anzahl von privilegierten Benutzern mit shell-Erlaubnis – allein 18 Kennungen waren shell-berechtigt, ohne Aufgaben der Systemverwal-

tung wahrzunehmen – war deshalb die Zugriffskontrolle (§ 8 Abs. 2 HmbDSG) nicht ausreichend realisiert. Aufgrund dieser Schwachstelle hatten mehrere Benutzer die Möglichkeit, auf sämtliche gespeicherten personenbezogenen Daten zuzugreifen.

Bei der Beurteilung der Zugriffskontrolle kommt hinzu, daß die Betriebssystemsperre, die für die offiziell nicht shell-berechtigten Benutzer vorgesehen ist, durch Ausführung von shell-Kommandos über ein standardmäßig bereitgestelltes Anwendungsprogramm umgangen werden konnte.

Eine unzureichende Zugriffskontrolle ergab sich auch aus der Tatsache, daß an zwei Benutzer außerhalb der eigentlichen Systemadministration weitreichende Systemverwalterrechte in bezug auf den Netzbetrieb vergeben waren.

Aufgrund von shell-berechtigten Benutzerkennungen ohne Paßwortschutz war die gemäß § 8 Abs. 2 HmbDSG vorgesehene Speicherkontrolle nicht ausreichend sichergestellt. Das Senatsamt verwies zwar darauf, daß diese Kennungen nur den Systemverwaltern bekannt waren und auch nur von ihnen genutzt worden sind. Allerdings waren die Kennungen identisch mit dem Nachnamen der Benutzer bzw. ihrem Leitzeichen. Der zufällige oder gar gezielte Versuch der Eingabe dieser Benutzerkennungen wurde dadurch sehr leicht gemacht.

Eine unzureichende Organisationskontrolle gemäß § 8 Abs. 2 Nr. 10 HmbDSG war zu bemängeln, da die vorhandene Systemdokumentation keine lückenlose Revision der automatisierten Datenverarbeitung zuließ. Insbesondere war aufgrund fehlender Freigabemitteilungen nicht abschließend nachvollziehbar, welche Verfahren auf den beiden Rechnern betrieben wurden. Ebenso fehlte eine Liste der shell-berechtigten Benutzer, die u. a. Auskunft über Gründe für erweiterte Zugriffsrechte gab.

Mangelnde Organisationskontrolle ergab sich nicht nur aus der lückenhaften Systemdokumentation, sondern auch aus der Tatsache, daß für die Benutzer der beiden SINIX-Rechner keinerlei Anweisungen darüber existierten, welche datenschutzrechtlichen und datensicherungstechnischen Anforderungen bestanden und wie diese in der Praxis umzusetzen waren.

3.9.3. Forderungen zur Verbesserung der Datensicherheit

Angesichts der beschriebenen datensicherungstechnischen Defizite wurden die nachfolgend beschriebenen Maßnahmen vorgeschlagen. Das Senatsamt für den Verwaltungsdienst hatte im Juli 1992 dazu Stellung genommen.

Die Systemverwaltung sollte dahingend verbessert werden, daß Kennungen ohne Paßwort ausgeschlossen werden. Das Senatsamt hat zugesagt, wie vorgeschlagen zu verfahren.

Shell-Berechtigungen dürfen nur auf ausdrücklichen Antrag unter Nennung der Gründe vergeben werden. Sie müssen nach Ablauf des Bewilligungsgrundes wieder zurückgenommen werden. Diesem Vorschlag wird im Senatsamt nunmehr entsprochen.

Die Berechtigung zur Nutzung der Kennungen „admin" und „root" sollten nur die für die Systemverwaltung zuständigen Mitarbeiter der Verwaltung (Referat –V–) haben. Personen außerhalb des für die Systemverwaltung zuständigen Bereichs dürfen keinen Superuser-Status erhalten.

Das Senatsamt sieht keine unzureichende Zugriffskontrolle darin, daß zwei fachkompetenten Mitarbeitern speziell für den Netzbetrieb Aufgaben der Systemadministration mit der dazu erforderlichen Berechtigung übertragen worden sind. Das Senatsamt hat jedoch zugesagt, zu prüfen, ob es organisatorisch zweckmäßig und wirtschaftlich vertretbar ist, diese speziellen Aufgaben organisatorisch anders wahrnehmen zu lassen. Ein Ergebnis steht noch aus.

Für jeden nicht shell-berechtigten Systembenutzer sollte nach unserer Auffassung das Ausführen von Betriebssystembefehlen über standardmäßig bereitgestellte Anwendungsprogramme unterbunden werden. Seit September 1992 ist diese Forderung erfüllt.

Der Zugriff auf sensible Daten sollte durch Vergabe restriktiver Zugriffsrechte so gesichert sein, daß der Lese- und Schreibzugriff durch unbefugte Benutzer ausgeschlossen ist. Nach Auffassung des Senatsamtes ist die vorgeschlagene Sicherung in vollem Umfang gewährleistet. Soweit Benutzergruppen eingerichtet werden, ist es seiner Meinung nach aufgrund der Aufgabenerledigung geboten, daß jeder der Gruppe auf alle Texte der Gruppenmitglieder zugreifen können muß. Darüber hinaus hat jeder Benutzer für die Textverarbeitung ein eigenes Verzeichnis, auf das nur er selbst zugreifen kann.

Die Dokumentation und Freigabe von Anwendungen soll gemäß der geltenden Freigaberichtlinie erfolgen. Das Senatsamt wird diesem Vorschlag entsprechen.

Unserer Anregung, das datenschutzrechtliche Regelungsdefizit möglichst bald durch Erlaß einer entsprechenden Dienstanweisung zu beseitigen, will das Senatsamt folgen. Die Dienstanweisung soll u.a. konkrete Regelungen beinhalten über

- Verantwortlichkeiten hinsichtlich der Systemadministration und der Systembenutzung,
- die Vergabe von Zugriffsberechtigungen,
- die Führung von Datei- und Geräteverzeichnissen,
- Wartungsarbeiten,
- die Aufbewahrung von Datenträgern,
- die Verwendung von Paßwörtern und
- Löschfristen.

Einzelne Probleme des Datenschutzes im öffentlichen Bereich

4. Telekommunikation und Neue Medien

4.1 Fangschaltungs-Beschluß des Bundesverfassungsgerichts

Das Bundesverfassungsgericht hatte sich mit der Zulässigkeit von Telefon-Fangschaltungen auseinanderzusetzen. Bei Fangschaltungen werden die Rufnummern der Anrufer bei bestimmten Anschlüssen registriert, z.B. um den Urheber von Belästigungen oder Bedrohungen ausfindig zu machen. Die Entscheidung des Bundesverfassungsgerichts vom 25. Februar 1992 hat über den konkret entschiedenen Fall hinaus grundsätzliche fernmelderechtliche und datenschutzrechtliche Bedeutung.

Das Bundesverfassungsgericht hat klargestellt, daß das Fernmeldegeheimnis des Art. 10 Abs. 1 GG nicht nur Kommunikationsinhalte, sondern auch den Kommunikationsvorgang, also auch die näheren Umstände der Kommunikation, schützt.

Nach den Feststellungen des Bundesverfassungsgerichts greift jegliche Registrierung von Telefon-Verbindungsdaten durch staatliche Stellen in das Fernmeldegeheimnis ein und bedarf folglich einer verfassungskonformen gesetzlichen Grundlage. Dies gilt auch für die Registrierung von Telefonnummern im Rahmen von Fangschaltungen.

Der Schutzbereich des Fernmeldegeheimnisses unterliegt keinen „betriebsbedingten" oder „immanenten" technischen oder organisatorischen Schranken und darf dementsprechend nicht eingriffsorientiert definiert werden. Daten über Art und Zeitpunkt der Kommunikation sind ebenso geschützt wie die Angaben über das Kommunikationsziel.

Dies schließt zwar die Aufzeichnung von geschützten Daten nicht grundsätzlich aus, doch bedarf eine derartige Datenverarbeitung einer ausdrücklichen gesetzlichen Erlaubnis. § 30 Abs. 2 Postverfassungsgesetz enthält selbst keine derartige Erlaubnis; die hier erteilte Verordnungsermächtigung für die Bundesregierung beschränkt sich auf Vorschriften zum Schutz personenbezogener Daten der am Post- und Fernmeldeverkehr Beteiligten. Eine ausdrückliche Ermächtigung zum Erlaß von Erhebungs-, Verarbeitungs- und Nutzungsregelungen für Verbindungsdaten wird nicht erteilt. Die in der Telekom-Datenschutzverordnung (TDSV) enthaltenen Erhebungs-, Verarbeitungs- und Nutzungsregelungen entbehren deshalb nach der Entscheidung des Bundesverfassungsgerichts einer ausreichenden parlamentarischen Ermächtigung.

Gleichwohl hat das Bundesverfassungsgericht die Klage abgewiesen, die sich gegen die Verwertung der bei einer Fangschaltung registrierten Daten richtete. Das Gericht hält den an und für sich verfassungswidrigen Zustand für vorübergehend hinnehmbar, da ansonsten den belästigenden Anrufen nicht wirkungsvoll entgegengetreten werden könnte. Der Gesetzgeber wird vom Bundesverfassungsgericht aufgefordert, den verfassungswidrigen Zustand durch gesetzliche Regelungen „alsbald" abzustellen.

Mit seiner Feststellung, es gebe keine ausreichende verfassungsgemäße Grundlage für die Verarbeitung der Fernmeldaten durch die Telekom, bestätigt das Bundesverfassungsgericht die von Datenschutzseite vorgebrachte Forderung, daß das Parlament die wesentlichen Entscheidungen über die Datenverarbeitung personenbezogener Daten bei der Telekommunikation selbst treffen muß und diese nicht delegieren kann (vgl. 7. TB, 3.5.2.3 ff).

Es ist zu hoffen, daß die Bundesregierung dem Spruch des Bundesverfassungsgerichts nicht nur in formaler, sondern auch in inhaltlicher Hinsicht Rechnung trägt und die in der TDSV (und auch in der für den privaten Bereich geltenden Teledienstunternehmen-Datenschutzverordnung – UDSV) vorgesehene Datenverarbeitung noch einmal kritisch – insbesondere unter dem Gesichtspunkt der Verhältnismäßigkeit – überprüft. Dabei sollte sie sich an der Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 8. März 1991 orientieren, in der datenschutzrechtliche Mindeststandards für die Regelung der Verarbeitung von Telekommunikationsdaten formuliert sind:

— Die Verbindungsdaten sind nach Ende der Verbindung grundsätzlich zu löschen; für die Erstellung von Einzelentgeltnachweisen sollten die Zielrufnummern um die letzten vier Ziffern gekürzt werden.

— Die Erstellung von „Kommunikationsprofilen", die Aussagen über das persönliche Telefonierverhalten des Bürgers und die Nutzung anderer Telekommunikationsdienste enthalten, muß ausgeschlossen sein.

— Bei der Rufnummernanzeige müssen Anrufer und Angerufener die Möglichkeit haben, diese Anzeige entweder auf Dauer oder im Einzelfall „auf Knopfdruck" zu unterdrücken.

Ausnahmen von diesen Grundsätzen, z.B. zur Aufklärung telefonischer Bedrohungen oder in Notfällen müssen ausdrücklich im Gesetz geregelt werden, für den Betroffenen transparent sein und haben sich auf das unerläßliche Maß zu beschränken. Mit dem Verhältnismäßigkeitsgrundsatz nicht zu vereinbaren ist die Regelung des § 12 Fernmeldeanlagengesetz, wonach praktisch in jeder beliebigen strafgerichtlichen Ermittlung auf gespeicherte Verbindungsdaten zugegriffen werden darf.

4.2 Prüfung der Telekommunikationsanlage des Fachbereichs Informatik der Universität Hamburg

Bei einer datenschutzrechtlichen Prüfung am 3. Februar 1992 im Fachbereich Informatik haben wir festgestellt, daß auf einem an die dortige Telekommunikationsanlage angeschlossenen Personal Computer ohne Vorliegen einer Rechtsgrundlage ungekürzte Zielrufnummern aus Ferngesprächen gespeichert wurden. Ebenfalls waren erhebliche Mängel bei den gemäß § 8 HmbDSG zu treffenden technischen und organisatorischen Maßnahmen festzustellen.

Wir haben die Baubehörde – Abteilung Fernmeldetechnik – und die Universität Hamburg mit dem Prüfungsbericht vom 2. März 1992 über das Prüfungsergebnis informiert und um Beseitigung der festgestellten Mängel gebeten. Die Abarbeitung unseres Prüfungsberichts wurde dadurch verzögert, daß es an einer klaren Zuständigkeitsregelung mangelte. Die beteiligten Stellen benötigten deshalb mehrere Monate, um hier eine Klärung herbeizuführen.

Bei einer am 4. September 1992 durchgeführten Nachprüfung haben wir festgestellt, daß – z. T. entgegen den Zusagen der beteiligten Stellen – wichtige Mängel nicht beseitigt wurden. Unsere Bedenken betrafen folgende Punkte:

Die Universität Hamburg hat entgegen ihrer zuvor gegebenen Zusage die Zielrufnummern nicht – wie in der in Vorbereitung befindlichen Telekommunikationsrichtlinie für die Hamburger Verwaltung vorgesehen – generell um die letzten drei Ziffern gekürzt. Bei der Nachprüfung am 4. September 1992 wurde festgestellt, daß nur die Rufnummern von privaten Telefongesprächen gekürzt wurden und die dienstlich angewählten Rufnummern entgegen der Zusage weiterhin ungekürzt verarbeitet wurden. Die über das erforderliche Maß hinausgehende Datenverarbeitung verstieß gegen § 13 Abs. 1 HmbDSG.

Bereits die erste Prüfung hatte verschiedene Mängel bei den technischen und organisatorischen Maßnahmen zur Sicherstellung des Datenschutzes bei dem Gebührencomputer ergeben. Auf die in unserem Prüfungsbericht aufgestellten Forderungen waren weder die Universität noch die Baubehörde inhaltlich eingegangen. Bei der Nachprüfung stellte sich heraus, daß die getroffenen Maßnahmen nach wie vor ungenügend waren und jede Person mit Zugang zum Rechner die auf diesem gespeicherten Verbindungsdaten lesen, verändern oder löschen konnte. Nicht einmal eine gesicherte Protokollierung derartiger Aktivitäten war gewährleistet. Hiermit hat die für die Absicherung des Gebührencomputers verantwortliche Baubehörde gegen § 8 HmbDSG verstoßen.

Auf Disketten, die für die Datenübernahme aus dem PC zur Weiterverarbeitung in der Datenverarbeitungszentrale (DVZ) benutzt werden, wurden die Daten unverschlüsselt gespeichert. Die Disketten wurden per Behördenpost vom Fachbereich Informatik zur Universitätsverwaltung transportiert. Datenträgerverzeichnisse wurden nicht geführt. Der Verbleib der Disketten nach ihrer Rückgabe durch die DVZ wurde nicht protokolliert.

Die Disketten sollen nach Auskunft der Universität nach „Löschung" der Daten durch den Schreibdienst neu etikettiert und für Schreibarbeiten genutzt worden sein. Inwieweit es sich bei der Löschung um eine tatsächliche oder bloß logische – und damit wiederaufhebbare – handelte, war nicht nachzuvollziehen. Die fehlende Datenträger- und Transportkontrolle verstieß gegen § 8 Abs. 2 Nummern 2 und 9 HmbDSG.

Sowohl auf dem Gebührenrechner im Fachbereich Informatik als auch in der Universität Hamburg wurden die Verbindungsdaten verarbeitet, ohne daß das dabei benutzte Verfahren ausreichend getestet und freigegeben war und ohne daß entsprechende Datenschutz- oder Datensicherheitsregelungen getroffen

waren. So wurden von den Gebührendateien Kopien angefertigt, von denen sich bei der Nachprüfung eine Kopie noch auf der Festplatte des Rechners eines Mitarbeiters der Universitätsverwaltung befand.

Diese Datenverarbeitung verstieß gegen die Regelungen der Freigaberichtlinie vom 12. März 1992, wonach die zuständige Behörde bei dem Betrieb von Arbeitsplatzrechnern die erforderlichen Regelungen, Maßnahmen und Anordnungen zu treffen hat, um die sachgerechte Nutzung der auf diesen Rechnern ablaufenden DV-Verfahren zu gewährleisten. Die Baubehörde und die Universität haben hiermit ebenfalls gegen § 8 Abs. 2 Nr. 10 HmbDSG (Organisationskontrolle) und gegen § 10 Satz 2 HmbDSG (Gewährleistung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme) verstoßen.

Nachdem wir mit Schreiben vom 24. September 1992 angekündigt hatten, die Gebührendatenverarbeitung im Fachbereich Informatik förmlich gem. § 25 Abs. 1 HmbDSG zu beanstanden, sofern die festgestellten Mängel nicht unverzüglich beseitigt würden, haben uns die Universität Hamburg und die Abteilung Fernmeldetechnik der Baubehörde Anfang Oktober 1992 mitgeteilt, daß die Gebührendatenerfassung in der TK-Anlage des Fachbereichs Informatik zunächst eingestellt werde, da der technische und organisatorische Aufwand in keinem Verhältnis zu den Gebühreneinnahmen für private Ferngespräche von vierteljährlich ca. 250 DM stehe. Allerdings sei geplant, die Gebührendatenerfassung und -auswertung des Fachbereichs zu einem späteren Zeitpunkt in die neu zu konzipierende Gebührendatenverarbeitung für die gesamte Universität einzubeziehen.

Wir haben daraufhin von einer Beanstandung abgesehen.

4.3 Digitalisierung des Behördennetzes

Die Baubehörde hat eine externe Firma damit beauftragt, ein Konzept zur Digitalisierung des Behördennetzes zu erarbeiten. Der Hamburgische Datenschutzbeauftragte hat von diesem Vorhaben erst im Nachhinein durch Vorlage des Ergebnisses erfahren und konnte so den der Studie zugrunde liegenden Auftrag nicht beeinflussen. Dies war um so bedauerlicher, als die Digitalisierung des Behördennetzes eine Vielzahl datenschutzrechtlicher Fragen aufwirft, und zwar sowohl bezüglich der Verarbeitung und des Schutzes von Verbindungsdaten als auch hinsichtlich der Schaffung der Infrastruktur zur zwischenbehördlichen Datenübermittlung (vgl. 3.1).

Die Ausführungen im Konzept zu „datenschutzrechtlichen Aspekten" sind wenig aussagekräftig und zum Teil problematisch. Entgegen der im Konzept zitierten Auffassung ist es nicht in erster Linie Ziel des Datenschutzes, „den Mißbrauch von sensitiven Daten (z.B. personenbezogenen Daten) bei Übermittlung, Speicherung und Verarbeitung zu verhindern", sondern „das Recht des einzelnen zu schützen, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen" (§1 Hamburgisches Datenschutzgesetz). Datenschutz ist

dementsprechend vor allem Gebrauchssteuerung und nicht mehr nur Mißbrauchsverhinderung.

Die Reduzierung datenschutzrechtlicher Fragestellungen auf Mißbrauchsverhinderung zieht sich durch das gesamte Konzept. Mit der Digitalisierung des Behördenfernsprechnetzes soll eine übergreifende Kommunikationsinfrastruktur auf der Grundlage eines Glasfaser-Backbone-Netzes geschaffen werden, um sämtliche dezentralen Rechner und lokalen Netzwerke vernetzen zu können.

Die Glasfaserverkabelung läßt sich überhaupt kostenmäßig nur unter der Prämisse rechtfertigen, daß sich das Übertragungsvolumen in Zukunft kontinuierlich stark erhöhen wird. Die vorgeschlagene Lösung wäre nur dann wirtschaftlich, wenn das installierte Netz zunehmend für Datenübertragung und nicht bloß als modernisiertes Fernsprechnetz genutzt würde. Die bisher bestehende finanzielle Schwelle für die Vernetzung einzelner Vorhaben würde abgesenkt, wenn auf eine mit großem finanziellen Aufwand ausgebaute Kommunikationsinfrastruktur zurückgegriffen werden kann. Damit wäre ein – datenschutzrechtlich problematischer – Druck zur Systemvernetzung verbunden.

Die einseitige Ausrichtung auf die Verhinderung eines Mißbrauchs „sensitiver Daten" führt weiterhin dazu, daß sich die „datenschutzrechtlichen" Ausführungen im Konzept auf die zu treffenden Datensicherungsmaßnahmen beschränken, ohne auf die materiell-rechtlichen Aspekte einzugehen. Doch selbst dieser – unzureichende – Ansatz wird in dem vorgelegten Konzept nicht durchgehalten. Da sich die zu treffenden Sicherungsmaßnahmen an der Schutzwürdigkeit (Sensibilität) und Gefährdung der Daten zu orientieren haben, wäre es eine selbstverständliche Mindestanforderung an das Konzept, aufzuzeigen, welche Daten zu schützen sind und wie die konkrete Gefährdungssituation ist. Daraus wären geeignete Schutzmaßnahmen abzuleiten. Eine derartige systematische Untersuchung unterbleibt. Statt dessen beschränken sich die Gutachter auf die Aufzählung einiger – offenbar zufällig ausgewählter – Sicherungsmaßnahmen, deren Zusammenhang völlig unklar bleibt.

Weder bei der Beschreibung und Bewertung des Ist-Zustandes noch im technischen Gesamtkonzept für die Digitalisierung werden Datenschutzaspekte berücksichtigt. So enthält Kapitel II, Abschnitt 2 (Entscheidungshilfen) nicht einmal einen Hinweis darauf, daß und geschweige denn welche Datenschutzaspekte für eine der diskutierten Lösungen zu beachten sind. Datenschutzgesichtspunkte werden auch nicht in das Bewertungsraster einbezogen.

Besonders bedauerlich ist es, daß das Gutachten weder die bereichsspezifischen fernmelderechtlichen Datenschutzregelungen (GG Art. 10, FAG, TDSV, UDSV), noch die hieran anknüpfende Rechtssprechung (vgl. 4.1) und Diskussion aufgreift.

4.4 Einführung eines Datenübertragungsdienstes in der Hamburger Verwaltung

Parallel zu den oben dargestellten Planungen zur Digitalisierung des Behördennetzes hat uns die Baubehörde im Sommer 1992 darüber informiert, daß ein behördenübergreifender Datenübertragungsdienst nach der Norm CCITT X.25 eingerichtet werden soll. Unter anderem soll dieser Dienst zur Verbindung der Zentralrechner in der Datenverarbeitungszentrale mit Geräten, die in den Behörden installiert sind, und zur Vernetzung von lokalen Netzwerken genutzt werden. Ferner soll der Dienst nach der Vorstellung der Baubehörde an öffentliche Wählnetze der Deutschen Bundespost Telekom (Datex-P) angeschlossen werden.

Ein solcher Dienst wirft erhebliche datenschutzrechtliche Probleme auf. Insbesondere soll von dem bislang in der Hamburger Verwaltung verfolgten Prinzip des alleinigen Anschlusses dezentraler Einheiten an die DVZ über Standleitungen abgewichen werden. Daher ist eine datenschutzrechtliche Risikoanalyse vor Vergabe entsprechender Planungen durchzuführen. Die Baubehörde hat zugesagt, eine derartige Risikoanalyse vorzunehmen und mit uns zu erörtern.

4.5 Risiken von Sprachinformationssystemen

Durch einen auch öffentlich diskutierten Hacking-Fall bei einem in Hamburg ansässigen Kreditinstitut sind wir auf Risiken von Sprachinformationssystemen aufmerksam geworden. Derartige Systeme – auch „Voice-Mail-Systeme" genannt – knüpfen in ihrer Funktionalität an herkömmliche Anrufbeantworter an. Sie gestatten die Eingabe und den Abruf von über Telefon gesprochenen Informationen. Die Steuerung des Systems – etwa das Abhören von eingegangenen Meldungen – erfolgt über die Eingabe von Zifferncodes, die über jedes Tastentelefon mit dem Frequenzwahlverfahren erzeugt werden. Auch die Berechtigung zum Abhören oder Löschen wird über die Eingabe von Zifferncodes erlangt.

Im vorliegenden Fall hatte die das System betreibende Firma die vom Hersteller standardmäßig eingestellten Codes nicht verändert, so daß Unbefugte über das öffentliche Telefonnetz in das Sprachinformationssystem eindringen und Nachrichten abhören konnten. Die Firma war dabei dem Irrtum erlegen, ihr System sei nur durch interne Telefone steuerbar, was jedoch – wie sie später feststellen mußte – nicht den Tatsachen entsprach.

Bei der Installation von derartigen Sprachinformationssystemen müssen die für den Betrieb der Anlagen zuständigen Stellen darauf achten, daß

— die vorinstallierten Steuer-Codes verändert werden,

— prinzipiell ein Abhören von Meldungen nur nach Eingabe einer Geheimzahl (PIN) in ausreichender Länge ermöglicht wird,

— die Teilnehmer über die Mißbrauchsrisiken informiert und zu einem risikominimierenden Verhalten angehalten werden,

— die Anlage in kurzen Abständen auf Unregelmäßigkeiten untersucht wird; hierzu gehört auch die Registrierung von unberechtigten Eindringversuchen.

Grundsätzlich müssen die digital gespeicherten Sprachinformationen genauso wirksam geschützt werden wie andere Formen automatisierter Datenverarbeitung. Das Kreditinstitut hat inzwischen die notwendigen Maßnahmen getroffen.

4.6 Datenschutzrechtliche Einordnung Neuer Medien

Die fortschreitende Diversifizierung im Bereich der „neuen" Medien und ihre zunehmende Verbreitung und Nutzung führt zu qualitativ neuen datenschutzrechtlichen Problemen, denen mit der herkömmlichen Datenschutz- und Fernmeldegesetzgebung nur ansatzweise begegnet werden kann.

Die Weiterentwicklung der technischen Basisstrukturen (Satellitenkommunikation, Verkabelung, Digitalisierung bestehender Netze, ISDN) geht einher mit der Einführung neuer Dienste, wobei die Grenzen zwischen Individual- und Massenkommunikation verschwimmen. Bildschirmtext und Mailboxsysteme sind typische Repräsentanten dieser relativ neuen Gattung von Diensten, die sowohl rundfunkartig Informationen an einen unbekannten Empfängerkreis weitergeben als auch die mehr oder minder direkte Kommunikation zwischen einzelnen Teilnehmern gestatten.

4.6.1 Mailbox-Systeme

Bei einer Mailbox handelt es sich um einen oder mehrere Rechner, auf denen für einzelne Teilnehmer „Postfächer" eingerichtet sind, auf die über Telekommunikationsnetze (z.B. Telefon, Datex-P, ISDN) zugegriffen werden kann. Damit wird die Möglichkeit zum direkten Informationsaustausch zwischen verschiedenen Teilnehmern eröffnet. Hinzu kommen weitere Dienstleistungen, etwa „Schwarze Bretter" – öffentliche Postfächer – die von allen Teilnehmern beschrieben oder gelesen werden können, Recherchedienste (Zugriff auf externe Datenbanken), Dienstübergänge zu anderen Telekommunikationsdiensten (z.B. Telefax).

Bereits im 8. TB hatten wir versucht, Unternehmen, die kommerziell derartige Mailbox-Dienste anbieten, in das datenschutzrechtliche Raster der Datenverarbeitung für eigene/fremde Zwecke einzuordnen (vgl. 8. TB, 4.4). Schon damals war deutlich geworden, daß sich dieses Raster nur begrenzt eignet und daß die Grenzlinie zwischen Datenverarbeitung für eigene Zwecke und Auftragsdatenverarbeitung nur schwierig zu ziehen ist. Wir waren gleichwohl zu dem Ergebnis gekommen, daß die reine Nachrichtenübermittlung (elektronische Post) als Datenverarbeitung im Auftrag anzusehen ist.

Erschwert wird die Bewertung allerdings dadurch, daß die Individualkommunikation nur ein – unter Umständen untergeordneter – Bestandteil von Mailboxleistungen ist. Ferner ist zu beachten, daß Mailboxen untereinander häufig zu offenen Netzen zusammengeschlossen sind und Daten austauschen.

Mailbox-Systeme sind – auch wenn sie sich z. T. einer anderen Technik bedienen – vergleichbar mit Bildschirmtextdiensten, für die sowohl im Länderstaatsvertrag über Bildschirmtext als auch in § 12 Telekom-Datenschutzverordnung (TDSV) und § 12 Teledienstunternehmen-Datenschutzverordnung (UDSV) bereichsspezifische Datenschutzregelungen getroffen worden sind. Daher ist weiterhin anzustreben, daß auch für Mailbox-Systeme eine klare rechtliche Regelung getroffen wird.

Thematisch gegliederte „schwarze Bretter" (Bulletin Board Systems – BBS) oder „elektronische Konferenzen" prägen Mailboxsysteme heute noch weitaus stärker als elektronische Postdienste (sogenannte Message Handling Systems – MHS), wobei die datenschutzrechtliche Problemlage bei BBS eine andere Ausprägung hat als bei MHS. Bei BBS überwiegen massenkommunikative Elemente; Hauptzweck der elektronischen „schwarzen Bretter" ist ein möglichst ungehinderter Informations- und Meinungsaustausch zwischen einer Vielzahl von Beteiligten.

Der Gesetzgeber hat darauf verzichtet, die Datenverarbeitung durch die Medien zu eigenen journalistisch-redaktionellen Zwecken in dem Maße zu reglementieren wie die sonstige kommerzielle Datenverarbeitung. Gemäß § 41 BDSG gelten hierfür nur die datenschutzrechtlichen Vorschriften über das Datengeheimnis und die technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes (§§ 5 und 9 BDSG). Entsprechend wäre das Datenschutzrecht auf die BBS nur insoweit anzuwenden, als sie Datenverarbeitung zu Abrechnung betreiben (Datenverarbeitung für eigene Zwecke) oder die Individualkommunikation gewährleisten (Datenverarbeitung für fremde Zwecke, Auftrags-DV).

In BBS sind die „Verbrauchsgewohnheiten" der Teilnehmer gegen unberechtigte Offenbarung und sonstigen Mißbrauch zu schützen, denn die Daten über tatsächlich abgerufene Informationen oder auch über „abonnierte" schwarze Bretter lassen Rückschlüsse über individuelle Vorlieben zu; die Verbindungsdaten sind entsprechend sensibel und schützenswert.

Hingegen können die Autoren von BBS-Meldungen für sich keine Vertraulichkeit beanspruchen, denn diese Meldungen sind ja für die Veröffentlichung bestimmt. Allerdings können Autoren mit dem BBS-Betreiber vereinbaren, daß ihre Identität geheim bleibt. Dann hat der Betreiber für die veröffentlichte Information einzustehen.

Bei der Individualkommunikation über Message-Handling Systeme (MHS) ist das Fernmeldegeheimnis, das sowohl die Kommunikationsinhalte als auch die näheren Umstände der Kommunikation umfaßt, zu beachten und zu schützen

(§ 10 Fernmeldeanlagengesetz – FAG). Dabei sind drei Komplexe zu unterscheiden:

— Die Vertraulichkeit der Kommunikationsinhalte ist zu wahren; durch vertragliche, technische und organisatorische Maßnahmen ist sicherzustellen, daß Unbefugte keinen Zugang zu den Kommunikationsinhalten erlangen (vgl. § 14a FAG).

— Verbindungsdaten, die Aufschluß über das Kommunikationsverhalten der Teilnehmer zulassen, sind ebenfalls geheimzuhalten; ihre Verarbeitung ist nur im Rahmen der Bestimmungen der UDSV/TDSV zulässig.

— Teilnehmerverzeichnisse gestatten einen – je nach Detaillierungsgrad unterschiedlich tiefen – Einblick in persönliche Verhältnisse der Teilnehmer. Die Betroffenen müssen die Möglichkeit haben, in öffentliche Teilnehmerverzeichnisse ganz oder teilweise nicht eingetragen zu werden (§ 10 UDSV/TDSV).

4.6.2 Videodat

Auch bei dem Dienst „Videodat" verschwimmt die Grenzlinie zwischen Massen- und Individualkommunikation.

Das System nutzt – ähnlich wie Videotext in anderen Fernsehprogrammen – die Austastlücke bei übertragenen Fernsehsendungen eines Veranstalters zur Übertragung von Informationen. Der Videodat-Empfang setzt einen speziellen Decoder voraus, der die empfangenen Signale in digitale Daten umsetzt und diese an einen angeschlossenen Personalcomputer weiterleitet.

Bei den übertragenen Daten handelt es sich um ablauffähige Computerprogramme und um Daten- und Textdateien (z.B. Börseninformationen und Nachrichtendienste), die zum Teil kostenlos und zum Teil gebührenpflichtig sind. Der Empfang bestimmter gebührenpflichtiger Dienste wird an die Leistung von Vorauszahlungen gebunden. Technisch wird die Empfangsbeschränkung dadurch realisiert, daß der Decoder erst nach Empfang der Decoder-Nummer für die abbonnierten Dienste freigeschaltet wird. Der Betreiber spricht von einem „vollständig adressierten System".

Das Konzept setzt die Registrierung sämtlicher Teilnehmer samt Decodernummern, der jeweils abbonnierten Leistungen und eine entsprechende Gebührenberechnung durch den Betreiber voraus. Durch die rundfunkartig verteilten Decodernummern wird praktisch veröffentlicht, welcher Teilnehmer welche Dienste in Anspruch nimmt. Dies setzt allerdings die Zuordnungsmöglichkeit von Nummer und Teilnehmer voraus; inwieweit diese gegeben ist, hängt von der eingesetzten Technik und ihrer organisatorischen Einbindung ab, wobei die Decodernummern mindestens auch den Händlern bekannt sein dürften, bei denen die Decoder gekauft wurden. Ferner können auch personenbezogene Daten im Rahmen der Dienste selbst übertragen werden.

Besonders kritisch ist es zu sehen, daß die für die Aufsicht privater Rundfunkveranstalter zuständigen Landesmedienanstalten über die Einspeisung entsprechender Fernsehprogramme entschieden haben, ohne von dem „blinden Passagier" Videodat zu wissen, der ebenfalls über Kabel oder terrestrisch ausgestrahlt wird. Wir werden die Entwicklung zusammen mit der Hamburgischen Anstalt für Neue Medien (HAM) weiter verfolgen.

5. Umweltschutz

5.1 EG-Richtlinie über den freien Zugang zu Informationen über die Umwelt

Der Rat der Europäischen Gemeinschaft hat in seiner Richtlinie vom 7. Juni 1990 über den freien Zugang zu Informationen über die Umwelt die Mitgliedsstaaten verpflichtet, allen natürlichen und juristischen Personen – ohne Nachweis eines besonderen Interesses – den freien Zugang zu den bei den Behörden in Schrift, Bild und Ton oder DV-Form verfügbaren umweltbezogenen Informationen zu ermöglichen.

Nach Art. 9 Abs. 1 der Richtlinie müssen die Mitgliedstaaten spätestens bis zum 31. Dezember 1992 entsprechende Rechts- und Verwaltungsvorschriften erlassen. Der vorliegende Referentenentwurf aus dem Bundesumweltministerium vom 13. Juli 1992 soll offensichtlich dieser Verpflichtung gerecht werden.

Leider hatten wir keine Möglichkeit, auf das Bund-Länder-Verfahren zur Abstimmung des Entwurfs einzuwirken, da die Umweltbehörde den Hamburgischen Datenschutzbeauftragten erst nach Fristablauf über den Referentenentwurf und die Stellungnahme Hamburgs hierzu unterrichtet hat. Dies ist umso bedauerlicher, als die zu regelnde Materie in vielen Punkten Datenschutzbezug aufweist.

5.2 Referentenentwurf eines Umweltinformationsgesetzes des Bundes

Es ist begrüßenswert, daß nun – ausgehend von der EG-Richtlinie – mit einem Umweltinformationsgesetz (UIG) das seit Jahren diskutierte Zugangsrecht des Bürgers zu Verwaltungsinformationen im Umweltbereich gewährleistet werden soll, nachdem entsprechende Initiativen – z.B. der von Hamburg eingebrachte Gesetzentwurf über ein Auskunftsrecht über Umweltdaten (Bundesrats-Drs. 172/87 vom 24. April 1987) – wiederholt gescheitert waren (vgl. 6. TB, 4.7).

Die mit dem Referentenentwurf beabsichtigte Herstellung von Öffentlichkeit ist eine Voraussetzung für die Ausübung demokratischer Kontroll-, Beteiligungs- und Mitwirkungsbefugnisse. Die Erhöhung der Transparanz von Verwaltungshandeln auf dem Gebiet des Umweltschutzes steht dem des Datenschutzes nicht entgegen; vielmehr ist die Informationsfreiheit ein notwendiges Korrelat

zum Datenschutz – nicht nur im Umweltbereich (vgl. 1.3). Leider genügt der Entwurf diesem Anspruch nur zum Teil.

5.2.1 Gesetzgebungskompetenz

Der Gesetzentwurf regelt in § 2 das Informationszugangsrecht sowohl gegenüber den Behörden des Bundes als auch gegenüber denen der Länder und Gemeinden und sonstigen Personen des öffentlichen Rechts. Der Bund verfügt jedoch beim Informationszugangsrecht in den Ländern und Kommunen weder über eine ausschließliche noch über eine konkurrierende Regelungskompetenz, so daß es den Ländern obliegt, im Rahmen ihrer Gesetzgebungskompetenz nach Art. 70 GG den Verpflichtungen der EG-Richtlinie Rechnung zu tragen.

Wir halten es daher für erforderlich festzulegen, daß dieses Gesetz für öffentliche Stellen der Länder und der Kommunen nur gilt, soweit das Informationszugangsrecht nicht durch Landesgesetz geregelt ist.

5.2.2 Informationsanspruch

Nach § 4 Abs. 1 des Entwurfs kann der Informationszugang nach Wahl des Antragstellers entweder durch Auskunftserteilung oder dadurch erfolgen, daß „Informationsträger" mit den „begehrten Informationen über die Umwelt" zur Verfügung gestellt werden.

Der im Referentenentwurf vorgesehene Zugang zu „Informationsträgern" mit Umweltinformationen bleibt weit hinter einem Akteneinsichtsrecht in Umweltakten zurück, denn das Zugangsrecht bezieht sich ausschließlich auf die ausdrücklich „begehrten" Informationen und nicht auf die Entwicklungen, die diesen Informationen zugrunde liegen.

Doch selbst das Wahlrecht zwischen Auskunftserteilung und Zugang zu Informationsträgern wird durch die vorgesehenen Einschränkungen faktisch ausgehöhlt: Bei aufwendigen Aussonderungsarbeiten oder wenn die Auskunft „auch ohne den Informationsträger verständlich wäre", reduziert sich der Informationsanspruch auf bloße Auskunftserteilung.

5.2.3 Beschränkungen des Informationsanspruchs

Im Gegensatz zu der in der Präambel der EG-Richtlinie vorgesehenen Begrenzung der Informationsverweigerung auf ganz bestimmte, genau bezeichnete Fälle übernimmt § 5 des Referentenentwurfs generalklauselartig den gesamten in Art. 3 der EG-Richtlinie enthaltenen Katalog möglicher nationaler Ausnahmen und überschreitet ihn sogar zum Teil.

So soll ein Informationszugangsanspruch unter anderem generell dann nicht bestehen, soweit das Bekanntwerden der Informationen die internationalen Beziehungen, die Landesverteidigung, die innere Sicherheit oder die Vertraulichkeit von Behördenberatungen beeinträchtigen kann. Nicht die tatsächliche Gefährdung ist hier ausschlaggebend, sondern die bloße Möglichkeit ihres Eintritts.

Besonders kritisch ist es zu sehen, daß auch Informationen aus verwaltungsbehördlichen Verfahren, deren Entscheidung gerichtlich überprüft werden kann, generell von dem Informationszugang ausgeschlossen werden sollen. Damit würde praktisch für das gesamte laufende nach außen gerichtete Verwaltungshandeln – seien es die Bearbeitung von Bauanträgen, sonstige Prüfungs- und Genemigungsaktivitäten oder die Vorbereitung von Planfeststellungsverfahren – kein Informationszugangsanspruch bestehen. Es ist sehr zweifelhaft, ob diese Ausnahmeregelung mit der EG-Richtlinie zu vereinbaren ist.

Gerade die aktuellen Daten, die anläßlich von verwaltungsbehördlichen Verfahren anfallen, sind besonders geeignet, Interessierten zugänglich gemacht zu werden. Werden diese Daten – wie im Referentenentwurf – vom Informationszugangsrecht ausgenommen, wird damit der mit der EG-Richtlinie angestrebte Zweck, ein unbürokratisches Recht für jedermann auf Umweltinformationen zu schaffen, grundsätzlich in Frage gestellt.

5.2.4 Unterrichtung der Öffentlichkeit

§ 8 des Referentenentwurfs verpflichtet Bund und Länder, die Öffentlichkeit regelmäßig über den Zustand der Umwelt zu unterrichten. Zur Wahrnehmung des Informationszugangsrechts halten wir es für geboten, die Unterrichtungspflicht auch darauf auszudehnen, bei welchen Behörden Informationen über die Umwelt bereitliegen (entsprechend den Regelungen zum Dateiregister in der Datenschutzgesetzgebung – vgl. § 24 HmbDSG). Nur so kann der Bürger seinem Informationsrecht wirksam Geltung verschaffen.

5.3 Hamburgisches Abwassergesetz

Der Senat hat den Entwurf für die Änderung des Hamburgischen Abwassergesetzes (HmbAbwG) in die Bürgerschaft eingebracht. Während der Referentenentwurf – entsprechend der Regelung in § 101 Hamburgisches Wassergesetz – ein umfassendes Auskunftsrecht hinsichtlich der Anforderungen an die Einleiter von Abwässer sowie über die Menge und Beschaffenheit der Abwasserströme vorsah, hat der Senat auf diese Vorschrift – zumindest vorläufig – verzichtet. Mit der Herausnahme der Offenlegungsvorschrift aus dem HmbAbwG wurde die Chance vertan, eine angemessene bereichsspezifische Regelung über den freien Informationszugang zu Abwasserdaten treffen.

Es bestehen starke Zweifel, ob mit dieser Entscheidung – wie beabsichtigt – Kosten in Zusammenhang mit der Auskünftsbearbeitung vermieden werden, da mit dem Umweltinformationsgesetz ohnehin entsprechende Auskunftsverpflichtungen und Informationsersuchen auf die zuständige Behörde zukommen (vgl. 5.2).

5.4 Referentenentwurf für ein Hamburgisches Bodenschutzgesetz

Die Umweltbehörde hat im Juni 1992 ein Bodenschutzkonzept und – als Anhang hierzu – den Entwurf für ein Hamburgisches Bodenschutzgesetz vorgelegt. Hiervon haben wir erst indirekt über die Justizbehörde erfahren und konnten innerhalb der von der Umweltbehörde gesetzten Frist nicht hierzu Stellung nehmen.

Inhaltlich ist der Gesetzentwurf problematisch, denn er enthält eine – bezogen auf den Bodenschutz – praktisch unbegrenzte Datenverarbeitungsbefugnis. Auch bei der Einrichtung eines Bodenschutzkatasters, gegen das prinzipiell keine datenschutzrechtlichen Bedenken bestehen, muß das Recht auf informationelle Selbstbestimmung gewahrt bleiben.

Weder in der Erhebungsnorm noch in der Vorschrift über die weitere Verarbeitung von Daten wird der Versuch unternommen, die zur Aufgabenerfüllung erforderlichen Daten zu definieren. Dadurch wird die mit bereichsspezifischen Vorschriften bezweckte Zielsetzung verfehlt. Gerade im Hinblick auf die weitgehenden Erhebungsbefugnisse – bis hin zur Einschränkung der Unverletzlichkeit der Wohnung (Art. 13 Grundgesetz) – ist eine präzise Beschreibung der zu erhebenden Daten unverzichtbar.

Des weiteren fehlt die Festlegung, bei wem unter welchen Umständen welche Daten erhoben werden dürfen. Zu fordern ist, daß auch hier von dem Grundsatz der Erhebung der Daten beim Betroffenen mit seiner Kenntnis auszugehen ist (§ 12 Abs. 2 Satz 1 Hamburgisches Datenschutzgesetz). Demgegenüber sollen mit dem Gesetzentwurf in einem Rundumschlag alle Behörden, Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts pauschal verpflichtet werden, der für den Bodenschutz zuständigen Behörde auf Antrag sämtliche Akten und Daten auch dann zu übermitteln, wenn sie für andere Zwecke erhoben worden sind.

Auch die im Entwurf enthaltene umfassende Zweckdurchbrechungserlaubnis, wonach die zuständige Behörde alle ihr zugänglichen Daten einschließlich der Daten, die ohne Kenntnis der Betroffenen oder zu anderen Zwecken erhoben wurden, verarbeiten (also speichern, übermitteln und nutzen) darf, widerspricht dem verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz.

Der Gesetzentwurf muß daher grundlegend überarbeitet werden. Dabei sollten die Erfahrungen aus der Überarbeitung des Entwurfs des Vermessungsgesetzes genutzt werden (vgl. 12.1). Dies bietet sich schon deshalb an, weil sich die von den Regelungen im Bodenschutzgesetz betroffenen Daten teilweise mit den im Vermessungsgesetz genannten Daten überschneiden.

5.5 Automationsvorhaben abfallwirtschaftliche Planung

Die Hamburger Stadtreinigung hat uns im August 1992 von dem Vorhaben informiert, eine Datenbank für abfallwirtschaftliche Planungsmaßnahmen im

Zusammenhang mit der Getrenntmüllsammlung einzurichten. Die Datensammlung soll für die Ermittlung abfallwirtschaftlicher Kenndaten, z.B. der detaillierten Aufschlüsselung der abschöpfbaren Wertstoffmengen, genutzt werden, um auf dieser Grundlage eine entsprechende Sammel- und Transportlogistik aufzubauen.

In der Datenbank sollen Angaben über den Grundeigentümer und ggf. Verwalter, Geschoßzahl, Anzahl der Wohnungen im Gebäude, Baualter und -form, Nutzungsform des Siedlungsgebiets, Sozialwohnungs- und Ausländeranteil je Baublockseite und Anzahl der Einwohner je Gebäude, Anzahl der Müllgefäße, Gebührenklasse und Leerungshäufigkeit zusammengefaßt werden. Die Daten stammen aus der Gebührenschuldnerdatei der Stadtreinigung, der Stromzählerdatei der Hamburgischen Electricitäts-Werke, dem Nutzungsartenkatalog des Liegenschaftsamtes und dem Melderegister.

Gemäß § 5 Hamburgisches Datenschutzgesetz ist die Verarbeitung personenbezogener Daten nur aufgrund einer Rechtsvorschrift oder bei Einwilligung des Betroffenen zulässig. Mangels einer bereichsspezifischen Regelung kommt als Rechtsgrundlage § 30 Hamburgisches Datenschutzgesetz (Datenverarbeitung für Planungszwecke) in Betracht, allerdings nur dann, wenn der Planungszweck auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

Die Stadtreinigung hat zugesagt, die Datei gemäß § 30 HmbDSG nur zu Planungszwecken und keinesfalls für den Verwaltungsvollzug zu verwenden. Ferner werden die Vermieter-/Verwalterangaben gelöscht, sofern die Adresse des Behälterstandortes mit der Anschrift des Gebührenschuldners übereinstimmt. Gegen das Vorhaben bestehen unter diesen Voraussetzungen keine Bedenken.

5.6 Nachtrag zur Prüfung der Stadtreinigung

Wie bereits im 10. TB (12.3) geschildert, hatten wir im letzten Quartal 1990 die Datenverarbeitung der Stadtreinigung geprüft. Erfreulicherweise sind die damaligen Sicherheitsdefizite mittlerweile vom Landesbetrieb zu unserer Zufriedenheit behoben worden. Die zwischenzeitlich aufgetretenen Unstimmigkeiten hinsichtlich des Zeitplans für die Umsetzung der vorgeschlagenen Sicherungsmaßnahmen sind damit ausgeräumt.

6. Sozialwesen

6.1 Entwurf des Zweiten SGB-Änderungsgesetzes

Bereits im 10. TB (6.5) haben wir kurz über den Entwurf für das Zweite SGB-Änderungsgesetz (2. SGBÄndG-E) berichtet. Er sieht für den Sozialleistungsbereich bereichsspezifisch umfassende Regelungen der Datenerhebung, -verarbeitung und -nutzung vor und paßt zugleich die Terminologie des Sozial-

gesetzbuches (SGB) der des Bundesdatenschutzgesetzes (BDSG) an. Darüber hinaus sieht er auch inhaltliche Änderungen einzelner Vorschriften in den besonderen Teilen des SGB (SGB-IV bis SGB-VIII) vor. Der Entwurf ist in der Zwischenzeit mehrfach überarbeitet worden. Leider ist er auch in seiner letzten Fassung sehr unzureichend.

Der Gesetzentwurf stellt – gemessen an der noch geltenden Rechtslage – einen Rückschritt dar. Er führt nicht dazu, daß nur unter eingeschränkten Voraussetzungen eine Datenerhebung, -verarbeitung und -nutzung erfolgen darf; vielmehr ermöglichen die Regelungen dieses Entwurfes eine fast schrankenlose Datenerhebung, -verarbeitung und -nutzung innerhalb des Sozialleistungsbereichs. Das beginnt damit, daß die Erhebung der Daten in vielen Fällen ohne Mitwirkung und Kenntnis der Betroffenen erfolgen darf. Wenn die Daten einmal erhoben sind, dürfen sie nicht nur für die ursprünglichen Zwecke, sondern für eine Vielzahl anderer Zwecke verarbeitet und genutzt werden, die die Betroffenen nicht kennen. Lediglich für Datenübermittlungen bleibt es im wesentlichen bei den bisherigen einschränkenden Regelungen.

Ein solch umfassender „Sozialdatenpool" widerspricht den Anforderungen, die das Bundesverfassungsgericht 1983 im Volkszählungsurteil aufgestellt hat. Will man die Sozialleistungsberechtigten nicht zum Objekt beliebiger und nicht nachvollziehbarer Aktivitäten der Leistungsträger degradieren, sondern als mündige Bürger mit einem Rechtsanspruch auf Sozialleistungen akzeptieren, bedarf es einer erheblichen Korrektur dieser Regelungen.

Neben diesem grundsätzlichen Mangel, der konzeptionelle Änderungen des Gesetzentwurfes erforderlich macht, sind auch noch viele Mängel im Detail vorhanden. Beispielsweise enthält der Entwurf Regelungen für Übermittlungen aus dem Melderegister, obwohl diese im SGB wirklich nichts zu suchen haben. Völlig unannehmbar ist es zudem, daß in dem empfindlichen Bereich der Sozialleistungsträger, wie zum Beispiel Krankenkassen, bei Datenverarbeitung in Akten nur eine Anlaßkontrolle erfolgen soll. Damit wäre die Datenschutzkontrolle durch die Datenschutzbeauftragten nur in schwächerer Form möglich als bei anderen öffentlichen Stellen, wie beispielsweise Schulen.

Wir haben die Einzelheiten dieses umfangreichen Änderungsbedarfs der Behörde für Arbeit, Gesundheit und Soziales (BAGS) mitgeteilt und hoffen, daß diese sich gegenüber dem Bundesminister für Arbeit und Sozialordnung nachdrücklich für entsprechende Verbesserungen einsetzt.

Skepsis ist jedoch angebracht, was die ernsthafte Bereitschaft des Bundesgesetzgebers zur Berücksichtigung datenschutzrechtlicher Belange angeht. Während nämlich bereits der 2. SGBÄndG-E die Datenverarbeitung auch in der Gesetzlichen Krankenversicherung ändern soll, enthält der wesentlich jüngere Entwurf des Gesundheits-Strukturgesetzes-1993 (s.u. 21.2) zu teilweise denselben Vorschriften ebenfalls Änderungen, die aber über den im 2. SGBÄndG-E vorgesehenen Umfang deutlich hinausgehen.

Allerdings ist auch zweifelhaft, ob beide Gesetzentwürfe überhaupt miteinander koordiniert sind. Teilweise sollen dieselben Vorschriften in redaktionell unterschiedlicher Weise geändert werden, ohne daß inhaltliche Abweichungen bestünden.

6.2 Projekt Sozialhilfe-Automation (PROSA)

In der datenschutzrechtlichen Diskussion um PROSA hat die Behörde für Arbeit, Gesundheit und Soziales (BAGS) zur Erhebung der Dauer der Arbeitslosigkeit (siehe 10. TB, 6.1.1) ein überzeugendes Konzept vorgelegt, nach dem die Dauer der Arbeitslosigkeit dann erhoben wird, wenn im Einzelfall eine Arbeitsaufnahme zumutbar ist. Nicht erhoben wird sie danach z.B. bei Alleinerziehenden mit Kindern bis zum vollendeten 3. Lebensjahr und bei Personen vom vollendeten 60. Lebensjahr an.

Die statt der Erhebung der Staatsangehörigkeit relevanten Statusgruppen haben sich gegenüber der Berichterstattung im letzten TB (6.1.5) leicht verändert. Es sind dies jetzt die Statusgruppen Asylbewerber, Asylfolgeantragsteller, Asylberechtigte, Kontingentflüchtlinge, de-facto-Flüchtlinge, Aussiedler, Aussiedlerbewerber und sonstige Ausländer. Das ist ebenfalls ein datenschutzrechtlich tragbares Ergebnis.

Zu der im Hinblick auf die statistischen Anforderungen notwendigen Datenauswertungskonzeption haben wir die BAGS gebeten, das dazu bislang lediglich vorliegende unabgestimmte Papier fortzuschreiben und dabei die für die jeweiligen Statistikbedarfe vorhandenen Rechtsgrundlagen anzugeben. Eine inhaltliche Diskussion hierzu ist aber nach wie vor nicht erfolgt.

Im übrigen haben wir gegenüber PROSA die Frage aufgeworfen, wie der datenschutzrechtliche Auskunftsanspruch der Hilfeempfänger praktisch realisiert werden soll. Dieser Anspruch umfaßt nämlich nicht nur die Auskunft über die gespeicherten Daten, sondern auch die Auskunft über Herkunft und Empfänger dieser Daten. Er gilt zudem auch für die bei PROSA in Akten gespeicherten Daten. Diese Frage ist bei PROSA noch nicht abschließend geklärt. Über die automatisiert gespeicherten Daten wird dem Hilfeempfänger zwar auf Antrag ein Ausdruck sämtlicher Bildschirminhalte zur Verfügung gestellt. Dieser enthält jedoch keine Angaben über Herkunft und Empfänger der Daten.

Ungeklärt ist auch, wie Übermittlungen von PROSA an andere Stellen dokumentiert werden. Die Zulässigkeit und Erforderlichkeit dieser Übermittlungen muß im Einzelfall im nachhinein überprüfbar sein. Von besonderer Bedeutung ist dies bei Übermittlungen, die ohne entsprechendes Ersuchen erfolgen, z.B. nach dem Ausländergesetz.

6.3 Projekt Jugendamts-Automation (PROJUGA)

Der Senat hatte erstmals mit der Bürgerschaftsdrucksache 14/390 vom 18. Oktober 1991 auf eine Voruntersuchung hingewiesen, die die Prüfung des Einsatzes von IuK-Technik in den bezirklichen Jugendämtern zum Gegenstand hat.

Am 7. September 1992 hat uns das Senatsamt für Bezirksangelegenheiten (SfB) offiziell über das Projekt Jugendamts-Automation (PROJUGA) in Kenntnis gesetzt. Kurze Zeit später wurde uns auch die Vorstudie zur Verfügung gestellt. An der Projektgruppe PROJUGA sollen wir beteiligt werden; bislang ist eine inhaltliche Diskussion aber noch nicht erfolgt.

Ausweislich der Vorstudie soll das Projekt einer Verringerung des Personalbedarfs bei gleichzeitiger Verbesserung des Dienstleistungsangebots und der Wirtschaftlichkeit dienen. Neben den durch Personalverringerung bedingten Einsparungen wird ein positiver wirtschaftlicher Effekt in Form von Mehreinnahmen durch ein effizienteres Mahn- und Vollstreckungsverfahren erwartet.

Im einzelnen sollen die Aufgabenfelder

— Mündelverwaltung,

— Abwicklung wirtschaftlicher Hilfen,

— Verwaltung von Einrichtungen,

— Verwaltung und Abrechnung von Honorarkräften,

— Statistiken,

— Textverarbeitung

und

— Urkundenerstellung

abgedeckt werden.

Innerhalb dieses Aufgabenrahmens sind Schnittstellen vorgesehen

— zur Landeshauptkasse,

— zum Statistischen Landesamt,

— zu Jugendämtern anderer Bezirke

und

— zu Standesämtern.

Nicht integriert werden sollen Aufgaben

— der bezirklichen Ämter für Soziale Dienste,

— des Amtes für Jugend

und

— bezirklicher Einrichtungen (Häuser der Jugend, Elternschulen, Spielhäuser u. a.).

Eine ausdrücklich genannte Maxime des Projektes ist die Wahrung des informationellen Selbstbestimmungsrechts der Bürgerinnen und Bürger. Daher soll nicht nur die eingesetzte Technik mit den erforderlichen Datensicherungsmechanismen ausgestattet werden, sondern die Speicherung und Weitergabe von Daten sollen restriktiv gehandhabt werden.

Wir werden das SfB beim Wort nehmen. Schnittstellen können dort akzeptiert werden, wo ihre Einrichtung unabweisbar ist. Mit den datenschutzrechtlich erforderlichen Restriktionen wäre eine umfassende Vernetzung der bezirklichen Jugendämter nicht zu vereinbaren. Nach Möglichkeit ist daher der Verzicht auf eine solche Vernetzung zu bevorzugen. Dies entspräche auch der beim Projekt Sozialhilfe-Automation (PROSA) gewählten Lösung. Ansonsten wird zumindest die Schaffung definierter Zugriffsbedingungen erforderlich sein.

Unbedingt sinnvoll ist es, für PROJUGA eine Datenschutzkonzeption zu erarbeiten, die zunächst den rechtlichen Rahmen absteckt und darauf aufbauend die Verfahrensabläufe festlegt. Mit der PROSA-Datenschutzkonzeption steht dafür ein geeignetes Vorbild zur Verfügung.

6.4 Fachliche Weisung zum Sozialdatenschutz

Die Behörde für Arbeit, Gesundheit und Soziales (BAGS) hat in Abstimmung mit uns ihre Dienstvorschrift zum Schutz der Sozialdaten überarbeitet. Sie soll künftig als Fachliche Weisung auch unmittelbar für die bezirklichen Dienststellen gelten.

Neu sind u. a. Aussagen zum Schutz der Daten Verstorbener, zum Recht auf Einzelberatung und zu Übermittlungen an die Ausländerbehörde. Wenngleich nicht in jeder Detailfrage völlige Übereinstimmung erzielt werden konnte, stellt der Entwurf insgesamt eine begrüßenswerte Fortschreibung der gegenwärtigen Dienstvorschrift dar. Eine möglichst baldige Inkraftsetzung wäre daher sachgerecht.

6.5 Basisuntersuchung beim Landesbetrieb Pflegen & Wohnen

In der Presse wurde am 6. März 1992 berichtet, die staatlichen Pflegeheime seien besser als ihr Ruf. In einem kritischen Leserbrief dazu hieß es seinerzeit, daß dem alten Menschen bei der Aufnahme ins Pflegeheim Fragen gestellt würden, „die ihm den Eindruck vermitteln müssen, man sei in einer Nervenklinik gelandet". Wir bekamen durch eine Eingabe Veranlassung, uns hierzu ein eigenes Bild zu machen.

Innerhalb des zur Behörde für Arbeit, Gesundheit und Soziales (BAGS) gehörenden Landesbetriebes Pflegen & Wohnen wird bei jedem neu aufgenommenen Heimbewohner eine sogenannte Basisuntersuchung durchgeführt. Diese beinhaltet eine höchst differenzierte Erhebung des Gesundheitszustandes und Persönlichkeitsbildes der Betroffenen. Die Fragestellungen zielen darauf ab, ob

der Betroffene seine Wohnung aufgelöst hat, häufig Besuch bekommt, Medikamente bekommt (ggf. welche), alleine essen kann, agressiv ist, depressiv ist, mobil ist, Orientierungsschwierigkeiten hat, inkontinent ist, sich artikulieren kann, in seinen Denk- und Wahrnehmungsfähigkeiten eingeschränkt ist und vieles mehr.

Diese Daten werden teilweise unmittelbar durch die ärztliche Untersuchung und Befragung der Betroffenen erhoben. Teilweise werden sie aber auch im Gespräch mit Angehörigen und Pflegepersonal erhoben, also ohne Kenntnis der Betroffenen. Sogar über Heimbewohner, die bereits verstorben waren, sollten diese Daten – soweit noch möglich – zusammengetragen werden. Die Ergebnisse wurden sämtlich in Fragebögen eingetragen, die die betroffene Person u. a. mit Namen und Geburtsdatum exakt kennzeichneten.

Von diesen Fragebögen verblieb ein Durchschlag in dem jeweiligen Pflegeheim und das Original ging an die Zentrale des Landesbetriebes. In der Zentrale wurden die Bögen einer graphischen Auswertung zugeführt und diese graphischen Auswertungen an die Pflegeheime zurückgeschickt, damit dort eine leichtere und schnellere Einschätzung der Bewohner möglich ist. Die Fragebögen selbst blieben jedoch in der Zentrale und wurden dort zentral gespeichert, ohne daß der Personenbezug gelöscht wurde.

In der Diskussion mit uns hob der Landesbetrieb darauf ab, daß 40% der Pflegeheimbewohner demenzkrank seien und von den weiteren 60% ein ganz überwiegender Teil bereits geistigen Beeinträchtigungen unterliege; ein Großteil der Pflegeheimbewohner sei um die 80 Jahre alt. Demzufolge müsse die Basisuntersuchung als Instrument der individuellen ärztlichen/medizinischen Versorgung gesehen werden. Diese Argumentation ließ sich mit juristischen Erwägungen nicht entkräften. Zweifel an ihrer Stichhaltigkeit blieben uns jedoch, da mit dieser Begründung die Katalogisierung der Verstorbenen zu keinem Zeitpunkt hätte erfolgen dürfen. Im übrigen kann diese Begründung nicht rechtfertigen, daß eine personenbezogene zentrale Speicherung erfolgt.

Um nach Möglichkeit sicherzustellen, daß diese Untersuchungen nur bei den Bewohnern erfolgen, bei denen dies individuell erforderlich ist, sind wir mit dem Landesbetrieb übereingekommen, daß die Untersuchung und Dokumentation bei bereits Verstorbenen unterbleibt und daß generell der jeweilige Arzt im Einzelfall zunächst die Grundsatzfrage entscheidet, ob die Betreuung des jeweiligen Bewohners die Untersuchung erforderlich macht. In den Fällen, wo dies verneint wird, unterbleibt die Untersuchung.

Im Betreuungsvertrag wird künftig ausdrücklich auf die Möglichkeit solcher Untersuchungen hingewiesen und auch darauf, daß auf Wunsch Einzelheiten durch den behandelnden Arzt erläutert werden.

Der Landesbetrieb will außerdem ein Verfahren einführen, bei dem die Dokumentationsbögen nur noch innerhalb des jeweiligen Pflegeheims alle die Per-

son identifizierenden Einzelangaben enthalten. An die Zentrale gehen nur noch Durchschläge der Dokumentationsbögen, die keine Identifizierungsangaben enthalten und somit anonym sind. Um beim Rücklauf der graphischen Auswertungen eine Zuordnung im Pflegeheim vornehmen zu können, erhalten alle Bögen eine Codenummer. Bis Redaktionsschluß war dieses geänderte Dokumentationsverfahren aber noch nicht eingeführt worden.

Kurz nachdem diese Einigung erzielt werden konnte, berichtete der Wochendienst der Staatlichen Pressestelle Nr. 25 vom 19. Juni 1992, daß der Landesbetrieb Pflegen & Wohnen die Möglichkeit biete, für befristete Zeiträume in einem der 13 staatlichen Pflegeheime zu wohnen. Das Angebot richte sich vor allem an pflegebedürftige ältere Menschen, deren Pflegepersonen vorübergehend an der Pflege im Hause gehindert sind. Für eine fachgerechte Pflege und individuelle Betreuung sei gesorgt. Die BAGS hat uns dazu mitgeteilt, daß die Basisuntersuchung mit diesen „gastweise" versorgten Senioren nicht durchgeführt wird.

6.6 Schweigepflicht-Entbindungserklärung des Versorgungsamtes

Im 6. TB (4.16.4) berichteten wir über ein 1987 mit uns abgestimmtes Verfahren zur Anforderung von Unterlagen und Auskünften. In diesem Zusammenhang war auch der Text einer Schweigepflicht-Entbindungserklärung abgestimmt worden, mit der den regelmäßigen Bedürfnissen des Massenbetriebes Rechnung getragen werden soll. Bereits im 8. TB (3.1.5) mußten wir leider berichten, daß das Versorgungsamt seine Zusagen nur teilweise eingehalten hat.

Inzwischen mußten wir erneut in eine Diskussion um die Schweigepflicht-Entbindungserklärung eintreten. Das Versorgungsamt hatte die abgestimmte Schweigepflicht-Entbindungserklärung ohne erneute Abstimmung mit uns erweitert. Zudem erfuhren wir, daß es sich auf diese Schweigepflicht-Entbindungserklärung nicht nur gegenüber den Stellen beruft, die der Antragsteller angegeben hat, sondern auch gegenüber Stellen, von denen es auf anderem Wege erfährt.

Eine Schweigepflicht-Entbindungserklärung kann sich aber wirksam nur auf Stellen beziehen, die dem Antragsteller bekannt sind oder die er zumindest in etwa abschätzen kann. Dies sind typischerweise die Stellen, die der Antragsteller in seinem Antrag nennt.

Die Betroffenen sind zwar in der Regel an einer ganzheitlichen Feststellung der Behinderung interessiert. Dennoch können sie im Einzelfall durchaus ein Interesse daran haben, daß bestimmte Informationen dem Versorgungsamt nicht bekannt werden. Dafür werden sie möglicherweise auch in Kauf nehmen, daß der Grad der festgestellten Behinderung etwas geringer ausfällt.

Wenn die Schweigepflicht-Entbindungserklärung ohne Kenntnis des Betroffenen auch gegenüber Stellen verwendet wird, von denen das Versorgungsamt auf Umwegen erfahren hat, bringt das die Betroffenen in die Situation, daß sie nach einer einmal erklärten Schweigepflicht-Entbindung für die Dauer des Verwaltungsverfahrens bei jedem Besuch eines Arztes oder Psychologen damit rechnen müssen, daß alle dort bekannt gewordenen Daten später auch dem Versorgungsamt zufließen. Dies ist mit dem informationellen Selbstbestimmungsrecht nicht zu vereinbaren.

Wir haben mit der BAGS Einigkeit über den Text der Einwilligungserklärung erzielt, die den Betroffenen die Möglichkeit gibt, ihre Erklärung auf bestimmte Stellen zu beschränken. Die konkrete Umsetzung dieses Ergebnisses steht aber noch aus.

6.7 Offenbarung von Jugendhilfedaten

6.7.1 Akteneinsicht in Jugendhilfeakten

Im Berichtszeitraum wurden wir um Stellungnahme gebeten, inwieweit

— Deputierten,

— dem Hauptausschuß der Bezirksversammlung und

— dem Jugendhilfeausschuß

Akteneinsicht insbesondere in Jugendhilfeakten zu gewähren ist. Die Schwierigkeiten, die bei der Beantwortung dieser Fragen auftreten, sind zum Teil darauf zurückzuführen, daß die Struktur der hamburgischen Verwaltung und die sie regelnden Rechtsvorschriften aus einer Zeit stammen, als datenschutzrechtliche Fragen keine Bedeutung hatten und das informationelle Selbstbestimmungsrecht mit Verfassungsrang in seiner heutigen Form unbekannt war.

Die abstrakte Beurteilung der Rechtslage führt in den genannten Fällen im wesentlichen zu dem gleichen Ergebnis. Die Gewährung von Akteneinsicht ist grundsätzlich nur eine spezielle – allerdings besonders sensible – Form der Offenbarung von Sozialdaten. Sofern die jeweils betroffene Person nicht ausdrücklich ihr Einverständnis erklärt hat, dürfen Daten, die unter die besonderen Schutzvorschriften der §§ 65 SGB-VIII, 76 SGB-X fallen, keinesfalls offenbart werden. Dies sind z.B. Daten aus ärztlichen und psychologischen Gutachten und Daten, die im Rahmen eines besonderen Vertrauensverhältnisses, z.B. durch Sozialarbeiter, erhoben wurden. Im übrigen dürfen Daten offenbart werden, soweit dies im Einzelfall jeweils erforderlich, d.h. unerläßlich ist. Sofern irgendwie möglich, ist der Verwendung anonymisierter Daten der Vorzug zu geben. Darüber hinaus ist zu beachten, daß in den Ausschüssen nur eine nichtöffentliche Behandlung der Einzelfälle erfolgen darf. Zudem empfiehlt sich, daß

die offenbarende Stelle die Adressaten der Offenbarung schriftlich auf deren Verschwiegenheitsverpflichtung hinweist.

Die Frage, was jeweils erforderlich ist, muß zwar im Einzelfall entschieden werden. Dabei ist jedoch folgendes zu beachten:

— Deputierte

Das Akteneinsichtsrecht der Deputierten ist in § 14 Verwaltungsbehördengesetz (VwBehG) geregelt. Es muß in Verbindung mit den Aufgaben der Deputierten gesehen werden (siehe auch 7. TB, 4.1.1). Die einzelnen Deputierten haben nach dem VwBehG ein Mitwirkungsrecht, das sich auf Fragen allgemeiner bzw. grundsätzlicher Natur bezieht. Insbesondere geht es um die sachliche Erledigung von Beschwerden von allgemeiner Bedeutung. Dies verdeutlicht, daß es nicht um die Erledigung von Einzelfällen geht, die an bestimmte Personen gebunden sind.

Die Deputierten haben auch kein allgemeines Kontrollrecht über die Verwaltung, das über die im VwBehG beschriebenen Aufgaben hinausgeht. Zwar kann Kontrolle auch in Form einer internen Aufsicht erfolgen, wie sie mit Vorgesetzten-/Leitungsfunktionen verbunden ist. Wenngleich die Deputation das oberste Leitungsgremium einer Fachbehörde ist, kann daraus für den einzelnen Deputierten jedoch nicht abgeleitet werden, daß er eine Vorgesetzten- oder Leitungsfunktion im allgemeinen Sinne hat. Die gesetzliche Aufgabenbeschreibung in § 9 VwBehG hat vielmehr einen einschränkenden Charakter. Der Deputierte hat daher einen Zusammenhang seines Akteneinsichtsbegehrens zu seinen gesetzlichen Aufgaben plausibel darzulegen.

— Hauptausschuß der Bezirksversammlung

Die Bezirksversammlung hat nach § 16 Buchst. b Bezirksverwaltungsgesetz (BezVG) interne Kontrollfunktionen gegenüber der Verwaltung des Bezirksamtes wahrzunehmen; diese kann sie im Einzelfall dem Hauptausschuß übertragen (§ 25 Abs. 2 BezVG). Akteneinsicht ist daher zu gewähren, soweit dies zur Wahrnehmung der Kontrollfunktion erforderlich ist.

— Jugendhilfeausschuß

Der Jugendhilfeausschuß ist zwar bei der Bezirksversammlung angesiedelt. Er ist aber kein Fachausschuß nach dem BezVG, sondern findet seine Grundlage im SGB-VIII und im Ausführungsgesetz zum Jugendwohlfahrtsgesetz (AGJWG). Er soll sich im wesentlichen anregend und fördernd mit Aufgaben der Jugendhilfe befassen. Kontrollrechte gegenüber der Verwaltung des Bezirksamtes stehen ihm nicht zu. Im Rahmen seiner allgemeinen Aufgaben kann es aber ausnahmsweise erforderlich sein, ihm Einzelfallinformationen zu geben. Diese müssen dann auf ein absolutes Minimum beschränkt bleiben.

Problematisch ist in diesem Zusammenhang die Regelung in § 2 Abs. 9 Satz 4 AGJWG. Diese Vorschrift schafft die Möglichkeit, dem Jugendhilfeausschuß Aufgaben eines Fachausschusses der Bezirksversammlung zu übertragen. Damit erhält der Jugendhilfeausschuß eine Doppelfunktion und nimmt an den Kontrollaufgaben der Bezirksversammlung teil. Er erhält dadurch einen Anspruch auf Informationen, die ihm eigentlich nicht zustehen.

Da nach dem Außerkrafttreten des Jugendwohlfahrtsgesetzes das AGJWG ohnehin zu novellieren sein wird, sollte in diesem Zusammenhang die Regelung des § 2 Abs. 9 Satz 4 ersatzlos gestrichen werden.

6.7.2 Verwendung von Jugendhilfedaten in öffentlichen Bürgerschaftsdebatten

Vor dem Hintergrund der öffentlichen Diskussion über die Jugendhilfe gilt es festzuhalten, daß allgemeine Aussagen zu strukturellen Fragen der Jugendhilfe in einer öffentlichen Bürgerschaftsdebatte datenschutzrechtlich unproblematisch sind.

Es ist Senatsvertretern aber rechtlich verwehrt, dem Sozialgeheimnis unterliegende Informationen in diesen Debatten zu verwenden; insbesondere ist es unzulässig, aus psychiatrischen Gutachten zu zitieren.

Die gesetzlichen Regelungen zum Sozialgeheimnis lassen es zwar zu, daß unzutreffende Behauptungen richtiggestellt werden. Wenn solche unzutreffenden Behauptungen öffentlich erfolgen, kann auch die Richtigstellung öffentlich geschehen. Zu beachten ist aber, daß dieses Recht zur Richtigstellung nur dann besteht, wenn der Sozialleistungsempfänger selbst diese unzutreffenden Behauptungen gemacht hat. Eine öffentliche Richtigstellung unzutreffender Behauptungen Dritter darf nicht unter Verwendung von Informationen erfolgen, die dem Sozialgeheimnis unterliegen.

Die zuständigen Amtsträger sind gerade in öffentlichen Auseinandersetzungen gefordert, den Sozialdatenschutz zu wahren. Das entspräche auch der Praxis des Senates, z.B. bei bürgerschaftlichen Anfragen ggf. eine Beantwortung unter Hinweis auf den Sozialdatenschutz zu verweigern.

6.8 Kontrollzuständigkeit bei der Vereinigung Städtischer Kinder- und Jugendheime

Am Beispiel der Vereinigung Städtischer Kinder- und Jugendheime der Freien und Hansestadt Hamburg e.V. (nachstehend: Vereinigung) hat uns im Berichtszeitraum die Frage beschäftigt, ob ein Sozialleistungsträger als öffentlicher Träger allein deshalb nicht unserer Kontrolle nach dem Sozialgesetzbuch unterliegt, weil er formal privatrechtlich organisiert ist. Die Vereinigung, die ihre Tagesheime bereits seit 1940 in Form eines eingetragenen Vereins führt,

vertritt die Auffassung, daß sie aufgrund ihrer Organisationsform als Verein nur unserer Kontrolle als Aufsichtsbehörde nach dem Bundesdatenschutzgesetz (BDSG) unterliegt.

Nach den gesetzlichen Regelungen des Sozialgesetzbuches/Erstes und Achtes Buch (SGB-I und SGB-VIII) werden Leistungen der Kinder- und Jugendhilfe sowohl durch Träger der öffentlichen Jugendhilfe als auch durch Träger der freien Jugendhilfe erbracht (§ 3 SGB-VIII). Dort wo freie Träger ausreichende Leistungsangebote vorhalten, soll von einem entsprechenden Angebot durch öffentliche Träger abgesehen werden (§ 4 Abs. 2 SGB-VIII).

Während die öffentlichen Träger in Hamburg kraft Gesetzes einer datenschutzrechtlichen Kontrolle durch uns unterliegen, ist dies bei freien Trägern nicht der Fall; ihnen gegenüber haben wir nur die Rechte der Aufsichtsbehörde nach dem Bundesdatenschutzgesetz. In der Kinder- und Jugendhilfe gilt insoweit § 61 Abs. 3 SGB-VIII. Danach sollen öffentliche Träger, wenn sie freie Träger in Anspruch nehmen, sicherstellen, daß der Datenschutz in gleicher Weise wie bei Leistungsträgern gewährleistet ist. Daraus folgt jedoch kein unmittelbares Kontrollrecht für uns. Ein solches haben wir nur dann, wenn sich der freie Träger unserer Kontrolle unterwirft; hierauf hat der öffentliche Träger ggf. hinzuwirken.

Die Vereinigung betrachtet sich als Betrieb, der – obwohl er die Umsetzung der Ziele der Freien und Hansestadt Hamburg auf dem Gebiet der Kindertagesbetreuung zur Aufgabe hat – nach dem SGB-VIII rechtlich als freier Träger der Jugendhilfe einzustufen ist und damit eine nicht-öffentliche Stelle i.S.d. Bundesdatenschutzgesetzes darstellt. Dies wird auch in ihrer Satzung zum Ausdruck gebracht; außerdem hat sie nach dem BDSG eine betriebliche Datenschutzbeauftragte bestellt, wozu sie im übrigen auch nach dem SGB verpflichtet wäre.

Sie ist jedoch nach unserer Auffassung datenschutzrechtlich wie ein öffentlicher Träger der Jugendhilfe zu behandeln. Dies wird an folgendem deutlich:

Anläßlich der Neuorganisation der Vereinigung 1987 hat der Senat darauf hingewiesen (Bürgerschaftsdrucksache 12/491), daß die Vereinigung an den politischen Willen von Senat und Bürgerschaft gebunden bleiben sollte. Die Kontrollrechte von Senat und Bürgerschaft seien zu erhalten bzw. sogar zu erhöhen.

Die für Fragen der Jugendhilfe fachlich zuständige Behörde für Schule, Jugend und Berufsbildung (BSJB) hat uns im Berichtszeitraum ausdrücklich bestätigt, daß die Vereinigung Aufgaben der öffentlichen Verwaltung wahrnehme; die Freie und Hansestadt habe mit der Vereinigung unmittelbar ein Leistungsangebot geschaffen. Später hat die BSJB zwar versucht, diese Aussagen durch die Behauptung zu relativieren, die Vereinigung sei weder ein freier noch ein

öffentlicher Träger von Aufgaben der Jugendhilfe. Diese Auffassung findet in den Regelungen des SGB jedoch keinen Raum.

Organe des Vereins sind der Vorstand und die Mitgliederversammlung. Die Tätigkeit des Vorstandes unterliegt dabei einer weitgehenden Überwachung durch die Mitgliederversammlung. Sie bestellt den Vorstand, stellt ihn an und beruft ihn ab. Die Anstellung bedarf der Zustimmung der BSJB. Alle bedeutsamen Entscheidungen des Vorstandes bedürfen aufgrund der Satzung der Zustimmung der Mitgliederversammlung. Die Mitgliederversammlung kann darüber hinaus noch weitere Geschäfte ihrer Zustimmung vorbehalten. Die Mitgliederversammlung setzt sich aus zwölf Personen zusammen. Eine dieser Personen ist der Präses der BSJB, der zugleich Vorsitzender der Mitgliederversammlung ist und bei Stimmengleichheit entscheidet. Er beruft sieben weitere Mitglieder, unter denen sich mit Vertretern der Finanzbehörde und des Senatsamtes für den Verwaltungsdienst mindestens zwei weitere Senatsvertreter befinden. Durch diesen Einfluß hat also der Senat in der Mitgliederversammlung eine Zweidrittelmehrheit.

Wenn sich der Verein auflösen oder sein Zweck wegfallen sollte, fällt sein Vermögen an die Freie und Hansestadt Hamburg.

Dies alles macht deutlich, daß die Vereinigung zwar privatrechtlich organisiert, aber damit keinesfalls ein freier Träger von Sozialleistungen geworden ist. Sie entspricht vielmehr in vielfältiger Hinsicht dem Bild eines öffentlichen Trägers der Jugendhilfe. Demzufolge unterliegt sie unserer vollen datenschutzrechtlichen Kontrolle, wie andere öffentliche Leistungsträger auch. Bemerkenswert ist in diesem Zusammenhang im übrigen, daß die Vereinigung in ihrer Satzung die Prüfungsrechte des Rechnungshofes ausdrücklich anerkannt hat.

Wir haben die Vereinigung daher um eine Überprüfung ihres bisherigen Standpunktes gebeten; sie lehnt unsere Aufassung jedoch weiterhin ab. Auch unserem Vorschlag, sich – ohne Präjudiz für die Rechtslage – unserer datenschutzrechtlichen Kontrolle zu unterwerfen, will sie aus grundsätzlichen Überlegungen zur Zeit nicht folgen.

Somit bleibt im Rahmen der allgemeinen Diskussion um ein Kontrollrecht bei öffentlichen Unternehmen (siehe 1.4.1) eine Klärung der Rechtslage abzuwarten.

6.9 Verfolgung von Mietpreisüberhöhungen

Die Sozialhilfe- und Wohngelddienststellen erfahren im Rahmen ihrer Tätigkeit regelmäßig, wie hoch die Mietzinsverpflichtungen der Hilfeempfänger sind. Sie können daher auch in etwa ersehen, ob überhöhte Mieten verlangt werden.

Im Dezember 1991 bat uns das Senatsamt für Bezirksangelegenheiten (SfB) um Stellungnahme, ob es zulässig wäre, wenn diese Dienststellen solche vermuteten Fälle von Mietpreisüberhöhung an die zuständige Einwohnerdienststelle mitteilen, damit von dort aus ein Ordnungswidrigkeitenverfahren gemäß § 5 Wirtschaftsstrafgesetz eingeleitet werden kann.

Wir haben daraufhin deutlich gemacht, daß wir ein solches Verfahren für unzulässig halten. Die Einwohnerdienststelle würde dem Vermieter zwangsläufig preisgeben müssen, daß ihre Information vom Mieter stammt. Damit würde dem Vermieter offenbart werden, daß sein Mieter Sozialleistungsempfänger ist. Abgesehen davon, daß die Sozialleistungsempfänger damit oftmals Repressalien ihrer Vermieter ausgesetzt würden, ist es auch keine gesetzliche Aufgabe der Sozialhilfe- und Wohngelddienststellen, die Einleitung solcher Ordnungswidrigkeitenverfahren zu veranlassen, so daß die Weitergabe dieser Sozialdaten an die Einwohnerdienststelle unzulässig ist.

Unbedenklich wäre dagegen ein Hinweis der Sozialhilfe- und Wohngelddienststellen an die Mieter, daß die Einwohnerdienststellen für diese Ordnungswidrigkeitenverfahren zuständig sind. Die Mieter könnten dann – ohne Preisgabe der Tatsache, daß sie Sozialleistungsempfänger sind – selbst entscheiden, ob sie ein Ordnungswidrigkeitenverfahren veranlassen wollen.

6.10 Unzulässige Datenerhebung der Sozialämter

Kindern und Eltern von Sozialhilfeempfängern wird in aller Regel ein Fragebogen zugesandt, in dem sie nach ihren Einkommens- und Vermögensverhältnissen befragt werden. Dagegen ist grundsätzlich nichts einzuwenden. Das Sozialamt muß nämlich versuchen, die geleistete Sozialhilfe bei diesen unterhaltspflichtigen Angehörigen zurückzufordern. § 116 Abs. 1 Bundesozialhilfegesetz (BSHG) verpflichtet diese Personen, dem Sozialamt Auskunft über ihre Einkommens- und Vermögensverhältnisse zu geben.

In Hamburg wird in diesen Fragebögen jedoch auch nach den Einkommensverhältnissen der Ehegatten gefragt. In den Erläuterungen zu dem Fragebogen wird zugleich behauptet, auch hinsichtlich dieser Angaben bestünde eine Auskunftspflicht.

Wir haben die Behörde für Arbeit, Gesundheit und Soziales (BAGS) darauf hingewiesen, daß dieses Verfahren rechtswidrig ist, denn § 116 Abs. 1 BSHG verpflichtet die Unterhalts- und Kostenersatzpflichtigen nur zur Auskunft über ihre Einkommens- und Vermögensverhältnisse, nicht jedoch über die Einkommensverhältnisse ihrer Ehegatten.

Zulässig wäre die Frage nach den Einkommensverhältnissen der Ehegatten der Unterhaltspflichtigen nur auf rein freiwilliger Basis. Das wäre insofern auch sinnvoll, als eine Unterhaltspflicht gegenüber dem Ehegatten sich mindernd auf die Unterhaltspflicht gegenüber dem Sozialhilfeempfänger auswirken kann.

Die BAGS weigert sich jedoch bislang, unserem Hinweis zu folgen. Sie beruft sich auf eine Entscheidung des Verwaltungsgerichtshofs (VGH) Baden-Württemberg. Diese Entscheidung ist jedoch nicht geeignet, ein anderes Ergebnis zu rechtfertigen. Auch der VGH stellt primär nur darauf ab, daß im Sozialhilferecht einkommensmindernde Belastungen als zu den eigenen Einkommensverhältnissen zählend anerkannt seien. Er geht keineswegs so weit, daß der Erhalt von Unterhaltszahlungen eine Unterhaltsverpflichtung des Zahlungsempfängers gegenüber Dritten begründet. Diese Auffassung ist mit geltendem Unterhaltsrecht unvereinbar.

Wir haben die BAGS daher gebeten, ihre Aufassung noch einmal zu überdenken. Die Unhaltbarkeit ihrer Position wird auch daran deutlich, daß fast alle Datenschutzbeauftragten des Bundes und der Länder und auch die Sozialministerien mehrerer Bundesländer eine Auskunftspflicht der Unterhaltspflichtigen hinsichtlich der Einkommens- und Vermögensverhältnisse der Ehegatten verneinen.

7. Personalwesen

7.1 Automationsvorhaben Projekt Personalwesen (PROPERS)

Im 10. TB (7.1) haben wir ausführlich über die geplante Reorganisation der hamburgischen Personalverwaltung berichtet. Dabei haben wir auch auf die datenschutzrechtliche Problematik eines umfassenden automatisierten Personalinformationssystems hingewiesen.

Die Lenkungsgruppe hat nunmehr Ende September 1992 beschlossen, daß für die Aufgabenbereiche

— Bezügeabrechnung,

— Personalverwaltung,

— Personalplanung und

— Personalentwicklung

eine Lösung verteilter Datenverarbeitung (Zentral- und Abteilungsrechner) auf der Basis eines seit Jahren auf dem Markt befindlichen Software-Produkts und der in der hamburgischen Verwaltung eingesetzten arbeitsplatzunterstützenden Bürofunktionalitäten entwickelt wird.

Die Projektgruppe wurde beauftragt, die erforderlichen Voraussetzungen für eine Anpassung der Standardsoftware an die Anforderungen der hamburgischen Verwaltung zu schaffen und eine konkrete Kapazitäts- und Kostenschätzung für die Projektdurchführung einschließlich der Test- und Freigabeverpflichtung nach der Freigaberichtlinie vorzulegen.

Die Lenkungsgruppe hat dabei erneut bekräftigt, daß über die Zulässigkeit der Informationsspeicherung und -auswertung nach näherer Aufbereitung konkret im Einzelfall entschieden werden soll. Die voraussehbaren Auswertungen würden aufgelistet und verbindlich im Rahmen einer Vereinbarung gemäß § 94 HmbPersVG geregelt. Dies gelte auch für die Teilbereiche Personalentwicklung und Personalplanung.

Diese Entscheidung der Lenkungsgruppe kommt unseren Vorstellungen zunächst entgegen. In unseren bisherigen Stellungnahmen haben wir wiederholt darauf hingewiesen, daß die jetzt ausgewählte Standardsoftware gegenüber dem im Jahr 1991 vorab für Testzwecke installierten Produkt die datenschutzrechtlichen Anforderungen insbesondere hinsichtlich der Zugriffskontrolle und Revisionsfähigkeit wesentlich wirkungsvoller erfüllt.

Eine verteilte Datenverarbeitung (Bezügeabrechnung, „zentrale Auswertungen" in der Datenverarbeitungszentrale, Stammdatenverwaltung, Textverarbeitung, Tabellenkalkulation usw. in den Behörden auf eigenen Abteilungsrechnern) bedingt in sich gegenüber einer reinen Großrechnerlösung selbstverständlich zusätzlichen organisatorischen und technischen Aufwand zur Gewährleistung des Datenschutzes. So ist z.B. in jeder Behörde sicherzustellen, daß die dezentral aufgestellten Rechner räumlich gesichert werden müssen und der Zugriff auf die Personaldaten gegenüber möglichen anderen Anwendungen auf diesen Anlagen abgegrenzt wird.

Bei einer reinen Zentralrechnerlösung hätte der gesamte Personalbestand der öffentlichen Verwaltung gesichert werden müssen. Den einzelnen Behörden hätte nur Zugriff auf ihren eigenen Bestand eingeräumt werden dürfen.

Besondere Beachtung werden wir zukünftig dem Umfang der Daten widmen, zum einen den Dateien, die dezentral in den Behörden vorgehalten werden sollen, zum anderen den Informationen über Beschäftigte in der hamburgischen Verwaltung, die neben der Bezügeabrechnung für übergeordnete Aufgaben der Personalplanung und -entwicklung in der Datenverarbeitungszentrale gespeichert und ausgewertet werden sollen.

Wir gehen davon aus, daß wir auch weiterhin so umfassend an der Fortentwicklung des Automationsvorhabens beteiligt werden wie bisher. Die Zusammenarbeit in bezug auf den Datenschutz ist im Projekt Personalwesen nach wie vor vorbildlich.

7.2 Neues Personalaktenrecht

Nach mehrjährigen Vorarbeiten, über die wir im 8. TB (3.2.6) und 9. TB (4.2.3.1) berichteten, wurde am 11. Juni 1992 das Neunte Gesetz zur Änderung dienstrechtlicher Vorschriften vom Bundestag verabschiedet. Es tritt am 1. Januar 1993 in Kraft und regelt in nahezu gleichlautenden Bestimmungen im Bundes-

beamtengesetz (BBG) und im Beamtenrechtsrahmengesetz (BRRG) die Führung und Verwaltung von Personalakten.

Gegenüber den von uns kommentierten Entwürfen enthalten BBG und BRRG nun auch eine Datenerhebungsvorschrift und ein Einsichtsrecht des Beamten in „andere Akten, die personenbezogene Daten über ihn enthalten und für sein Dienstverhältnis verarbeitet oder genutzt werden". In Hamburg kommen dafür z.B. die Unterlagen des psychologischen oder des personalärztlichen Dienstes (siehe 7.3) in Betracht.

Bereits vor Verabschiedung des Bundesgesetzes legte das Senatsamt für den Verwaltungsdienst im März 1992 einen Entwurf für ein 15. Gesetz zur Änderung des Hamburgischen Beamtengesetzes vor, das die geplanten Bestimmungen des BRRG zum Personalaktenrecht in Landesrecht umsetzen soll. In Abstimmung mit dem Senatsamt konnte weitgehende Einigkeit über notwendige Änderungen des Gesetzentwurfs aus datenschutzrechtlicher Sicht erreicht werden. Dabei verfolgten wir das Ziel, von den Bestimmungen des BRRG nur zugunsten der Betroffenen abzuweichen und konkretere Festlegungen des BRRG nicht durch allgemeinere zu ersetzen. Letzteres galt etwa für die Umschreibung des Zweckes, der eine Erhebung von Personaldaten rechtfertigt. „Personalverwaltung oder Personalwirtschaft" hielten wir ohne eine nähere gesetzliche Definition für zu unbestimmt.

Die auch den Spitzenverbänden der Gewerkschaften zugeleiteten Entwürfe vom Juni und November 1992 berücksichtigen unsere Wünsche zum größten Teil, soweit diese nicht über die im BRRG vorgesehenen Datenschutzrechte hinausgingen. Nicht durchsetzen konnten wir etwa, daß Auskünfte aus der Personalakte nur bei Vorliegen eines „rechtlichen", nicht nur eines „berechtigten" Interesses eines privaten Dritten zulässig sind. Erreicht haben wir dagegen z.B., daß die Löschungsvorschriften für unzutreffende und möglicherweise nachteilig sich auswirkende Unterlagen in der Personalakte auch auf „andere Akten" mit personenbezogenen Daten erstreckt werden. Ferner wurde die Aufbewahrungszeit für Versorgungsakten von 10 auf 5 Jahre nach der letzten Versorgungszahlung halbiert.

Kritik haben wir noch an zwei Abschnitten der Gesetzesbegründung:

Die organisatorische Trennung von Personalverwaltung und Beihilfesachbearbeitung ist im Gesetzentwurf entsprechend dem BRRG leider nur als Soll-Vorschrift vorgesehen. Während die geforderte Abschottung in den Behörden und Ämtern durch die Zentralisierung der Beihilfe bei der Besoldungs- und Versorgungsstelle realisiert wurde, soll es nach der Begründung bei den landesunmittelbaren juristischen Personen des öffentlichen Rechts für eine Ausnahme bereits ausreichen, „daß Bearbeiter allein mit Beihilfevorgängen nicht ausgelastet sind". Dies wird dem datenschutzrechtlich bedeutsamen Trennungsgebot nach unserer Auffassung nicht gerecht.

Nach dem Gesetzestext wird die erwähnte Löschungsfrist bei unzutreffenden oder sich nachteilig auswirkenden Unterlagen „durch erneute Sachverhalte im Sinne dieser Vorschrift oder durch die Einleitung eines Straf- oder Disziplinarverfahrens unterbrochen". Die Frist gilt als nicht unterbrochen, wenn „der erneute Vorwurf" sich als unbegründet herausstellt. Wir stehen auf dem Standpunkt, daß es sich bei dem „erneuten Vorwurf" um ein Ereignis handeln muß, das in irgendeinem Zusammenhang mit den vorausgegangenen Vorwürfen, Behauptungen usw. steht. Anderenfalls könnten sowohl Bürger als auch (frühere) Kollegen durch Anschuldigungen oder Beschwerden aus ganz anderen Bereichen und Zusammenhängen eine Unterbrechung der Löschungsfrist erreichen.

Die Novellierung des Hamburgischen Beamtengesetzes hat Auswirkungen auf den § 28 HmbDSG, der die „Datenverarbeitung bei Beschäftigungsverhältnissen" im öffentlichen Dienst regelt – und zwar sowohl für Beamte als auch für Arbeitnehmer. Im Sinne einer Meistbegünstigung wollen wir die neuen datenschutzfreundlichen Regelungen aus dem Beamtengesetz auch auf Arbeitnehmer angewendet wissen, aber umgekehrt jene Aussagen des § 28 HmbDSG erhalten, die für die Betroffenen vorteilhafter sind. Unter Verzicht auf eine Doppelung nun auch in das Beamtenrecht aufgenommener Regelungen haben wir der Justizbehörde deswegen vorschlagen, § 28 HmbDSG um folgenden Absatz zu ergänzen:

„Soweit in den Absätzen 1 bis 7 nichts anderes bestimmt ist, gelten die in den §§ 96—96 h des Hamburgischen Beamtengesetzes getroffenen Regelungen des Personalaktenrechts entsprechend für Beschäftigungsverhältnisse von Arbeitnehmern."

Nach Inkrafttreten des neuen Personalaktenrechts wird sich die Praxis der Personalabteilungen und des Personalamtes nicht nur in einzelnen untergeordneten Bereichen ändern müssen. So gehört das uns häufig entgegengehaltene Prinzip der Vollständigkeit der Personalakte nunmehr der Vergangenheit an. Zur Umsetzung des Personalaktenrechts wird es insbesondere einer grundsätzlichen Neufassung der bislang geltenden Anordnung zur Führung und Verwaltung von Personalakten bedürfen. Wir haben die Absicht, diese intensiv zu begleiten.

7.3 Personalärztlicher Dienst

Im 10. TB (7.3) hatten wir ausführlich über die Ergebnisse einer Prüfung beim Personalärztlichen Dienst berichtet und eine Reihe datenschutzrechtlicher Probleme benannt. Der größte Teil der Fragen wurde inzwischen geklärt. So werden z.B. die Unterlagen von nicht geeigneten Bewerbern, mit denen „ein Beschäftigungsverhältnis nicht zustande kommt" (§ 28 Abs. 5 Satz 1 HmbDSG), nun nur noch ein Jahr aufbewahrt, um eventuelle Rechtsmittel berücksichtigen zu können.

Für nicht befriedigend gelöst halten wir nach wie vor das Problem der Risikofaktoren: Der personalärztliche Dienst faßt das Ergebnis seiner Eignungsuntersuchungen jetzt nicht mehr in „geeignet" oder „nicht geeignet" zusammen, sondern in „. . . bestehen keine gesundheitlichen Bedenken . . ." bzw. „bestehen gesundheitliche Bedenken wegen . . .". Die Bedenken werden der auftraggebenden Behörde in Form von Risikofaktoren mitgeteilt. Die Stellungnahme des Senats zum 10. TB (Drucksache 14/1516, S. 8) gibt dafür Beispiele: „Übergewicht mit Fettstoffwechselstörungen, Diabetes, Hypertonus, Nikotinabusus".

Wie in der Sitzung des Unterausschusses Datenschutz der Bürgerschaft am 1. September 1992 erläutert, halten wir eine Mitteilung derartiger Gesundheitsdaten jedenfalls dann für datenschutzrechtlich nicht erforderlich und damit für unzulässig, wenn der Bewerber für die vorgesehene Einstellung gesundheitlich geeignet ist. Dem Personalsachbearbeiter der Beschäftigungsbehörde fehlt in aller Regel das medizinische Wissen, um personalrechtliche Konsequenzen aus diesen „Risikofaktoren" ziehen oder vorschlagen zu können. Sollten die mitgeteilten Risikofaktoren so gravierend sein, daß vor einer endgültigen Personalentscheidung eine weitere Untersuchung erforderlich erscheint, sollte der Personalärztliche Dienst allein dies bzw. den Untersuchungstermin mitteilen.

Unproblematisch ist dagegen die Mitteilung rein tätigkeitsbezogener Risikofaktoren verbunden mit einer konkreten umsetzbaren Empfehlung – z.B. Tragen einer Schutzbrille, Gebrauch eines ergonomischen Stuhls. Wir haben der Justizbehörde dementsprechend vorgeschlagen, durch eine Ergänzung des § 28 Abs. 4 Satz 1 HmbDSG klarzustellen, daß mit den dort genannten „Risikofaktoren" allein „tätigkeitsbezogene Risikofaktoren" gemeint sind.

Ebenfalls nicht befriedend beantwortet ist für uns die Frage der Aufbewahrungsfristen für die Untersuchungsunterlagen eingestellter Bewerber. Im Unterausschuß Datenschutz der Bürgerschaft erklärte der Senatsvertreter, die Unterlagen auch der Eignungsuntersuchungen würden bis 10 Jahre nach dem Ausscheiden aus dem Dienst aufbewahrt.

Es fragt sich jedoch, welchen Wert die Befunde der Eignungsuntersuchung Jahrzehnte nach der Einstellung überhaupt noch haben können. Während des Dienstes kommt es auf die aktuelle Eignung bzw. Dienstfähigkeit, nicht auf früher einmal erhobene Daten an. Wir halten die Aufbewahrung der Eignungsuntersuchungsdaten bis zu 10 Jahren nach der Untersuchung für vertretbar, um eventuelle Vergleiche zu ermöglichen und Entwicklungen nachzuvollziehen. 10 Jahre beträgt grundsätzlich auch die berufsrechtliche Dokumentationspflicht der Ärzte bei Behandlungen. Darüber hinaus können wir eine datenschutzrechtliche Erforderlichkeit der Aufbewahrung jedoch nicht erkennen.

Während der Auseinandersetzung mit dem Personalärztlichen Dienst um unsere Aussagen im 10. TB ergab sich schließlich ein Dissens hinsichtlich der Akteneinsicht in die Unterlagen des Personalärztlichen Dienstes. Dieser steht auf dem Standpunkt: „Die Einsichtnahme der Untersuchten in Arztaufzeichnungen im Zusammenhang mit Begutachtungen ist generell nicht gegeben." Dem müssen wir widersprechen. Soweit die Unterlagen nicht ohnehin zur Personalakte im materiellen Sinne gehören und damit dem Einsichtsrecht nach § 96 des Hamburger Beamtengesetzes unterliegen, kann der Betroffene jedenfalls sein Auskunftsrecht nach § 18 HmbDSG geltend machen.

Das am 1. Januar 1993 in Kraft tretende Beamtenrechtsrahmengesetz sieht darüber hinaus in § 56 c ausdrücklich vor: „Der Beamte hat . . . ein Recht auf Einsicht in seine vollständige Personalakte . . . (Abs. 4:) Der Beamte hat ein Recht auf Einsicht auch in andere Akten, die personenbezogene Daten über ihn enthalten und für sein Dienstverhältnis verarbeitet oder genutzt werden, soweit gesetzlich nichts anderes bestimmt ist; . . ." Dasselbe sieht § 96 d Abs. 2 des Entwurfs für eine Änderung des Hamburgischen Beamtengesetzes vor.

Ein generelles Einsichtsrecht von Patienten in ihre Untersuchungs- und Behandlungsunterlagen in Krankenhäusern normiert im übrigen auch § 13 Abs. 1 des Hamburgischen Krankenhausgesetzes. Darin ist zwar eine „Vermittlung" durch den Arzt vorgesehen, aber kein Ausschluß des Einsichtsrechts aufgrund des vielfach in Anspruch genommenen sog. therapeutischen Privilegs, des Schutzes des Patienten vor sich selbst. Es ist nicht einzusehen, warum die Unterlagen beim Personalärztlichen Dienst anders und für den Betroffenen restriktiver behandelt werden müssen.

Spätestens mit Verabschiedung der Änderungen des Hamburgischen Beamtengesetzes kann am Recht des Beamten auf Einsicht in seine Unterlagen beim Personalärztlichen Dienst nicht mehr gezweifelt werden.

7.4 Bewerbungen aus den neuen Bundesländern

Gemäß Empfehlung der Personalabteilungsleiterbesprechung vom 21. Januar 1991 und 26. August 1991 sollen in Hamburg Bewerber aus den neuen Bundesländern in einem Einstellungsgespräch nach einer etwaigen Tätigkeit für den Staatsicherheitsdienst gefragt werden. Die Antwort ist aktenkundig zu machen und unterzeichnen zu lassen. Zusätzlich soll das Einverständnis der Bewerber mit der Einholung einer Auskunft vom Bundesbeauftragten für die personenbezogenen Unterlagen des Staatsicherheitsdienstes nach Maßgabe der dafür geltenden Vorschriften gefordert werden. Ob die Einstellungsbehörden um Auskunft ersuchen, steht in ihrem pflichtgemäßen Ermessen. Daraus folgt, daß grundsätzlich nur bei vorliegenden Anhaltspunkten für eine Stasi-Mitarbeit ein Auskunftsersuchen gestellt werden kann.

Dieses Verfahren ist aus datenschutzrechtlicher Sicht nicht zu beanstanden. Wir haben jedoch in Erfahrung bringen können, daß in Teilbereichen der Hamburger Verwaltung über die geschilderten Empfehlungen hinausgegangen wird. So legt die Justizbehörde den Bewerberinnen und Bewerbern einen Erklärungsbogen vor, der eine Einverständniserklärung mit einem Auskunftsersuchen an die Zentrale Erfassungstelle der Landesjustizverwaltung in Salzgitter vorsieht. Außerdem wird nach leitenden Funktionen in ehemaligen DDR-Betrieben gefragt. Die Einstellungsstelle der Landespolizeischule Hamburg verwendet eine gesonderte „Erklärung zum Bewerbungsbogen". Dieser Erklärungsbogen fragt etwaige Tätigkeiten in der Nationalen Volksarmee, in der SED und in sonstigen Massenorganistionen sowie für den Staatsicherheitsdienst ab.

Wir sind in dieser Angelegenheit mit dem Senatsamt für den Verwaltungsdienst im Gespräch; eine abschließende Stellungnahme des Senatsamtes ist angekündigt. Erst nach abschließender Äußerung des Senatsamtes wird sich der Hamburgische Datenschutzbeauftragte zu den zusätzlichen Bewerberfragebögen äußern können. Im nächsten Tätigkeitsbericht wird darauf zurückzukommen sein.

7.5 Weitergabe von Personaldaten an private Versicherungsgesellschaften

Wiederholt haben sich Petenten an uns gewandt, deren Verbeamtung unmittelbar bevorstand und die in diesem Zusammenhang von privaten Krankenversicherungsgesellschaften angesprochen worden sind. Die Petenten fragen sich, wie die Krankenversicherungen von den Verbeamtungen erfahren konnten.

Die Versicherungen behaupteten, daß sie Namen einerseits durch Empfehlung Dritter und andererseits aus öffentlich zugänglichen Quellen beziehen wie etwa öffentlich ausgehängten Seminarlisten der Universität Hamburg. Die Fachbereiche Rechtswissenschaft I und Erziehungswissenschaft haben uns aber auf Anfrage mitgeteilt, daß Seminarlisten nur in Ausnahmefällen ausgehängt werden und daß die Semesterzahl der Teilnehmer dort nicht genannt wird. Eine „Hochrechnung" der vermeintlichen Studiendauer der Betroffenen durch Mitarbeiter von Versicherungsgesellschaften scheint damit ausgeschlossen.

Leider kann nicht gänzlich ausgeschlossen werden, daß die Versicherungen aus der Verwaltung gezielte Hinweise erhalten. Das Senatsamt für den Verwaltungsdienst hat deshalb auf Bitte und in Abstimmung mit dem Hamburgischen Datenschutzbeauftragten in den Mitteilungen für die Verwaltung Nr. 9 vom 10. September 1992, Seite 193, auf das Problem hingewiesen.

Ein Hintergrundgespräch, das wir bei einer Versicherungsgesellschaft führten, brachte keine wesentlichen neuen Erkenntnisse. Als nächsten Schritt haben wir uns vorgenommen, die offenbar zahlreichen Nebenbeschäftigungsgenehmigungen, die Tätigkeiten für Versicherungsgesellschaften betreffen, zum Gegenstand näherer Erörterungen zu machen.

7.6 Mitarbeiterdaten im Hamburg Handbuch

Aus Anlaß der Neuauflage des Hamburg Handbuchs durch das Senatsamt für den Verwaltungsdienst (SfV) beschäftigte uns die Frage, ob Vornamen und Dienstbezeichnungen von Mitarbeitern veröffentlicht werden dürfen.

Grundsätzlich muß davon ausgegangen werden, daß die öffentliche Verwaltung in einem freiheitlichen und demokratischen Rechtsstaat transparent sein muß. Die öffentliche Verwaltung kann nicht „incognito" arbeiten. Der Bürger hat ein Recht darauf, Entscheidungsträger feststellen und Entscheidungen einschließlich ihrer Urheber nachvollziehen zu können.

Vor diesem Hintergrund war die Veröffentlichung der Nachnamen der Mitarbeiter unbedenklich. Auch gegen die Veröffentlichung ihrer Funktion (Sachbearbeiter, Abteilungsleiter u.ä.) bestehen keine datenschutzrechtlichen Bedenken.

Anders ist jedoch die Veröffentlichung der Vornamen der Mitarbeiter zu beurteilen. Gegen eine Veröffentlichung spricht das Interesse vieler Mitarbeiter an der Geheimhaltung ihrer Vornamen. Gerade in Dienstleistungsbereichen mit schwierigem Publikum kommt es immer wieder vor, daß Mitarbeiter, die mit vollem Vor- und Nachnamen bekannt sind, aus dem Telefonbuch herausgesucht und dann privat belästigt werden. Deshalb haben zahlreiche Mitarbeiter der Veröffentlichung ihrer Vornamen widersprochen.

Auch das SfV sah hinsichtlich der Veröffentlichung der Vornamen schutzwürdige Interessen der Bediensteten berührt. Es verzichtete bereits im März 1992 generell auf die Veröffentlichung der Vornamen im Handbuch, während wir nur die Information über ein Widerspruchsrecht und dann die Beachtung von Widersprüchen im Einzelfall verlangt hatten.

Befremdet hat uns dementsprechend, daß der für das SfV zuständige Senator bei der Herausgabe des neuen Hamburg Handbuchs der Öffentlichkeit erklärte, er habe für das Weglassen der Vornamen kein Verständnis. Diese Aussage steht im Widerspruch zu den vorangegangenen schriftlichen Erklärungen des SfV. Ebenso widersprüchlich erscheint die am Anfang des Hamburg Handbuchs abgedruckte Bemerkung, die Redaktion habe sich kurzfristig entschlossen, auf die Nennung der Vornamen zu verzichten, „um das Erscheinen dieser Ausgabe nicht zu verhindern"; das Ergebnis entspreche keineswegs den Vorstellungen des Herausgebers.

Die Frage der Veröffentlichung der Dienstbezeichnungen konnte jedenfalls im Ergebnis einvernehmlich geregelt werden. Auf sie wurde schließlich verzichtet.

Das SfV hatte ursprünglich die Ansicht vertreten, die Dienstbezeichnungen müßten veröffentlicht werden, um das Geschlecht der Mitarbeiter und ihre hierarchische Stellung zu kennzeichnen. Schließlich durchgesetzt hat sich dann die vergleichsweise einfachere Lösung, das Geschlecht durch den Zusatz

„Herr" oder „Frau" zu kennzeichnen. Die jeweilige Stellung wird am besten gekennzeichnet durch einen Hinweis auf die Funktion und durch die Reihenfolge der Namen, wie es jetzt geschehen ist. Aus der Dienstbezeichnung läßt sich auf die Stellung ohnehin nicht zwingend schließen, weil Mitarbeiter mit derselben Dienstbezeichnung in verschiedenen Bereichen der öffentlichen Verwaltung auf unterschiedlicher Ebene tätig sind.

7.7 HVV-Großkundenabonnement

Im Jahr 1991 führte das Senatsamt für den Verwaltungsdienst in den Behörden und Ämtern eine Umfrage durch, die klären sollte, wie weit die öffentlich Bediensteten ein Angebot des Hamburger Verkehrsverbundes (HVV) für ein Großkundenabonnement nutzen würden. Wir wurden an der Erstellung des Anschreibens und des Fragebogens sehr kurzfristig beteiligt.

Da einerseits die Freiwilligkeit der Beantwortung im Anschreiben ausdrücklich erwähnt und andererseits weder der Name noch die Hausnummer abgefordert wurde, hatten wir keine durchgreifenden datenschutzrechtlichen Bedenken. Nicht deutlich wurde den Befragten allerdings, daß die Angabe der Dienstadresse und der Straße der Wohnadresse dem HVV eine Übersicht über die Verkehrsströme ermöglichen sollte.

Aufgrund der Umfrage vereinbarten die Freie und Hansestadt Hamburg und der HVV die Einführung des Großkundenabonnements (GKA). Der Vertrag sieht eine weitgehende Übernahme der Abonnementverwaltung durch die Personalstellen der Bediensteten und eine Übermittlung personenbezogener Daten an den HVV zur Kontrolle der Fahrtberechtigung vor. Dienstliche Vorgänge wie etwa eine Versetzung werden dem HVV, „private" Vorgänge wie z.B. ein Mißbrauch der Fahrkarte werden der Personalstelle bekannt.

Mit unserem Wunsch, die Abonnementverwaltung entweder ganz den Personalstellen oder ganz dem HVV zu übertragen, um die sonst notwendigen Datenübermittlungen zu vermeiden, drangen wir nicht durch. Erreichen konnten wir jedoch die Aufnahme einer Zweckbindungsklausel in den GKA-Vertrag. Danach darf weder der HVV noch die Personalstelle die im Zusammenhang mit dem GKA verarbeiteten personenbezogenen Daten für andere Zwecke – etwa Werbung bzw. personalrechtliche Maßnahmen – nutzen.

Inzwischen wurde der GKA-Vertrag umgesetzt und die Fahrkartenausgabe durchgeführt. Eingaben und datenschutzrechtliche Beschwerden haben uns seitdem nicht mehr erreicht.

7.8 Erhebung von Gesundheitsdaten bei Bewerbern

Durch Eingaben erfuhren wir von einem Attest, dessen Vorlage die zum Allgemeinen Krankenhaus St. Georg gehörende Lehranstalt für medizinisch-technische Assistenten von Ausbildungsplatzbewerbern verlangte.

Bei diesem Attest handelt es sich um ein Formular der Lehranstalt, das den Bewerbern ausgehändigt wurde, damit diese es von ihrem Hausarzt ausfüllen lassen und dann der Lehranstalt zurückreichen. Das Formular sah neben der datenschutzrechtlich unbedenklichen Gesamtbeurteilung der Eignung des Bewerbers umfangreiche einzelne Angaben vor, die sich auf

- Krankheiten in der Familie,
- die gesundheitliche Vorgeschichte des Bewerbers, einschließlich Unfällen, Operationen, Krankheiten und akuten Beschwerden,
- die allgemeine Körperbeschaffenheit und
- Untersuchungsbefunde von Rachen, Hals, Gebiß, Drüsen, Stimme, Herz, Lunge, Bauchorganen, Haut, Gefäßsystem, Psyche, Zentralnervensystem, Sinnesorgane, Wirbelsäule, Gliedmassen, Bruchanlage und Krampfadern

beziehen.

In einem Fall hatte der Hausarzt der Bewerberin richtigerweise nur die Gesamtbeurteilung in das Attest eingetragen. Daraufhin forderte die Lehranstalt von der Bewerberin, sie solle ihren Arzt zur vollständigen Ausfüllung des Attestes bewegen. Anderenfalls würde ihre Bewerbung abgelehnt werden. Im Interesse seiner Patientin machte der Arzt daraufhin die eigentlich unzulässigen Angaben.

In einem anderen Fall weigerte sich eine Bewerberin, die gesundheitlichen Details der Lehranstalt bekanntzugeben und legte nur ein Attest über die persönliche Eignung vor. Daraufhin wurde ihre Bewerbung abgelehnt.

Auf unsere Intervention hin hat die Lehranstalt das Formular für das Attest inzwischen geändert und läßt sich die Eignung jetzt nur noch in Form einer Gesamtbeurteilung attestieren.

Dadurch sind zwar für die Zukunft unsere datenschutzrechtlichen Bedenken ausgeräumt. Es bleibt aber festzuhalten, daß unter Verstoß gegen das Datenschutzrecht einzelnen Bürgern nicht nur eingehende persönliche Angaben abverlangt, sondern bei Ablehnung der Angaben massive persönliche Nachteile bereitet wurden.

7.9 Personaldatenschutz bei Zuwendungsemfängern

Aus gegebenem Anlaß haben wir uns mit der Frage beschäftigt, wie weit das Kontrollrecht staatlicher Zuwendungsgeber gegenüber privat-rechtlichen Zuwendungsempfängern gehen darf. Im Vordergrund steht die Frage, ob der Zuwendungsempfänger verpflichtet ist, dem Zuwendungsgeber personenbezogen detailliert Angaben über die Tätigkeit/Auslastung der einzelnen Mitarbeiter zu machen. Veranlassung zu dieser prinzipiellen Fragestellung gaben uns entsprechende Erörterungen mit der Wirtschaftsbehörde, die Zuwendungen für

private Beratungsfirmen bewilligt. In diesem Zusamenhang hält sich die Wirtschaftsbehörde für berechtigt und verpflichtet, u.a. die Auslastung und die Tätigkeit der einzelnen Berater zu prüfen.

Wir haben uns mit dem Problem an die für Zuwendungsangelegenheiten zuständige Finanzbehörde gewandt. Wir haben die Finanzbehörde darauf hingewiesen, daß weder die Landeshaushaltsordnung noch die entsprechenden Verwaltungsvorschriften eine normenklare Rechtsgrundlage für die Datenübermittlung enthalten.

Soweit allerdings öffentliche Stellen Zuwendungen erhalten, ist die Verarbeitung von Personaldaten zu Kontrollzwecken gemäß § 13 Abs. 3 HmbDSG legitimiert. Wir sind uns mit den beteiligten Behörden darüber einig, daß bei einer datenschutzgerechten Lösung eine effektive Kontrolle der Zuwendungsnehmer möglich bleiben muß.

8. Statistik

8.1 Landesstatistiken ohne Auskunftspflicht

Neben den „großen" bundesweiten statistischen Erhebungen (z.B. Volkszählungen, Mikrozensus, Handels- und Gaststättenzählung), für die eine Auskunftspflicht besteht, führen hamburgische Behörden vielfältige eigene statistische Erhebungen durch, bei denen die Teilnahme freiwillig ist. Die Ergebnisse derartiger Erhebungen fließen nicht selten in allgemeine Planungsvorhaben ein oder die Erhebungen sind Teil von Forschungsvorhaben.

Im Jahr 1992 ging es erneut in verschiedenen Fällen um die Frage, inwieweit für derartige statistische Erhebungen (Elternbefragung zum Bedarf außerfamiliärer Kinderbetreuung, Befragung über die finanzielle Belastung von Mieterhaushalten, Hamburger Mietenspiegel – 12.3; vgl. auch die Ausführungen zum Hamburger Altenbericht im 10. TB, 6.10) bereichsspezifische Regelungen erforderlich sind. Nachdem im Senat zunächst Zweifel bestanden hatten, ob in solchen Fällen eine Regelung durch Rechtsvorschrift notwendig und angebracht ist, ist diese Frage – auch durch einen Vergleich mit der Rechtslage in anderen Bundesländern – inzwischen für die Praxis erledigt. In den angegebenen Fällen wurde oder wird eine Rechtsvorschrift auch bei Landesstatistiken ohne Auskunftspflicht erlassen.

8.1.1 Abgrenzung von Planung, Forschung und Statistik

Bei den einzelnen Vorhaben war dabei jeweils das Verhältnis von Planung, Forschung und Statistik zu beurteilen, für die jeweils unterschiedliche Rechtsvorschriften einschlägig sind.

Während mit § 27 HmbDSG bereichsspezifische Regelungen für die wissenschaftliche Forschung getroffen wurden und die Datenverarbeitung für Planungszwecke in § 30 HmbDSG geregelt ist, sind für Landesstatistiken die Vorschriften des Hamburgischen Statistikgesetzes einschlägig.

Nach § 5 Hamburgisches Datenschutzgesetz ist die Datenverarbeitung mit Einwilligung des Betroffenen auch ohne ausdrückliche Regelung in einer Rechtsvorschrift zulässig. Dagegen muß gem. § 2 Abs. 3 HmbStatG auch eine statistische Erhebung auf freiwilliger Basis durch Rechtsverordnung angeordnet werden. Somit ist die Frage, inwieweit es sich bei den betreffenden Erhebungen jeweils um Statistiken handelt, bedeutsam.

Weder in den Datenschutzgesetzen noch im Statistikrecht finden sich handhabbare Abgrenzungen der Begriffe „wissenschaftliche Forschung", „Statistik" und „Planung". Aus der Literatur ergibt sich, daß eine Erhebung immer dann statistischen Charakter hat, wenn sie auf die Analyse von Massenerscheinungen abzielt, ohne damit über die Verhältnisse der einzelnen Individuen Aussagen zu machen. Statistik ist also immer abstrakt; das Erkenntnisinteresse richtet sich auf Sachverhalte, die bei einer Vielzahl von Erhebungseinheiten anzutreffen sind, nicht jedoch auf den einzelnen Betroffenen. Statistik stellt stets in gewisser Weise eine Datenhaltung auf Vorrat dar, da die Interpretation der gewonnenen Ergebnisse – z.B. im Rahmen von Forschungsvorhaben – zu neuen Auswertungsansätzen und damit zu Zweckänderungen der erhobenen Daten führen kann.

Allgemein gilt: Je größer die Anzahl der Erhebungseinheiten ist und je weniger konkret der Bezug zwischen der Einzelangabe und dem Erkenntnisziel ist, desto wahrscheinlicher ist es, daß es sich im jeweiligen Fall um eine Statistik handelt, die einer Anordnung durch Rechtsvorschrift bedarf. Dies gilt nicht für die statistische Auswertung bereits vorhandenen Materials, das z.B. beim Verwaltungsvollzug angefallen ist. Für derartige „Geschäftsstatistiken" muß gem. § 2 Abs. 2 Nr. 4 HmbStatG keine Rechtsvorschrift erlassen werden.

8.1.2 Umsetzungsprobleme

Den auftretenden Datenschutzproblemen kann bei der Statistik vor allem dadurch Rechnung getragen werden, daß die bei der Erhebung gewonnenen personenbezogenen Angaben frühestmöglich anonymisiert werden und die Daten – mindestens bis zu ihrer Anonymisierung – von anderen Daten der Verwaltung strikt abgeschottet werden.

Nach § 5 HmbStatG ist im allgemeinen das Statistische Landesamt zuständig für die Durchführung von Statistiken. Soweit es sich dabei um klassische „Nur-Statistiken" ohne einen direkten Bezug zu einem Planungs- oder Forschungsvorhaben handelt, ist diese Zuständigkeit unbestritten. Dagegen tendieren Fachbehörden dazu, auch den statistischen Teil von Planungen (z.B. bei der Datenerhebung für den Hamburger Altenbericht) in eigener Regie durchzuführen oder aber im Rahmen eines Gesamtvorhabens an Forschungsinstitute zu vergeben.

Da die Fachbehörden regelmäßig auch Daten für Verwaltungszwecke verarbeiten, müssen die mit der Durchführung der statistischen Arbeiten betrauten Stellen von der übrigen Behörde wirksam abgeschottet werden. Dies kann im Einzelfall zu erheblichen Problemen führen. So wäre es nicht hinzunehmen, wenn diejenigen Personen, die Zugang zu personenbezogenen statistischen Angaben haben, zugleich auch andere Verwaltungsaufgaben innerhalb der Behörde wahrnehmen, bei denen ebenfalls personenbezogene Daten verarbeitet werden. Problematisch wäre auch die Verarbeitung noch nicht anonymisierter Daten auf Datenverarbeitungsanlagen (z.B. PC oder Abteilungsrechnern), die auch für sonstige Verwaltungsaufgaben genutzt werden.

Auch die Festlegung des Fragenkatalogs kann zu Schwierigkeiten führen. Nach § 2 Abs. 3 HmbStatG müssen die Ergebnisse der Erhebung für bereits festliegende Aufgaben des Landes erforderlich sein. Gerade bei allgemeinen Planungs- und Forschungsvorhaben ist nur schwer zu beurteilen, inwieweit die einzelnen Erhebungstatbestände für die Aufgabenerfüllung erforderlich sind. Grundsätzlich sollte daher für jedes Erhebungsmerkmal dargelegt werden, inwieweit es jeweils erforderlich ist.

Ein besonderes Problem stellen sogenannte Telefoninterviews dar. Das Hamburgische Statistikgesetz schreibt vor, daß sich die Interviewer auszuweisen haben. Damit soll sichergestellt werden, daß sich der Befragte von der Identität und Berechtigung des Interviewers überzeugen kann. Dies ist bei Telefoninterviews nur zu gewährleisten, wenn zwischen der befragenden Stelle und dem Befragten ein vertraulicher individueller Schlüssel (z.B. ein bestimmtes „Stichwort") ausgetauscht wird und der Betroffene die Möglichkeit hat, sich durch Rückruf bei der für die Befragung zuständigen Stelle von der Identität des Interviewers zu überzeugen. Ferner muß eine rechtzeitige schriftliche Information erfolgen, wobei insbesondere auf die Freiwilligkeit hingewiesen wird und eine Aufklärung über die Rechtsgrundlage und die Hilfs- und Erhebungsmerkmale erfolgt.

8.2 Umstellung der Prüfungsstatistik auf das neue Hochschulstatistikgesetz des Bundes

Durch eine Eingabe haben wir davon erfahren, daß die Universität Hamburg noch im Sommer 1992 bei Prüfungskandidaten für die Prüfungsstatistik umfangreiche Angaben erhob, obwohl nach dem am 1. Juni 1992 in Kraft getretenen Hochschulstatistikgesetz vom 2. November 1990 die Prüfungsstatistik auf eine reine Sekundärerhebung mit reduziertem Erhebungsumfang hätte umgestellt werden müssen. Die Erhebung geschah auf alten Erhebungsunterlagen unter Hinweis auf nicht mehr gültige Rechtsgrundlagen und die in diesen enthaltenen Auskunftspflichten.

Das Vorgehen der Prüfungsämter war schwer nachvollziehbar, weil zwischen der Verkündung des Gesetzes und seinem Inkrafttreten achzehn Monate lagen und die zuständigen Stellen damit genügend Zeit für die Umstellung der Statistik hatten. Die Behörde für Inneres – Statistisches Landesamt – hatte die Hamburger Hochschulen frühzeitig über die zum 1. Juni 1992 notwendigen Umstellungen informiert.

Offenbar hatte die Universität Hamburg die Arbeiten gleichwohl viel zu spät in Angriff genommen. Die zuständigen Prüfungsämter waren weder von der Universitätsverwaltung noch von der Behörde für Wissenschaft und Forschung darüber in Kenntnis gesetzt worden, daß das neue Hochschulstatistikgesetz mit einem umgestellten Erhebungsverfahren und -katalog ab 1. Juni 1992 anzuwenden ist.

Wir haben bei dieser Sachlage die zuständigen Stellen aufgefordert, auf die unzulässige Datenerhebung umgehend zu verzichten.

Da die Verarbeitung der alten Erhebungsunterlagen durch das Statistische Landesamt vom Beginn des Wintersemesters 1992/93 an aus technischen Gründen nicht mehr möglich ist, hat die Universität Hamburg zugesagt, die Verfahrensumstellung nunmehr nicht – wie bislang geplant – erst zum Sommersemester 1993, sondern bereits zum Wintersemester 1992/93 vorzunehmen. Die automatisierte Erfassung der Erhebungsunterlagen, die von den Prüfungsämtern nach dem neuen Verfahren an das Studentensekretariat gesandt werden, wird wegen der noch zu erledigenden ADV-Entwicklungsarbeiten in der Universität erst im nachhinein erfolgen.

Diejenigen Absolventen, die zwischen dem 1. Juni und dem 30. September 1992 bereits alte Erhebungsvordrucke abgegeben haben, werden von den Prüfungsämtern angeschrieben und erhalten die Möglichkeit, der Verarbeitung ihrer Daten zu widersprechen. Sofern sie hiervon Gebrauch machen, werden ihre Daten gelöscht. Auf alten Formularen erhobene Daten von dem Sommersemester 1992 zuzuordnenden Absolventen, die ab dem 1. Oktober 1992 ihre Prüfung beenden (dies sind solche Perüfungskandidaten, die ihre Prüfung zwar im Sommersemester begonnen, jedoch nicht abgeschlossen haben), werden nur mit ausdrücklicher schriftlicher Einwilligung verarbeitet.

Gegen dieses Verfahren bestehen keine datenschutzrechtlichen Bedenken.

9. Schulwesen

9.1 Schulgesetzentwurf

Die Behörde für Schule, Jugend und Berufsbildung (BSJB) hat im Berichtszeitraum einen deutlich verbesserten Gesetzentwurf zur Einfügung datenschutzrechtlicher Bestimmungen in das Schulgesetz vorgelegt. Dieser ist in erfreulich enger Abstimmung mit uns überarbeitet und weiter verbessert worden. Kurz vor Redaktionsschluß erhielten wir dann einen deutlich gekürzten Gesetzentwurf;

die zuvor erzielte Entwurfsfassung war der BSJB „zu lang" geworden. Besondere Erwähnung verdienen folgende Punkte:

— Differenziert nach den verschiedenen Beratungs- und Untersuchungsaufgaben des schulärztlichen Dienstes und des Schulberatungsdienstes sollen die Mitwirkungspflichten der Schüler und Erziehungsberechtigten geregelt werden.

  Die schulärztlichen Untersuchungen sollen weit über die Feststellung der Schulfähigkeit hinausgehen und eine umfassende Prüfung der Gesundheit der Schüler beinhalten. Ihre Ergebnisse werden im Rahmen der schulärztlichen Dokumentation ausgewertet.

  Da wir der Auffassung sind, daß es in einem freiheitlichen Gemeinwesen generell jedem selbst überlassen ist, ob und aus welchen Gründen er sich ärztlich untersuchen läßt, hatten wir hinsichtlich des vorgesehenen Umfangs der schulärztlichen Untersuchung zunächst Bedenken geäußert. Wir verkennen aber nicht, daß das Grundgesetz die Pflege der Kinder der Überwachung durch die staatliche Gemeinschaft unterwirft. Daher haben wir unsere grundsätzlichen Bedenken fallengelassen. Einigkeit haben wir darüber erzielt, daß die Beantwortung von Fragen zur gesundheitlichen Situation und Vorgeschichte freiwillig ist.

— Die Daten, die im Schulbereich verarbeitet werden dürfen, sollten ursprünglich im einzelnen und abschließend aufgeführt werden. Diese Datenkränze sind jedoch weitgehend nicht mehr im Gesetzentwurf enthalten und bleiben nun einer Rechtsverordnung vorbehalten.

— Für die Datenübermittlungen, die in besonders empfindlicher Weise in das informationelle Selbstbestimmungsrecht der Betroffenen eingreifen, soll es ausdrückliche Regelungen geben, die speziell auf die Bedürfnisse des Schulbereichs zugeschnitten und damit enger gefaßt sind, als im Hamburgischen Datenschutzgesetz (HmbDSG). Auch die Übermittlung der besonders sensiblen Daten des schulärztlichen und schulpsychologischen Dienstes soll aufgabenspezifisch geregelt werden.

— Für die Anforderungen an eine automatisierte Datenverarbeitung sollen grundsätzlich die Regelungen des HmbDSG gelten. Zwei Besonderheiten des Schulbereiches sollen aber im Schulgesetz ausdrücklich geregelt werden. Dies betrifft zum einen das Verbot der Vernetzung bestimmter Geräte und zum anderen die Zulässigkeitskriterien für den Einsatz privater PC durch Lehrer (s. auch 9.2).

— Um ein einheitliches Datenschutzrecht an allen Schulen zu erreichen, haben wir der BSJB empfohlen, für Privatschulen datenschutzrechtliche Bestimmungen zu schaffen, die denen für die staatlichen Schulen entsprechen. Bislang ist aber offen, ob die BSJB diesem Vorschlag folgt.

— Einer Rechtsverordnung vorbehalten bleiben neben den zulässigen Datenkränzen insbesondere ergänzende Regelungen über Aufbewahrungsfristen und über das Verfahren bei Auskunfts- und Einsichtsgewährung.

Damit die Datenverarbeitung im Schulbereich umfassend geregelt wird, ist es erforderlich, die Rechtsverordnung mit den ergänzenden Regelungen, insbesondere der Datenkränze, gleichzeitig mit dem Gesetzentwurf auf den Weg zu bringen. Beide Regelungen sollten möglichst bald umgesetzt werden.

9.2 Regelung zur Verwendung privater PC durch Lehrer

Wir hatten im letzten TB (9.2) darüber berichtet, daß wir der Behörde für Schule, Jugend und Berufsbildung (BSJB) vorgeschlagen haben, ihr bisheriges Verbot der Verwendung privater PC durch Lehrer außerhalb von Diensträumen durch eine grundsätzliche, an Bedingungen gebundene Gestattung zu ersetzen.

Die BSJB hat inzwischen in Abstimmung mit uns eine Regelung entworfen, die weitgehend unseren Vorstellungen entspricht. Da dieser Regelungsentwurf in Teilen der Elternschaft zu regen Diskussionen geführt hat, sei zunächst noch einmal dargestellt, welche Gründe uns zu unserem Vorstoß bewogen haben:

Die Arbeit der Lehrer ist – anders als die der meisten anderen Berufsgruppen – dadurch gekennzeichnet, daß sie in erheblichem Umfang außerhalb von Diensträumen verrichtet werden muß. Lehrer sind also schon seit jeher gefordert, in ihrem privaten Bereich Daten zu verarbeiten, diese Daten zu schützen und demgemäß ihren häuslichen Arbeitsplatz an die Erfordernisse des Datenschutzes anzupassen.

Während diese Datenverarbeitung in der Vergangenheit noch manuell erfolgte, entspricht es dem Trend der Zeit, auch insoweit automatisierte Datenverarbeitung einzusetzen. Lehrern war bisher aber die häusliche Benutzung von PC verboten; zugleich war bekannt, daß das Verbot vielfach nicht beachtet wird. Statt eines nur theoretischen Verbots halten wir es im Interesse des Datenschutzes für wirksamer, eine automatisierte Datenverarbeitung in diesem Bereich hinzunehmen, sofern dabei die notwendigen Datensicherungsmaßnahmen eingehalten werden.

Die Einhaltung der Datensicherungsmaßnahmen hängt wesentlich davon ab, daß sie von den Lehrern als praxisgerecht akzeptiert werden, denn eine Überwachung der Lehrer ist nur begrenzt möglich.

Der Regelungsentwurf ist in seiner letzten Fassung wie folgt konzipiert:

— Die Regelung gestattet nur die Verarbeitung von Daten solcher Schüler, die der Lehrer unterrichtet bzw. betreut. Insoweit darf er allerdings auch Daten über Kollegen verarbeiten, die die jeweiligen Schüler ebenfalls unterrichten.

— Der Kranz der Daten, die ohne Einwilligung gespeichert werden dürfen, wird abschließend geregelt. Hinsichtlich einzelner Daten wie der Staatsangehörigkeit erscheint zwar einerseits zweifelhaft, ob sie in diesen Datenkranz einbezogen werden mußten; unseren insoweit geäußerten Bedenken hat die BSJB nicht Rechnung getragen. Andererseits gilt auch innerhalb des Datenkranzes der Erforderlichkeitsgrundsatz: Jeder Lehrer darf ihn nur insoweit ausschöpfen, als dies für seine Aufgabenerfüllung erforderlich ist.

— Sobald einzelne Daten nicht mehr benötigt werden, sind sie physikalisch zu löschen. Bei der Konkretisierung dieses Grundsatzes konnten wir mit der BSJB kein völliges Einvernehmen erzielen.

  Wir hatten einen Hinweis empfohlen, daß Zeugnisdaten spätestens nach Erteilung des nächsten Zeugnisses zu löschen sind. Dem lag die Erwägung zugrunde, daß die Beurteilung eines Schülers sich grundsätzlich nur auf sein Auftreten und seine Leistung innerhalb des Beurteilungszeitraums beziehen soll. Daten aus der davor liegenden Vergangenheit sollten gerade nicht zum Gegenstand einer Beurteilung gemacht werden. Da auf automatisiert gespeicherte Daten leichter zugegriffen werden kann, bergen sie die Gefahr, daß der „Segen des Vergessens" den Schülern öfter versagt bleibt.

  Letztlich haben wir uns mit der BSJB auf einen Kompromiß verständigt, demzufolge das Löschungsgebot in der Weise konkretisiert wird, daß Zeugnisdaten gelöscht werden sollen, „wenn sie für die Beurteilung der Leistungs- und Schullaufbahnentwicklung nicht mehr benötigt werden". Dies ist nach unserer Auffassung regelmäßig dann der Fall, wenn das jeweils nächste Zeugnis erteilt worden ist.

— Die Daten dürfen nur von dem jeweiligen Lehrer verwendet werden. Um dies zu erreichen, sind Datenübertragungen und der Austausch von Datenträgern untersagt, soweit sie nicht innerhalb der Schule im Rahmen der Schulverwaltung erfolgen.

— Datenträger sind so unter Verschluß zu halten, daß sie Unbefugten, z.B. Familienmitgliedern, nicht in die Hände gelangen. Ebenfalls ist die Festplatte davor zu schützen, daß Unbefugte die auf ihr gespeicherten Daten lesen können.

— Der Lehrer muß der Schulleitung und der BSJB jederzeit einen Ausdruck aller gespeicherten Daten zur Verfügung stellen. Dadurch ist auch die Erfüllung des Auskunftsanspruchs sichergestellt.

— Dem Hamburgischen Datenschutzbeauftragten ist Gelegenheit zur datenschutzrechtlichen Überprüfung zu geben. Diese kann im Regelfall in der Schule erfolgen, wohin der Lehrer Hard- und Software zu bringen hat.

Auf eine Regelung, die uns auch gegen den Willen der Lehrer berechtigt, in deren Privaträumen eine datenschutzrechtliche Kontrolle vorzunehmen, haben wir bewußt verzichtet. In einer Zeit, in der staatliche Stellen zunehmend bemüht sind, in die Privatsphäre der Bürger eindringen zu dürfen, halten wir es für unangebracht, ein solches Recht einem Datenschutzbeauftragten einzuräumen.

— Ein Lehrer, der seinen privaten PC für Schulverwaltungsaufgaben nutzen will, verpflichtet sich durch Abgabe einer entsprechenden schriftlichen Erklärung gegenüber der Schulleitung, die Modalitäten der Regelung einzuhalten. Über die Abgabe dieser Verpflichtungserklärung erhält er eine Empfangsbestätigung, mit deren Erhalt die Verwendung des privaten PC als genehmigt gilt.

— Die Verpflichtungserklärungen werden dezentral in Karteien an den Schulen gesammelt. Da sie auch die Angaben über Hard- und Software enthalten, die nach § 9 Abs. 3 HmbDSG im Geräteverzeichnis enthalten sein müssen, bilden diese Karteien zugleich ein Geräteverzeichnis.

— Da damit zu rechnen ist, daß ein großer Teil der Lehrerschaft von der Regelung Gebrauch macht, galt es, für die Dateibeschreibungen und -meldungen ein vereinfachtes Verfahren zu finden, denn weder die BSJB noch wir haben ein Interesse daran, daß tausende von Dateibeschreibungen administrativ bewältigt werden müssen. Auch dem Datenschutz würde das nicht dienen. Wir haben uns daher auf folgendes Verfahren verständigt:

  Die BSJB meldet entsprechend der abgestimmten Regelung pauschaliert eine Datei zum Dateienregister. In dieser pauschalierten Dateimeldung sind die Angaben nach § 9 Abs. 1 HmbDSG enthalten, ausgenommen der konkrete Standort der Dateien. Die pauschalierte Dateimeldung wird kombiniert mit dem Hinweis auf die an den Schulen geführten Karteien der Verpflichtungserklärungen. Dadurch wird mittelbar auch der Standort der Dateien deutlich.

  Ein solches Verfahren entspricht in jeder Hinsicht dem Sinn und Zweck von Dateibeschreibung und -meldung. Insbesondere können die in § 24 Abs. 2 Satz 3 HmbDSG verankerten subjektiven Rechte weiterhin geltend gemacht und erfüllt werden. Vorsorglich soll eine generelle Regelung über pauschalierte Dateimeldungen bei der bevorstehenden Novellierung des HmbDSG aufgenommen werden.

9.3 Betriebspraktika von Schülern

In einer Vielzahl öffentlicher Stellen machen Schüler sogenannte Berufsfindungs- oder „Schnupper"-Praktika. Dabei kommen sie teilweise zwangsläufig mit personenbezogenen Daten in Berührung, darunter auch Sozialdaten und Steuerdaten, also solchen Daten, die besonderen Schutzvorschriften unterliegen.

Die Behörde für Schule, Jugend und Berufsbildung (BSJB) hat bislang zwar verschiedene Richtlinien für diese Praktika erlassen, die u. a. regeln, wo diese Praktika erfolgen sollen. Sie weiß jedoch nicht, wo sie tatsächlich stattfinden. Die Dienststellen wiederum, die die Praktika durchführen, kennen diese Richtlinien gar nicht. So finden im Bereich der Polizei Praktika statt, obwohl dies nach den Richtlinien untersagt ist. Mit der Frage der Gewährleistung des Datenschutzes befassen sich diese Richtlinien ohnehin überhaupt nicht. Die BSJB weist insoweit auch jegliche Zuständigkeit von sich.

Damit im Rahmen dieser Praktika kein schrankenloser Umgang mit personenbezogenen Daten erfolgt, haben wir den Kranken-, Renten- und Unfallversicherungsträgern Empfehlungen zur Gewährleistung des Datenschutzes gegeben. Im Hinblick auf die zahlreichen weiteren öffentlichen Stellen der hamburgischen Verwaltung haben wir dem Senatsamt für den Verwaltungsdienst (SfV) vorgeschlagen, entsprechend diesen Empfehlungen in seinen „Richtlinien über die Ausbildungsbedingungen der Hospitanten" Maßnahmen vorzusehen.

Inhaltlich sollte von folgendem ausgegangen werden:

Es muß stets eine sorgfältige Abwägung mit den schutzwürdigen Interessen der Betroffenen erfolgen. Dort wo der Einsatz von Lehrmaterial, Testdaten u.ä. erfolgen kann, sollte er auch erfolgen. Der Umgang mit Echtdaten sollte auf ein Minimum beschränkt bleiben. Ein Umgang mit Gesundheitsdaten sollte ganz unterbleiben.

Dort wo ein Umgang mit Echtdaten erfolgt, muß den Schülern in deutlicher Weise klargemacht werden, daß sie zur Verschwiegenheit verpflichtet sind. Dies sollte vorzugsweise durch eine förmliche Verpflichtung nach dem sog. Verpflichtungsgesetz erfolgen, wie es für Rechtspraktikanten bereits in § 6 der Juristenausbildungsordnung und im übrigen in der DS-Richtlinie des SfV vorgesehen ist. Darüberhinaus wäre es sinnvoll, auch die Erziehungsberechtigten über die Verschwiegenheitsverpflichtung ihrer Kinder zu unterrichten.

Im Hinblick auf die erforderliche Einsichtsfähigkeit sollten die Schüler ein Mindestalter haben, das nicht unter der Vollendung des 14. Lebensjahres liegen sollte. Als weiteres Korrektiv zu einer unbeschränkten Informationsverbreitung sollte für die Praktika eine maximal zulässige Dauer von höchstens 4 Wochen vorgesehen werden. Zum Publikumsverkehr sollte ein Schüler allenfalls hinzugezogen werden, wenn sich die Betroffenen zuvor ausdrücklich damit einverstanden erklärt haben.

Eine Stellungnahme des SfV steht noch aus.

10. Steuerwesen

10.1 Keine Änderung der Abgabenordnung (AO)

Im letzten Tätigkeitsbericht (10. TB, 10.1) haben wir über die beabsichtigte Änderung der Abgabenordnung berichtet, die immer noch nicht erfolgt ist. Ein

Schwerpunkt des Gesetzentwurfs ist die Ergänzung der Abgabenordnung um bereichsspezifische Datenschutzvorschriften. Insbesondere die vorgesehene Neufassung des § 30 AO soll der neueren Datenschutzgesetzgebung Rechnung tragen und den Umgang mit Daten, die dem Steuergeheimnis unterliegen, klarer als bisher regeln.

Der aktuelle Entwurf des Gesetzes zur Änderung der Abgabenordnung (AOÄG, Stand August 1992) berücksichtigt nunmehr die im vergangenen Jahr erhobene Kritik, mit der Änderung der AO würden bestehende Bestimmungen in den Landesdatenschutzgesetzen auf verfassungsrechtlich unzulässige Weise eingeschränkt. Gemäß § 31 b AOÄG sollen jetzt die Vorschriften der Landesdatenschutzgesetze über die Bestellung, die Rechtsstellung sowie die Rechte und Pflichten der Landesdatenschutzbeauftragten gegenüber den Landesfinanzbehörden ausdrücklich unberührt bleiben. Es soll auch gewährleistet werden, daß den Landesdatenschutzbeauftragten ein Zeugnisverweigerungsrecht zusteht und daß ihnen bei der Wahrnehmung ihrer Kontrollaufgaben nicht das Steuergeheimnis entgegengehalten werden kann.

Während unserer Kritik in diesem wesentlichen Punkt Rechnung getragen wurde, greift die aktuelle Fassung des Referentenentwurfs auch weiterhin nicht alle wiederholt vorgetragenen Forderungen zur Änderung der AO auf.

§ 105 Abs. 2 AOÄG sieht bei den Auskunfts- und Vorlagepflichten öffentlicher Stellen gegenüber Finanzbehörden noch immer nicht den Schutz des Sozialgeheimnisses und die Anerkennung der ärztlichen Schweigepflicht vor. Statt dessen wird darauf verwiesen, daß außer dem grundrechtlich geschützten Brief-, Post- und Fernmeldegeheimnis weitere Amts- und Berufsgeheimnisse den Auskünften und Vorlagen nur dann entgegengehalten werden können, wenn ein Bundesgesetz dies an anderer Stelle ausdrücklich regelt.

Verzichtet wird auch darauf, die Voraussetzungen für Auskunftsersuchen nach §§ 93, 208 AO – insbesondere der Steuerfahndung – genauer zu definieren, da insoweit eine gefestigte Rechtsprechung des Bundesfinanzhofs vorliege und das Bundesverfassungsgericht diese Vorschriften in anderem Zusammenhang zuletzt für datenschutzrechtlich unbedenklich gehalten habe. Gerade im Hinblick auf das verfassungsrechtliche Gebot der Normenklarheit sollten aber nach unserer Auffassung die bisher von der Rechtsprechung entwickelten Grundsätze in die Abgabenordnung aufgenommen werden, nach denen Ermittlungen nur zulässig sind, wenn ein hinreichender Anlaß hierfür besteht und die Möglichkeit einer objektiven Steuerverkürzung vorliegt.

Offen bleibt neben den Bemühungen um eine Änderung der Abgabenordnung weiterhin der Erlaß einer Rechtsverordnung gemäß § 93a AO, die Art und Umfang von Mitteilungen öffentlicher Stellen an die Finanzbehörden regelt. Es fehlt daher zur Zeit immer noch an jeglicher Rechtsgrundlage für die allgemeine Übermittlung von Kontrollmitteilungen an die Finanzämter.

10.2 Private PC im Betriebsprüfungsdienst

Wie im 10. TB (10.2) angekündigt, versucht die Finanzbehörde, den Einsatz privater Personal Computer (PC) für dienstliche Zwecke auf Dauer einzuschränken. Zu diesem Zweck sind für das Haushaltsjahr 1993 erhebliche finanzielle Mittel für den Kauf von tragbaren Rechnern eingeworben worden, so daß davon ausgegangen werden kann, daß die privat eingesetzten Geräte Zug um Zug durch dienstlich bereitgestellte PC ersetzt werden.

Die zugesagte Dienstvereinbarung, in der die Nutzung der PC umfassend geregelt werden sollte, ist bisher leider immer noch nicht in Kraft getreten. Entsprechende Entwürfe befinden sich derzeit noch in der Behördenabstimmung.

10.3 Zeichnungsvorbehalt der Finanzamtsvorsteher

Im 10. TB (10.3) haben wir deutlich zum Ausdruck gebracht, daß wir die gegenwärtige Regelung in § 23 Abs. 1 Nr. 4 der bundeseinheitlich geltenden Geschäftsordnung für die Finanzämter (FAGO), nach der der Finanzamtsvorsteher die Steuerangelegenheiten von amtsangehörigen Mitarbeitern abschließend zu zeichnen hat, für eine unverhältnismäßige Beeinträchtigung des informationellen Selbstbestimmungsrechts der Betroffenen halten.

Unserem Vorschlag, grundsätzlich eine abweichende örtliche Zuständigkeit, z.B. in der Abgabenordnung (AO), vorzusehen, sind die obersten Finanzbehörden des Bundes und der Länder nicht bereit zu folgen. Es genüge eine Zuständigkeitsvereinbarung nach § 27 AO, die bei Bedarf in jedem Bundesland im Wege der Verwaltungsanweisung angeordnet werden könne.

Im Juni 1992 hat sich nun auch die Deutsche Steuer-Gewerkschaft öffentlich dafür ausgesprochen, § 23 Abs. 1 Nr. 4 FAGO ersatzlos zu streichen, da es sich dabei einerseits um eine unbefugte Offenbarung und Verwertung der steuerlichen Verhältnisse von Amtsangehörigen handelt, andererseits der Finanzamtsvorsteher disziplinar- und strafrechtlichen Risiken ausgesetzt sein könnte.

Die Oberfinanzdirektion Hamburg befürwortet eine Änderung der FAGO. Sie hat eine entsprechende Stellungnahme an die Finanzbehörde geleitet. Außerdem hat sie die Bediensteten der hamburgischen Steuerverwaltung auf ihr Recht hingewiesen, in den Fällen, in denen sie als Amtsangehörige auch im selben Finanzamt steuerlich geführt werden, ihre Steuerangelegenheiten von einem anderen Hamburger Finanzamt bearbeiten zu lassen. Jeder Bedienstete, der von seinem Recht, nach § 27 AO eine abweichende Zuständigkeitsvereinbarung zu treffen, Gebrauch machen möchte, soll den Wunsch seinem Vorsteher unterbreiten.

Eine bindende Verwaltungsanordnung, wie sie in einigen anderen Bundesländern bereits erlassen worden ist, wurde in Hamburg bisher zwar noch nicht veröffentlicht. Wir sind jedoch auch weiterhin der Auffassung, daß das Recht der Finanzamtsangehörigen auf eine grundsätzlich abweichende Zuständigkeit für die Bearbeitung ihrer Steuerangelegenheiten gesetzlich abgesichert werden muß. Nur dadurch kann verhindert werden, daß sich der betroffene Bedienstete einem Begründungszwang für sein Anliegen ausgesetzt sieht.

10.4 Zugriff der Steuerfahndung auf Patientendaten

Im Dezember 1991 hat der Bundesgerichtshof (BGH) entschieden, daß die strafprozessuale Beschlagnahme und Verwertung einer Patientenkartei zulässig ist, wenn der Arzt selbst Beschuldigter ist und die Maßnahme dem Gebot der Verhältnismäßigkeit (Erforderlichkeit und Angemessenheit) entspricht.

Zugrunde lag die Revision gegen eine Entscheidung des Landgerichts Memmingen, daß einen Frauenarzt wegen Abbruchs der Schwangerschaft in mehreren Fällen zu einer Freiheitsstrafe verurteilt hatte (Fall „Dr. Theissen"). Wohnung und Praxis des Arztes waren wegen des Verdachts der Steuerhinterziehung von der Steuerfahndung durchsucht worden. Dabei war die Patientenkartei beschlagnahmt worden, dann an das Amtsgericht wegen des Verdachts eines Schwangerschaftsabbruches ohne ärztliche Feststellung abgegeben und dort im gerichtlichen Ermittlungsverfahren und der Hauptverhandlung verwertet worden.

Der BGH hat in seinem Urteil klargestellt, daß § 97 Strafprozeßordnung der Beschlagnahme der Patientenkartei nicht entgegensteht. Das Zeugnisverweigerungsrecht des Arztes sei nur dann zu berücksichtigen, wenn sich die Ermittlungen gegen einen Patienten richten. Wird der Arzt beschuldigt, kann die Steuerfahndung die Patientenkartei beschlagnahmen. Auch in der Abgabe an das Amtsgericht sah der BGH keine Verfahrensverletzung, da § 30 Abs. 4 Nr. 5 Abgabenordnung diese Datenübermittlung rechtfertigen würde.

Die Wahrheitsermittlung im Strafverfahren genieße den Vorrang gegenüber privaten Geheimhaltungsinteressen, wenn der Arzt selbst Beschuldigter sei, der Einblick in die Patientenkartei zur Aufklärung der Straftat erforderlich sei und die Maßnahme dem Grundsatz der Verhältnismäßigkeit nicht widerspreche. Diese Voraussetzungen wurden als gegeben angesehen, insbesondere weil der Verdacht zahlreicher illegaler Schwangerschaftsabbrüche bestanden habe.

Das Zeugnisverweigerungsrecht des Arztes gilt demnach also nur dann, wenn der Arzt als Zeuge in einem Verfahren gegen den Patienten auftreten soll. Wenn der Arzt selbst beschuldigt wird, soll der Zugriff auf hochsensible personenbezogene Daten unbeteiligter Patienten erlaubt sein. Der Schutz von Patientendaten wird mit dieser Entscheidung völlig unzureichend berücksichtigt. Die Patienten haben ein begründetes Interesse daran, daß ihre gesund-

heitlichen Verhältnisse nur für Zwecke der Behandlung von den Ärzten verwendet werden, denen sie sich anvertraut haben.

Schon das bisher geltende Recht gestattet eine Prüfung der Verhältnismäßigkeit der Beschlagnahme von Patientendateien. Im Einzelfall wäre z. B. die Möglichkeit einer Anonymisierung zu prüfen gewesen. Die Steuerfahndung hat in dem beschriebenen Fall davon aber nicht Gebrauch gemacht. Wenn das Bundesverfassungsgericht aufgrund der von dem betroffenen Arzt eingelegten Verfassungsbeschwerde die Entscheidung des BGH bestätigen sollte, sind eindeutige datenschutzrechtliche Regelungen in der Strafprozeßordnung erforderlich.

11. Wissenschaft und Forschung

11.1. Datenerhebung durch die Hochschulen

11.1.1. Hochschuldatenverordnung

Mit dem im April 1992 vorgelegten Entwurf einer Hochschuldatenverordnung wird erstmalig auf dem Verordnungsweg geregelt, welche Verwaltungsdaten von Studienbewerbern und Studenten den Hochschulen im einzelnen mitzuteilen sind. Dem Entwurf vorausgegangen war eine entsprechende Änderung von § 142 HmbHG (Hochschulrechtsänderungsgesetz vom 18. April 1991). Wir begrüßen, daß nunmehr auch in diesem Bereich den Forderungen des Bundesverfassungsgerichts aus dem Volkszählungsurteil nach einer bereichsspezifischen und präzisen gesetzgeberischen Regelung Rechnung getragen wird.

Ursprünglich hatte der Entwurf einen Gesamtkatalog der von den Studenten und Studienbewerbern mitzuteilenden Daten vorgesehen. Wie auch andere Behörden haben wir uns mit Erfolg dafür eingesetzt, daß nunmehr normenklar geregelt ist, zu welchem Zweck im einzelnen welche Daten mitzuteilen sind.

Bezogen auf die einzelnen Daten haben wir darauf hingewirkt, daß die Angabe des Familienstandes entfällt und die Konfessionszugehörigkeit nur noch bei der Prüfungszulassung im Studiengang Evangelische Theologie abgefragt wird. Ein Lebenslauf wird jetzt nur noch in künstlerischen Fächern bei der Aufnahmeprüfung verlangt. Auf unseren Vorschlag hin entfiel die Begründung für vorherige Immatrikulationen im Zulassungsverfahren.

11.1.2. Fragebogen der Hochschule für bildende Künste

Einen praktischen Anlaß, uns mit der Datenerhebung duch die Hochschulen zu befassen, bot eine Eingabe, die sich gegen den Fragebogen für Studienplatzbewerber an einem Fachbereich der Hochschule für bildende Künste richtete.

Der Fragebogen bestand aus insgesamt 10 Fragen, die teilweise stark in den Persönlichkeitsbereich der Studienbewerber eingreifen. Frage 10 etwa lautete: „Was bedeutet für Sie Erfüllung im Leben?"; unter Frage 8 hieß es „Welche Bücher haben Sie in letzter Zeit gelesen?". Einleitend wurde im Fragebogen vermerkt. „Ihre Aussage soll uns ein Bild von Ihrer Persönlichkeit vermitteln . . .".

Wir haben uns an den Fachbereich mit der Frage gewandt, inwieweit ein umfassendes Persönlichkeitsbild für die Studienplatzvergabe erforderlich ist, und baten zusätzlich um Erläuterung einzelner Fragen aus dem Fragebogen.

Der Fachbereich hat daraufhin auf die weitere Verwendung des Fragebogens verzichtet und zugesagt, alle entsprechenden Unterlagen nicht zu verwerten, sondern zu vernichten.

Wir begrüßen diese Entscheidung und erwarten, daß in dem neu zu gestaltenden Aufnahmeverfahren der Datenschutz gebührend Berücksichtigung findet.

11.2 Forschungsvorhaben

Im Bereich der Justiz wurde im Berichtszeitraum eine Reihe von Forschungsvorhaben durchgeführt, die zum Teil sensible Verfahren aus der NS-Zeit zum Gegenstand hatten. Der wichtigste Fall war eine Dokumentation der neueren Hamburger Justizgeschichte. Datenschutzrechtlich im Vordergrund stand die Abwägung des Interesses an der Darstellung historischer Tatsachen mit den Persönlichkeitsrechten der Betroffenen. Wir haben uns dafür eingesetzt, daß grundsätzlich nur besonders herausgehobene Funktionsträger aus der NS-Zeit oder aber Opfer des damaligen Regimes in der Dokumentation namentlich genannt werden.

Bei anderen wissenschaftlichen Forschungsvorhaben, bei denen eine spätere Namensnennung zur Erreichung des Forschungszweckes nicht erforderlich ist, haben wir für eine möglichst frühzeitge Anonymisierung Sorge getragen. Außerdem ist jeweils Voraussetzung für die Verwendung personenbezogener Daten, daß die Wissenschaftler einen umfangreichen Pflichtenkatalog akzeptieren.

Bei einem bundesweiten Forschungsvorhaben tauchte die Frage auf, inwieweit Daten aus dem Melderegister zu wissenschaftlichen Forschungszwecken abgefragt werden können. Gemäß § 6 Hamburgisches Meldegesetz hat hier die zuständige Meldebehörde regelmäßig zu prüfen, ob schutzwürdige Belange der Betroffenen beeinträchtigt werden. Bei dieser Prüfung bietet es sich an, § 27 HmDSG (Datenverarbeitung zum Zwecke wissenschaftlicher Forschung) als Beurteilungsmaßstab heranzuziehen. Auf diese Weise kommen die datenschutzrechtlichen Sicherungen, die § 27 HmbDSG bei der Verarbeitung personenbezogener Daten durch öffentliche Stellen für Forschungsvorhaben vorsieht, auch bei der zunächst rein melderechtlichen Prüfung zur Geltung. Wir haben das zuständige Amt für zentrale Meldeangelegenheiten (des Bezirksamtes Harburg) auf diesen Aspekt aufmerksam gemacht.

12. Bauwesen

12.1 Entwurf eines Hamburgischen Vermessungsgesetzes

Der Hamburgische Datenschutzbeauftragte fordert bereits seit längerer Zeit (vgl. 9. TB, 4.8.1) die Vorlage eines Hamburgischen Vermessungsgesetzes. Nachdem ein erster Entwurf von der Baubehörde im Jahre 1990 in das Behördenabstimmungsverfahren gegeben worden war, sind die Arbeiten an diesem Gesetzentwurf von der Baubehörde erst wieder im Berichtszeitraum aufgenommen worden. Wir begrüßen, daß die Baubehörde sowohl die Justizbehörde als auch den Hamburgischen Datenschutzbeauftragten in einem sehr frühen Stadium in ihre Überlegungen einbezogen hat und somit auch uns Gelegenheit gab, datenschutzrechtliche Gesichtspunkte des Gesetzentwurfs rechtzeitig abzustimmen.

Mit der nunmehr erarbeiteten und mehrfach fortgeschriebenen Entwurfsfassung soll eine – in Hamburg bislang fehlende – zusammenfassende Normierung von Aufgaben und Tätigkeiten des Vermessungswesens erfolgen. Die Vorschriften über die Nutzung des Liegenschaftskatasters als Basissystem für ein Flächenbezogenes Informationssystem und die hierzu vorgesehenen datenschutzrechtlichen Regelungen sind im wesentlichen neu und auch in Kataster- und Vermessungsgesetzen anderer Bundesländer erst teilweise und in jüngerer Zeit eingeführt worden.

Das Flächenbezogene Informationssystem enthält neben den flurstücksbezogenen Angaben des bisherigen Liegenschaftskatasters Hinweise auf flächenrelevante Festsetzungen sowie rechtliche und tatsächliche Eigenschaften der Flurstücke, die im einzelnen in Fachinformationssystemen anderer Stellen erhoben und gespeichert werden. So sind in dem System beispielsweise Hinweise auf das Altlastenkataster, das Vorhandensein eines Bombenblindgängerverdachts oder einer Baulücke vorgesehen. Wir haben anerkannt, daß solche Indexdaten im Flächenbezogenen Informationssystem verarbeitet werden dürfen, wenn sichergestellt wird, daß für diese Daten die fachlich zuständige Stelle auch speichernde Stelle bleibt.

Der vorgelegte Gesetzentwurf sieht ferner vor, die Nutzung des Flächenbezogenen Informationssystems durch eine Reihe hamburgischer öffentlicher Stellen im unmittelbaren lesenden und/oder schreibenden Zugriff (online-Verfahren) zu ermöglichen, damit sowohl die planende als auch die vollziehende Verwaltung ihre Aufgaben qualitativ und quantitativ besser wahrnehmen kann. Damit wird eine gemeinsame Datei für mehrere Stellen mit flächendeckendem Aufgabenbereich für ganz Hamburg eingeführt. Dies ist ein wesentlicher Zwischenschritt zum Infrastrukturansatz, für den besondere Datenschutzvorkehrungen notwendig sind (siehe 1.1 und 3.1).

Insbesondere hinsichtlich des verändernden Zugriffs haben wir darauf gedrungen, daß die eingebenden Stellen feststellbar sein müssen. Die Verantwortung als speichernde Stelle gegenüber dem Betroffenen muß auch in einem solchen

Fall die Stelle tragen, die für die Führung des Flächenbezogenen Informationssystems zuständig ist. Außerdem hat sie die technischen und organisatorischen Maßnahmen nach § 8 des Hamburgischen Datenschutzgesetzes zu treffen.

Mit der Baubehörde besteht Einvernehmen darüber, daß der lesende Zugriff durch eine Rechtsverordnung des Senats gemäß § 11 Absatz 2 des Hamburgischen Datenschutzgesetzes geregelt werden muß. Auch für den verändernden Zugriff bedarf es einer Rechtsverordnung des Senats, wobei § 11 Hamburgisches Datenschutzgesetz nicht unmittelbar, sondern nur entsprechend gelten kann.

Bei Redaktionsschluß hatte die Baubehörde das förmliche Behördenabstimmungsverfahren zwar noch nicht eingeleitet. Der bisherige Diskussionsverlauf läßt jedoch erwarten, daß die von uns vorgetragenen datenschutzrechtlichen Gesichtspunkte zur Verarbeitung personenbezogener Daten berücksichtigt werden. Wir hoffen, daß wir im 12. TB über den Abschluß des Gesetzgebungsverfahrens berichten können.

12.2 Fehlbelegungsabgabe-Verfahren

12.2.1 Änderung des Verfahrens

Die datenschutzrechtliche Prüfung des Fehlbelegungsabgabe-Verfahrens der Mietenausgleichszentrale (MAZ) als Abteilung der Hamburgischen Wohnungsbaukreditanstalt ist endlich mit einem überwiegend positiv zu bewertenden Ergebnis abgeschlossen worden. Nachdem es uns zunächst nach einjähriger abwechslungsreicher Auseinandersetzung um die Zuständigkeit des Hamburgischen Datenschutzbeauftragten für die MAZ doch noch gelungen war, das Fehlbelegungsabgabe-Verfahren überhaupt zu prüfen, hat es nun ein weiteres Jahr gedauert, bis Maßnahmen zur Beseitigung der von uns beanstandeten und im 10. TB (12.1) aufgeführten Mängel von der MAZ getroffen worden sind.

Die größte Hürde galt es im Hinblick auf die Bereinigung von 66 000 Akten mit einem hohen Anteil von nicht für die Sachbearbeitung erforderlichen Dokumenten zu überwinden, die von der MAZ im Verlauf des Fehlbelegungsabgabe-Verfahrens archiviert wurden. Mittlerweile ist jedoch mit der Hamburgischen Wohnungsbaukreditanstalt eine datenschutzgerechte Lösung vereinbart worden: Die 15 000 Akten der fehlbelegungspflichtigen Mieter wurden inzwischen fast vollständig durchgesehen; dabei wurden nicht mehr erforderliche Dokumente herausgenommen. Die restlichen 51 000 Akten der nicht abgabepflichtigen Mieter sind gesperrt und für die Sachbearbeitung nicht mehr zugänglich. Der Zugriff auf die gesperrten Daten ist nur noch in gesetzlich festgelegten Ausnahmen möglich, beispielsweise zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder zu Revisionszwecken. Die Akten werden nach 6 Jahren gelöscht; in der Zwischenzeit werden die Akten sicher unter Verschluß gehalten.

Für die regelmäßig stattfindenden Wiederholungen des Fehlbelegungsabgabe-Verfahrens hat die MAZ ein geändertes Verfahren mit einer entsprechenden Dienstanweisung vorgesehen. So brauchen die Mieter in vielen Fällen die entsprechenden Unterlagen bei der Wohnungsbaukreditanstalt lediglich vorzulegen; die Dokumente werden nicht mehr kopiert und zur Akte genommen. Der Mieter hat zudem die Möglichkeit, nicht erforderliche Daten auf entsprechenden Dokumenten unkenntlich zu machen.

Die ebenfalls von uns seinerzeit beanstandeten Anfragen der MAZ beim Finanzamt und beim Arbeitgeber sollen dadurch eingeschränkt werden, daß der Mieter zumindest vorab nochmals angeschrieben wird. Er erhält somit die Möglichkeit, eventuelle Zweifel durch Vorlage weiterer Unterlagen möglichst selbst auszuräumen.

12.2.2 Novellierung des Hamburgischen Gesetzes über den Abbau der Fehlsubventionierung im Wohnungswesen

Die gesetzliche Grundlage zur Erhebung der Fehlbelegungsabgabe in Hamburg ist im Berichtsjahr novelliert worden. Bei der Behördenabstimmung über das neue Gesetz über den Abbau der Fehlsubventionierung im Wohnungswesen in Hamburg (HmbAFWoG) wurde der Hamburgische Datenschutzbeauftragte – anders als beim bisher geltenden Gesetz (vgl. 9. TB, 4.8.2) – von der Baubehörde beteiligt. Die wesentlichen Änderungen im Gesetz sehen wie folgt aus:

— Die Leistungspflicht beginnt zwar nach wie vor, wenn die für den Bezug einer Sozialwohnung maßgebliche Einkommensgrenze von mehr als 50 % mit 2,00 DM je qm Wohnfläche monatlich überschritten wird. Jedoch sind nunmehr zwei weitere Einkommensgrenzen von 75 bzw. 100 % oberhalb der Einkommensgrenze mit Ausgleichszahlungen von 3,00 bzw. 4,00 DM je qm Wohnfläche monatlich neu eingeführt worden.

— Die Ausgleichszahlung wird gekappt – ohne daß es dazu eines Antrags des Mieters bedarf –, wenn die Miete plus Ausgleichszahlung einen am Mittelwert des jeweils geltenden Mietenspiegels orientierten Wert übersteigt.

— Auf die bisher geltenden Brutto-Kalt-Mietgrenzen als Leistungsvoraussetzung wurde verzichtet. Damit werden grundsätzlich alle öffentlich geförderten Mietwohnungen in das Erhebungsverfahren einbezogen.

Wir konnten im Behördenabstimmungsverfahren zwar erreichen, daß die Pflicht der zuständigen Stelle, über die Einkommensverhältnisse des Mieters Auskunft zu geben, nicht gegenüber allen Behörden, sondern nur gegenüber den Steuerbehörden und dem Arbeitgeber gilt. Dennoch kann der Entwurf für die Neufassung des Gesetzes aus datenschutzrechtlicher Sicht nicht zufriedenstellen.

Das Gesetz enthält keine klaren Regelungen über die Datenerhebung und die weitere Datenverarbeitung. Wir hatten beispielsweise vorgeschlagen, die per-

sonenbezogenen Daten von Mietern, Mitbewohnern sowie deren Bevollmächtigten, die von der MAZ für die Erfüllung ihrer gesetzlichen Aufgaben verarbeitet werden dürfen, abschließend aufzuzählen. Es wäre ohne weiteres möglich gewesen, diese Daten in Personendaten, Berechnungsdaten, Bevollmächtigtendaten und Daten, die Ausnahmen von der Leistungspflicht dokumentieren, zu unterteilen.

Weiterhin fehlt ein Hinweis, daß eine Übermittlung dieser Daten an Dritte nur zulässig ist, soweit es zur Erfüllung gesetzlicher Aufgaben erforderlich ist. Daß dabei schutzwürdige Belange der Betroffenen durch die Übermittlung nicht beeinträchtigt werden dürfen, wird ebenfalls im Gesetz nicht geregelt.

Der Verzicht auf diese bereichsspezifischen Bestimmungen zum Schutz personenbezogener Daten ist umso unverständlicher, als sie sich seit dem Volkszählungsurteil des Bundesverfassungsgerichts zu einem Standard bei Gesetzesnovellierungen entwickelt haben.

12.3 Hamburger Mietenspiegel

Die Praxis zur Datenerhebung anläßlich des Hamburger Mietenspiegels 1991 ist von uns im 10. TB (12.2) ausführlich dargestellt worden. Inzwischen hat das Hamburger Institut GEWOS einen Bericht über die Ergebnisse eines Feldexperiments vorgelegt, das die Reaktion von Befragungspersonen darstellt, wenn sie vor dem Interview ihr Einverständnis mit der Befragung schriftlich erklären müssen. Nach dem Zahlenwerk des Berichtes muß festgestellt werden, daß sich die Zahl der Verweigerer verdreifachte im Vergleich zu denjenigen Mietern, die ihre Einwilligung nicht schriftlich bestätigen mußten.

Es ist anzunehmen, daß die signifikant höhere Verweigerungsquote bei der schriftlichen Einwilligungserklärung auf die Schriftform zurückzuführen ist. Dabei kann die im Vergleich zur mündlichen Einwilligung erhöhte Verweigerungsquote auch als Ausdruck der Mündigkeit der Befragten interpretiert werden, denen erst bei schriftlicher Einwilligung die Tatsache der Freiwilligkeit und die Tragweite der ihnen gestellten Fragen bewußt geworden sind. Es war jedoch nicht ersichtlich, daß die Verweigerung aus Datenschutzgründen erfolgte, da dieser Ablehnungsgrund nicht entsprechend häufiger angegeben wurde. Daher ist es hinnehmbar, wenn in den Fragebögen vermerkt wird, daß die Befragten eindeutig auf die Ablehnungsmöglichkeit hingewiesen wurden und dennoch ihre Einwilligung mündlich erklärten.

Um vor der nächsten Mietenspiegelerhebung rechtzeitig sowohl über diesen Punkt als auch über die anderen im 10. TB angesprochenen Punkte Klarheit zu erzielen, haben wir die Baubehörde aufgefordert, das Verfahren zur Aufstellung von Mietenspiegeln präzise bereichspezifisch zu regeln. Da es bislang an einer solchen Regelung mangelt, hat die Baubehörde – unabhängig von den Vorbereitungen für den nächsten Mietenspiegel – den Bund gebeten, von der Verordnungsermächtigung des § 2 Abs. 5 Satz 4 des Gesetzes zur Regelung

der Miethöhe (MHG) Gebrauch zu machen, wonach u.a. Vorschriften für das Verfahren zur Aufstellung von Mietenspiegeln erlassen werden können. Dies wäre die rechtssystematisch sauberste Lösung.

Da der Bund jedoch seit mehr als 10 Jahren von dieser Verordnungsermächtigung keinen Gebrauch gemacht hat, muß befürchtet werden, daß eine solche Regelung nicht mehr rechtzeitig vor dem nächsten Hamburger Mietenspiegel getroffen werden wird. Deshalb wurde mit der Baubehörde vereinbart, losgelöst von der Initiative auf Bundesebene landesrechtliche Regelungen auf der Grundlage des § 2 Hamburgisches Statistikgesetz zu treffen. Bis zum Redaktionsschluß hat die Baubehörde allerdings noch keinen Entwurf in das behördliche Abstimmungsverfahren gegeben.

12.4 Projekt Bauaufsicht mit Computerunterstützung (BACom)

Am 1. Juli 1991 wurde im Senatsamt für Bezirksangelegenheiten eine Projektorganisation eingerichtet, die im wesentlichen eine umfassende Technikunterstützung bei der Erledigung aller Aufgaben des bezirklichen Baugenehmigungsverfahrens realisieren soll. Bisher ist die Arbeit in den bezirklichen Bauprüfdienststellen – mit Ausnahme der Programmierten Textverarbeitung (PTV) – weitgehend durch manuelle Arbeitsabläufe bestimmt. Der Einsatz von IuK-Technik soll im Ergebnis dazu führen, daß

— das Baugenehmigungsverfahren beschleunigt wird,

— zuverlässige Daten über die Entwicklung der Bautätigkeit in Hamburg und für administrative Entscheidungen jederzeit zur Verfügung stehen,

— die Rechtssicherheit erhöht und

— auch die Durchführung von Folgeaufgaben beschleunigt wird.

Es ist geplant, die verwaltungsmäßige Vorgangsbearbeitung im Dialog am Bildschirm mit Hilfe eines Datenbanksystems durchzuführen. Da in einem solchen Verfahren auch Belange des Datenschutzes und der Datensicherheit berührt sind, wurde der Hamburgische Datenschutzbeauftragte bereits frühzeitig an der Projektorganisation beteiligt.

Aus datenschutzrechtlicher Sicht ist bislang von besonderem Interesse, daß auch an die Übernahme von Daten aus anderen IuK-Verfahren bzw. die Übermittlung an andere IuK-Verfahren gedacht ist. Am Beispiel einer möglichen Verbindung zum Liegenschaftskataster haben wir deutlich gemacht, daß die Realisierung solcher Online-Anschlüsse nicht ohne eine jeweils ausreichende bereichsspezifische Rechtsgrundlage möglich ist. Insofern ist dieses Projekt u. a. auch abhängig von der Verabschiedung eines Hamburgischen Vermessungsgesetzes (vgl. 12.1).

Da angestrebt wird, Mitte 1993 mit der praktischen Einführung eines computerunterstützten Baugenehmigungsverfahrens in den bezirklichen Bauprüfdienststellen zu beginnen, werden wir voraussichtlich im 12. TB abschließend über das Projekt berichten.

12.5 Parlamentarischer Untersuchungsausschuß SAGA

Die Mietpreisgestaltung bei den stadteigenen Wohnungen und Häusern, die von der Hamburger Wohnungsgesellschaft SAGA verwaltet werden, ist in diesem Jahr in die öffentliche Kritik geraten. Die Bürgerschaft hat deshalb am 3. September 1992 eine Aktenvorlage gemäß Art. 32 der Hamburgischen Verfassung (HV) beschlossen. Sie hat den Senat ersucht, ihr alle die stadteigenen Wohnungen und Häuser betreffenden Akten, insbesondere die der Baubehörde und Finanzbehörde, die sich mit der Vermietung und Unterhaltung befassen, sowie die relevanten Akten der stadteigenen SAGA vorzulegen.

Darüber hinaus hat die Bürgerschaft am 30. September 1992 einen Parlamentarischen Untersuchungsausschuß (PUA) eingesetzt. Er soll im Zusammenhang mit der Verwaltung und Vermietung von Wohnungen im Eigentum der Freien und Hansestadt Hamburg oder städtischer Unternehmen die politischen Verantwortlichkeiten klären und die Geschäftstätigkeit städtischer Unternehmen untersuchen.

Wir haben der für das Aktenvorlageersuchen an die Bürgerschaft federführenden Finanzbehörde eine abgestufte Verfahrensweise vorgeschlagen, bei der die datenschutzrechtlichen Belange der betroffenen Mieter angemessen berücksichtigt werden. In einer ersten Teillieferung wurden deshalb auch nur solche Akten vorgelegt, in denen die Namen der Mieter anonymisiert sowie Daten oder Vorgänge streng persönlichen Charakters geschwärzt bzw. herausgenommen worden sind.

Die Bürgerschaft hat inzwischen am 29. Oktober 1992 beschlossen, das Aktenvorlageersuchen gemäß Art. 32 HV aufzuheben, da es aufgrund der Aktenanforderung des Parlamentarischen Untersuchungsausschusses nicht mehr erforderlich sei.

Nach der Rechtsprechung des Bundesverfassungsgerichts sind für die Aktenvorlage an einen Parlamentarischen Untersuchungsausschuß Art und Bedeutung des Ziels, das mit der beabsichtigten Beweiserhebung verfolgt wird, im Rahmen des erteilten Auftrags sowie die Schutzwürdigkeit und -bedürftigkeit der betroffenen Daten angemessen zu berücksichtigen. Auf Informationen, deren Weitergabe wegen ihres streng persönlichen Charakters (z. B. gesundheitliche Verhältnisse) für den Betroffenen unzumutbar ist, erstreckt sich das Beweiserhebungsrecht nicht. Darüber hinaus ist zu prüfen, ob nach den Umständen eine öffentliche Beweisaufnahme gerechtfertigt ist oder ob die Grundrechte bestimmte Vorkehrungen parlamentarischer Geheimhaltung erfordern.

Der Ermittlungsauftrag des Untersuchungsausschusses ist vor allem auf die Aufdeckung von möglichen Unregelmäßigkeiten und Mißständen bei der Woh-

nungsvergabe sowie der Gestaltung von Mietkonditionen gerichtet. Für die Aufklärung dieser Fragen ist es nicht erforderlich, dem Untersuchungsausschuß die Namen sämtlicher Mieter – für die über 150 000 Mietobjekte – zu offenbaren. In Abstimmung mit Baubehörde, Finanzbehörde und Justizbehörde haben wir deshalb für die Aktenvorlage folgende Verfahrensweise für vertretbar gehalten:

In den vom Vorlageersuchen betroffenen Akten werden grundsätzlich alle Angaben anonymisiert, die eine eindeutige Zuordnung auf eine bestimmte natürliche Person zulassen. Namen von Mietern bzw. Käufern, bei Bedarf auch Hausnummern werden geschwärzt. Daten von hervorgehobener Schutzwürdigkeit werden darüber hinaus auf Kopien der zu übersendenden Vorgänge geschwärzt oder die entsprechenden Seiten werden den Akten vorher entnommen.

In einer ersten Verfahrensstufe werden dem Untersuchungsausschuß die auf die beschriebene Art und Weise anonymisierten Akten vorgelegt. Auf besondere Anforderung im Einzelfall, wenn Anhaltspunkte für einen konkreten Verdacht im Sinne des Untersuchungsauftrages vorliegen, werden in einer zweiten Verfahrensstufe die Mieter bestimmter stadteigener Wohnungen und Häuser namentlich benannt, wenn der Ausschuß zuvor Behandlung in nicht-öffentlicher Sitzung mit der Folge der Vertraulichkeit beschlossen hat.

Sollte der Ausschuß auch hinsichtlich geschwärzter streng persönlicher Daten im Einzelfall Ermittlungsbedarf äußern, kann eine Übermittlung nur mit ausdrücklich erteilter Zustimmung des betroffenen Mieters erfolgen.

Auf der Grundlage dieser Verfahrensweise hat der Senat dem Parlamentarischen Untersuchungsausschuß am 1. November 1992 eine erste Teillieferung von Behördenakten zur Verfügung gestellt. Die SAGA hatte die Herausgabe von Akten an die Bürgerschaft verweigert und sieht einer direkten Anforderung des Parlamentarischen Untersuchungsausschusses entgegen.

Am 26. November 1992 habe ich dem Untersuchungsausschuß die genannten Grundsätze und die Umsetzung schriftlich dargestellt und entsprechend erläutert. Die Frage, ob dem Untersuchungsausschuß die Namen sämtlicher Mieter zu offenbaren sind, blieb bis Redaktionsschluß dieses Tätigkeitsberichtes streitig. Falls sich der Untersuchungsausschuß wegen der Namen von Mietern bzw. Käufern oder auch wegen streng persönlicher Daten selbst vergewissern will, daß ihm keine Unregelmäßigkeiten oder Mißstände vorenthalten werden, habe ich gemäß der Rechtsprechung des Bundesverfassungsgerichts auf die Möglichkeit hingewiesen, daß einigen wenigen Ausschußmitgliedern vertraulich Einblick in diese Unterlagen gegeben wird.

Der Untersuchungsausschuß kann demnach alle Daten einschließlich der Namen von Mietern bzw. Käufern bei Anhaltspunkten für Unregelmäßigkeiten und Mißstände erhalten. Eine effektive Wahrnehmung des Untersuchungsauftrags und die gebotene Wahrung des Datenschutzes können damit zum Ausgleich gebracht werden, wie es das Bundesverfassungsgericht verlangt.

13. Meldewesen

Im 10. TB (13.1.1) war der geplante Wegfall der örtlichen Zuständigkeiten örtlicher Meldebehörden problematisiert worden. Über dieses Thema kann nichts Neues berichtet werden, da bei Redaktionsschluß noch kein überarbeiteter Entwurf für eine Novellierung des Hamburgischen Meldegesetzes vorlag.

13.1 Verwechslungen im Melderegister

Während früher nur das Einwohnerzentralamt aufgrund der Meldekartei Auskünfte über sämtliche in Hamburg gemeldete Bürger erteilen konnte, haben seit 1991 alle örtlichen Meldedienststellen zur Auskunftserteilung Zugriff auf das gesamte automatisierte Melderegister (siehe 9. TB, 4.9.2). Früher waren Verwechslungen bei der Auskunftserteilung eher selten: es gab binnen 8 Jahren kaum Eingaben an den Hamburgischen Datenschutzbeauftragten; 1983 teilte der damalige Leiter des Einwohnerzentralamtes mit, daß bei jährlich über einer Million Melderegisterauskünften nur 2 bis 4 Verwechslungen bekannt geworden seien.

Im Berichtszeitraum erreichte uns jedoch eine Reihe von Eingaben, in denen Bürger sich darüber beschwerten, mit anderen Personen verwechselt worden zu sein. Auch das Amt für zentrale Meldeangelegenheiten beim Bezirksamt Harburg (Leitstelle) erfuhr vermehrt von Verwechslungsfällen. Hinzu kam, daß auch der Polizei bei ihren Direktanfragen im Online-Verfahren (siehe 9. TB, 4.12.4) Verwechslungen unterliefen.

Ursache hierfür war meist, daß Behörden oder Privatpersonen sich nach jemandem erkundigten, der früher in Hamburg gewohnt hat, jedoch inzwischen verzogen ist. Beim Zugriff auf den automatisierten Meldedatenbestand erfolgte eine Rückmeldung, die nicht die gesuchte Person betraf, sondern eine gleichen oder sehr ähnlichen Namens. Eine weitere Überprüfung anhand weiterer Identifizierungsdaten, z.B. des Geburtsdatums oder einer früheren Anschrift unterblieb. Die Erteilung der Auskunft hatte dann sehr unangenehme Folgen: polizeiliche und gerichtliche Schreiben gingen an Personen, die gar nicht gemeint waren; Arztrechnungen, die Rückschlüsse auf Diagnosen zuließen, wurden falsch adressiert.

Die Leitstelle hat daher die Meldedienststellen darauf hingewiesen, daß die Suche im automatisierten Bestand grundsätzlich nur mit vollständigen Identifizierungsdaten, also Namen und Geburtsdatum erfolgen soll. Bei der Verwendung unvollständiger Daten – etwa weil das Geburtsdatum nicht bekannt ist – sind Anfragetechniken vorgesehen, die eine Überprüfung der angezeigten Computerrückmeldung ermöglichen. In Zweifelsfällen muß der Auskunftssuchende nach zusätzlichen Identifizierungsdaten befragt werden oder eine Auskunft muß unterbleiben. Wenn diese Vorgaben eingehalten werden, dürfte sich die Gefahr von häufigen Verwechslungen verringern.

Allerdings wird man durch Appelle an individuelles Verhalten der zuständigen Sachbearbeiter nicht grundsätzlich automationsbedingte Risiken beseitigen

können. Wir haben daher vorgeschlagen, daß in Fällen, in denen bei sehr ähnlichen Identifizierungsdaten die Gefahr von Verwechslungen besteht und erkannt wird, auf Antrag eines der Betroffenen ein Hinweis hierauf gespeichert wird. Damit könnten wenigstens die Fälle vermieden werden, die Grund für die Eingaben von betroffenen Bürgern an uns waren. Sie wurden nämlich immer wieder mit einer anderen Person verwechselt, die aus guten Gründen intensiv von Behörden und privaten Stellen gesucht wurde, weswegen besonders häufig Anfragen an das Melderegister erfolgten.

Unseren Vorschlag konnte die Leitstelle für das Meldewesen bislang nicht aufgreifen, weil sie sich mit viel grundsätzlicheren Problemen des Melderegisters auseinandersetzen muß.

13.2 Wachsende Unzuverlässigkeit des Melderegisters

Hamburg verfügt zwar über einen automatisierten Meldedatenbestand, doch er deckt nicht alle gesetzlichen Anforderungen ab. Bei den Planungen zur Automation des Meldewesens seit 1983 (vgl. 3. TB, 3.7.1.1) sind alle Beteiligten davon ausgegangen, daß der nach dem Melderecht vorgegebene Leistungsumfang nur in mehreren Teilschritten durch das automatisierte Verfahren erreicht werden kann. Bislang ist dies nur für den aktuellen Datenbestand gelungen.

Ein funktionsfähiges Meldewesen erfordert jedoch auch die Dokumentation einer sog. „Historie". Wenn sich z.B. Straßennamen ändern oder neue Hausnummern vergeben werden, müssen die früher gültigen Angaben auffindbar bleiben. Dies ermöglicht das Hamburger Verfahren jedoch noch nicht, es zwingt bei derartigen Änderungen vielmehr dazu, die alten Angaben durch die neuen zu überschreiben. Ein wesentliches Identifikationsmerkmal geht damit verloren. Weitere Probleme entstehen, wenn Bürger, die früher einmal aus Hamburg fortgezogen sind, später wieder zuziehen. Hier muß jedesmal ein neuer Datensatz angelegt werden, so daß es inzwischen Einwohner mit mehr als zehn Datensätzen gibt. Wegen der fehlenden Historie ist eine sichere Zuordnung insbeondere bei Namensänderungen durch Eheschließung oder Scheidung nicht mehr gewährleistet.

Auch Nachweisdaten über andere Sachverhalte wie z.B. Geburten, Eheschließungen, Scheidungen, Sterbefälle, Namensänderungen, die Austellung von Pässen und Personalausweisen sowie Nachweise zur Staatsangehörigkeit können nicht im automatisierten Verfahren erfaßt werden. Vielmehr muß auf die Papierbelege zurückgegriffen werden. Wenn die Speichermöglichkeit später einmal geschaffen wird, ist ein enormer Rückstand nachzuarbeiten, was voraussichtlich nur mit erheblichen personellen und organistorischen Belastungen möglich sein wird.

Früher wurden diese Aufgaben „von Hand" durch das Einwohnerzentralamt wahrgenommen. Mit der Auflösung der dortigen Abteilung für Meldeangelegenheiten und der Übertragung der Aufgaben an die Bezirke hätte die Fortentwicklung des automatisierten Meldeverfahrens auch in diesem Bereich einher-

gehen müssen. Dies ist jedoch unterblieben. Die fachlich zuständige Behörde für Inneres hat lediglich angekündigt, die überfällige Programmierung des sog. „Rückmeldeverfahrens" für Einwohner, die in Hamburg mehrere Wohnungen haben, im Jahr 1992 durchzuführen, was u. a. eine wesentliche Voraussetzung für die Erhebung der Zweitwohnungsteuer ist. Alle übrigen ebenfalls rechtlich vorgeschriebenen Anforderungen können dagegen zur Zeit nicht realisiert werden, weil im IuK-Plan hierfür keine Mittel zur Verfügung gestellt wurden.

Damit wird ein Grundsatzproblem von Automationsvorhaben in Hamburg deutlich: Die Verfahren werden zunächst mit großem Aufwand an Personal und Mitteln begonnen. Wenn sie dann halbwegs laufen, werden andere Prioritäten gesetzt und neue Großverfahren begonnen, die die zur Verfügung stehenden Ressourcen binden. Die Pflege und Fortentwicklung der bestehenden Verfahren wird jedoch vernachlässigt. Verstöße gegen zwingende gesetzliche Regelungen werden bewußt in Kauf genommen. So schreibt das Meldegesetz vor, daß Daten, die zur Aufgebenerfüllung der Meldebehörden nicht mehr erforderlich sind, vor der Löschung dem Staatsarchiv anzubieten sind. Dies ist bei den derzeitigen technischen Gegebenheiten nicht möglich.

Wir haben gegenüber der Behörde für Inneres, dem Senatsamt für Bezirksangelegenheiten und dem Organisationsamt deutlich gemacht, daß damit die datenschutzrechtliche Verantwortlichkeit nach § 10 HmbDSG in Frage gestellt wird. Uns ist daraufhin mitgeteilt worden, daß eine Behebung der derzeitigen Mängel nur mit einer umfassenden Neuentwicklung des automatisierten Meldeverfahrens geleistet werden könne. Diese würde bei einer Eigenentwicklung drei bis vier Jahre dauern und allein 6 Millionen DM Personalkosten erfordern. Damit wird deutlich, daß die ursprünglichen Wirtschaftlichkeitsberechnungen falsch waren, weil sie diesen Aufwand überhaupt nicht berücksichtigt haben.

Nunmehr wollen das Senatsamt für den Verwaltungsdienst und die Behörde für Inneres abwarten, bis sich das bisherige Verfahren mit den unbehebbaren Unzulänglichkeiten amortisiert hat, und mit der Neuentwicklung frühestens 1995 beginnen. Demnach stünde ein Meldeverfahren, das alle gesetzlichen Anforderungen erfüllt, erst Ende des Jahrhunderts nach erneutem erheblichem finanziellen und personellen Aufwand zur Verfügung. Das Argument, automatisierte Verfahren führten zur Einsparung von Mitteln, wird damit letztlich hinfällig.

14. Standesamt

In der zweiten Hälfte des Jahres 1991 hat die elektronische Datenverarbeitung auch in den hamburgischen Standesämtern Einzug gehalten. Das Projekt Automation Standesämter (PASTA), an dem wir von Beginn an beteiligt waren (vgl. 8. TB, 3.7.2), wurde nach einer Erprobungsphase im Bezirksamt Eimsbüttel erfolgreich abgeschlossen, so daß nunmehr in allen Standesämtern mit einem PC-Netzwerk gearbeitet wird.

Nach der Aufnahme des Echtbetriebs haben wir im Standesamt des Bezirksamtes Hamburg-Mitte die Datenverarbeitung geprüft und keine datenschutz-

rechtlichen Mängel festgestellt, die zu einer förmlichen Beanstandung führten. Trotzdem gab es für uns Anlaß zu einigen Hinweisen, die im wesentlichen folgende Punkte betrafen:

— Außer dem Programm AUTISTA, mit dessen Hilfe die klassischen Aufgabenstellungen im Standesamt, nämlich die Beurkundung von Geburten, Eheschließungen und Todesfällen, wahrgenommen werden können, wird zusätzlich das Produkt F&A eingesetzt. Dies war uns bislang von dem projektleitenden Senatsamt für Bezirksangelegenheiten nicht mitgeteilt worden.

  Neben der Textverarbeitung unterstützt dieses Produkt auch die einfache Anlage und Führung von Dateien. Im Verlauf unserer Prüfung bestand unter F&A die Möglichkeit, Dateiverzeichnisse anzusehen, Dateien zu kopieren, zu löschen oder zu verschieben. Ferner konnten Programmdateien durch die Anwender in ihre Menüs eingebaut und aus den so veränderten Menüs heraus auch gestartet werden. Durch diesen Mechanismus war es den Anwendern möglich, auf Betriebssystemebene zu gelangen und die in F&A enthaltenen Möglichkeiten zu nutzen. Die eigentlichen DOS-Betriebssystembefehle (z. B. Formatierung einer Festplatte) konnten jedoch nicht angewendet werden.

  Das Senatsamt für Bezirksangelegenheiten hat zugesagt, Anfang 1993 spezielle Zugriffsbeschränkungen für F&A festzulegen, damit im Ergebnis nur von den Anwendern selbst erstellte Text- oder Datenbankdateien innerhalb der jeweiligen Festplatte gelöscht oder kopiert werden können. Wir werden die Wirksamkeit dieses Verfahrens im Rahmen einer Nachschau überprüfen.

— Die Ausarbeitung von Dienstanweisungen für Systemverwalter und Benutzer ist zwar durch das Senatsamt für Bezirksangelegenheiten in den Grundzügen abgeschlossen. Es fehlt jedoch noch an einer abschließenden Verbindlichkeit der darin enthaltenen Regelungen. Dieser Organisationsmangel muß vom Senatsamt für Bezirksangelegenheiten kurzfristig beseitigt werden, damit möglichen Fehlverhalten der Systemverwalter und Anwender entgegengewirkt werden kann.

Im übrigen ist daran zu erinnern, daß die derzeitigen Erlaubnisvorschriften für die personenbezogene Datenverarbeitung, insbesondere die Übermittlungsvorgänge, im Standesamtsbereich unzureichend sind. Die Dienstanweisung für Standesbeamte entspricht als Verwaltungsvorschrift nicht den Anforderungen, die durch das Volkszählungsurteil des Bundesverfassungsgerichts an eine Befugnisnorm zu richten sind.

Wann mit einer Änderung der personenstandsrechtlichen Vorschriften – insbesondere des Personenstandsgesetzes – durch den Bundesgesetzgeber gerechnet werden kann, ist weiterhin nicht absehbar, da die unterschiedlichen Strukturen des Personenstandswesens in den alten und neuen Bundesländern eine Fülle neuer Fragen aufgeworfen haben. Deshalb haben wir den Bundesbeauftragten für den Datenschutz gebeten, die hiermit verbundene datenschutzrechtliche Problematik gegenüber dem Bundesminister des Innern zu klären.

15. Ausländerbehörde

15.1 Automation der Ausländerverwaltung

15.1.1 Registriernummern

Die Vorarbeiten zur Einführung eines automatisierten Verfahrens für die Ausländerbehörde (siehe 10. TB, 14.1) haben weitere Fortschritte gemacht. Inzwischen liegt der Katalog sämtlicher Daten vor, die in diesem Dialogverfahren gespeichert werden können. Er umfaßt über 30 eng beschriebene Seiten und macht deutlich, daß die dateimäßige Erfassung von Ausländern weit über das hinausgeht, was in anderen Verwaltungsbereichen üblich ist.

Bei der Durchsicht des Datenkataloges fiel die große Anzahl von vorgesehenen Registriernummern auf. Neben der Nummer, die für jeden Ausländer in Deutschland für das Ausländerzentralregister (AZR) vergeben wird (AZR-Nummer), und der Dokumentennummer des ausländischen Passes soll jeder Ausländer, der im automatisierten Verfahren der Ausländerbehörde erfaßt wird, ein ihm zugeordnetes Ordnungsmerkmal in Form einer gesonderten Nummer erhalten. Darüber hinaus sind Registriernummern für sämtliche Formen der Aufenthaltsgenehmigung und auch von sonstigen Bescheiden, die sich auf den Aufenthaltsstatus beziehen, vorgesehen.

Im Volkszählungsurteil hatte das Bundesverfassungsgericht die Verknüpfung von verschiedenen Datenbeständen durch ein einheitliches Personenkennzeichen noch als Beispielsfall einer verfassungswidrigen, die Menschenwürde verletzenden Form der Datenverarbeitung bezeichnet. Im Verfahren zur Automation der Ausländerverwaltung scheint man diesem Diktum ausweichen zu wollen, indem man kein einheitliches Kennzeichen, sondern eine ganze Palette von Registrier- und Identifizierungsnummern vorsieht.

Die Funktion der AZR-Nr. als Identifizierungsmerkmal für Anfragen beim Ausländerzentralregister ist zwar für sich gesehen bereits problematisch. Wegen der Nachweisfunktion des Ausländerzentralregisters ist ihre Speicherung durch die Ausländerbehörden jedoch hinnehmbar. Die Ausländerdateienverordnung sieht dies auch vor.

Dies gilt aber nicht für die Speicherung der Registriernummern jeder einzelnen Aufenthaltserlaubnis und Bescheinigung. Seit Inkrafttreten des neuen Ausländergesetzes werden von der Bundesdruckerei Aufkleber für die Erteilung von Aufenthaltsgenehmigungen ausgegeben. Sie enthalten eine Seriennummer, die bundesweit nur einmal vergeben wird. Eine gesetzliche Grundlage für diese Praxis gibt es nicht. Die Behörde für Inneres ist der Auffassung, diese Seriennummern müßten personenbezogen registriert werden, um bei vermuteten Fälschungen schnell erkennen zu können, ob die vorgelegte Aufenthaltsgenehmigung auch tatsächlich dem betreffenden Ausländer erteilt worden ist. Weiterhin solle eine mißbräuchliche Verwendung dieser Aufkleber durch Bedienstete der Ausländerbehörde weitestgehend ausgeschlossen werden. Zu diesem Zweck werde die Zahl der an die Mitarbeiter gegen Unterschrift ausgehändigten

und tatsächlich erteilten Aufkleber verglichen. Derzeit erreichten das Einwohner-Zentralamt täglich mehrere Anfragen der Polizei unter Angabe der entsprechenden Seriennummern.

Für die ganze überwiegende Mehrzahl von ca. 40 000 jährlich in Hamburg erteilten Aufenthaltsgenehmigungen, in denen weder die betroffenen Ausländer noch Mitarbeiter der Ausländerbehörde Mißbrauch betreiben, können diese Überlegungen nicht gelten.

Sie überzeugen auch für die Mißbrauchsfälle nicht, denn mit dem automatisierten Verfahren bei der Ausländerbehörde sollen Genehmigungen und Bescheinigungen erstellt und dokumentiert werden. Zur Feststellung, ob eine vorgelegte Aufenthaltsgenehmigung tatsächlich erteilt worden ist, reichen Datum und konkrete Angaben zum Dokument aus. Auch die Speicherung der Angaben zur Aufenthaltsgenehmigung im Ausländerzentralregister dient diesem Nachweis. Wenn nunmehr primär eine nummernmäßige Erfassung stattfinden soll, wird diese Nachweisfunktion in Frage gestellt.

Wir haben der geplanten Speicherung aller Registriernummern, die in der Ausländerdateienverordnung nicht vorgesehen sind, daher widersprochen.

15.1.2 Warnmeldungen

Ein weiteres im Datenkatalog für die Ausländerbehörde vorgesehenes Datenfeld, das unsere Kritik hervorrief, betraf sogenannte „Warnmeldungen". Damit waren Hinweise in Form von Freitexten gemeint, die vor bestimmten Personen „warnen" sollten. Die Behörde hat hierzu mitgeteilt, daß die Mitarbeiter mit diesen Hinweisen vor Personen gewarnt werden sollen, die zu Gewalttätigkeiten neigen, polizeilich gesucht oder ansteckend erkrankt sind. Die Warnmeldungen sollen von der Leitstelle des Verfahrens eingegeben werden.

Bereits diese Zuweisung von inhaltlichen Aufgaben an die Leitstelle, die für die technische und organisatorische Systembetreuung zuständig ist, wäre sachfremd und würde die datenschutzrechtlich gebotene Trennung von Systemverwaltung und Anwendern unterlaufen.

Die den „Warnmeldungen" zugrunde liegenden Bewertungen sind entweder nicht verifizierbar und somit zur Aufgabenerfüllung ungeeignet, oder die Informationen ergeben sich richtiger und vollständiger aus den gespeicherten Unterlagen. Wenn jemand als „Illegaler" gesucht wird, läßt sich dies aus den jeweiligen statusbezogenen Datenfeldern bzw. bei vorliegenden Ausweisungsgründen wegen besonderer Gefährlichkeit aus der Akte ersehen. Erlaubte zusätzliche Informationen kann das Datenfeld somit nicht vermitteln. Wir haben daher die ersatzlose Streichung gefordert.

15.2 INPOL-Ausschreibung von Ausländern

Ausländer, die aus der Bundesrepublik ausgewiesen oder abgeschoben werden, werden nicht nur bei der zuständigen Ausländerbehörde, im Ausländer-

zentralregister und zusätzlich im Bundeszentralregister, sondern auch noch im bundesweiten Informationssystem der Polizei INPOL, das vom Bundeskriminalamt betrieben wird, gespeichert. Begründet wird dies damit, daß die Polizei und der Bundesgrenzschutz die Möglichkeiten haben müsse, Personen, die sich illegal im Bundesgebiet aufhalten oder nach einer Ausweisung wieder einreisen wollen, zu erkennen.

Diese Ausschreibungen in INPOL werden durch die zuständige Ausländerbehörde veranlaßt, die damit die Verantwortung für die Zulässigkeit und Dauer der Speicherung übernimmt. Eine gesetzliche Grundlage für diese Nutzung des polizeilichen Informationssystems zu Zwecken der Ausländerverwaltung gibt es ebensowenig wie für die damit verbundene Datenübermittlung von der Ausländerbehörde an die Polizei. Maßgeblich sind die sogenannten Dateienrichtlinen des Bundes von 1981. Die Richtlinien geben für die Speicherung von Ausweisungen oder Abschiebungen grundsätzlich eine kürzere Frist als 10 Jahre vor. Die im Einzelfall erforderliche Frist ist bereits bei der Ausschreibung durch die Ausländerbehörde festzulegen. Durch Verfügung des Präses der Behörde für Inneres vom 1. März 1981 ist für die Speicherung von Ausweisungen und Abschiebungen eine Frist von fünf Jahren festgelegt.

Die Nutzung des polizeilichen Informationssystems durch die Ausländerbehörden ist nicht nur wegen der fehlenden gesetzlichen Grundlage und unter dem Gesichtspunkt der Zweckbindung polizeilicher Datenverarbeitung kritisch zu sehen. Vielmehr führt sie in der Praxis dazu, daß diese Speicherungsmöglichkeit von der Ausländerbehörde zwar bedenkenlos genutzt wird, man jedoch meint, sich nicht mehr um die Daten kümmern zu müssen, wenn sie erst einmal bei der Polizei abgelegt sind.

Als wir uns aufgrund einer Eingabe im Mai 1992 danach erkundigten, warum eine ausländerrechtliche INPOL-Ausschreibung noch bestehe, die nach unserer Meinung wegen Fristablaufs zu löschen war, gab sich die Ausländerabteilung des Einwohnerzentralamtes unwissend. Dies könne vielleicht die Polizei wissen oder das BKA, die Ausländerbehörde sei jedenfalls für INPOL nicht zuständig und könne insbesondere auch keine Löschung von Daten veranlassen.

Als wir dann der Polizei und dem Einwohnerzentralamt Muster der für die Ausschreibung und die Löschung gleichermaßen vorgesehenen Formblätter übersandten, aus denen sich klar ergibt, daß die ausschreibende Stelle auch die Löschung veranlaßt, antwortete nur die Polizei und verwies zu Recht auf die Ausländerbehörde. Die Polizei forderte sie sogar auf, die Ausschreibung zu überprüfen und gegebenenfalls die Löschung zu verfügen. Bis zum Oktober geschah dann nichts. Zwischenzeitlich hatten wir die Behörde für Inneres aufgefordert, die einschlägigen Regelungen, die eine Befristung von ausländerrechtlichen INPOL-Ausschreibungen vorsehen, in Form einer Dienstanweisung in der Ausländerbehörde bekannt zu machen und bei jeder neuen Ausschreibung maximal eine Frist von 5 Jahren festzulegen. Dies lehnte die Behörde für Inneres ab. Sie vertrat die Auffassung, die Verfügung ihres Präses von 1981 beziehe sich nur auf aktenmäßige Unterlagen und nicht auf Ausschreibungen

in INPOL. Nach dem eindeutigen Wortlaut der Richtlinien, in die die Verfügung eingearbeitet worden ist, trifft das nicht zu. Bis zum Redaktionsschluß dieses Berichts blieb das Problem ungelöst.

16. Personalausweisregister

16.1 Zugriff der Polizei auf Paßfotos

„Wie kommt die Polizei zu meinem Foto?" Das ist eine Frage, die Bürger regelmäßig in Eingaben an den Hamburgischen Datenschutzbeauftragten stellen. Hintergrund ist meistens ein Sachverhalt wie dieser: Ein Fahrzeug wird in einer Radarkontrolle wegen zu hoher Geschwindigkeit oder Überfahren einer roten Ampel fotografiert. Der Halter des Fahrzeugs teilt mit, nicht gefahren zu sein. Aufgrund besonderer Umstände des Einzelfalls spricht viel dafür, daß eine bestimmte andere Person die Verkehrsordnungswidrigkeit begangen hat. Diese äußert sich auf Befragen nicht oder erscheint nicht zu einer Vorladung durch die Polizei. Nunmehr läßt sich die Polizei aus dem Personalausweisregister das dort abgelegte Lichtbild schicken, vergleicht die bei dem Verkehrsverstoß fotografierte Person mit dem Paßfoto und stellt fest, daß die Vermutung über den Verursacher des Verkehrsverstoßes zutrifft.

Wir teilen den Betroffenen, die sich an uns wenden, in den meisten Fällen mit, daß dieses Verfahren datenschutzrechtlich zulässig ist. Allerdings ist bei der Heranziehung von Lichtbildern aus dem Personalausweisregister eine Reihe von Voraussetzungen zu beachten, die in der polizeilichen Praxis nicht immer bekannt ist.

Maßgeblich ist das Personalausweisgesetz. Nach § 2a Personalausweisgesetz wird das Lichtbild eines Ausweisinhabers im Personalausweisregister der zuständigen Ausweisbehörde gespeichert. § 2b Abs. 2 Personalausweisgesetz sieht vor, daß Daten aus dem Register – also auch das Lichtbild – anderen Behörden, z.B. der Polizei, übermittelt werden dürfen.

Dabei muß die Polizei die wesentliche Voraussetzung nach § 2b Abs. 2 Satz 2 Nr. 3 Personalausweisgesetz beachten: Die Datenerhebung beim Betroffenen hat Vorrang vor der Heranziehung eines Lichtbilds aus dem Register. Es wird bei Verkehrsordnungswidrigkeiten nie prinzipiell unmöglich, zu aufwendig oder von der Sache her untunlich sein, den in Betracht kommenden Fahrer vorzuladen. Die Polizei kann ihn auch aufsuchen, um sich selbst davon zu überzeugen, ob er die Person ist, die bei einem Verkehrsverstoß fotografiert worden ist. Dies sehen auch die einschlägigen Dienstvorschriften der Polizei vor. Wenn der Betroffene jedoch nicht erscheint und auch der Versuch fehlschlägt, ihn persönlich aufzusuchen, bleibt kein anderes Mittel zur Aufklärung des Verkehrsverstoßes als der Lichtbildvergleich.

Ferner ist zu fragen, ob die Heranziehung des Paßbildes im Einzelfall verhältnismäßig ist. Es ist allgemein anerkannt, daß im Bußgeldverfahren nicht alle nach § 163b StPO zulässigen Maßnahmen zur Identitätsfeststellung erlaubt

sind. Eine erkennungsdienstliche (ed-) Behandlung in Ordnungswidrigkeitsverfahren ist in der Regel ausgeschlossen. Die Heranziehung von Paßbildern führt zwar zum selben Ergebnis wie die Anfertigung von Lichtbildern bei der ed-Behandlung, greift aber längst nicht so tief in die Sphäre des Betroffenen ein.

Wir haben daher in der Vergangenheit die Übermittlung von Lichtbildern in Bußgeldverfahren als zulässig angesehen, sofern es sich um Ordnungswidrigkeiten von einigem Gewicht handelte. Zur Abgrenzung der Fälle, in denen dieses Vorgehen zulässig ist, läßt sich bei Verkehrsordnungswidrigkeiten die Schwelle heranziehen, ab der eine Eintragung im Verkehrszentralregister erfolgt.

Die Polizei ist dem gefolgt und macht die Heranziehung von Lichtbildern in Dienstvorschriften davon abhängig, ob mit einem Bußgeld von mindestens DM 80 und einer Eintragung im Verkehrszentralregister zu rechnen ist. In einigen Eingabefällen der letzten Zeit wurde das Lichtbild entweder zu früh herangezogen, ohne daß versucht worden war, den Betroffenen aufzusuchen, oder es lagen nur Bagatellfälle vor, bei denen der Lichtbildvergleich nicht erlaubt ist. Uns ist zugesagt worden, daß die Voraussetzungen für die Heranziehung von Lichtbildern verstärkt im Dienstunterricht der Polizei behandelt werden.

16.2 Paßfotos in Ermittlungsakten

„Wie kommt mein Foto in die Akte?" Dies war die zweite Frage eines Bürgers in einer Eingabe, nachdem wir die erste beantwortet hatten, ob es zulässig ist, daß sich die Polizei bei Straßenverkehrsverstößen ein Lichtbild aus dem Ausweisregister schicken ließ. Sein Anwalt war bei der Einsicht in die Bußgeldakte der für die Verfolgung der Ordnungswidrigkeit zuständigen Behörde auf ein Foto seines Mandanten gestoßen. Auch uns war diese Praxis neu. Früher wurde das Original des Lichtbildes aus dem Register an die Polizei gesandt, dort verglichen und dann sofort wieder zurückgeschickt. Es war nicht möglich, eine aussagefähige Kopie des Bildes anzufertigen. Der ermittelnde Polizeibeamte machte also einen Bericht, indem er das Ergebnis seines Lichtbildvergleichs festhielt, und schickte diesen an die Bußgeldbehörde.

Die Automatisierung hat jedoch auch beim Ausweisregister Einzug gehalten und diese ebenso einfache wie datenschutzkonforme Praxis geändert. Die Ausweisunterlagen sind seit einiger Zeit mikroverfilmt. Von den Mikrofilmen können beliebig viele Kopien (Mikroprints) angefertigt werden, die den Originalen entsprechen und an denen das Ausweisregister keinen eigenen Bedarf mehr hat. Sie enthalten nicht nur das Foto, sondern auch alle Personalausweisdaten, die zum Zwecke des Lichtbildvergleichs gar nicht erforderlich sind. Im Fall der Eingabe hatte der ermittelnde Polizist nunmehr nicht nur pflichtgemäß den Lichtbildvergleich vorgenommen und sein Ergebnis schriftlich fixiert, sondern auch noch die Kopie aus dem Ausweisregister beigefügt. So wanderte das Lichtbild und alle weiteren Daten vom Ausweisregister über die Polizei zur Bußgeldbehörde und von dort zum Gericht.

Wir haben diese Praxis kritisiert. Es ist jedenfalls unzulässig, Daten aus dem Ausweisregister an die Polizei oder auch andere Behörden zu übermitteln,

nach denen gar nicht gefragt war. Somit wird man bei der neuen Technik nicht darum herumkommen, auf den Mikroprints enthaltene nicht erforderliche Daten zu schwärzen. Wenn die Polizei aufgrund ihrer Ermittlungsbefugnisse und der Vorschriften des Personalausweisgesetzes ein Lichtbild anfordert, wird es nur ihr zur Erfüllung eigener Aufgaben übersandt. Der ermittelnde Polizeibeamte trifft eigenverantwortliche Feststellungen über den Verantwortlichen für einen Verkehrsverstoß und ist nicht nur Bote zwischen Register und Ordnungswidrigkeitenbehörde. Erfüllt er diese Aufgabe, ist auch der Zweck der Datenübermittlung aus dem Ausweisregister erledigt. Die Kopie des Lichtbilds aus dem Register ist zu vernichten.

Auch die Bußgeldstelle beim Einwohnerzentralamt hat erklärt, daß sie die kopierten Bilder aus dem Personalausweisregister für das weitere Ordnungswidrigkeitenverfahren nicht benötigt. Daher wird die Polizei in Zukunft nur noch das Ergebnis des Identifizierungsversuchs in der Akte vermerken und das Bild nicht mehr in die Akte aufnehmen.

17. Polizei

17.1 Projekt Computerunterstützte Vorgangsbearbeitung bei der Polizei (COMVOR)

17.1.1 Neue Konzeption für das Projekt

Im 10. TB (16.1.4) war der damalige Planungsstand für das Projekt zur Computerunterstützten Vorgangsbearbeitung bei der Polizei (COMVOR) beschrieben worden. Inzwischen hat sich gezeigt, daß das Projekt nicht genügend Kapazitäten hat, die ursprünglich bis Ende 1993 geplante erste Realisierungsstufe selbst zu entwickeln, und auch nicht die Möglichkeit besteht, Verfahren aus anderen Bundesländern zu übernehmen. Daher sind die bisher vorgesehenen drei Realisierungsstufen in einzelne Teilleistungen zerlegt worden. Maßgeblich hierfür war die Zielsetzung, die Steuerbarkeit und die Überschaubarkeit des Projektes zu verbessern, den Schaden bei einem möglichen Scheitern auf die jeweils betroffenen Teilbereiche zu begrenzen, Erfahrungen bei der schrittweisen Einführung für künftige Teilleistungen nutzbar zu machen und die Anwenderschulung zu entzerren.

Auch die Datenschutzproblematik, die im 10. TB (16.1.1 bis 16.1.3) angesprochen worden ist, wird hierdurch für die absehbare Zukunft entschärft. Die erste Teilleistung, die nach derzeitigem Planungsstand Mitte 1993 abgeschlossen sein soll, sieht vor, den Mitarbeitern der Polizei eine einheitliche Benutzeroberfläche für die Anfertigung standardisierter Texte (Formulare, Meldungen) zur Verfügung zu stellen. Die einzelnen Texte (sog. Vorgangsteile) können nur zwischengespeichert werden.

Besondere Datenschutzprobleme entstehen nach unserer bisherigen Einschätzung durch diese bevorstehende erste Teilleistung noch nicht. Vielmehr würde

dadurch nach und nach die „gute alte“ Schreibmaschine aus den Diensträumen der Polizei verdrängt und durch eine zeitgemäße Textverarbeitung ersetzt. Es wird auch von uns begrüßt, wenn die Alltagsarbeit des Polizeidienstes sehr bald durch diese Form der IuK-Technik unterstützt wird. Andernfalls stünde zu erwarten, daß sich im Bereich der Polizei der Druck auf die Verwendung privater PC's, die derzeit nicht zugelassen werden, erheblich verstärkt. Der dabei zu erwartende „Wildwuchs“ unkontrollierbarer automatisierter Datenverarbeitung wäre ein Rückschritt und würde die Einführung eines datenschutzgerechten Verfahrens zur Vorgangsbearbeitung erheblich erschweren.

Der in der ersten Teilleistung noch fehlende dezentrale Vorgangsdatenbestand soll im nächsten Abschnitt aufgebaut werden. Damit werden die mit COMVOR erarbeiteten Texte im Zuge polizeilicher Ermittlungstätigkeit automatisiert abrufbar gespeichert. Diese Teilleistung bringt insofern eine Neuerung, als die sogenannten Tagebuchfunktionen nicht mehr nur zentral bei den Polizeidirektionen, sondern auch dezentral bei den einzelnen Sachbearbeitern wahrgenommen werden. Tagebuchfunktionen geben Auskunft darüber, bei wem und in welchem Bearbeitungszustand sich ein bestimmter Vorgang (z.B. eine polizeiliche Ermittlungsakte) zur Zeit befindet. Polizeiliche Erkenntnisse zur vorbeugenden Bekämpfung von Straftaten werden damit noch nicht erfaßt, sondern sind erst Gegenstand zukünftiger Abschnitte des Verfahrens.

Die ersten Teilleistungen sollen zunächst als Pilotanwendungen in einzelnen Dienststellen auf wenigen Arbeitsplätzen getestet werden. Damit bleibt die Möglichkeit, Tagebuchfunktionen vorzunehmen, den zuständigen polizeilichen Sachbearbeitern vorbehalten. Erst im Zuge des weiteren Ausbaus des Verfahrens zu einem zentralen Vorgangsdatenbestand flächendeckend für die Polizei Hamburg, der bis Mitte 1994 vorgesehen ist, wird es möglich sein, auch Anfragen zu einem Vorgang zu beantworten, der sich nicht im eigenen Zuständigkeitsbereich befinden. Hier fangen dann die eigentlichen datenschutzrechtlichen Probleme an.

17.1.2 Datenschutzkonzept

Da die Konzeption für die letzte Ausbaustufe bereits jetzt vollständig vorliegt, haben wir im Berichtszeitraum mit den Mitarbeitern des Projekts und der für die Datenverarbeitung zuständigen Dienststelle des Landeskriminalamtes intensiv ein Datenschutzkonzept für das umfassende Verfahren zur Vorgangsbearbeitung beraten, das nach den derzeitigen Planungen bis Ende 1995 eingeführt sein soll. Ausgangspunkt dafür war die Unterscheidung zwischen Funktionen der Bearbeitung und Verwaltung einzelner polizeilicher Vorgänge und der Bearbeitung und Verwaltung vorgangsunabhängiger polizeilich relevanter Erkenntnisse.

Vorgangsbezogene Funktionen werden grundsätzlich nur die jeweils zuständigen Sachbearbeiter ausführen können. Zugriffe auf den sogenannten „Abgleichsdatenbestand“ über polizeilich relevante Erkenntnisse, der besonderen gesetzlichen Voraussetzungen unterliegt, werden dagegen eine große Zahl

von Mitarbeitern der Polizei haben. Es geht also darum, die vorgangsbezogenen Daten, die über Anzeigeerstatter, Geschädigte, Zeugen gespeichert werden, von den Abgleichsdaten, die nur für Beschuldigte eines Strafermittlungsverfahrens in Betracht kommen, zu unterscheiden und im einzelnen abzuwägen, ob die rechtlichen Voraussetzungen eingehalten sind.

Das Datenschutzkonzept lag bei Redaktionsschluß des Tätigkeitsberichts noch nicht abgeschlossen vor. Seine Wiedergabe bis in die Details, in denen bekanntlich der Teufel steckt, würde den Rahmen dieses Tätigkeitsberichts sprengen. Es ist daher beabsichtigt, in zukünftigen Berichten entsprechend der schrittweisen Einführung des Verfahrens die jeweils maßgeblichen Teile des Datenschutzkonzepts und gegebenenfalls die Probleme bei seiner Umsetzung darzustellen.

17.2 Probleme des bundesweiten Informationssystems der Polizei (INPOL)

Das Gesetz über das Bundeskriminalamt (BKA-Gesetz) enthält keine bereichsspezifischen Vorschriften über die Datenverarbeitung im Informationssystem der Polizei (INPOL) (vgl. 8. TB, 3.8.2.1). Gleichwohl ist nach der seit 1990 geltenden INPOL-Neukonzeption eine wesentliche Erweiterung des Verbundsystems vorgesehen.

Im Berichtszeitraum hat sich der Arbeitskreis Sicherheit der Datenschutzbeauftragten intensiv mit den Problemen befaßt, die sich aus der Neukonzeption im Hinblick auf die dringend notwendige Novellierung des BKA-Gesetzes ergeben. Als Ausgangspunkt für die weitere Diskussion sind die grundlegenden Forderungen in einem Arbeitspapier zusammengefaßt worden, das auf einen von uns vorbereiteten Entwurf zurückgeht (siehe 17.2.1). Der Bundesbeauftragte für den Datenschutz hält die weitere Diskussion der Aussagen dieses Arbeitspapiers zur Zentralstellenfunktion für erforderlich.

17.2.1 Datenschutzrechtliche Anforderungen an Regelungen für das INPOL-System im Gesetz über das Bundeskriminalamt

In diesem Arbeitspapier zur INPOL-Neukonzeption heißt es:

„Als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen verarbeitet das BKA personenbezogene Daten, die es in der Regel nicht selbst erhoben hat, sondern die ihm von den Polizeibehörden der Länder übermittelt worden sind. Eine wesentliche Ausprägung der Zentralstellenfunktion des Bundeskriminalamtes ist das INPOL-System. Es strukturiert als gemeinsames, arbeitsteiliges Informationssystem der Polizeien des Bundes und der Länder die polizeiliche Datenverarbeitung.

Daneben gibt es unter der Bezeichnung INPOL-Land z.B. für den Kriminalaktennachweis vergleichbare Systeme der Länderpolizeien.

INPOL-Bund umfaßt z. Zt. die personenbezogenen Anwendungen:

— Personen- und Sachfahndung

— Kriminalaktennachweis

— Haftdatei

— Erkennungsdienst und Daktyloskopie

— Arbeitsdateien für besondere Kriminalitätsbereiche (PIOS)

— Falldateien für bestimmte Kriminalitätsbereiche

— Spurendokumentation in Ermittlungsverfahren (SPUDOK)

Die Speicherung und Nutzung von Daten in diesen INPOL-Anwendungen greift in das informationelle Selbstbestimmungsrecht vieler Bürger ein. Die Entscheidung, welchen Umfang das Informationssystem haben soll und wie es ausgebaut werden soll, war bisher weitgehend der Exekutive unter Ausschluß der parlamentarischen und öffentlichen Kontrolle überlassen. Insoweit sind die Regelungen im Gesetz über das Bundeskriminalamt (BKA-Gesetz) nicht ausreichend. Die Innenministerkonferenz entscheidet mangels gesetzlicher Grundlagen gleichsam als „Ersatzgesetzgeber" über die Grundzüge des INPOL-Systems, wenn die Beschlüsse zur INPOL-Neukonzeption ohne gesetzliche Regelung umgesetzt werden.

Danach ist vorgesehen, durch INPOL einen Rahmen für alle polizeilichen Anwendungen der Datenverarbeitung im Bund und den Ländern vorzugeben. Das INPOL-Kommunikationsnetz soll schrittweise mit den anderen Sondernetzen der Polizei zusammengeführt und zu einem autonomen dienstintegrierenden digitalen Sondernetz der Polizei für den Austausch von Daten, Textnachrichten, Sprach- und Bildinformation auf der Basis postalischer Datenübermittlungsdienste fortentwickelt werden. Durch eine anwendungsunabhängige „einheitliche Kommunikationsschnittstelle" soll die „offene Kommunikation" aller Teilnehmer im Netz ermöglicht werden. Die Gewährleistung des Zweckbindungsgrundsatzes ist dann nicht mehr erkennbar.

Unter diesen Umständen werden mindestens folgende Regelungen zum INPOL-System – insbesondere bei der dringend erforderlichen Novellierung des BKA-Gesetzes – für geboten gehalten:

1. Zweck der Einrichtung einer Zentralstelle beim Bundeskriminalamt ist es, die Strafverfolgungs- und Polizeibehörden bei ihrer Aufgabenerfüllung zu unterstützen. Die Verfolgung und die vorbeugende Bekämpfung von Straftaten sind grundsätzlich Sache der Länder. Wenn eine Länderbehörde Daten, die sie erhoben hat, zur Erfüllung ihrer Aufgaben im INPOL-System speichert, muß sie ihre Verantwortung für die Zulässigkeit, Richtigkeit und Dauer der Speicherung und weiteren Verarbeitung behalten (vergleiche die Regelungen zur Datenverarbeitung im Auftrag); wenn mehrere Behörden Daten zu einer Person gespeichert haben, ist jede Behörde nur für ihre Speicherung zuständig und verantwortlich. Die sachnächste Stelle, die die Daten im Rahmen ihrer Zuständigkeit erhoben hat, kann und muß gewährleisten, daß Speicherungen entsprechend dem Gang der Ermittlungen und nach dem Ausgang eines Strafverfahrens korrigiert werden. Dieser Gesichtspunkt der materiellen Datenverantwortung muß bei den Regelungen des neuen BKA-Gesetzes über die Datenverarbeitung in INPOL gewahrt werden.

2. Die Verfahrensregelungen zum INPOL-System im neuen BKA-Gesetz müssen sich nach den materiellen Vorschriften des Bundes insbesondere in der Strafprozeßordnung richten. Die Zentralstellenbefugnis (Art. 73 Nr. 10a und Art. 87 Abs. 1 Satz 2 GG) beinhaltet keine Kompetenzzuweisung an den Bund für materielle Regelungen auf den Gebieten Strafverfolgung und Gefahrenabwehr.

   Das neue BKA-Gesetz darf auch bereichsspezifische Vorschriften der Länder zur Datenverarbeitung der Polizei nicht in der Weise überlagern, daß die jeweils strengeren Vorschriften ausgehöhlt werden. Dies bedeutet auch, daß der Bund unter Berufung auf die Zentralstellenkompetenz des BKA nicht die Übermittlung und Speicherung von Daten bestimmen kann, die nach den Landesgesetzen nicht erhoben oder übermittelt oder nicht solange gespeichert werden dürfen.

   Polizeiliche Datenverarbeitung kann – auch soweit es um die Aufgabenerfüllung des BKA als Zentralstelle geht – nur zu Zwecken der Strafverfolgung oder Gefahrenabwehr erfolgen. Zu berücksichtigen ist dabei, daß Daten, die bei der Strafverfolgung erhoben worden sind, zu präventiven Zwecken nur nach Maßgabe der jeweils geltenden bereichsspezifischen Vorschriften verwendet werden dürfen. Regelungen im BKA-Gesetz über das INPOL-System müssen sich hieran orientieren und haben keinen hiervon losgelösten Verwendungszweck hinzuzufügen, der aus der Aufgabenzuweisung an das Bundeskriminalamt als Zentralstelle abgeleitet wird.

3. Ferner sehen die neuen Gesetze über die Datenverarbeitung der Polizei und auch die Strafprozeßordnung Erhebungsmethoden von höchst unterschiedlicher Eingriffstiefe vor. Danach unterliegen Daten, die auf dem Einsatz verdeckter oder technischer Mittel beruhen, bestimmten Verwendungsbeschränkungen, z.B. nur Katalogtaten. Das Stichwort „offene Kommunikation" in der INPOL-Neukonzeption läßt erwarten, daß solche Verwendungsbeschränkungen dort nicht vorgesehen und auch nicht durchführbar sind. Es wäre deshalb bei offener Kommunikation nicht hinnehmbar, wenn derartige Daten in INPOL verarbeitet würden.

   Demgegenüber käme eine Verarbeitung solcher Daten nur unter der Voraussetzung in Betracht, daß im neuen BKA-Gesetz die Einhaltung der Verwendungsbeschränkungen in INPOL technisch und organisatorisch gewährleistet wird. Eine bloße Verweisung auf die Aufgabenerfüllung der Zentralstelle oder die Vorgabe eines technischen Rahmens reichen zur Sicherung der Verwendungsbeschränkungen nicht aus.

4. Im BKA-Gesetz ist festzulegen, für welche Teilbereiche der polizeilichen Datenverarbeitung eine Nutzung des Verbundsystems erfolgen darf. Die unterschiedlichen Anwendungen von INPOL lassen sich nicht ohne Betrachtung ihrer Zweckbestimmung, ihrer Struktur und Leistungsfähigkeit unter dem Oberbegriff eines einheitlichen dienstintegrierenden Systems zusammenfassen, wie es die INPOL-Neukonzeption beabsichtigt.

   Maßgeblich für eine Aufnahme in INPOL sind die Kriterien Schwere und überregionale Bedeutung der Tat, die aufgeklärt oder verhütet werden soll. Die Regelungen zum Verbundsystem müssen auch die Frage beantworten, unter welchen Voraussetzungen welche Arten von Dateien eingerichtet werden dürfen."

Wir haben die Behörde für Inneres gebeten, das Arbeitspapier bei den weiteren Beratungen einzubeziehen und zu dem Papier Stellung zu nehmen.

17.2.2 Übermittlung von Kfz-Sachfahndungsdaten durch das Bundeskriminalamt an Hersteller und den HUK-Verband

Anfang 1992 erfuhren wir davon, daß das Bundeskriminalamt beabsichtige, den gesamten Datenbestand der Kfz-Sachfahndung an einzelne Hersteller und den HUK-Verband der Versicherungen zu übermitteln. In die INPOL-Sachfahndung werden Daten von gestohlenen Fahrzeugen eingestellt, um deren Wiederauffinden zu ermöglichen. Primär handelt es sich also um Sachdaten, die allerdings insofern einen Personenbezug aufweisen, als die Fahrgestellnummer (sog. Fahrzeug-Identifizierungsnummer) Auskunft über den rechtmäßigen Halter eines Fahrzeuges gibt.

Zweck der Übermittlung des Sachfahndungsbestands ist es, den Herstellern und ihren angeschlossenen Werkstätten sowie dem HUK-Verband insbesondere auch im Ausland die Feststellung zu ermöglichen, ob ein gestohlenes Fahrzeug oder Teile daraus wieder auftauchen, um dies dem Bundeskriminalamt zurückzumelden. Nachdem das Bundeskriminalamt die Modalitäten für diese Datenübermittlung mit den Herstellern und dem HUK-Verband abgestimmt hatte, wurde der Bundesbeauftragte für den Datenschutz informiert. Er verwies darauf, daß es sich bei dem Kfz-Sachfahndungsbestand in erster Linie um Strafverfolgungsdaten, die von Länderpolizeien eingegeben worden sind, handelt und daher die Länder zu beteiligen seien. Das BKA fragte daraufhin mit Fernschreiben bei den Landeskriminalämtern nach, ob sie Bedenken hätten. Einige Landeskriminalämter meldeten zunächst Bedenken an. Die Behörde für Inneres wurde erst durch uns auf die Pläne des BKA aufmerksam gemacht.

Die Meinungsbildung bei den Datenschutzbeauftragten führte dann mehrheitlich zu der Auffassung, daß aus datenschutzrechtlicher Sicht grundsätzlich nichts gegen die geplante Übermittlung einzuwenden sei, da schutzwürdige Interessen der aus den Sachfahndungsdaten ersichtlichen Fahrzeughalter nicht verletzt sein können. Die Maßnahme liegt eher in ihrem Interesse oder dem ihrer Versicherung, da sie die Wiedererlangung gestohlener Fahrzeuge auch aus dem Ausland unterstützen kann. Ein sachbezogener Ansatz bei Fahndungsmaßnahmen ist aus datenschutzrechtlicher Sicht einem personenbezogenen vorzuziehen.

Allerdings haben wir auch darauf hingewiesen, daß es zur Zeit noch keine ausreichende Rechtsgrundlage für diese Übermittlung ganzer polizeilicher Datenbestände an private Unternehmen gibt, und daß die Einbeziehung Privater in Maßnahmen polizeilicher Fahndung die Ausnahme bleiben muß. Nachdem die

Bundesrepublik mit Polen ein Abkommen über die polizeiliche Zusammenarbeit geschlossen hat, ist klärungsbedürftig, ob es einer Einschaltung privater Stellen für diesen Bereich überhaupt noch bedarf.

Als vordringlich haben wir die Frage der Datensicherung bei den Empfängern angesehen, da unbedingt vermieden werden muß, daß organisiert arbeitende Kraftfahrzeugdiebe in irgend einer Weise Zugang zu polizeilichen Fahndungsdaten erhalten. Dies dürfte gerade auch im Interesse der Polizei und der Datenempfänger liegen.

Da über diese Fragen aus unserer Sicht zwischen allen Beteiligten Einvernehmen zu erzielen war, können wir nicht recht nachvollziehen, warum das BKA hierüber nur sehr zögerlich informiert. Obwohl wir mehrfach intensiv auf die erforderlichen Vorkehrungen zur Datensicherheit hingewiesen hatten und uns auch in einer Besprechung beim Bundesminister des Innern im August 1992 Informationen über die mit den Empfängern getroffenen Vereinbarungen zur Datensicherung zugesagt wurden, fehlten bis Redaktionsschluß nachprüfbare Angaben des BKA. Es ist nicht einmal geklärt, ob es überhaupt schriftliche Vereinbarungen hierüber gibt.

Statt dessen betont das BKA immer wieder, es allein sei befugt, die Daten der INPOL-Sachfahndung zu übermitteln. Die Tatsache, daß der INPOL-Datenbestand aus Fahndungsmaßnahmen herrührt, die die Länderpolizeien zu verantworten haben, ändere daran nichts. Das BKA pocht damit auf seine sogenannte Zentralstellenbefugnis, die es berechtige, unabhängig vom „Wohlwollen" der Länder mit den Daten zu verfahren. Es vermeidet dagegen, sich auf seine – unstrittige – Kompetenz als Bundespolizei, die für die internationale Verbrechensbekämpfung zuständig ist, zu berufen. Offenbar ist dem Bundeskriminalamt die abstrakte Frage, ob seine sog. Zentralstellenbefugnis es ermöglicht, ohne vorheriges Einvernehmen mit den Länderpolizeien INPOL-Daten an Private zu übermitteln, wichtiger als Klarheit in der Sache.

17.2.3 Verlängerung der Speicherfristen für die Arbeitsdatei Innere Sicherheit (APIS)

Die Problematik der Arbeitsdatei Innere Sicherheit (APIS) war in den letzten Jahren ein immer wiederkehrendes Thema im unseren Tätigkeitsberichten (zuletzt 10. TB, 16.9). Diese INPOL-Verbunddatei soll Erkenntnisse über politisch motivierte Kriminalität vermitteln, die gegen die freiheitliche demokratische Grundordnung gerichtet ist.

In APIS werden nicht nur Beschuldigte erfaßt, gegen die ein strafrechtliches Ermittlungsverfahren eingeleitet worden ist. Es werden auch sogenannte „andere Personen" erfaßt, gegen die kein konkreter Tatverdacht vorliegt, die jedoch mit Beschuldigten in einer für den Zweck der Datei relevanten Verbindung stehen.

Bisher war die Speicherungsfrist für diesen Personenkreis in APIS auf drei Jahre festgelegt. Nach unserer Vorstellung ist dies eine zwingend notwendige

Begrenzung, da für die „anderen Personen" keinerlei justizförmige Überprüfung des Vorwurfs und der Motivation stattfinden kann. Nur mit einer kurzen Frist kann der Zweck der Datei, relevante Erkenntnisse von nutzlosen zu unterscheiden, erfüllt werden.

Nach dem letzten Mordanschlag der RAF im Frühjahr 1991 wurden seitens einiger Innenminsterien Forderungen nach einer Verlängerung der Speicherungsfrist für andere Personen auf 5 Jahre laut. Diese Forderungen konnten sich schließlich auf der Innenministerkonferenz im Mai 1992 durchsetzen. Allerdings ist die Einschränkung vorgesehen, wonach die 5-Jahresfrist nicht für alle Teilnehmer bindend sein soll, sondern nur den äußeren Rahmen vorgibt.

Hamburg hat erklärt, die bisherige 3-Jahresfrist beizubehalten. Dies war auch gesetzlich geboten, denn das in Hamburg maßgebliche Gesetz über die Datenverarbeitung der Polizei (PolDVG) läßt für die „anderen Personen" maximal nur eine Speicherungsdauer von drei Jahren zu. Es nimmt die weitere Einschränkung vor, daß nicht alle „anderen Personen" gespeichert werden können, sondern nur „Kontakt- und Begleitpersonen". Diese werden gesetzlich definiert. Voraussetzung ist, daß die Erhebung und Speicherung von Daten über diesen Personenkreis zur vorbeugenden Bekämpfung von Straftaten erheblicher Bedeutung unerläßlich ist. Längst nicht alle der in APIS erfaßten Straftaten sind solche von erheblicher Bedeutung. Die in Hamburg zuständige Staatsschutzabteilung des Landeskriminalamtes ist daher gesetzlich gehalten, einen sehr restriktiven Maßstab bei der Speicherung von „anderen Personen" zu beachten.

Dieses Beispiel macht deutlich, daß wesentliche Entscheidungen über die Speicherungspraxis im INPOL-System in der Innenministerkonferenz gefällt werden. Dies hebt die Bindung der beteiligten Minister an ihre jeweiligen Landesgesetze jedoch nicht auf.

17.2.4. Personenbezogene Hinweise

Während wir aufgrund der eindeutigen Gesetzeslage und der entsprechenden Ankündigungen der Behörde für Inneres hoffen können, daß sich die von der Innenministerkonferenz für die INPOL-Datei APIS getroffenen Entscheidungen in Hamburg nicht auswirken, gibt es inzwischen bei den sogenannten personenbezogenen Hinweisen andere Anzeichen.

Mit personenbezogenen Hinweisen (PHW) wird der Datensatz in INPOL-Dateien ergänzt. Für INPOL-Dateien sind derzeit die folgenden PHW vorgesehen:

— bewaffnet

— gewalttätig

— Ausbrecher

— Ansteckungsgefahr

— geisteskrank

— Betäubungsmittel-Konsument

— Freitodgefahr

— Prostitution

Die drei erstgenannten Hinweise (bewaffnet, gewalttätig und Ausbrecher) sind aus unserer Sicht zum Zwecke der Eigensicherung von Polizeibeamten und als Hinweis auf besonders zu treffende Vorkehrungen in der Personenfahndungsdatei zu rechtfertigen, wenn sie auf nachprüfbaren Fakten beruhen. Die übrigen PHWs sind seit langem Gegenstand der Diskussion zwischen Datenschutzbeauftragten und der Polizei (7. TB, 4.11.9).

In Hamburg wird unter „Ansteckungsgefahr" nicht erfaßt, ob eine HIV-Infektion vorliegt, in anderen Bundesländern geschieht dies. Auch der PHW „Freitodgefahr" darf in Hamburg aufgrund eines Ersuchens der Bürgerschaft und eines Senatsbeschlusses von 1986 im Unterschied zu anderen Ländern nicht mehr gespeichert werden (7. TB, 4.11.6).

Inzwischen stellt sich jedoch heraus, daß auch diese PHW über die „Hintertür" INPOL wieder Eingang in die Datenverarbeitung der Polizei in Hamburg finden. So erfuhren wir, daß auf Beschluß der Innenministerkonferenz vom Mai 1992 bundesweit eine Verbunddatei über Vermißte und unbekannte Tote eingeführt worden ist. Bei ihr sind auch die PHW „Ansteckungsgefahr" und „Freitodgefahr" vorgesehen. Die Innenbehörde ist der Auffassung, sie müsse diese PHW von anderen Ländern entgegennehmen, um nicht von wesentlichen Informationen abgeschnitten zu werden. Die anderen Länder verzichteten auf die Aufnahme spezieller Hinweise zur Eigensicherung oder Gefahrenabwehr im Interesse der Betroffenen und benutzten statt dessen die PHW.

Diese Begründung erstaunt in mehrfacher Hinsicht. Zum einen werden für die Länder Berlin und Nordrhein-Westfalen überhaupt keine PHW in der Vermißtendatei ausgegeben. Diese Länder halten die PHWs daher insgesamt für nicht erforderlich. Zum anderen erscheint es kaum sachgerecht, sich mit der Vergabe pauschaler und undifferenzierter Kürzel in Form von PHW zu begnügen, wenn wesentliche Zusatzinformationen notwendig erscheinen.

17.3 Zugriffssicherung für das polizeiliche Auskunftssystem (POLAS)

Im 9. TB (4.12.4) und 10. TB (16.4) hatten wir kritisiert, daß für das polizeiliche Auskunftssystem POLAS immer noch keine wirksame Zugriffssicherung eingeführt worden war. Dieser unhaltbare Zustand ist seit Anfang 1992 beseitigt. Wir haben uns davon überzeugt, daß das Verfahren zur Prüfung der Zugriffsberechtigung mittels einer Magnetkarte sowohl bei der Herstellung und Verwaltung der Karten als auch bei deren Benutzung den Anforderungen des Hamburgischen Datenschutzgesetzes entspricht.

Der Zugang zu den Daten des Verfahrens zur Prüfung der Zugriffsberechtigung ist nur von den Terminals der zuständigen Dienststelle möglich und steht dort

nur vier Mitarbeitern zur Verfügung. Keiner dieser Mitarbeiter ist berechtigt, den eigenen Datensatz mit seinen Zugriffsklassen zu ändern. Dialoge mit dieser Datenbank werden im Auskunfts- wie im Änderungsdienst protokolliert. Der Dialog mit der Benutzerdatenbank muß zunächst mit der Magnetkarte des Berechtigten eröffnet werden. Die Eingabe der Prüfungsmerkmale erfolgt über die neu anzufertigende Magnetkarte. Die Beendigung des Dialogs erfolgt wiederum über die Anwenderkarte. Beim zweiten Anmelden werden die nunmehr eingelesenen Daten mit den zuerst angemeldeten verglichen; wird ein anderer Ausweis eingeführt, erfolgt ein Abbruch des Dialogs.

Jeder Dialog mit POLAS-Anwendungen kann nur durch Einlesen der auf diese Weise hergestellten Karte eröffnet werden. Die Steuerung des Dialogs erfolgt über das in der Benutzerdatei eingetragene Benutzerprofil. Entsprechend ihrer jeweiligen Funktion haben die Bediensteten unterschiedliche Berechtigungen. Über gesperrte Daten erhalten nur ganz wenige Auskunft. Mitarbeiter des Landeskriminalamtes erhalten im übrigen in der Regel POLAS-Vollauskünfte, die Mitarbeiter der Direktionen und Reviere Teilauskünfte. Während des gesamten Dialogs wird geprüft, ob die Karte eingelesen ist. Beim Verlust der Karte wird die für die Herstellung und Verwaltung zuständige Dienststelle benachrichtigt, so daß durch den Entzug aller Berechtigungen die Sperrung der Karte erfolgt. Beim Versuch des Gebrauchs einer gesperrten Karte erfolgt eine Benachrichtigung über Ort und Art der Benutzung.

Einen Schönheitsfehler hat das Verfahren zur Berechtigungsprüfung für POLAS allerdings, denn es deckt nur einen Teil der Gesamtheit polizeilicher Informationssysteme ab. Zur Zeit erschließt die Magnetkarte nur die POLAS-Anwendungen in Hamburg einschließlich des Online-Zugriffs auf das Melderegister. Der Zugriff auf die Anwendungen des bundesweiten INPOL-Systems (siehe 17.2) erfolgt derzeit noch im Wege des Terminal-Rechner-Verbundes über bestimmte Datenstationen, die vom Bundeskriminalamt für diese Anwendungen generiert sind. Erst im Zuge der Einführung des POLAS-INPOL-Vollverbunds (Rechner-Rechner-Verbunds) werden die hier betriebenen Verfahrensteile von POLAS über die Ausweisiesegeräte die Zugriffssicherung gewährleisten. Bisher werden lediglich dienststellenbezogene Paßwörter verwendet.

Der Zugriff auf den Kfz-Datenbestand (ZEVIS) des Kraftfahrtbundesamtes erfolgt zwar auch über die POLAS-Terminals. Hier wirkt die Magnetkarte jedoch nicht, es gelten vielmehr Terminalkennungen. Die besonderen abgeschlossenen PIOS-Dateien in den Bereichen Staatsschutz, organisierte Kriminalität und Rauschgiftkriminalität werden nicht über POLAS-Terminals abgewickelt; hier ist die Eingabe eines individuellen Paßwortes erforderlich.

17.4 Prüfung von Kriminalakten über Kinder

17.4.1 Speicherung auch von Kindern

Im 10. TB (16.6) war die Aussage enthalten, daß strafunmündige Kinder unter 14 Jahren bisher nicht in kriminalpolizeilichen Sammlungen gespeichert würden.

Inzwischen hat sich herausgestellt, daß diese Aussage unrichtig war. Vielmehr werden schon seit längerem auch Kriminalakten (siehe hierzu 10. TB, 16.3) über Kinder unter 14 Jahren angelegt und dementsprechend Speicherungen in POLAS vorgenommen.

Unsere Aussage im 10. TB war eine Schlußfolgerung aus der Tatsache, daß die Speicherung von Kindern in der Vergangenheit bei einzelnen Dateien mehrfach intensiv erörtert und das Mindestalter im Ergebnis entsprechend unserer Forderung auf 14 Jahre festgelegt worden ist. Bei der Datei über den Straßendrogenhandel (10. TB, 16.6) ist das Erfordernis der Erfassung von Kindern besonders begründet worden und eine einschränkende Formulierung – mit dem Ausschluß der POLAS-Speicherung – für die Errichtungsanordnung übernommen worden. Bei dieser Vorgeschichte in Zusammenhängen, in denen ein Bezug zu Strafunmündigen bestand, überraschte es, daß die POLAS-Speicherung von Kindern bereits Praxis war.

Wir haben die Speicherungspraxis der Polizei daher anhand einer Liste über alle Personen unter 14 Jahren, die in POLAS gespeichert sind, und anhand etwa eines Viertels der zugrunde liegenden Kriminalakten geprüft. Zum Zeitpunkt der Prüfung waren 198 Kinder erfaßt. Zum Vergleich: insgesamt waren zum Zeitpunkt der Prüfung ca. 142 000 Personen in POLAS gespeichert. Die Polizei schätzt die Zahl der von Schuldunfähigen unter 14 Jahren begangenen Straftaten auf jährlich 3000 Fälle.

17.4.2 Rechtliche Ausgangsposition

Nach § 19 Strafgesetzbuch (StGB) beginnt die strafrechtliche Schuldfähigkeit erst mit dem 14. Lebensjahr, das heißt, jüngere Personen können nicht bestraft werden. Auch ein strafrechtliches Ermittlungsverfahren kann gegen sie nicht eingeleitet werden; die Ermittlungen werden vielmehr eingestellt, wenn sich herausstellt, daß der Täter noch nicht 14 Jahre alt ist.

Damit greift die üblicherweise für die Speicherung in Kriminalakten geltende Vorschrift von § 16 Abs. 2 S. 3 des Gesetzes über die Datenverarbeitung der Polizei (PolDVG) nicht; denn diese Regelung setzt zunächst voraus, daß gegen die Person, die gespeichert werden soll, ein Ermittlungsverfahren eingeleitet worden ist. Damit fehlt auch der Ansatzpunkt für die geforderte Prognoseentscheidung, wonach wegen Art, Ausführung oder Schwere der Tat und der Persönlichkeit des Betroffenen die Gefahr der Begehung weiterer Straftaten besteht. Ferner fehlen die verfahrensmäßigen Sicherungen nach Abschluß des Verfahrens; denn die Zulässigkeit der weiteren Speicherung von Personen, gegen die die Polizei ermittelt hat, hängt davon ab, ob die Staatsanwaltschaft oder das Gericht den polizeilichen Verdacht bestätigt.

Das PolDVG enthält ferner in § 16 Abs. 1 die Regelung, wonach die Polizei personenbezogene Daten in Akten und Dateien speichern kann, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist. Diese Generalklausel kann nicht so

ausgelegt werden, daß sie die Speicherung von Kindern zur Erfüllung aller denkbaren polizeilichen Aufgaben ermöglicht. Bei dieser Auslegung wären die Speicherungsmöglichkeiten für schuldunfähige Kinder erheblich weiter als die für straffällige Erwachsene, was weder der polizeilichen Intention noch der festgestellten Praxis entspricht.

Einen Ansatzpunkt bietet ferner die Regelung in § 15 PolDVG, wonach für Kinder eine verkürzte Speicherfrist von 2 Jahren gilt. Im Unterschied zu anderen Personen wird diese Frist nicht durch später hinzukommende Ereignisse neu in Gang gesetzt, sondern gilt selbständig für jeden Anlaß der Speicherung ab dem jeweiligen Zeitpunkt der Erfassung.

Im automatisierten POLAS-Verfahren, das auch der Fristüberwachung dient, ist diese für Kinder geltende Besonderheit bisher nicht vorgesehen gewesen. Sie wird jedoch demnächst programmtechnisch umgesetzt. Bei einigen der geprüften Akten war die zweijährige Frist überschritten, sie wurden daraufhin gelöscht.

17.4.3 Einzelne Fallgruppen

Die den Speicherungen zugrunde liegenden Ereignisse unterscheiden sich beträchtlich. Wir haben daher einzelne Fallgruppen gebildet, um die jeweiligen Probleme besser zu veranschaulichen.

Die mit Abstand größte Gruppe, die ca. die Hälfte der gespeicherten Kinder unter 14 Jahren umfaßte, betraf Serienstraftaten etwa bei Wohnungseinbrüchen oder Ladendiebstählen in großem Umfang und teilweise auch Drogenkriminalität.

In diesen Fällen lag aufgrund der Sachverhaltsbeschreibungen in den Merkblättern der Kriminalakten quasi „berufsmäßiges" Vorgehen vor, wobei auch außer Zweifel stand, daß die gestohlenen Gegenstände oder Summen nicht nur zum „Eigenverbrauch" bestimmt waren. Die Kinder werden als Werkzeuge in Bereichen der Erwachsenenkriminalität benutzt und teilweise in extremer Form ausgebeutet.

Eine Speicherung von Informationen über diesen Personenkreis kann den Zweck der Aufklärung der Hintergründe von Serientaten und Täterverflechtungen (z.B. Drogenkriminalität) erfüllen, ist also eher in den Bereich der aktuellen Strafverfolgung als den der Prävention einzuordnen. Präventiv könnten die Speicherungen der Abwehr von Gefahren für die Betroffenen dienen, da offensichtlich ist, daß die Kinder massiv für kriminelle Zwecke von „Hintermännern" mißbraucht werden.

Diese Zwecke können jedoch nur erfüllt werden, wenn sich die polizeiliche Ermittlungstätigkeit nicht in der Feststellung der Kinder als „Täter" und ihrer Speicherung in polizeilichen Unterlagen und Dateien erschöpft, sondern die bei den Kindern vorliegenden Anhaltspunkte für Hintermänner weiterverfolgt

werden. Den Merkblättern in diesen Fällen, die sich z.Zt. nicht von allen anderen unterscheiden, ließ sich hierfür wenig entnehmen. Allenfalls Mittäter waren erfaßt und könnten Anhaltspunkte für weitere Ermittlungen geben. Wir haben daher vorgeschlagen zu prüfen, welche Möglichkeiten bestehen, Informationen aufzunehmen, die den Zweck der Speicherung besser erfüllen als die Standardmerkblätter. Eine zeitliche Verzögerung bei der Fertigung der Merkblätter oder auch der völlige Verzicht hierauf sollte in Kauf genommen werden, wenn die Informationen insgesamt besser werden.

Wesentlich weniger Personen umfaßte die Fallgruppe mit besonderen Deliktsbereichen wie Auto-Aufbrüche und Folgetaten, die in letzter Zeit erhebliche öffentliche Aufmerksamkeit auf sich gezogen haben. Auch der Raub von Kleidungsstücken zum Nachteil anderer Kinder und Jugendlicher kann in diese Kategorie eingeordnet werden.

In einigen der Akten waren Hinweise auf Gruppierungen enthalten, die im Zusammenhang mit den hier genannten besonderen Deliktsgruppen in Erscheinung getreten sind. Hierin kann auch der über das Einzeldelikt hinausgehende Informationswert der Speicherung gesehen werden. Wie in der ersten Fallgruppe läßt sich eine Speicherung dann mit den Zwecken Strafverfolgung und insbesondere der Gefahrenabwehr für die Kinder selbst begründen, wenn die Einzelfälle weitergehende Informationen über einschlägige Gruppierungen, Hintergründe und Tatzusammenhänge vermitteln. Auch hier sollte überlegt werden, welche Möglichkeiten bestehen, die Speicherung vom Vorliegen derartiger weiterführender Informationen abhängig zu machen.

Die Speicherung von vermißten Kindern in Kriminalakten und POLAS ist zur Gefahrenabwehr für die Betroffenen gerechtfertigt, wenn Informationen vorliegen, die das Wiederauffinden in zukünftigen Fällen ermöglichen können. Wir haben gefordert, die Speicherung von Delikten im Zusammenhang mit dem Vermißtwerden auf die Fälle zu begrenzen, die derartige Hinweise vermitteln können. Die Speicherung des Diebstahls einer Tafel Schokolade oder von Spielzeug während des Vermißtseins ist dagegen für den Zweck der Gefahrenabwehr nicht erforderlich. Wir haben daher die Löschung solcher Angaben in entsprechenden Akten gefordert, was auch geschehen ist.

In einer Reihe von Fällen war nach der Schilderung in den Merkblättern der zugrunde liegende Sachverhalt bzw. dessen strafrechtliche Würdigung nicht ohne Weiteres nachvollziehbar. Teilweise hatte die für die Kriminalaktenhaltung zuständige Dienststelle bei den Sachbearbeitern Rückfrage gehalten, ob die Speicherung auch bei dem für Kinder geltenden strengeren Maßstab vorgenommen werden solle. Hierauf erfolgten jedoch keine die Notwendigkeit der Speicherung begründenden Antworten.

Derartige Fälle waren nach unserem Eindruck bei der Prüfung von Kriminalakten über Beschuldigte im Jahr 1991 (10. TB, 16.3) nicht so häufig feststellbar. Hier wurde deutlich, daß die fehlende Verpflichtung, das tatsächliche Geschehen

bei schuldunfähigen Tätern auszuermitteln, zu einem Qualitätsverlust bei den in Kriminalakten aufgenommenen Informationen führen kann.

Aufgrund unserer Feststellungen sind die dieser Gruppe zugeordneten Akten von der Polizei überprüft worden. Eine Reihe von Akten oder einzelne Merkblätter mit den dazugehörigen POLAS-Datensätzen wurden gelöscht, bei anderen wurde die Notwendigkeit der weiteren Aufbewahrung bestätigt.

Weiter lagen Akten vor, deren zugrunde liegende Sachverhalte nicht bloß als Bagatelldelikte abgetan werden können, sondern z.T. zu beträchtlichen Schäden geführt haben, die andererseits aufgrund der Vorgehensweise der Verursacher erhebliche Unterschiede zu typisch kriminellem Verhalten von Erwachsenen aufweisen. Beispielsfälle hierfür waren Körperverletzungen als Reaktion auf kindliche Hänseleien, sinnlose Sachbeschädigungen oder Brandstiftungen.

In diesen Fällen ist es sehr fraglich, ob die gespeicherten Informationen relevante Erkenntnisse für die polizeiliche Aufgabenerfüllung liefern können. Der Zweck der Aufklärung von Tathintergründen scheidet hier aus. Eine einigermaßen gesicherte Prognose über zukünftiges Verhalten bei den hier Betroffenen scheint kaum möglich, sie würde auch nicht ausreichen, da der Gesichtspunkt der vorbeugenden Verbrechensbekämpfung bei Schuldunfähigen nicht greift. Vielmehr wäre die Erforderlichkeit der Speicherung für bestimmte polizeiliche Aufgaben im Einzelfall zu begründen. Dies ist in den von uns angezweifelten Fällen in der Stellungnahme der Behörde für Inneres zu unserem Prüfbericht geschehen, sodaß die weitere Aufbewahrung gerechtfertigt erscheint.

Fälle von kleinen Ladendiebstählen waren ebenfalls in einigen Akten erfaßt. In diesem Deliktsbereich kann schon bei Erwachsenen die Speicherung der bloßen Tatsache, daß die Tat begangen worden ist, nur sehr eingeschränkt relevante Informationen für die Zukunft liefern. Dies gilt erst recht bei schuldunfähigen Kindern, da hier die Begehensweise noch stärker von Zufälligkeiten oder kinderspezifischer Motivation (z.B. Diebstahl von Spielzeug oder Süssigkeiten) geprägt ist. Die Mehrzahl der Akten, die dieser Fallgruppe zugeordnet wurde, ist gelöscht worden; in einigen Fällen begründen erhebliche andere Delikte die weitere Aufbewahrung.

17.4.4 Zusammenfassende Bewertung

Insgesamt kann anhand der Anzahl der gespeicherten Kinder und auch der überprüften Einzelakten festgestellt werden, daß bei der Anlegung von Kriminalakten für Schuldunfähige unter 14 Jahren ein erheblich restriktiverer Maßstab angelegt wird, als bei Schuldfähigen über 14 Jahren. Die oben beschriebenen Fälle, in denen aus unserer Sicht Zweifel an der Erforderlichkeit bestanden, lassen sich eher auf Unsicherheiten in der Praxis als auf mangelnde Sensibilität zurückführen.

Um diese Unsicherheiten zu verringern, hatten wir zunächst vorgeschlagen, die Merkblätter für diesen Personenkreis anhand vorformulierter Prüffragen zu

konkretisieren. Dem ist die Polizei nicht gefolgt. Sie hat überzeugend dargelegt, daß man sich dann nicht mehr primär mit dem konkreten Einzelfall auseinandersetzen würde, sondern lediglich mit den vorformulierten abstrakten Kategorien. Dies könnte zur Folge haben, daß tatsächlich mehr Daten von Kindern als bisher gespeichert würden. Statt dessen soll eine Einzelfallprüfung durch den Leiter der für die Kriminalaktenhaltung zuständigen Dienststelle des Landeskriminalamtes stattfinden. Die Aufarbeitung unserer Prüfung läßt erwarten, daß der bisherige restriktive Maßstab bei der Speicherung von Kindern beibehalten wird.

17.5 Datei über Zuhälter- und Milieukriminalität

Seit mehr als zwei Jahren wird innerhalb der Behörde für Inneres und der Polizei intensiv die Frage diskutiert, in welcher Form eine Datei über Zuhälter- und Milieukriminalität geführt werden soll. Ausgangspunkt ist die bereits seit langem bestehende Zuhälter- und Prostituiertenkartei. In ihr sind nicht nur Zuhälter und Prostituierte erfaßt worden, gegen die ein strafrechtliches Ermittlungsverfahren eingeleitet wurde. Besonders problematisch war vielmehr die Erfassung von Prostituierten ohne strafrechtlich relevante Anlässe, etwa aufgrund von Anhaltemeldungen. Dies soll nach gemeinsamer Auffassung nicht fortgesetzt werden.

Im Sommer 1992 ist uns dann der Entwurf einer Errichtungsanordnung für die zukünftige Führung der Datei übersandt worden. Zwischen der Polizei und uns besteht Einvernehmen darüber, daß die Speicherung in der Datei nur dann erfolgen kann, wenn dies erforderlich ist, um weiterführende Hinweise zur Aufklärung von Straftaten zu erlangen, die für das sog. Rotlichtmilieu typisch sind. Wir stimmen mit der Polizei auch in der Einschätzung überein, daß die Besonderheiten dieses Milieus, das durch Abschottung und Ausbeutungsdruck geprägt ist, andere Formen der Datenverarbeitung notwendig machen als in anderen Deliktsbereichen. Andererseits ist aus unserer Sicht unverzichtbar, daß nicht allein die Zugehörigkeit zum Milieu zum Ausgangspunkt für Speicherungen genommen wird, sondern der Bezug zu strafrechtlichen Vorwürfen im Einzelfall gewahrt werden muß.

Die Diskussion über die Ausgestaltung der Errichtungsanordnung und der Datei selbst, die wir ausgehend von einer Prüfung des bisherigen Zustands aufgenommen haben, war bei Redaktionsschluß noch nicht abgeschlossen. Wir hoffen jedoch, im nächsten Tätigkeitsbericht über ein für alle Beteiligten vertretbares Ergebnis berichten zu können.

17.6 Akten über politische Organisationen beim polizeilichen Staatsschutz

Die frühere Sammlung von sogenannten „Fallakten" bei der Staatsschutzabteilung des Landeskriminalamtes ist im 10. TB (16.5) dargestellt worden. Nachdem die Polizei das Problem mehr als ein Jahr lang ungelöst vor sich hergeschoben hatte, wurde die Bereinigung des Aktenbestandes dann durch die öffentliche

Diskussion aufgrund unseres Berichts und einer Debatte in der Bürgerschaft beschleunigt. Im April 1992 teilte die Behörde für Inneres mit, daß von den ursprünglich etwa 700 Akten noch 83 übrig geblieben sind. Der Rest, soweit er nicht zuvor bereits vernichtet worden war, ist an das Staatsarchiv abgeliefert worden. Wie wir inzwischen erfahren haben, ist die Ablieferung allerdings erst Ende August 1992 erfolgt, nachdem wir der Polizei eine Prüfung des Aktenbestandes angekündigt hatten.

Ferner legte die Behörde Grundsätze für das Anlegen und Führen von Sachakten vor. Danach sollen in Zukunft Sachakten geführt werden, um Gefährdungssachverhalte bzw. Angriffsziele zu erkennen, Gefahren bei Versammlungen und Aktionen erkennen zu können, Organisationen, Institutionen und Objekte, die als Gefahrenquelle oder als gefährdet anzusehen sind, zu beurteilen und die erforderlichen polizeilichen Maßnahmen veranlassen zu können. Hierfür sollen die folgenden Kategorien von Akten gebildet werden:

— Organisationen und Institutionen, von denen Gefahren und Straftaten mit extremistischem Hintergrund ausgehen;

— Organisationen usw., die keine extremistischen Ziele verfolgen, jedoch im Rahmen ihrer Aktivitäten Straftaten oder Gefahren für die öffentliche Sicherheit und Ordnung verursachen;

— Organisationen usw., die durch Gruppierungen/Personen aus dem politisch motivierten Bereich gefährdet sind oder sein können;

— Organisationen usw., die selbst weder Gefahrenquelle noch gefährdet sind, aber für die Gefahreneinschätzung im Rahmen der Aufgabenstellung der Staatsschutzabteilung von Bedeutung sind. Hierbei sollen nur allgemein zugängliche Informationen aufgenommen werden und die Betroffenen informiert werden. Personenbezogene Daten über Ansprechpartner sollen nur mit Einverständnis der Betroffenen erfaßt werden.

— Themenkomplexe, die für die Aufgabenstellung der Staatsschutzabteilung von Bedeutung sind (z.B. Bürgerschaftswahl oder Fremdenfeindlichkeit).

Die Akten sollen je nach Kategorie gekennzeichnet und geordnet werden. Bei der Zuordnung zu mehreren Kategorien (Gefahrenquelle und zugleich gefährdet) sollen gesonderte Akten angelegt werden, um Mischakten zu vermeiden.

Als mögliche Inhalte der Akten sind neben Grundinformationen über die Organisation oder Institution, die aus allgemein zugänglichen Quellen oder von den Betroffenen selbst stammen, Angaben über polizeiliche Maßnahmen bei der Strafverfolgung oder Gefahrenabwehr sowie personenbezogene Daten über Beschuldigte oder Störer, vermutliche Störer, Geschädigte oder Gefährdete, sowie Ansprechpartner vorgesehen. Nicht mehr aufgenommen werden dagegen Handakten zu Ermittlungsvorgängen und insbesondere keine Informationen über Demonstrationen und sonstige Versammlungen, die wir bei der Akte über amnesty international kritisiert hatten.

Die Aufbewahrungsfrist orientiert sich an den Vorgaben des Gesetzes über die Datenverarbeitung der Polizei (PolDVG), d.h. eine Akte kann maximal 10 Jahre nach dem letzten relevanten Ereignis aufbewahrt werden. Es ist jedoch eine fortlaufende Überprüfung vorgesehen, ob die Akte noch erforderlich ist.

Um der Polizei ausreichend Zeit zu geben, diese eigenen Vorgaben auch umzusetzen, haben wir die Angelegenheit zunächst ruhen lassen, um uns dann einen Eindruck von der neuen Konzeption für die Aktenhaltung zu verschaffen. Bei einer Prüfung im September 1992 war noch exakt der Zustand vorzufinden, der nach der großen Aussonderungsaktion im März vorlag. Das heißt, die Akten waren noch nicht nach den vorgesehenen unterschiedlichen Kategorien geordnet. Dies soll erst aufgrund einer detaillierten Arbeitsanweisung geschehen, die im September erstellt wurde. Zwischenzeitlich wurden weder neue Akten angelegt noch zusätzliche Informationen in die Akten aufgenommen.

Aufgrund einiger Stichproben haben wir festgestellt, daß in aller Regel nur Merkblätter über strafrechtlich relevante Vorgänge in den Akten aufgenommen waren, die personenbezogene Daten über Beschuldigte oder Geschädigte enthielten. Diese Angaben können nicht mit personenbezogenen Merkmalen recherchiert werden, sie enthalten auch nichts, was sich nicht aus den Handakten über die einzelnen strafrechtlichen Ermittlungsvorgänge ergibt. Unter dem Gesichtspunkt des Schutzes personenbezogener Daten ist gegen den Aktenbestand daher grundsätzlich nichts einzuwenden.

Allerdings haben wir die Zulässigkeit einer Akte bestritten, die sich keiner Kategorie zuordnen ließ und in der sämtliche Vorstandsmitglieder der Organisation verzeichnet und somit mit einigem Hintergrundwissen auffindbar waren. Uns ist daraufhin mitgeteilt worden, daß diese Akte ausgesondert und dem Staatsarchiv angeboten wird. Ob sich im übrigen die Erwartung erfüllt, daß die Akten für polizeiliche Aufgaben nützlich sein werden, hängt von der Umsetzung der Arbeitsanweisung ab.

17.7 Einsatz besonderer Befugnisse zur Datenerhebung durch die Polizei

Das hamburgische Gesetz über die Datenverarbeitung der Polizei (PolDVG) und die durch das Gesetz zur Bekämpfung der Organisierten Kriminalität (OrgKG) novellierte Strafprozeßordnung lassen die Erhebung personenbezogener Daten mit verdeckten Methoden zu. Die einschlägigen Vorschriften der Strafprozeßordnung sind dann anwendbar, wenn der Verdacht besteht, daß eine Straftat bereits begangen worden ist. Sie sind erst im September 1992 in Kraft getreten. Daher liegen zum Zeitpunkt der Veröffentlichung dieses Tätigkeitsberichts noch keine aussagekräftigen Erfahrungen über die Anwendung der Vorschriften vor.

Das PolDVG gilt seit dem 1. August 1991. Es ist anwendbar, wenn Straftaten noch nicht begangen worden sind, sondern ihre bevorstehende Begehung verhütet werden soll oder andere Gefahren abgewehrt werden sollen. Wir haben die Behörde für Inneres ein Jahr nach Inkrafttreten des PolDVG um Mitteilung gebeten, in wie vielen Fällen Anordnungen zum Einsatz der besonderen Methoden zur Datenerhebung nach diesem Gesetz ergangen sind.

Danach ist in 6 Fällen eine längerfristige Observation nach § 9 PolDVG angeordet worden. Unter einer längerfristigen Observation ist die planmäßig angelegte Beobachtung von Personen zu verstehen, die entweder innerhalb einer Woche länger als 24 Stunden dauert oder über den Zeitraum einer Woche hinausgeht.

Anordnungen über den verdeckten Einsatz technischer Mittel nach § 10 Abs. 1 PolDVG sind in 38 Fällen ergangen. Hierunter fallen Mittel für Foto-, Film-, Video- und Tonaufnahmen (z.B. auch Personenschutzsender). Die Behörde hat darauf hingewiesen, daß es sich hierbei im wesentlichen um den Schutz von verdeckten Ermittlern und V-Leuten bei deren Einsatz zur Strafverfolgung handelte.

Es hat keine Anordnung zum Einsatz von verdeckten technischen Mitteln zur Abwehr einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person in oder aus Wohnungen gegeben, die nach § 10 Abs. 2 PolDVG grundsätzlich dem Richter vorbehalten ist. Nach längeren Diskussionen mit der Behörde für Inneres wurde inzwischen einvernehmlich klargestellt, daß die besonderen Voraussetzungen von § 10 Abs. 2 PolDVG auch dann gelten, wenn sich der verdeckte Einsatz der technischen Mittel gegen Wohnungen richtet, die von außen einsehbar oder einhörbar sind.

Der Einsatz von Personenschutzsendern in Wohnungen zum Schutz der bei einem polizeilichen Einsatz Tätigen steht nach § 10 Abs. 4 PolDVG allerdings nicht unter dem Richtervorbehalt.

Die Behörde hat auch auf unsere Fragen nach Anordnungen für den Einsatz verdeckter Ermittler und sog. V-Personen geantwortet; sie hat einer Veröffentlichung der Angaben über diesen Personenkreis jedoch nicht zugestimmt.

V-Leute im Sinne von § 11 PolDVG sind Personen, deren Zusammenarbeit mit der Polizei Dritten nicht bekannt ist. Es kommt darauf an, ob die Person von der Polizei angehalten wird, zu einem Sachverhalt oder zu Personen Informationen zu beschaffen. Verdeckte Ermittler nach § 12 PolDVG sind Beamte des Polizeivollzugsdienstes, die unter einer amtlich verliehenen, auf Dauer angelegten, veränderten Identität, einer sogenannten Legende, eingesetzt werden.

Gemeinsame Voraussetzung für die Anordnung dieser besonderen Methoden ist es, daß ihr Einsatz zur Abwehr einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist. Ferner kann der Einsatz dieser Methoden angeordnet werden, wenn Tatsachen die Annahme rechtfertigen, daß die Person sogenannte Strafaten von erheblicher Bedeutung begehen wird, zu deren Verhütung die verdeckte Datenerhebung erforderlich ist. Die

Straftaten von erheblicher Bedeutung werden in § 1 Abs. 4 PolDVG abschließend aufgezählt. Es handelt sich dabei um eine Reihe von Verbrechen, also Straftaten, die mit einer Freiheitsstrafe von mindestens einem Jahr bedroht sind, sowie gewerbs- und bandenmäßige Straftaten.

Eine Straftat von erheblicher Bedeutung ist auch das Vergehen der Bildung einer kriminellen Vereinigung nach § 129 StGB. Auf die Problematik dieses Tatbestands für die vorbeugende Bekämpfung von Straftaten hatten wir bereits im Gesetzgebungsverfahren hingewiesen (9. TB, 4.12.1). Die Behörde für Inneres hat mitgeteilt, daß in keinem der Fälle eine drohende Straftat nach § 129 StGB Ansatzpunkt für den Einsatz besonderer Erhebungsmethoden war.

Polizeiliche Beobachtungen sind in 66 Fällen angeordnet worden. Polizeiliche Beobachtung im Sinne von § 13 PolDVG (auch beobachtende Fahndung genannt) bedeutet, daß bestimmte Daten, insbesondere Personalien und Kfz-Kennzeichen in einer Datei – meist bundesweit in INPOL – ausgeschrieben werden. Auch für die polizeiliche Beobachtung ist maßgeblich, ob Straftaten von erheblicher Bedeutung begangen werden sollen. Für diese Annahme müssen entweder Tatsachen sprechen oder sie muß sich aus der Gesamtwürdigung der Person des Betroffenen ergeben.

Eine Rasterfahndung auf der Grundlage von § 22 PolDVG hat nicht stattgefunden. Bei der Rasterfahndung werden bestimmte personenbezogene Datenbestände mit anderen Beständen automatisiert abgeglichen, um festzustellen, auf welche Personen bestimmte Merkmale zutreffen. Sie ist nur zulässig zur Abwehr einer unmittelbar bevorstehenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person.

17.8 Videoaufnahmen von Versammlungen

Im Berichtszeitraum wurde aus verschiedenen Anlässen öffentlich diskutiert, unter welchen Voraussetzungen die Polizei befugt ist, Videoaufnahmen von Versammlungen anzufertigen.

Das Recht, sich ohne Anmeldung und Erlaubnis friedlich und ohne Waffen zu versammeln, steht unter dem besonderen Schutz von Art. 8 Grundgesetz (GG). Für Versammlungen unter freiem Himmel kann dieses Recht durch Gesetz oder auf Grund eines Gesetzes eingeschränkt werden. Videoaufnahmen von Versammlungen greifen in das Grundrecht ein, bedürfen daher einer gesetzlichen Rechtfertigung.

Das Versammlungsgesetz erlaubt in § 19a in Verbindung mit § 12a Bild- und Tonaufnahmen von Teilnehmern durch die Polizei bei oder im Zusammenhang mit öffentlichen Versammlungen, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß von ihnen erhebliche Gefahren für die öffentliche Sicherheit oder Ordnung ausgehen. Die Maßnahmen dürfen auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden. Dies gilt für angemeldete Versammlungen ebenso wie für unangemeldete Spontanversammlungen, die ebenfalls dem Grundrechtsschutz nach Art. 8 GG unterliegen.

Eine Prognose über auf Tatsachen beruhende Erkenntnisse, die den Schluß zulassen, daß von der Versammlung erhebliche Gefahren ausgehen werden, ist immer mit gewissen Unsicherheitsfaktoren verbunden. Die Polizei ist daher gehalten, den tatsächlichen Ablauf der Versammlung zu berücksichtigen. Stellt sich im Verlauf der Versammlung heraus, daß sich die zu Beginn begründete Prognose nicht bewahrheitet, müssen die Videoaufnahmen wieder eingestellt werden.

Andererseits ändert sich die Rechtsgrundlage, wenn während der Versammlung Straftaten begangen werden: Dann ist nicht mehr das Versammlungsgesetz maßgeblich, sondern die Strafprozeßordnung. Die Videoaufnahmen dienen dann nicht mehr der Abwehr von Gefahren, sondern der Beweisführung in einem Strafverfahren.

Die unterschiedlichen Rechtsgrundlagen haben wesentliche Bedeutung für die Frage, was mit den Aufnahmen nach Abschluß der Versammlung zu geschehen hat. Sind keine Strafaten begangen worden und ist auch kein Verdacht auf Straftaten einzelner Personen aufgekommen, sind die Aufnahmen unverzüglich nach Abschluß der Versammlung zu vernichten. Unverzüglich heißt in diesem Zusammenhang, daß der Polizei keine Auswertungs- und Prüfungsfrist zugestanden wird, um anhand der Videoaufnahmen erstmalig festzustellen, ob Straftaten begangen worden sind oder ein dahingehender Verdacht begründet ist. Dies muß sich vielmehr bereits aus dem Ablauf der Versammlung ergeben.

Hiervon ist die Regelung über Videoaufnahmen nach § 8 des Gesetzes über die Datenverarbeitung der Polizei (PolDVG) zu unterscheiden. Diese Vorschrift ist nur anwendbar, wenn es sich nicht um Versammlungen im Sinne von Art. 8 GG handelt, sondern um Veranstaltungen (z.B. Fußballspiele, Open-Air-Konzerte). Videoaufnahmen über Veranstaltungen setzen Tatsachen voraus, die die Annahme rechtfertigen, daß Straftaten begangen werden. Diese Aufnahmen dürfen höchstens einen Monat nach der Veranstaltung aufbewahrt werden und sind dann zu löschen, es sei denn, sie werden zur Strafverfolgung oder vorbeugenden Bekämpfung von Straftaten erheblicher Bedeutung benötigt.

Aufnahmen, die Beweismittel in einem Strafverfahren sind, darf die Polizei dagegen aus eigenem Entschluß überhaupt nicht löschen. Sie werden Bestandteil der staatsanwaltschaftlichen Ermittlungsakte und unterliegen damit der verantwortlichen Beurteilung durch die Staatsanwaltschaft und das Gericht.

Problematisch ist ferner die letzte Variante der weiteren Aufbewahrung von Videoaufnahmen. Nach § 12a Abs. 2 Versammlungsgesetz ist die weitere Aufbewahrung zum Zwecke der Abwehr zukünftiger erheblicher Gefahren, die von den gefilmten Personen für künftige öffentliche Versammlungen ausgehen, zulässig. Nach § 8 Abs. 1 S. 3 PolDVG ist die weitere Aufbewahrung von Aufnahmen über Veranstaltungen möglich, wenn dies zur vorbeugenden Bekämp-

fung von Straftaten von erheblicher Bedeutung dient. In beiden Fällen wird eine doppelte polizeiliche Prognose verlangt. Zum Zeitpunkt der Aufnahme muß die Annahme berechtigt sein, daß Straftaten oder erhebliche Gefahren eintreten, zum Zeitpunkt der Entscheidung über die weitere Aufbewahrung muß prognostiziert werden, daß die betroffenen Personen in Zukunft erhebliche Gefahren hervorrufen oder Straftaten von erheblicher Bedeutung begehen.

Als Korrektur für diese mit großen Unsicherheiten behafteten Prognosen muß das Kriterium der Erheblichkeit herangezogen werden. Dies gilt insbesondere bei Videoaufnahmen über grundrechtlich geschützte Versammlungen. Sie greifen nicht nur in das Persönlichkeitsrecht der Betroffenen ein, sondern auch in ihr Grundrecht auf Versammlungsfreiheit, das nach der Rechtsprechung des Bundesverfassungsgerichts auch vor staatlicher Beobachtung schützt. Deshalb kann nicht jeder Verstoß gegen Vorschriften des Versammlungsrechts herangezogen werden, um das Vorliegen erheblicher Gefahren im Sinne des Versammlungsgesetzes zu begründen.

Ausgangspunkt für die Prognose zur weiteren Aufbewahrung können in aller Regel nur Straftaten wie Landfriedensbruch, oder z.B. der Verstoß gegen das Verbot, bei Versammlungen Waffen zu tragen, sein. Ließe man dagegen den Vorwurf einer Nötigung nach § 240 StGB und die Erwartung, daß die Person auch in Zukunft eine vergleichbare Straftat begeht, zu, wäre die Verwendungsmöglichkeit von Aufnahmen über Versammlungen weiter als die über Aufnahmen von Veranstaltungen, die keinen Grundrechtsschutz genießen.

Die datenschutzrechtliche Prüfung, die wir aus Anlaß von Videoaufnahmen bei einer Versammlung eingeleitet haben, war bei Redaktionsschluß noch nicht abgeschlossen.

18. Verfassungsschutz

18.1 Entwurf des Hamburgischen Verfassungsschutzgesetzes

Im Berichtszeitraum wurde zunächst ein überarbeiteter Referentenentwurf zur Behördenabstimmung übersandt. Dieser Entwurf wies eine Reihe schwerwiegender datenschutzrechtlicher Mängel auf. Die schon im 8. TB. (3.9.1.2) entwickelten Anforderungen und die im 10. TB (18.2) wiedergegebenen Eckdaten hatten überwiegend keine Berücksichtigung gefunden. Grundsätzlich war anzumerken, daß die datenschutzrechtliche Terminologie in den Gesetzentwurf nur unvollkommen eingearbeitet war und erhebliche systematische Mängel erkennbar waren.

Bei der Aufgabenbeschreibung für den Verfassungsschutz war eine Ausdehnung der Aufgaben hin zur eigenen Gefahrenabwehr im Tätigkeitsfeld des Verfassungsschutzes vorgesehen. Der Verwendungszweck der Datensammlungen sowie die Erhebungsvorschriften waren wenig präzise geregelt. Auch weitete der Entwurf die Kompetenzen des Verfassungsschutzes durch eine spe-

zielle Auslegungsvorschrift für den Begriff der Bestrebungen, der zumindest eine Mehrzahl von Personen voraussetzt, auf isolierte Einzelpersonen aus. Die nachrichtendienstlichen Mittel sowie ihre Anwendung sollten lediglich in einer Dienstanweisung geregelt werden.

Die Form der Zusammenarbeit mit anderen Behörden, insbesondere die Form und Art der Einsichtnahme in die Akten und Dateien anderer Behörden, war datenschutzrechtlich nur unzureichend geregelt. Die Zusammenarbeit mit der Polizei war, was die Übermittlung von und an den Verfassungsschutz betrifft, so erweitert, daß von einer informationellen Trennung der Bereiche nur sehr eingeschränkt die Rede sein konnte.

Der Entwurf wurde dann – auch aufgrund der Stellungnahmen der anderen Behörden – erneut überarbeitet. Der überarbeitete Referentenentwurf stellt einen erheblichen Fortschritt dar, wenn auch gravierende Probleme nicht zu übersehen sind.

In dem Entwurf ist die Aufgabe der Gefahrenabwehr für den Verfassungsschutz zwar entfallen. Nach wie vor kann aber die Einzelperson eine „Bestrebung" im Sinne von § 5 Abs. 1 darstellen. Im Kontext des Grundgesetzes wird jedoch als „Bestrebung" nur die Tätigkeit mehrerer Personen unter einheitlicher Zielvorstellung verstanden. Die Ausdehnung des Begriffs der „Bestrebung" auf die Einzelperson eröffnet nach dem gegenwärtigen Stand die Möglichkeit der Prüfung von Einzelpersonen mit nachrichtendienstlichen Mitteln.

Positiv ist zu werten, daß die nachrichtendienstlichen Mittel abschließend in § 7 Abs. 3 aufgezählt werden, wenn auch eine Erweiterung durch Dienstanweisung möglich ist. Positiv ist weiterhin zu bewerten, daß für eine Reihe von gravierenden Eingriffen und Erhebungsmethoden der Behördenleitervorbehalt beibehalten wurde. Dieser Vorbehalt kann gewährleisten, daß von den unter Vorbehalt stehenden Befugnissen nur restriktiv Gebrauch gemacht werden wird.

Ferner ist herauszuheben, daß für das Auskunftsrecht des Betroffenen keine einschränkenden Spezialregelungen getroffen sind – wie ursprünglich vorgesehen; vielmehr soll das für alle Behörden maßgebliche Auskunftsrecht durch Verweis auf § 18 Hamburgisches Datenschutzgesetz gelten.

Hervorzuheben ist auch, daß eine Übermittlung von Daten in das Ausland dann unterbleibt, wenn die Übermittlung gegen den Zweck eines deutschen Gesetzes verstößt oder schutzwürdige Belange des Betroffenen entgegenstehen. Andererseits ist nicht in allen Fällen gewährleistet, daß das Landesamt für Verfassungsschutz (LfV) nur dann tätig werden kann, wenn tatsächliche Anhaltspunkte für Bestrebungen vorliegen. Die Zweckbindung der Daten ist nur unvollständig geregelt. Besonders hervorzuheben ist die Absicht, zukünftig auch Minderjährige ohne ein Mindestalter speichern zu können.

Im Bereich der Datenübermittlung an die Polizei sind noch Regelungslücken vorhanden, die aber geschlossen werden sollen. Die Registereinsicht ist nach

wie vor weitgehend unbeschränkt möglich, ohne daß die Register abschließend aufgezählt worden wären. Eine Verbesserung ergibt sich insoweit allenfalls dadurch, daß das LfV alle Registereinsichten einschließlich des hiermit verfolgten Zweckes protokollieren muß und die Protokollierungen im wesentlichen nur zur datenschutzrechtlichen Kontrolle dienen.

Die weitere Diskussion wird zeigen, inwieweit die hier exemplarisch dargestellten, noch offenen Problemfelder datenschutzrechtlich einwandfrei gelöst werden können. Die bisher konstruktive Diskussion gibt Veranlassung zur Hoffnung.

18.2 Sicherheitsüberprüfung von Beschäftigten

Eine gesetzliche Regelung über die Durchführung der Sicherheitsüberprüfungen von Beschäftigten fehlt nach wie vor. Mehrere Gesetzentwürfe wurden auf Bundesebene erstellt, ohne daß abzusehen ist, wie lange das Gesetzgebungsverfahren dauern wird. Auf Landesebene wurde durch eine länderübergreifende Kommission ein Gesetzentwurf vorbereitet, der aber nicht näher diskutiert werden soll, solange die bundesrechtliche Regelung fehlt.

In Hamburg enthält der Entwurf eines Verfassungsschutzgesetzes rudimentäre Regelungen zu diesem Problemkreis, die aber keinesfalls ausreichend sind. Vor allem die Sicherheitsüberprüfung von Beschäftigten der privaten Wirtschaft bedarf einer präzisen bereichsspezifischen Regelung.

Eine Prüfung der beim Landesamt für Verfassungsschutz (LfV) geführten Datei bzw. Kartei über die Personen, die einer Sicherheitsüberprüfung unterzogen wurden, ergab zum einen gravierende Mängel im Bereich der Datensicherheit. Außerdem wurde hinsichtlich der Speicherung von Mitarbeitern , die in privaten Unternehmen beschäftigt sind und in sicherheitsempfindlichen Bereichen arbeiten , festgestellt, daß ein nicht unerheblicher Teil der gespeicherten Personen nicht mehr in Sicherheitsbereichen tätig ist; ihre Daten hätten gelöscht werden müssen. Dieser Mangel war auch schon vom LfV erkannt worden.

Wir haben die erforderlichen Maßnahmen zur Datensicherheit sowie eine Überarbeitung des Verfahrens der Löschung verlangt, um sicherzustellen, daß nur diejenigen Personen gespeichert werden, die noch in sicherheitsrelevanten Funktionen tätig sind.

18.3 Automatisierung der Referatsarbeitskartei (RAK)

Im Landesamt für Verfassungsschutz wurden die Arbeiten zur Automatisierung der Referatsarbeitskartei (RAK) fortgeführt (vergleiche zum Projekt 10. TB, 18.3).

In diesem Bereich werden die personenbezogenen Daten aus dem rechts- und linksextremistischen Spektrum zentral in einer Anlage gespeichert. Wegen der Sensibilität der personenbezogenen Daten und der Bedeutung für die Innere Sicherheit ist hier ein Höchstmaß an Datensicherheit notwendig.

Leider war die Systementscheidung ohne ausreichende Beteiligung des Hamburgischen Datenschutzbeauftragten getroffen worden, so daß die grundlegenden Sicherheitsbedenken gegen die vorgesehene Systemkonzeption nicht mehr bei der Auswahl berücksichtigt werden konnten.

Das vorgesehene System weist durch die spezifische Kombination von Hard- und Software strukturelle Unsicherheiten auf, die nur durch eine aufwendige Programmierung möglicherweise beseitigt werden können. Insbesondere beim Rechnerzugang zeigten sich gravierende Mängel. Jede Erweiterung des Systems durch neue Anwendungen wird dazu führen, daß umfangreiche Nachbesserungsarbeiten notwendig werden, um den Sicherheitsstandard halten zu können.

Ob diese – immer komplexeren – Sicherheitsmaßnahmen dann den gewünschten Erfolg bringen werden, ist zu bezweifeln. Je komplexer in einem System versucht wird, konstruktionsbedingte Sicherheitsmängel durch zusätzliche Sicherheitsmaßnahmen zu kompensieren, desto größer wird die Wahrscheinlichkeit, daß eine „Lücke" übersehen wird. Diese kostspieligen Arbeiten und die Sicherheitsmängel wären vermeidbar gewesen, wenn ein schon vom Ansatz her sichereres System ausgewählt worden wäre, welches eine nachträgliche Härtung nicht erforderlich macht.

Umso bedauerlicher ist es, daß offenbar die Systementscheidung von anderen Behörden wegen des beim Landesamt für den Verfassungsschutz vermuteten hohen Sicherheitsstandards übernommen wurde. Hierbei ist festzuhalten, daß wir überwiegend auch an den Auswahlentscheidungen dieser Behörden – bis auf eine Ausnahme, wo das System nach dem derzeitigen Stand nicht beschafft werden wird – nicht beteiligt wurden.

19. Justiz

19.1 Gesetz zur Bekämpfung der organisierten Kriminalität und Lauschangriff

Mit dem Gesetz zur Bekämpfung der organisierten Kriminalität (OrgKG) sind die Rechtsgrundlagen für den Einsatz verdeckter Methoden zur Datenerhebung in der Strafprozeßordnung geschaffen worden. Dazu gehören die Rasterfahndung, der Einsatz von verdeckten Ermittlern und V-Leuten, sowie von verdeckten technischen Methoden zur Datenerhebung. Diese Regelungen sind im September 1992 in Kraft getreten. Ausgespart wurden allerdings Befugnisse, die den Einsatz von technischen Methoden zur Datenerhebung in oder aus Wohnungen zur Strafverfolgung zulassen. Der Ausdruck „Lauschangriff" für diese technischen Methoden ist nicht ganz ausreichend, denn es geht nicht nur um den Einsatz von Wanzen und anderen Mikrophonen zur Aufzeichnung des gesprochenen Wortes, sondern auch um verdeckte Bildaufnahmen.

Bei der Verabschiedung des OrgKG im Deutschen Bundestag haben die Koalitionsfraktionen in einer Entschließung zum Ausdruck gebracht, daß die Zulässigkeit derartiger Methoden in Wohnungen noch besonders sorgfältiger Prüfung bedarf und nach dieser Prüfung vom Gesetzgeber wieder aufgegriffen werden solle.

Bei der Diskussion um den Lauschangriff ist zu unterscheiden zwischen den jeweiligen Zwecken, denen die Ton- oder Bildaufnahmen in oder aus Wohnungen dienen sollen.

Wenn es um die Abwehr unmittelbar bevorstehender Gefahren für Leib, Leben oder Freiheit von Personen geht, ist das Polizeirecht einschlägig, das vom Landesgesetzgeber geregelt wird. Das hamburgische Gesetz über die Datenverarbeitung der Polizei (PolDVG) läßt den Lauschangriff zu diesem Zweck auf richterliche Anordnung in § 10 Abs. 2 zu (siehe oben 17.7). Ein Sonderfall sind sogenannte Personenschutzsender. Sie werden eingesetzt, um Gefahren für Leib, Leben oder Freiheit von verdeckten Ermittlern und V-Leuten abwehren zu können (siehe oben 17.7). Auch wenn der Einsatz dieser Personen der Strafverfolgung dient, bezweckt der Einsatz der Personenschutzsender die Abwehr konkreter Gefahren. Personenschutzsender können zu diesem Zweck nach § 10 Abs. 4 PolDVG auch ohne richterliche Anordnung eingesetzt werden.

Als Regelungsbereich des Bundesgesetzgebers in der Strafprozeßordnung bleibt der „Lauschangriff" zur Aufklärung begangener Straftaten. Es ist anerkannt, daß die Datenerhebung in oder aus Wohnungen mit verdeckten technischen Mitteln einen Eingriff in das Grundrecht auf Unverletzlichkeit der Wohnung nach Art. 13 Grundgesetz (GG) darstellt. Art. 13 GG läßt Eingriffe zur Abwehr von Lebensgefahren zu; auf Grund eines Gesetzes sind sie auch zur Verhütung dringender Gefahren für die öffentliche Sicherheit und Ordnung gestattet. Während die landesgesetzlichen Regelungen des Polizeirechts über die verdeckte Datenerhebung aus Wohnungen zur Gefahrenabwehr damit an die Schrankenregelung im Grundgesetz anknüpfen können, läßt Art. 13 GG diese Maßnahmen nicht zur Strafverfolgung zu. Die Aufnahme des Lauschangriffs in die Strafprozeßordnung würde daher eine Grundgesetzänderung voraussetzen.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich auf ihrer Konzerenz am 1./2. Oktober 1992 mit der Problematik des Lauschangriffs befaßt und bei Gegenstimme Bayerns erklärt:

„Nachdem erst vor kurzem mit dem Gesetz zur Bekämpfung der organisierten Kriminalität die Befugnisse der Strafverfolgungsbehörden erheblich erweitert worden sind und obwohl über den Erfolg dieser Maßnahmen noch keine Erfahrungen gesammelt werden konnten, wird gegenwärtig parteiübergreifend vielfach die Forderung erhoben, der Polizei in bestimmten Fällen das heimliche Abhören und Herstellen von Bild- und Tonaufzeichnungen in und aus Wohnungen (sog. ‚Lauschangriff') zu ermöglichen.

1. Das Grundgesetz gewährt jedem einen unantastbaren Bereich privater Lebensgestaltung, der der Einwirkung der öffentlichen Gewalt entzogen ist. Dem einzelnen muß um der freien und selbstverantwortlichen Entfaltung seiner Persönlichkeit willen ein ‚Innenraum' verbleiben, in dem er ‚sich selbst besitzt' und ‚in den er sich zurückziehen kann, zu dem die Umwelt keinen Zutritt hat, in dem man in Ruhe gelassen wird und ein Recht auf Einsamkeit genießt' (BVerfGE 27,1 ff.). Jedem muß ein privates Refugium, ein persönlicher Bereich bleiben, der obrigkeitlicher Ausforschung – insbesondere heimlicher – entzogen ist. Dies gilt gegenüber Maßnahmen der Strafverfolgung vor allem deshalb, weil davon auch unverdächtige oder unschuldige Bürger betroffen sind. Auch strafprozessuale Maßnahmen dürfen nicht den Wesensgehalt eines Grundrechts, insbesondere nicht das Menschenbild des Grundgesetzes verletzen.
2. Die Datenschutzbeauftragten nehmen die Gefahren, die das organisierte Verbrechen für die Opfer und auch für die Demokratie und den Rechtsstaat heraufbeschwört, sehr ernst. Sie sind allerdings der Meinung, daß eine angemessene Abwägung zwischen der Verfolgung der organisierten Kriminalität und dem Schutz der Persönlichkeitsrechte der Bürger geboten und möglich ist und es eine Wahrheitserforschung um jeden Preis auch künftig im Strafprozeßrecht nicht geben darf. Daraus folgt, daß der Lauschangriff auf Privatwohnungen für Zwecke der Strafverfolgung auch in Zukunft nicht erlaubt werden darf.
3. Eine andere Frage ist, ob und unter welchen Voraussetzungen der Gesetzgeber für Räume, die allgemein zugänglich sind oder beruflichen oder geschäftlichen Tätigkeiten dienen (z.B. Hinterzimmer von Gaststätten, Spielcasinos, Saunaclubs, Bordelle), einen Lauschangriff zulassen kann. Hierfür sind Mindestvoraussetzungen ein eng begrenzter abschließender Straftatenkatalog, die Verwendung der gewonnenen Erkenntnisse ausschließlich zur Verfolgung dieser Straftaten, ein strikter Richtervorbehalt sowie die Wahrung besonderer Amts- und Berufsgeheimnisse."

Die Position des Datenschutzes ist damit deutlich umschrieben worden, insbesondere für die Grenzen immer weitergehender Eingriffe in den persönlichen Lebensbereich. Andererseits sind vertretbare Handlungsmöglichkeiten für den Schutz der inneren Sicherheit aufgezeigt worden. Es bleibt abzuwarten, ob und wie diese Hinweise vom Gesetzgeber aufgegriffen werden.

19.2 Entwurf des Justizmitteilungsgesetzes

Trotz der seit Jahren von den Datenschutzbeauftragten geforderten gesetzlichen Regelungen zu den Mitteilungen der Justiz an Dritte in Zivil- und Strafsachen fehlt es noch immer an einer gesetzlichen Regelung. Allerdings ist festzuhalten, daß die Gesetzgebungsarbeiten 1992 ein gutes Stück vorangekommen sind. So liegen zu dem Gesetzentwurf der Bundesregierung inzwischen eine Stellungnahme des Bundesrates sowie eine Gegenäußerung der Bundesregierung vor.

Leider wurde eine Reihe von Forderungen der Datenschutzbeauftragten – vgl. hierzu auch 10. TB, 19.1.3 – nicht berücksichtigt.

Der Gesetzentwurf und die Diskussion hierüber werden durch die Bemühungen charakterisiert, die bisherige Praxis zumindest beizubehalten und in wesentlichen Teilbereichen sogar auszudehnen und „lediglich" den formalen Erfordernissen des Volkszählungsurteils zu genügen, ohne das Grundrecht auf informationelle Selbstbestimmung mit Leben zu erfüllen und die schon bisher weitreichenden Übermittlungsbefugnisse zu begrenzen. Wir werden über das Gesetzgebungsverfahren weiter berichten.

19.3 Kontrollzuständigkeit bei den Gerichten

Der im 10. TB (19.2) dargestellte Problemstand besteht im wesentlichen unverändert fort.

Die Bemühungen des Hamburgischen Datenschutzbeauftragten und der Justizbehörde, eine Abgrenzung von Verwaltungsaufgaben – die der Kontrolle des Datenschutzbeauftragten unterliegen – von der originär gerichtlichen Tätigkeit zu erreichen, sind von den Gerichten nicht unterstützt worden. Ursache hierfür ist die offenbar fehlende Bereitschaft der Gerichte, sich dieses Themas anzunehmen – von einer kooperativen Zusammenarbeit zur Lösung des Problems ganz zu schweigen.

So wurde den Gerichten zum Beispiel eine Auflistung der gerichtlichen Tätigkeiten aus einer Reorganisationsstudie übersandt, verbunden mit der Anregung, die Verwaltungstätigkeiten zu kennzeichnen. Trotz mehrerer Mahnungen der Justizbehörde sind die Gerichte auf diese Anregung nicht näher eingegangen, bis auf einen – nicht autorisierten – „Irrläufer", bei dem der Bogen differenziert und mit überwiegend vertretbaren Ergebnissen angekreuzt und postwendend zurückgeschickt worden war.

In einem Einzelfall war schließlich eine Prüfung des gerichtlichen Schuldnerverzeichnisses (19.4) nach intensiven Diskussionen möglich, nachdem mehrfach die angekündigten Prüfungstermine verschoben worden waren, bis die verschiedenen Einwendungen des Amtsgerichts Hamburg gegen die Prüfung ausgeräumt waren.

Der Rechtsausschuß der Bürgerschaft hat am 16. November 1992 im Anschluß an die Beratungen im Unterausschuß Datenschutz als Ersuchen an den Senat empfohlen, bis Ende 1992 die inhaltliche Klärung der Kontrollzuständigkeit des Hamburgischen Datenschutzbeauftragten bei den Gerichten herbeizuführen. Damit wurde in derselben Sache ungewöhnlicherweise ein zweites Mal ein Ersuchen an den Senat – nach dem Ersuchen vom 13./14. März 1991 zum 8. TB – vorgeschlagen.

Mit Nachdruck wiederholen wir außerdem den Vorschlag aus dem 10. TB, in Hamburg § 24 Abs. 2 des Berliner Datenschutzgesetzes zu übernehmen, der lautet:

„Setzen Gerichte zur Erfüllung ihrer gesetzlichen Aufgaben automatische Datenverarbeitungsanlagen ein, so unterliegen unbeschadet der richterlichen Unabhängigkeit die Ordnungsmäßigkeit und Rechtmäßigkeit der Verfahren der Kontrolle des Datenschutzbeauftragten."

19.4 Prüfung des Schuldnerverzeichnisses

Das beim Amtsgericht Hamburg auf einem Abteilungsrechner (Betriebssystem SINIX) geführte Schuldnerverzeichnis wurde datenschutzrechtlich geprüft. In diesem Verzeichnis befinden sich Angaben über ca. 170 000 natürliche und ca. 25 000 juristische Personen, die die Richtigkeit ihres Vermögensverzeichnisses in einer eidesstattlichen Versicherung bekräftigt haben bzw. in Konkurs gefallen sind. Aus diesem Verzeichnis wird voraussetzungslos jedem Auskunft erteilt, ob eine Person in diesem Verzeichnis gespeichert ist oder nicht.

Neben diesem zentralen Schuldnerverzeichnis existieren bei weiteren Amtsgerichten in Hamburg „lokale" Verzeichnisse. Der dortige Datenbestand und dessen Änderungen werden in unregelmäßigen Abständen per Datenträger an das zentrale Schuldnerverzeichnis beim Amtsgericht Hamburg übermittelt. Aus diesem zentralen Schuldnerverzeichnis werden die Änderungen des Datenbestandes einmal wöchentlich an einen Verlag übermittelt.

Bedingt durch die mangelnde Koordination zwischen dem in unregelmäßigen Abständen erfolgenden Abgleich mit den Daten der dezentralen Schuldnerverzeichnisse einerseits und der regelmäßigen Übermittlung an einen Verlag andererseits, kommt es hinsichtlich der Richtigkeit der an den Verlag übermittelten Daten zu Problemen. Die Datenübermittlung an den Verlag, die für Hamburg zentral durch das Amtsgericht Hamburg erfolgt, enthält – strukturbedingt – nicht immer die aktuellen Daten der dezentralen Schuldnerregister.

Die Justizbehörde wurde aufgefordert, Arbeitsabläufe zu entwickeln, um eine tagesaktuelle Übermittlung des hamburgischen Datenbestandes an Dritte sicherzustellen.

Weiterhin wurde bei der Prüfung festgestellt, daß es eine Möglichkeit zur Löschung von Datensätzen gab, die für die Übermittlung an Dritte nicht protokolliert wurde. Außerdem war aufgrund der Speicherung nicht nachzuvollziehen, welcher Mitarbeiter welchen Datensatz eingegeben oder verändert hatte.

19.5 Private und dienstliche PC bei der Staatsanwaltschaft

Im Bereich der Staatsanwaltschaft Hamburg sind insgesamt ca. 60 PC aufgestellt; davon sind ca. 20 privat beschaffte Geräte.

Auf diesen PC findet fast ausschließlich Textverarbeitung (z.B. Anklageschriften, Durchsuchungsbeschlüsse, Strafbefehle usw.) statt; Datenbankanwendungen sind die Ausnahme.

Die Staatswaltschaft hat eine Dienstanweisung erlassen, in der die Nutzungsbedingungen für PC geregelt sind. Die Dienstanweisung geht grundsätzlich von einem Verbot der Benutzung privater PC aus, sieht aber die Möglichkeit einer Genehmigung vor. Diese Genehmigung wird nur erteilt, wenn sich der Eigentümer (Benutzer) verpflichtet, das Gerät wie ein dienstliches behandeln zu lassen. Insbesondere muß sich der Betreffende der Datenschutzkontrolle durch den Hamburgischen Datenschutzbeauftragten unterwerfen. Soweit dienstliche PC beschafft werden, werden bevorzugt privaten Benutzern dienstliche Geräte zur Verfügung gestellt und die Genehmigung zur Nutzung privater PC dann entzogen.

Insgesamt wurden 11 private Geräte sowie 4 dienstliche Geräte einer datenschutzrechtlichen Kontrolle unterzogen. Der Schwerpunkt der Kontrolle lag in den Abteilungen, die mit besonderen Sicherheitsanforderungen arbeiten müssen (Organisierte Kriminalität, Staatsschutz).

Unzulässige Anwendungen wurden nicht festgestellt. Allerdings zeigten sich gravierende Mängel bei der Datensicherheit.

Nur bei drei PC (2 privat/1 dienstlich) der insgesamt 15 überprüften Geräte war ein ausreichender Zugangsschutz gewährleistet. Dabei zeigte sich, daß die beiden privat beschafften PC auf unterschiedliche Weise einen ziemlich effektiven Zugangsschutz realisiert hatten. Bei zwei der dienstlichen PC war zwar eine Sicherheitssoftware installiert; allerdings war das Leistungspotential der Sicherheitssoftware nicht ausgeschöpft worden, so daß doch bei einem Gerät deutliche Schwachstellen erkennbar waren. Bei den Anwendern mit hohem Sicherheitsstandard fanden sich im übrigen ausgesprochen professionelle Anwendungen, die die wirkungsvollen Unterstützungmöglichkeiten eines PC am Einzelarbeitsplatz eines Staatsanwalts exemplarisch deutlich machten.

Alle übrigen PC einschließlich der dienstlich beschafften (!) verfügten noch nicht einmal über die elementarsten Sicherheitsvorkehrungen, wie einen Paßwortschutz. Zwar wird mit der Beschaffung von dienstlichen PC bei der Justizbehörde für den Bereich der Staatsanwaltschaft immer eine – grundsätzlich geeignete – Sicherheitssoft- und -hardware beschafft. Sie wird aber offensichtlich nicht regelmäßig installiert. Wenn sie installiert wird, wird das Sicherheitspotential überwiegend nicht genutzt.

Die Ursache für diese Sicherheitsmängel liegt nach unserem Eindruck weniger in einem mangelnden Problembewußtsein. Auf allen Ebenen war man sich der Bedeutung von Sicherheitsanforderungen mehr oder weniger ausgeprägt bewußt. Dies zeigt sich auch daran, daß die Staatsanwaltschaft einem Staatsanwalt u. a. die Aufgabe zugewiesen hat, die PC und deren Anwender einschließlich der privaten Benutzer zu betreuen. Diese Aufgabe wird auch im Rahmen des Möglichen wahrgenommen. Allerdings ist der Betreuungsaufwand – vor allem hinsichtlich der fachlichen Einsatzmöglichkeiten eines PC –

erheblich, so daß ein Einzelner diese Aufgabe angesichts der Vielzahl der PC nicht leisten kann.

Weiterhin ist berichtenswert, daß bei der vollständigen Begehung eines Gebäudes, in dem im wesentlichen die Staatsanwaltschaft untergebracht ist, immerhin 3 private PC festgestellt wurden, die überhaupt nicht angemeldet waren. In weiteren Fällen stimmten die genehmigten Komponenten nicht (mehr) mit dem tatsächlichen Zustand überein.

Auch wurde in keinem Fall ein vollständig der Dienstanweisung entsprechendes Handbuch mit Protokollierung usw. vorgefunden. Überwiegend war zwar das Handbuch vorhanden, die vorgesehenen Eintragungen waren aber nicht vorgenommen worden.

Eine derartig unzureichende Beachtung datenschutzrechtlicher Anforderungen in sensiblen Bereichen der Staatsanwaltschaft ist nicht vertretbar. Nach unserer Aufforderung hat die Staatsanwaltschaft zugesagt, bis Ende 1992 die aufgetretenen Sicherheitsmängel bei privaten und dienstlichen PC zu beseitigen.

20. Strafvollzug und Postkontrolle

Die im 10. TB (20.2) dargestellten Bedenken gegen die Praxis der Überwachung des Schriftverkehrs sind durch eine Entscheidung des Bundesgerichtshofs weiter erhärtet worden.

Für eine vergleichbare Fallkonstellation betreffend Sichtspione hat der Bundesgerichtshof entschieden, daß eine pauschale, vom Einzelfall abstrahierte Begründung für die Gefahrenprognose und hierauf gestützte Maßnahmen nicht ausreichen. Vielmehr muß bei der Gefahrenprognose konkret auf das Gefährdungspotential des Betreffenden abgestellt werden.

Überträgt man diesen Ansatz der konkreten Gefährdungsprognose auf die Postkontrolle von Strafgefangenen, kommt eine pauschale Kontrolle der Post bloß deshalb, weil ein Betroffener in einer bestimmten Anstalt einsitzt, nicht in Betracht. Von daher ist die Praxis der Kontrolle der gesamten Korrespondenz z. B. in der JVA Fuhlsbüttel ohne Differenzierung nach dem konkreten Gefährdungspotential nach unserer Auffassung unzulässig.

Verschärft wird diese Problematik noch dadurch, daß offenbar selbst die wenigen Ausnahmen von der Postkontrolle, z. B. bei Abgeordnetenpost oder der Post von Datenschutzbeauftragten, nicht immer beachtet werden. Mehrere Eingaben lassen den Schluß zu, daß gegen diese Beschränkungen in der Praxis verstoßen wird. Angesichts der sich wiederholenden Fälle halten wir es nicht mehr für ausreichend, daß die Mitarbeiter nur generell vom Strafvollzugsamt auf die Einhaltung der Bestimmungen über die Postkontrolle hingewiesen werden. Es ist nunmehr geboten, daß im Einzelfall gegen die verantwortlichen Bediensteten Maßnahmen bei Verstößen getroffen werden.

21. Gesundheitswesen

21.1 Verstärkte Automation in den Krankenhäusern

Nicht zuletzt wegen des großen politischen Drucks auf das Gesundheitswesen, Kosten zu sparen, entwickelt sich die elektronische Datenverarbeitung in den Hamburger Krankenhäusern besonders schnell. Wirtschaftlichkeits- und Qualitätsanforderungen sowie die entsprechenden Aufsichts- und Kontrollaufgaben haben den Bedarf an Daten, maschinenlesbaren Speicherungen und elektronischen Datenauswertungen sprunghaft gesteigert. Die gesetzlichen Grundlagen – vor allem das umstrittene neue Gesundheits-Strukturgesetz (siehe 21.2) – sollen dem Rechnung tragen.

Dem Hamburgischen Datenschutzbeauftragten wurden im Berichtszeitraum neben Dienstanweisungen für die Einführung neuer EDV-Verfahren (siehe 21.3) eine ganze Reihe von einzelnen Automationsvorhaben vorgestellt: aus dem Bereich des Landesbetriebs Krankenhäuser (LBK) etwa das Qualitätssicherungsverfahren Geburtshilfe (siehe 21.5.2), das klinische Krebsregister Gynäkologie, das Programm zur Instandhaltungswirtschaft, die Verfahren Pflegedienst im Krankenhaus (PIK) und Pflegedienstunterstützung (PULS). Aus dem Universitätskrankenhaus Eppendorf wurde uns ein System zur automatisierten Verarbeitung von Daten HIV-Infizierter vorgestellt und die Patientenüberwachungsanlage des neuen Operativen Zentrums skizziert. Schließlich wurden wir unterrichtet vom Labordatensystem des Hygienischen Instituts und vom Informations- und Kommunikationssystem ISmed des Medizinischen Dienstes der Krankenversicherungen.

Für den Patientendatenschutz ergeben sich durch diese Entwicklung der beschleunigten und verstärkten Automatisierung Probleme und Gefährdungen:

— Die zunehmende Vernetzung ganzer Krankenhauskomplexe mit Glasfaser- und Kupferkoaxialkabeln birgt gravierende datensicherungstechnische Risiken: So sind sämtliche berechtigen Benutzer – entsprechende Hardware und Software sowie Systemkenntnisse vorausgesetzt – in der Lage, die über das Netz übertragenen Daten jederzeit mitzulesen. Selbst das Anzapfen eines Kabels durch Unbefugte kann kaum verhindert bzw. bemerkt werden.

— Je mehr Anwendungen über Netze abgewickelt werden, desto größer ist die Gefahr, daß auch sensible Daten ohne ausreichende Kontrolle im Einzelfall elektronisch übermittelt und mit anderen verknüpft werden. Die datensicherungstechnischen Probleme des Systemmanagements und der Wartung potenzieren sich, so daß angesichts der neuen Dimensionen datenschutzrechtlicher Herausforderungen und Gefährdungen eine Vernetzung als solche einer besonderen Rechtfertigung bedarf.

— Die auch vom Sozialgesetzbuch geforderte Qualitätssicherung ärztlicher Leistungen wird in den Krankenhäusern zunehmend implementiert. Sie

setzt eine umfangreiche Datenerhebung und -auswertung auch durch Personen voraus, die möglicherweise nicht unmittelbar an der Behandlung der Patienten beteiligt sind. Hier gilt es, so früh und so weitgehend wie möglich eine Anonymisierung der Patientendaten zu erreichen. Bei der externen Qualitätssicherung durch krankenhausfremde Gremien ist dies eine Grundvoraussetzung datenschutzrechtlicher Zulässigkeit (siehe 21.5).

— Durch den Automatisierungsdruck einerseits und die immer stärkere Spezialisierung der Software-Anbieter andererseits werden die anwendenden Krankenhäuser zunehmend abhängig von einzelnen Herstellern und von deren Konditionen. So sehen sich Anwender etwa gezwungen, einer Fernwartung durch den Hersteller zuzustimmen, obwohl ein dadurch möglicher Zugriff auf sensible personenbezogene Daten datenschutzrechtlich nicht nur dann bedenklich ist, wenn der Hersteller seinen Sitz im Ausland hat (siehe 3.3).

— Die Verbreitung der EDV-Sachkenntnis und -Anwendungsbereitschaft auch unter Ärzten hat zur Folge, daß sie – etwa bei Forschungsaufgaben oder verzögerter dienstlicher Beschaffung – private PC im Krankenhaus nutzen wollen. Dies würde jedoch wegen der z. T. sehr einfachen, datenschutzrechtlich unzureichenden Systeme und möglicher Vermischungen mit privater Nutzung zusätzliche Lücken in der Sicherung sensibler Gesundheitsdaten aufreißen.

— Die Beschleunigung der Automatisierung in den Krankenhäusern birgt auch Probleme für die datenschutzrechtliche Kontrolle: Die von § 23 Abs. 4 HmbDSG geforderte „rechtzeitige" Unterrichtung des Datenschutzbeauftragten über Planungen neuer Anwendungen (siehe 1.9) ist ebensowenig gängige Praxis wie die Koordination und datenschutzrechtliche Prüfung der einzelnen Krankenhaus-Projekte durch die Geschäftsführung des Landesbetriebes Krankenhäuser. Die Bemühungen um eine einheitliche Dienstanweisung des LBK gestalten sich schwierig und langwierig, ihre Durchsetzung in allen LBK-Krankenhäusern erscheint nicht selbstverständlich.

— Schließlich schränkt die oft kurzfristig angekündigte Anwendung andernorts entwickelter und angeblich bewährter Standard-Software die Wirkung der Beratung und Aufsicht durch den Datenschutzbeauftragten zumindest faktisch stark ein.

21.2 Gesundheits-Strukturgesetz

Der gesundheitspolitisch stark umstrittene Entwurf eines Gesetzes zur Sicherung und Strukturverbesserung der gesetzlichen Krankenversicherung (Gesundheits-Strukturgesetz 1993) wurde uns – anders als in anderen Bundesländern – erst mit der regelmäßigen Verteilung der Bundesrats-Drucksachen zugeleitet, nicht bereits als Referentenentwurf. Ein Interesse der Behörde für Arbeit, Gesundheit und Soziales an einer datenschutzrechtlichen Stellungnahme wurde erst aufgrund unserer Anfrage signalisiert.

Angesichts der Neuaufnahme von Gesprächen zwischen dem Bundesgesundheitsminister, den Ärzteverbänden, den Krankenkassen und den Fraktionen des Bundestages Mitte September 1992 erschien uns anstelle eines Eingehens auf Details vor allem der Hinweis auf zwei Grundprobleme des Gesetzentwurfs geboten:

— In mehreren Bestimmungen zwingt der Gesetzentwurf zu einer weiteren Automatisierung der Patientendatenverwaltung, weil er eine maschinenlesbare Erfassung, Speicherung und Übermittlung von Leistungs- und Abrechnungsdaten vorsieht. Ohne eine eindeutige Begrenzung der Auswertungsmöglichkeiten besteht die Gefahr, daß Krankenkassen, der Medizinische Dienst oder die Kassenärztlichen Vereinigungen in Zukunft arztbezogene Leistungsprofile oder auch patientenbezogene Gesundheitsprofile erstellen können. Die Gefahr ist um so größer, als nun auch ausdrücklich Diagnosen zu den Leistungsdaten gerechnet werden und der Datenkatalog, den das Krankenhaus an die Krankenkassen zu übermitteln hat, erheblich erweitert wurde.

  Hinzu kommt die Absicht der Krankenkassen, die Krankenversicherungskarte in Form einer Chipkarte einzuführen, deren Verarbeitungskapazität technisch ungleich größer ist, als es der derzeit zur Speicherung vorgesehene Datenumfang erfordert. Hier wird eine Entwicklung eingeleitet, die weitreichende Folgen hat. Es gilt zu verhindern, daß unter dem Vorwand der Kostendämpfung eine Transparenz und Vergleichsmöglichkeit geschaffen wird, die den Bürger als Patienten zum Objekt von Überwachung, Kontrolle und Einflußnahme macht. Hier sind eindeutige Auswertungsschranken zur Sicherung des informationellen Selbstbestimmungsrechts der Patienten nötig.

  Auf unsere Initiative stellte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 1./2. Oktober 1992 in einem Beschluß fest, „daß eine Speicherung auf einer Chip-Karte als elektronische Krankenversicherungskarte auf die gesetzlich festgelegten Grunddaten beschränkt bleiben muß und nicht auf Gesundheitsdaten ausgedehnt werden darf. Eine technische Sicherung dieser Beschränkung ist zu gewährleisten."

— Der Gesetzentwurf verpflichtet die Krankenhäuser dazu, in Zukunft wesentlich mehr Daten an die Krankenkassen zu übermitteln als bisher. Andererseits bleibt es den Krankenkassen- und den Krankenhausverbänden unbenommen, den Umfang der zu übermittelnden Abrechnungsbelege einzuschränken und auf die Angabe einzelner Abrechnungsdaten zu verzichten. Diese gesetzliche Möglichkeit legt die Vermutung nahe, daß eine volle Ausschöpfung des neuen Regel-Katalogs in § 301 SGB V oft nicht notwendig ist. Datenschutzrechtlich sollte dem dadurch Rechnung getragen werden, daß die Übermittlungsverpflichtung auf die für die Krankenkassen „erforderlichen Daten" eingeschränkt wird.

Die Datenschutzbeauftragten wenden sich nicht gegen eine kosteneinsparende Strukturreform der Krankenkassen; wir fordern jedoch eine normenklare gesetzliche Regelung zum Schutz des informationellen Selbstbestimmungsrechts, welche die automatisierte Datenverarbeitung für den Patienten transparent macht und auf das unerläßliche Maß beschränkt.

21.3 Dienstanweisungen zum Datenschutz in den Krankenhäusern

21.3.1 Überblick

Im 10. TB hatten wir die neue Dienstanweisung des Universitäts-Krankenhauses Eppendorf (UKE) „über die Führung und Herausgabe von Krankenunterlagen und Röntgenbildern" vorgestellt und gleichzeitig für den Bereich der Behörde für Arbeit, Gesundheit und Soziales (BAGS) entsprechende Regelungen angemahnt (21.1.1: Landesbetrieb Krankenhäuser (LBK); 21.2: Bernhard-Nocht-Institut). Anders als das UKE trennt die BAGS die Bereiche „IuK-Anwendungen" und „Patientenakten"; außerdem werden für die Krankenhäuser des LBK einerseits und die Stellen des Amtes für Gesundheits- und Veterinärwesen der BAGS andererseits jeweils eigene Vorschriften geschaffen. Seit dem 10. TB ist folgendes geschehen:

— Im April 1992 erhielten wir den „Entwurf einer Dienstanweisung Datenschutz", die im IuK-Bereich des LBK Datenschutz und Datensicherheit gewährleisten soll (siehe 21.3.2).

— In der Sitzung des Unterausschusses Datenschutz der Bürgerschaft am 1. September 1992 wurde uns ein vorläufiger Entwurf einer „Dienstvorschrift Datenschutz und Datensicherung beim Einsatz von DV-Systemen in der BAGS" übergeben.

— Für das Bernhard-Nocht-Institut kündigte die BAGS in derselben Sitzung einen Dienstanweisungsentwurf an. Er ging uns am 8. Oktober 1992 zu und entspricht in Aufbau und Einzelregelungen der Dienstanweisung des UKE vom 15. Juli 1991.

— Hinsichtlich der Dienstanweisung des LBK „über die Führung und Herausgabe von Krankenakten und Röntgenbildern" vom 6. Januar 1987 erklärte die BAGS bei derselben Gelegenheit, es bestehe kein Aktualisierungsbedürfnis. Dem widerspricht ein Protokoll der Geschäftsführung des LBK über ein Gespräch mit den Datenschutzbeauftragten der Krankenhäuser am 3. September 1992, in dem die „Überarbeitung der entsprechenden Dienstsanweisung von 1987" als Teil der neuen Dienstanweisung Datenschutz angekündigt wird. Der Aktualisierungsbedarf ergibt sich in der Tat daraus, daß seit 1987 einerseits das Gesundheitsreformgesetz im neuen SGB V eine ganze Reihe von Bestimmungen über den Datenaustausch zwischen Krankenhäusern und Krankenkassen und andererseits das Hamburgische Krankenhausgesetz vom 17. April 1991 detaillierte Regelungen zum Patientendatenschutz enthalten.

Selbst wenn die genannte Dienstanweisung den neuen gesetzlichen Bestimmungen nur selten widerspricht, erscheint ihre strukturelle und begriffliche Anpassung und auch eine Ergänzung z.B. zur Zweckbindung, zur Zugriffsberechtigung und zum Datenumfang bei Übermittlungen geboten.

— Von den aufgeführten Dienstanweisungen nicht abgedeckt sind Regelungen über die Führung von Patientenakten im Bereich der BAGS außerhalb des Bernhard-Nocht-Instituts (BNI). Dies trifft etwa auf das Hygienische Institut und die Umweltmedizinische Beratungsstelle zu. Hier bietet sich möglicherweise ein Rückgriff auf die BNI-Bestimmungen oder die aktualisierte LBK-Dienstanweisung von 1987 an.

Insgesamt erscheint die verwirrende Vielzahl unterschiedlich strukturierter Dienstanweisungen zum Datenschutz innerhalb der BAGS nicht optimal. Mit jedem einzelnen Entwurf mußten wir uns gesondert auseinandersetzen. Faktisch übernahmen wir dabei die eigentlich der BAGS obliegende notwendige Koordinierungsfunktion und Abstimmung der Regelungen untereinander.

21.3.2 Dienstanweisung Datenschutz für IuK-Anwendungen im Landesbetrieb Krankenhäuser

Intensiv geführt wurde die Auseinandersetzung über die Dienstanweisung Datenschutz des Landesbetriebs Krankenhäuser (LBK) für den IuK-Bereich:

Der Entwurf der Dienstanweisung zum Datenschutz nimmt in seinen technischen Vorschriften erfreulicherweise detailliert Bezug auf die im IuK-Konzept des LBK definierten Standards wie den Einsatz von

— UNIX als Mehrplatzsystem und File-Server,

— NFS als Netzwerksoftware,

— TCP/IP als Transport- und Netzwerk-Protokoll,

— Ethernet als Netzwerkbasis.

Obwohl durch den Entwurf datensicherungstechnische Defizite der genannten Produkte durch standardisierte Vorgaben behoben werden, bestehen in einigen Punkten noch Bedenken. Zwar lassen sich einige der Defizite von NFS, TCP/IP und Ethernet durch administrative Maßnahmen und Einsatz der NFS-Version 4.0 reduzieren, dennoch sind – angesichts der Sensibilität der Daten – weitere technisch-organisatorische Maßnahmen erforderlich.

Die Notwendigkeit derartiger Maßnahmen wird jedoch vom LBK nicht geteilt. Vielmehr wird – diese Grundauffassung wird im Entwurf besonders deutlich – Datensicherheit nur soweit umzusetzen versucht, wie es durch verbreitete Standardprodukte möglich ist. Weder sind seinerzeit bei der Systementscheidung für NFS und TCP/IP datensicherheitstechnische Alternativen ausreichend erörtert worden, noch werden Strategien entwickelt, möglicherweise

durch Eigenprogrammierung Defizite ausgleichen zu können. Zudem wird Datensicherheit permanent vor dem Hintergrund wirtschaftlicher Überlegungen diskutiert. Grundlegender Dissens zwischen LBK und uns besteht in den Punkten Speicherung von hochsensiblen Daten trotz fehlender Datenverschlüsselung im Netz, Verschlüsselung von Datenträgern, Protokollierung von Systemverwaltertätigkeiten und Fernwartung:

1. Unsere Hauptbedenken richten sich gegen den Grundgedanken des Entwurfs, auf eine Verschlüsselung der über das Netz übertragenen Daten zu verzichten und statt dessen die Sicherheitsrisiken durch Verplomben sämtlicher Hardwareeinrichtungen einzugrenzen. Dabei wäre angesichts der Ethernet-Schwäche, daß einerseits jeder im Netz angeschlossene Rechner den gesamten Datenverkehr auf der Leitung mitverfolgen kann, andererseits ein Anschluß netzfremder Rechner weitgehend unbemerkt bleibt, die Verschlüsselung der über das Netz übertragenen Daten die einzige sichere Lösung.

   Da die Ethernet-Schwäche jedoch nicht kurzfristig durch veränderte TCP/IP-Versionen behoben werden kann, stellt sich die Frage, wie in der Zwischenzeit verfahren werden soll. Während der LBK das Problem durch Verplombung als generell beseitigt ansieht, halten wir es für datenschutzrechtlich erforderlich, zumindest auf die Verwaltung sehr sensibler Daten im Netz (beispielsweise personenbezogene HIV-Daten) zu verzichten und derartige Daten nur auf unvernetzten Systemen zu verwalten.

2. Aufgrund der Sensibilität der Daten ist es nicht nur erforderlich, die über das Netz übertragenen Daten zu verschlüsseln, sondern auch die Daten auf sämtlichen Datenträgern, insbesondere auf externen Sicherungsbändern, zu chiffrieren (vgl. 9. TB, 3.2.2.7).

   Der LBK hat gegen diesen Vorschlag erhebliche Bedenken: Zum einen wird zusätzlicher Aufwand bei der Verwaltung der Chiffrier-Schlüssel befürchtet, zum anderen würden dem LBK zusätzliche Software-Kosten entstehen. Die Datensicherheit ist nach Meinung des LBK durch Verschluß der Sicherungsbänder in Sicherheitsschränken ausreichend garantiert.

   Demgegenüber halten wir angesichts der Tatsache, daß im gesamten Bereich des LBK aufgrund von Vertretungsregelungen ca. 30 Personen Zugriff zu sämtlichen Schrankschlüsseln haben müssen, einen weiteren Schutz der Datenträger für notwendig. Falls die Verschlüsselung als Hintergrundprozeß abgewickelt wird, wäre die Verwaltung der Chiffrier-Schlüssel sogar weniger aufwendig als der Umgang mit traditionellen Schrankschlüssein.

3. Während wir die Protokollierung von Systemverwalteraktivitäten für notwendig erachten (vgl. 9. TB, 3.2.2.6 und 3.3.1), ist der LBK der Meinung, durch Protokollierung keine weitere Datensicherheit zu erreichen und daher hierauf verzichten zu können. Gleiches gilt für das von uns geforderte Vier-Augen-Prinzip. Nach Ansicht des LBK ist es für den Systemverwalter jeder-

zeit möglich, die durch Protokollierung und Vier-Augen-Prinzip erreichte zusätzliche Sicherheit durch selbst programmierte Systemprozeduren auszuschalten.

Hierbei stellt sich jedoch die Frage, inwieweit ein derartiges Vorgehen Spuren hinterläßt und ob nicht durch entsprechende Sicherheitsmaßnahmen ein Löschen der Spuren verhindert werden kann. Zwar ist es beispielsweise durch Verschlüsselung der Protokolldatei nicht möglich, ihre Löschung zu verhindern, dennoch kann ihre Manipulation jederzeit erkannt werden.

4. Der Stellenwert der Fernwartung und deren datenschutzrechtliche Brisanz zeigt sich auch im Bereich des LBK (siehe 3.3). Während wir es u.a. für erforderlich halten, daß dem Wartungstechniker keine personenbezogenen Daten offenbart werden, sieht der LBK keinen Regelungsbedarf zu diesem Thema. Nach Aussage des LBK sind gerade in den Anwendungsbereichen Radiologie und Labor kaum Produkte erhältlich, die traditionell gewartet werden können.

Obwohl im Jahr 1992 – auch wegen ungeklärter Fragen im Mitbestimmungsverfahren – nicht mehr mit einem Inkrafttreten der Dienstanweisung gerechnet werden kann, beabsichtigt der LBK dennoch, in nächster Zeit Datenbankanwendungen wie etwa die Qualitätsssicherung in der Chirurgie (vgl. 21.5.1) im Echtbetrieb einzusetzen. Wir gehen unabhängig von einer Dienstanweisung davon aus, daß die erforderlichen Sicherungsmaßnahmen vom Landesbetrieb in ausreichendem Maße sichergestellt werden. Wir werden dies möglicherweise auch kurzfristig nach Einführung der Verfahren vor Ort überprüfen.

21.4 Gesundheitsberichterstattung

Im letzten Jahr hatten wir berichtet über den Beitrag der schulärztlichen Dokumentation zur Gesundheitsberichterstattung Hamburgs (vgl. 10. TB, 21.4). In diesem Jahr hatten wir Stellung zu nehmen zu einer wissenschaftlichen Studie im Rahmen der schulärztlichen Untersuchung über die „Melanomwirksamkeit ultravioletter Strahlung" und zu einem Informationssystem mit kinderärztlichen Beobachtungspraxen. Dabei ging es vor allem um eine ausreichende Aufklärung der Eltern und um die Anonymisierung von Patientendaten vor ihrer Weitergabe an die Behörde für Arbeit, Gesundheit und Soziales.

In diesem Zusammenhang sind wir auch noch einmal der Frage nachgegangen, wie die in der Gesundheitsberichterstattung veröffentlichten Statistiken und Übersichten zustande kommen. Bekannt wurden uns die Studie „Gesundheitliche Beeinträchtigung von Kindern im Umweltzusammenhang", die Analyse „Epidemiologie kindlicher Leukämien in Hamburg" und der Gesundheitsbericht „Stadt-Diagnose". Außer den Daten des Hamburgischen Krebsregisters, das ebenfalls in der Abteilung „Gesundheitsindikatorensysteme" geführt wird, werden die Daten für die Gesundheitsberichterstattung grundsätzlich in aggregierter tabellarischer Form, also nicht personenbezogen, übermittelt. Vom Statistischen Landesamt kommen zwar auch Einzeldatensätze, sie sind jedoch durch Weglassen der identifizierenden Merkmale faktisch anonymisiert.

Datenschutzrechtlich bestehen gegen eine derartige anonymisierte Gesundheitsberichterstattung keine Bedenken. Bei den einzelnen Untersuchungen, aus denen dann für die Berichterstattung die Daten entnommen werden, ist allerdings weiterhin jeweils zu prüfen, ob die oft sehr detaillierten Fragen und Antworten wirklich erforderlich sind.

21.5 Qualitätssicherung im Krankenhaus

Ziel und datenschutzrechtliche Probleme der Qualitätssicherung im Krankenhaus wurden im 9. TB (4.16.2.3) angesprochen. Inzwischen hat die in § 137 SGB V festgeschriebene Qualitätssicherungspflicht sowohl im Hamburgischen Krankenhausgesetz (HmbKHG) als auch in einem Vertrag zwischen der Hamburgischen Krankenhausgesellschaft und den Krankenkassenverbänden nach § 112 SGB V ihren Niederschlag gefunden.

§ 10 Abs. 1 Nr. 7 HmbKHG bestimmt: „In dem Krankenhaus dürfen Patientendaten genutzt werden, soweit dies erforderlich ist für die Qualitätskontrolle der Leistungen des Krankenhauses." Im Katalog der Zwecke, die eine personenbezogene Übermittlung von Patientendaten an Dritte legitimieren (§ 11 HmbHKG), fehlt die Qualitätssicherung jedoch. Eine externe Qualitätssicherung mit personenbezogenen Daten ist damit unzulässig.

21.5.1 Projekt Qualitätssicherung in der Chirurgie (Quasic)

Besondere Probleme bereitete uns im Jahr 1991 das Projekt Qualitätssicherung in der Chirurgie, das 1985 als Modellversuch der Ärztekammer geplant und seit 1991 im AK Barmbek als Pilotprojekt Quasic ausprobiert wird. Bereits im Jahr 1991 hatten wir schwerwiegende Bedenken vor allem gegen den Test des Programms mit Echtdaten, gegen den Datenzugriff auch lange nach der Entlassung des Patienten, gegen den Echtdatenzugriff durch (studentische) Systementwickler und gegen verschiedene Mängel der Datensicherheit geltend gemacht. Wir forderten umgehende Abhilfe oder eine Einstellung des weiteren Echtdaten-Betriebs.

Die Rechts- und die EDV-Abteilung des Landesbetriebs Krankenhäuser (LBK) teilten unsere datenschutzrechtlichen Bedenken und kündigten eine vollständige Rekonstruktion des Projekts nach den LBK-Standards an. Dennoch konnten sie sich dem Drängen der Chirurgischen Abteilung nach einer vorläufigen Fortsetzung von Quasic nicht entziehen und baten um Duldung des Verfahrens für eine Übergangszeit bis zur Einführung des neuen Programms.

Aufgrund unserer Mitteilung, daß wir eine formelle Beanstandung des Verfahrens erwägen, kündigte der Vorsitzende der LBK-Geschäftsführung folgende Maßnahmen zur Mängelbeseitigung an: Die Systemverwaltung wird auf die IuK-Abteilung des AK Barmbek übertragen, um eine Trennung zwischen Anwendung und Systemmanagement zu gewährleisten. Ein Zugriff auf Patientendaten darf nur während der Behandlung, danach nur mit Einwilligung des

Patienten erfolgen. Im 3. Quartal 1992 soll Quasic durch das allen Datenschutzanforderungen gerecht werdende neue LBK-Programm ersetzt werden. Trotz verbleibender Bedenken habe ich diese Übergangslösung als vertretbar akzeptiert.

21.5.2 Projekt Qualitätssicherung Geburtshilfe

Aus der geburtshilflich-gynäkologischen Abteilung des AK Barmbek erhielten wir Ende letzten Jahres ein erstes Konzept für ein EDV-unterstütztes Qualitätssicherungsverfahren. Im März 1992 wurden die datenschutzrechtlichen Problempunkte gesondert erläutert. In unserer Stellungnahme gingen wir davon aus, daß letztlich nur die Fachmediziner beurteilen können, welche Daten im einzelnen zur krankenhausinternen Qualitätskontrolle erforderlich sind.

Besonderen Wert legten wir jedoch auf die Beschränkung des Datenzugriffs auf die Personen, die sie „zur rechtmäßigen Erfüllung der ihnen obliegenden Aufgaben" (§ 10 Abs. 2 HmbKHG) wirklich brauchen. Ferner betonten wir die Notwendigkeit, die identifizierenden Merkmale oder „Stammdaten" (z.B. Name und Anschrift der Patientin) getrennt zu speichern und nach Abfassung des Arztbriefes zu löschen bzw. zu sperren. Für statistische Auswertungen und Forschungen sowie zur externen Qualitätssicherung stehen dann ausschließlich anonyme Daten zur Verfügung. Das Konzept des AK Barmbek sieht vor, daß ein Zugriff auf die gesperrten Stammdaten und die medizinischen Daten zusammen „der Einwilligung der Patientin bei Wiederaufnahme oder einem Notfall vorbehalten" ist.

Das Projekt Qualitätssicherung Geburtshilfe geht aus von der bundesweit durchgeführten sog. Perinatologischen Basiserhebung, einem derzeit noch manuell auszufüllenden Formular, das die wichtigsten Diagnosen, Risiken, Maßnahmen und Vorgänge im Zusammenhang mit Geburten standardisiert. Eine Durchschrift des Basis-Erhebungsbogens wird ohne Namen und Adresse der Patientin an die kassenärztliche Vereinigung (KV) übermittelt, die es zu Vergleichszwecken auswertet. Hamburger Geburtshilfe-Krankenhäuser nehmen an diesem Verfahren seit 1982 teil. Die Angaben auf dem Formular wurden 1985 auch mit dem Hamburgischen Datenschutzbeauftragten abgestimmt.

Um so erstaunter waren wir, als uns aufgrund einer Routine-Nachfrage ein Formular zugesandt wurde, das gegenüber dem abgestimmten nicht nur weitere medizinische Daten enthält, sondern auch die Angabe „Berufstätigkeit als Belastung empfunden" und „HIV+". Das letztgenannte Datum ist für die Frauen- und ggf. auch für die Kinderklinik sicher unverzichtbar. Wir halten es jedoch aus folgenden Gründen nicht für vertretbar, dieses Datum auch der KV zu übermitteln:

Durch die Angaben des Geburtskrankenhauses, der Geburtsnummer und anderer Daten der Schwangeren auch auf dem Durchschlag für die KV ist mit einem gewissen Aufwand die Identität der Betroffenen trotz des Verzichts auf

den Namen und die Adresse durchaus zu ermitteln. Je sensibler die übermittelten Daten sind, desto höhere Anforderungen müssen an die Anonymisierung gestellt werden.

Auf unsere Nachfrage hat die zuständige Arbeitsgemeinschaft Peri-/Neonatal-Erhebung der KV das Formular geändert: Die Frage „Berufstätigkeit als Belastung empfunden" wurde herausgenommen und die Angabe „HIV +" wird nun nicht mehr auf den Erfassungsbogen für die KV durchgeschrieben.

Die erreichten Verbesserungen haben wir den Datenschutzbeauftragten der anderen Bundesländer mitgeteilt.

21.5.3 Externe Qualitätssicherung

Bereits am 1. März 1991 hatten die Hamburgische Krankenhausgesellschaft und die Landesverbände der Krankenkassen einen Vertrag über die externe Qualitätssicherung in der stationären Versorgung abgeschlossen. § 9 Abs. 1 Satz 1 bestimmt: „Die Erfassung, Speicherung, Auswertung und Überprüfung der erhobenenen Daten für die vereinbarten Qualitätssicherungsmaßnahmen sind mit dem Hamburgischen Datenschutzbeauftragten abzustimmen." In einem Symposium im November 1991 in der Ärztekammer tauschten Mediziner verschiedener Fachrichtungen ihre Erfahrungen aus und erörterten Qualitätssicherungskonzepte. Forderungen des Datenschutzes wurden eher als Störfaktoren angesprochen, aber nicht vertieft.

Auf unsere Anfrage vom April und Mai 1992 erhielten wir schließlich Ende Juni die Mitteilung, daß die Projektgeschäftsstelle für die Externe Qualitätssicherung zum 1. April 1992 ihre Arbeit aufgenommen habe und zunächst die Projekte Chirurgie und Anästhesie, nicht aber das Projekt Geburtshilfe behandeln werde. Sowie von den Fachgremien Konzepte erarbeitet seien, werde der Hamburgische Datenschutzbeauftragte sofort unterrichtet. Im übrigen versicherte uns die Geschäftsstelle, daß zum Zwecke einer externen Qualitätssicherung in keinem Falle Patientendaten aus den Krankenhäusern an die Projektgeschäftsstelle übermittelt würden.

Angesichts der Erfahrungen mit der perinatologischen Basiserhebung werden wir vor allem der Frage einer ausreichenden Anonymisierung, also der Abtrennung identifizierender Merkmale nachzugehen haben.

21.6 Übermittlungen vom Krankenhaus an Krankenkassen

Im 10. TB (6.9) hatten wir über die Gemeinsame Datenverarbeitungsstelle der Krankenversicherung in Hamburg (GDKV) berichtet. Über sie sollte die Patientendaten-Übermittlung der Krankenhäuser an die Krankenkassen erfolgen. Nach intensiven Gesprächen mit den Krankenkassen konnte über das Datensicherungskonzept der GDKV Einvernehmen erzielt und der Krankenhausgesellschaft eine entsprechende Erklärung abgegeben werden.

Nicht entgegenkommen konnten wir allerdings dem Wunsch der Krankenkassen, für eine Übergangszeit einen erweiterten Datenkatalog, insbesondere mit Krankenhaus-Verweilzeiten und den medizinischen Begründungen hierfür, zu verarbeiten. Wir vertraten vielmehr den Standpunkt, daß eine Änderung des zugelassenen Datenkataloges dem Gesetzgeber überlassen bleiben müsse. Im übrigen waren auch die Krankenhäuser nicht bereit, über den in § 301 SGB V festgelegten Datenkatalog hinauszugehen.

Im August 1992 teilte uns die Arbeitsgemeinschaft der Krankenkassenverbände in Hamburg schließlich mit, daß die GDKV weiterhin auf eine personenbezogene Datenspeicherung verzichte, „bis eine Modifizierung des § 301 SGB V erfolgt ist".

Gegenstand von Eingaben war ferner die Frage, ob die Krankenkassen und der Medinzinische Dienst von den Krankenhäusern Entlassungsberichte anfordern dürfen. Diese gehen in ihren Angaben weit über den Datenkatalog in § 301 SGB V hinaus. Hinsichtlich der Entlassung werden dort nur der Tag, der Grund der Entlassung und die Entlassungsdiagnose genannt, nicht aber z.B. einzelne Befunde und Therapiemaßnahmen, die oft Inhalt von Entlassungsberichten sind. Eine regelmäßige Übermittlung von Entlasssungsberichten ohne die Einwilligung der betroffenen Patienten kommt deswegen nicht in Betracht. Das gilt auch für Anforderungen des Medizinischen Dienstes.

Anders ist es bei der Überprüfung von Einzelfällen. Hier sehen die §§ 100 SGB X und 276 Abs. 4 SGB V eine Übermittlung der zur Aufgabenerfüllung erforderlichen Daten vor. Der Medizinische Dienst darf „die Räume der Krankenhäuser . . . betreten, um dort die Krankenunterlagen einzusehen . . .". Dazu zählen auch die Entlasssungsberichte.

Anders als der Medizinische Dienst können wir dem Gesetzeswortlaut jedoch nicht entnehmen, daß die Krankenhäuser verpflichtet wären, dem Medizinischen Dienst auf Anforderung die Patientenunterlagen auch zu übersenden. Mehrere Krankenhäuser hatten sich gegen eine solche vom Medizinischen Dienst behauptete Pflicht gewehrt. Aus datenschutzrechtlicher Sicht haben wir allerdings keine Bedenken gegen eine – freiwillige – Übersendung der Akten, wenn die Transportsicherheit gewährleistet ist. Für das informationelle Selbstbestimmungsrecht ist es nicht entscheidend, wo die Daten zur Kenntnis genommen werden.

21.7 Mitteilungen der Krankenhäuser an Sozialämter

Beamte haben einen Anspruch auf staatliche Beihilfe zu ihren Krankheitskosten. Die sehr hohen Kosten einer Krankenhausbehandlung können sie in der Regel erst nach Erhalt der Beihilfe begleichen. Da aber die Beihilfe meist erst nach Ablauf der Zahlungsfrist des Krankenhauses ausgezahlt wird, müssen die Betroffenen zunächst eine Stundung der Krankenhauskosten beantragen.

Durch eine Eingabe wurden wir darauf aufmerksam, daß das Allgemeine Krankenhaus Harburg den Eingang solcher Stundungsanträge stets der für den Beamten örtlich zuständigen Sozialdienststelle mitgeteilt hat. Diese Mitteilung umfaßte auch die jeweilige Diagnose des Krankenhauses.

Mit der Zentrale des Landesbetriebes Krankenhäuser (LBK) und der Behörde für Arbeit, Gesundheit und Soziales (BAGS) erzielten wir schnell Einigkeit über die Rechtswidrigkeit dieser Verfahrensweise. Daraufhin hat das AK Harburg sie dann eingestellt.

Um sicherzustellen, daß nicht andere Krankenhäuser dieses Verfahren fortsetzen, hat der LBK auf unsere Bitte auch seine weiteren Krankenhäuser entsprechend unterrichtet.

21.8 Neue Berufsordnung für Hamburger Ärzte

Im Mai 1992 sandte uns die Behörde für Arbeit, Gesundheit und Soziales (BAGS) die neue „Berufsordnung der Hamburger Ärztinnen und Ärzte" zur Stellungnahme. Die Hamburger Ärztekammer hatte sie der Behörde bereits Anfang 1989 zur Genehmigung vorgelegt.

Unsere umfangreiche Stellungnahme enthielt folgende Hauptpunkte:

— Auch nach der neuen Berufsordnung kann der Arzt die Behandlung ablehnen, wenn er der Überzeugung ist, daß das notwendige Vertrauensverhältnis zum Patienten fehlt. Dies darf jedoch nicht dazu führen, daß Patienten, die sich auf ihre Datenschutzrechte berufen und z.B. nicht in die Datenweitergabe an Verrechnungsstellen oder Praxisnachfolger einwilligen, nicht mehr behandelt werden.

— An mehreren Stellen wird die geltende Berufsordnung dahingehend abgeändert, daß eine bisher geforderte ausdrückliche Einwilligung durch eine mutmaßliche Einwilligung (nach Auffassung des Arztes) bzw. das Einwilligungserfordernis überhaupt durch die bloße Kenntnis ersetzt wird. Zweimal soll überdies die bisherige Formulierung „soweit der Patient nicht widerspricht" ersatzlos entfallen. Diese datenschutzrechtlichen Verschlechterungen zu Lasten des informationellen Selbstbestimmungsrechts des Patienten werden nicht näher begründet. Wir haben sie abgelehnt.

— Geregelt werden sollten nach unserer Auffassung die datenschutzrechtlichen Probleme einer Gemeinschaftspraxis. Für die Patienten muß die Möglichkeit bestehen, sich nur einem einzelnen Mitglied der Gemeinschaftspraxis anzuvertrauen und andere Mitglieder von der Einsichtnahme in die Patientenunterlagen bzw. in die Patientendaten in der EDV-Anlage auszuschließen. Gegebenenfalls bedarf es einer ausdrücklichen Schweigepflichtentbindungserklärung bzw. der – schriftlichen – Einwilligung.

— Schließlich schlugen wir vor, die neuere Rechtsprechung zur Patientendatenübermittlung bei Praxisverkauf und bei der Abrechnung durch Verrechnungsstellen zu berücksichtigen (siehe 21.10 und 21.11).

Um gerade bei den sensiblen Gesundheitsdaten datenschutzrechtlich einen Fortschritt zu erreichen, drängen wir nicht nur auf eine Umsetzung unserer Kritik und Anregungen, sondern auch auf eine möglichst zügige Genehmigung der geänderten Berufsordnung.

21.9 Mitgliedsbeiträge der Ärzte zur Ärztekammer

Alle Hamburger Ärzte sind Mitglied der „Ärztekammer Hamburg". Zur Erfüllung ihrer Aufgaben haben die Kammermitglieder einen Beitrag zu leisten, der sich nach dem Einkommen aus ärztlicher Tätigkeit richtet. „Die Beitragsfestsetzung erfolgt im Wege der Selbstveranlagung", § 4 der Beitragsordnung.

Für die Beitragsveranlagung 1992 ergänzte die Kammerversammlung die Beitragsordnung um folgende Regelung: „Der Selbsteinstufung muß eine Kopie des entsprechenden Auszuges des Einkommensteuerbescheides des Bezugsjahrs der Beitragsbemessung oder eine schriftliche Bestätigung des Steuerberaters über die Richtigkeit der Selbstveranlagung beigelegt werden." Fehlen diese Anlagen, „so wird der Beitrag nach Schätzung durch die Ärztekammer Hamburg mit mindestens DM 5000,— festgesetzt."

Hiergegen gingen bei uns 10 Eingaben von Ärzten ein, die darin einen Verstoß gegen das Steuergeheimnis und den Datenschutz sahen. Dem konnten wir uns im Ergebnis nicht anschließen:

Zwar enthält die Satzungsermächtigung für die Beitragsordnung der Ärtzekammer (§ 15 Abs. 4 Hamburgisches Ärztegesetz) keine ausdrückliche Ermächtigung, von den Kammermitgliedern auch Auszüge des Einkommenssteuerbescheides zu verlangen. Satzungsermächtigungen geben – anders als Verordnungsermächtigungen – die Regelung eines Bereichs jedoch in die Selbstverwaltung der Betroffenen.

Die Kammerversammlung selbst, also das Selbstverwaltungsorgan der Betroffenen, hielt die Neuregelung für geboten: In den letzten Jahren hatten umfangreiche Stichproben-Prüfungen, die auch schon bisher zulässig waren, ein hohes Maß an Unehrlichkeit bei der Selbsteinstufung offenbart. Vor diesem Hintergrund mußten wir bestätigen, daß die Datenerhebung aus dem Steuerbescheid bzw. der Bestätigung durch den Steuerberater zur Erfüllung der Kammeraufgaben erforderlich ist, wie es § 12 HmbDSG voraussetzt.

Da die Daten beim Betroffenen selbst und nicht beim Finanzamt abgefordert werden, war auch kein Verstoß gegen das Steuergeheimnis (§ 30 Abgabenordnung) ersichtlich. Wir haben die Petenten darüber hinaus an das Urteil des Bundesverfassungsgerichts zur Besteuerung der Zinseinkünfte erinnert, welches eine Sicherstellung faktischer Steuergerechtigkeit ausdrücklich forderte.

21.10 Schutz von Patientendaten bei Auflösung und Verkauf von Arztpraxen

Seit längerer Zeit erörtern wir mit der Ärztekammer Hamburg das Problem, was mit den Patientenunterlagen geschieht, wenn eine Arztpraxis aufgelöst oder an

einen Nachfolger verkauft wird. Wir hatten unsere Auffassung deutlich gemacht, daß die Schweigepflicht des Arztes auch gegenüber seinem Nachfolger besteht und dann verletzt wird, wenn diesem die Patientenkartei ohne eine Einwilligung des Patienten übergeben wird.

Mit Urteil vom 11. Dezember 1991 traf der Bundesgerichthof (BGH) hierzu folgende Entscheidung: „Eine Bestimmung in einem Vertrag über die Veräußerung einer Arztpraxis, die den Veräußerer auch ohne Einwilligung der betroffenen Patienten verpflichtet, die Patienten- und Beratungskartei zu übergeben, verletzt das informationelle Selbstbestimmungsrecht der Patienten und die ärztliche Schweigepflicht (Art.2 Abs.1 GG, § 203 StGB) . . .". Seine bisherige Rechtsprechung, nach der die Schweigepflichtverletzung durch eine mutmaßliche Einwilligung des Patienten gerechtfertigt sei, gibt der BGH ausdrücklich auf. Er stellt vielmehr fest, daß Hinweise auf einen möglichen Arztwechsel in den Wartezimmern sowie Anzeigen in der örtlichen Presse dem Einwilligungserfordernis nicht genügen. Nur dadurch, daß er sich von dem Praxis-Nachfolger behandeln läßt, erklärt der Patient zugleich seine Zustimmung dazu, daß der neue Arzt die Patientenunterlagen einsieht. Bis zur Behandlung durch den Nachfolger, bei früheren – „abgewanderten" – Patienten bis zur Anforderung durch den behandelnden Arzt muß die Patientenkartei grundsätzlich beim früheren Praxis-Inhaber verbleiben.

Bei einer Praxis-Auflösung hat der Arzt bzw. dessen Erbe die Patientenunterlagen „in gehörige Obhut" (§ 11 Abs. 4 Berufsordnung) – etwa bei der Ärztekammer – zu geben.

Für die Praxis ergeben sich aus diesem datenschutzrechtlich begrüßenswerten Urteil des BGH nicht unerhebliche Probleme: Wie kann die schnelle Verfügbarkeit der Patientenakte z.B. sichergestellt werden, wenn der Praxis-Vorgänger ins Ausland verzogen oder verstorben ist, ohne daß der Nachfolger hierüber unterrichtet wurde?

Die Ärztekammer Hamburg folgt hierzu einer Empfehlung der Rechtsberaterkonferenz von Bundesärztekammer und Kassenärztlicher Bundesvereinigung, die folgendes vorsieht: Soweit eine Einwilligung des Patienten nicht vorliegt, soll der Praxisübernehmer die Unterlagen, die im Eigentum des Praxisübergebers verbleiben, für den Praxisübergeber und getrennt von den Unterlagen des laufenden Patientenstamms in den übernommenen Praxisräumen aufbewahren. Unter Vereinbarung einer Vertragsstrafe im Falle der Verletzung soll sich der Übernehmer dem Übergeber gegenüber zudem verpflichten, nur mit Einverständnis des Patienten auf die jeweilige Unterlage zuzugreifen.

Wir halten diese Regelung nicht für ausreichend, um dem BGH-Urteil gerecht zu werden: Unstrittig ist, daß eine Verletzung der ärztlichen Schweigepflicht, d.h. ein „Offenbaren", bereits dann vorliegt, wenn die geschützten Unterlagen dem Praxis-Nachfolger in der Weise „übergeben" werden, daß er den tatsächlichen Gewahrsam über sie ohne eine Einflußnahme Dritter ausüben kann

(nicht: darf). Das schuldrechtliche Vertragsstrafeversprechen kann an dem Gewahrsam nichts ändern. Die Ausübung der „Sachherrschaft" über die Unterlagen ist im übrigen auch gerade Voraussetzung für die Erfüllung des „Verwahrungsvertrages" zwischen Praxis-Vorgänger und -Nachfolger.

Soll am Verbleib der Patientenkartei in der verkauften Praxis festgehalten werden, so muß die Zugriffsmöglichkeit des übernehmenden Arztes nicht nur normativ, sondern tatsächlich von der Einwilligung des Patienten abhängig gemacht werden. Eine klare technische Lösung ist nicht erkennbar. Als Kompromiß käme aber ein 2-Schlüssel-Verfahren in Betracht: Aufgrund einer schriftlichen Anforderung durch einen Arzt oder aufgrund einer unmittelbar mündlichen Einwilligung eines Patienten in der Praxis „entsperren" der Praxisübernehmer und ein weiterer Praxismitarbeiter zusammen das mit zwei verschiedenen Schlössern gesicherte Behältnis der „Alt-Patientenkartei". Der Arzt (Praxisübernehmer) besitzt selbst nur einen Schlüssel. Eine solche gegenseitige Abhängigkeit – möglicherweise über Hierarchiegrenzen hinweg – ist im Datenschutzrecht nicht ungewöhnlich: Die unabhängige Stellung des betrieblichen Datenschutzbeauftragten und das 4-Augen-Prinzip in der Datensicherung können eine ähnliche Wirkung haben.

Wird diese sicherlich auch nicht ganz problemlose Lösung verworfen, müssen die Unterlagen beim Praxisübergeber verbleiben. Wie bei jedem vom Patienten veranlaßten Arztwechsel sind die individuellen Unterlagen dann bei Bedarf von dem behandelnden Arzt, ggf. auch vom Praxisübernehmer, beim Praxisübergeber anzufordern. Der Praxisübergeber bzw. sein Erbe hat dafür Sorge zu tragen, daß die Unterlagen verfügbar sind.

Angesichts dieser Rechtsauffassung haben wir einer Veröffentlichung der genannten Empfehlungen der Rechtsberaterkonferenz durch die Hamburger Ärztekammer nur mit dem Hinweis zugestimmt, daß diese Regelung lediglich als eine vorläufige Handreichung verstanden werden kann, bis eine Regelung gefunden ist, die allen bislang geäußerten Bedenken gerecht wird.

Aus unserer Sicht ist es nun Aufgabe der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, zusammen mit der Bundesärztekammer eine dem BGH-Urteil gerecht werdende und dennoch praxisgerechte Lösung zu erarbeiten. Wir haben hierzu einen Anstoß gegeben.

Ein besonderes Problem in diesem Zusammenhang ist der Patientendatenschutz bei der Auflösung von Gemeinschaftspraxen. War die – ggf. elektronische – Patientendatenverarbeitung allen Mitgliedern der Gemeinschaftspraxis frei zugänglich und trennen sich dann die Mitglieder, um jeweils eigene Praxen aufzubauen, so fragt sich, wer Zugriff auf die „gemeinsamen" Daten haben darf. Wir haben die Auffassung vertreten, daß für eine kurze Übergangszeit von einem Quartal jedes ehemalige Gemeinschaftspraxen-Mitglied die gleiche Möglichkeit haben müßte, die Patienten, welche ihm in die neue Praxis folgen, ohne Zeitverlust anhand der früher erstellten Unterlagen zu behandeln. Dies bedeutet, daß der gesamte Patientendatenbestand zunächst vervielfältigt und verteilt werden muß. Nach einem Quartal sind die Daten derjenigen Patienten, die dem Arzt nicht gefolgt sind, bei diesem zu löschen und nur von dem Arzt weiterzuführen, zu dem der Patient nach der Auflösung der Gemeinschaftspraxis geht.

Das weitere Problem, wer die Dokumentationspflicht für jene Patienten erfüllt, die bei keinem der früheren Gemeinschaftspraxismitglieder bleiben, konnte zunächst offen bleiben, weil der entsprechende Fall eine Spezialpraxis betraf, für die sich kaum eine Alternative anbietet.

Deutlich ist jedoch, daß ein gleichberechtigter Zugriff aller Mitglieder einer Gemeinschaftspraxis auf automatisiert verarbeitete Patientendaten – selbst mit einer entsprechenden Einwilligung – erhebliche Probleme bei einer Auflösung der Praxis verursacht. Deswegen haben wir vorgeschlagen, dies schon in der Berufsordnung (siehe 21.8) anzusprechen und von Anfang an eine datenschutzgerechte Auseinandersetzungsregelung zu treffen.

21.11 Übermittlung von Patientendaten an Verrechnungsstellen

Aufgrund mehrerer Eingaben hatten wir mit der Ärztkammer und mit der Zahnärztekammer Hamburg folgende Frage zu klären: Darf ein niedergelassener Arzt die Behandlung eines Patienten davon abhängig machen, daß dieser in die Übermittlung von Abrechnungsdaten an eine private Verrechnungsstelle einwilligt?

Hintergrund dieses Problems ist ein Urteil des Bundesgerichtshofs (BGH) vom 10. Juli 1991. Danach stellt die Abtretung von ärztlichen Honorarforderungen und die Übermittlung von Patientendaten an gewerbliche Verrechnungsstellen ohne eine entsprechende Einwilligung des Patienten eine Verletzung der ärztlichen Schweigepflicht dar. Den Urteilsgründen ist zu entnehmen, daß diese Bewertung auch berufsständische Verrechnungsstellen der Ärzte trifft.

Das Gericht fordert: „Im Hinblick auf die ärztliche Schweigepflicht obliegt es nämlich dem Arzt, die Zustimmung des Patienten in eindeutiger und unmißverständlicher Weise einzuholen. Es ist grundsätzlich nicht Sache des Patienten, der Weitergabe seiner Daten zu widersprechen . . .".

Einige Ärzte sind daraufhin dazu übergegangen, die Patienten vor der Behandlung eine umfangreiche vorgedruckte Einwilligungserklärung unterschreiben zu lassen. Diese bezieht sich nicht nur auf die Weitergabe der Abrechnungsdaten an ein namentlich bestimmtes Rechenzentrum, sondern auch auf die „Weiterabtretung der jeweiligen Forderung an die kreditgebende Bank" durch das Rechenzentrum.

Ferner enthalten die uns bekannten Formulare auch Einwilligungen in die Weitergabe der Patientenunterlagen durch den Arzt „im Falle einer Veräußerung seiner Praxis" (siehe 21.10), „im Falle des Ausscheidens eines oder mehrerer (Zahn-)Ärzte aus einer Gemeinschaftspraxis/Praxisgemeinschaft", „im Falle

der Aufnahme eines anderen (Zahn-)Arztes in eine Gemeinschaftspraxis" sowie „Im Falle des Ablebens". Dem Patienten wird eine Widerrufsfrist von einer Woche eingeräumt, danach wird die unterzeichnete Einwilligungserklärung als „unwiderruflich" bezeichnet.

Eine Petentin berichtete uns davon, daß sich ihr Arzt vor einer Unterzeichnung dieser Erklärung geweigert hätte, die Behandlung aufzunehmen.

Da wir gegen das beschriebene Einwilligungsformular erhebliche datenschutzrechtliche Bedenken haben, baten wir die Zahnärztekammer und die Ärztekammer um eine Stellungnahme. Wir machten deutlich, daß zum einen die Beschränkung der Widerruflichkeit einer Einwilligungserklärung dem Datenschutzrecht widerspricht und daß zum anderen rein vorsorgliche Einwilligungen („im Falle . . .") mangels Bestimmtheit unwirksam sind. Soweit die Einwilligung in die Datenweitergabe an eine namentlich genannte Verrechnungsstelle abgefordert wird, darf nach unserer Auffassung der Arzt die Behandlung nicht von der Unterzeichnung abhängig machen. Es war das Ziel des genannten BGH-Urteils, das informationelle Selbstbestimmungsrecht des Patienten zu stärken und nicht über den faktischen Zwang einer Einwilligungserklärung vor der Behandlung einzuschränken.

Sowohl die Zahnärztekammer als auch die Ärztekammer teilten unsere rechtlichen Bedenken. Zu der konkreten Eingabe schrieb die Zahnärztekammer: „Auch wir halten das Vorgehen des Zahnarztes für berufsunwürdig und würden die Angelegenheit daher gerne unter Aspekten unserer Berufsordnung aufgreifen." Die Ärztekammer verwies allerdings auf die Möglichkeit, daß eine Arztpraxis sich aus innerbetrieblichen Gründen gezwungen sehen kann, die Abrechnung der Privatpatienten ausschließlich über eine Verrechnungsstelle abzuwickeln. In diesen Fällen müsse die Ablehnung einer Behandlung bei Verweigerung der Einwilligung möglich sein.

Beide Kammern wollten bisher unserem Vorschlag nicht folgen, durch eine Kammer-Veröffentlichung von der Nutzung der beschriebenen Einwilligungsformulare abzuraten und auf die datenschutzrechtlichen Bedenken hinzuweisen. Sowie wir von einer weiteren Verbreitung der Formulare Kenntnis erhalten, werden wir uns um einen öffentlichen Hinweis an alle Ärzte und Patienten bemühen. Dabei können die von der Ärztekammer genannten innerbetrieblichen Gründe für einen faktischen Einwilligungszwang nach unserer Ansicht keine Ausnahme rechtfertigen.

Einzelne Probleme des Datenschutzes im nicht-öffentlichen Bereich

22. Werbewirtschaft

22.1 Neue Regelung für unadressierte Postwurfsendung

Bis zu der Änderung der Ausführungsbestimmungen zu § 59 Abs. 2 Nr. 1 PostO am 28. Februar 1991 wurden Postwurfsendungen auch zugestellt, wenn die Briefkästen der Empfänger mit dem Hinweis versehen waren, keine Werbung erhalten zu wollen. Die Postzusteller durften davon nur absehen, sofern die Verweigerung der Annahme für die jeweils einzelne Sendung ausgesprochen worden war.

Erfreulicherweise hat sich diese Praxis nunmehr geändert. Allgemein gehaltene Hinweise auf Hausbriefkästen wie „Keine Werbung", sind jetzt als Annahmeverweigerung für Postwurfsendungen vom Zusteller zu beachten.

Eine entsprechende Regelung hat die Deutsche Bundespost Postdienst in die seit dem 1. Juli 1991 geltenden Allgemeinen Geschäftsbedingungen für den Briefdienst Inland aufgenommen, die die zuvor geltende Postordnung ersetzen:

„Bei der – anschriftlosen und im allgemeinen ohne Umschlag versandten – Sendungsart Wurfsendung wird ein am Hausbriefkasten angebrachter Klebezettel „Keine Wurfsendung" beachtet und gilt als Annahmeverweigerung. Allgemein gehaltene Erklärungen auf Klebezettel, z. B. „Keine Werbung", werden als Annahmeverweigerung lediglich für die Sendungsart Wurfsendung angesehen."

22.2 Interessentenwerbung durch Umfrage

Aufgrund einer Eingabe erhielten wir davon Kenntnis, daß eine Umweltschutzorganisation die angeschriebenen Personen aufforderte, weitere evtl. Interessenten für die Arbeit der Organisation mit Adressen zu benennen. Den neuen Interessenten wurde dann Informationsmaterial mit einem Begleitschreiben zugesandt, in dem die Betroffenen von der Speicherung ihrer Daten und ihrem Widerspruchsrecht unterrichtet wurden.

Das Bundesdatenschutzgesetz verbietet derartige Umfragen nicht. Nach § 28 Abs. 1 Satz 2 BDSG müssen Daten nach Treu und Glauben und auf rechtmäßige Weise erhoben werden. Eine Datenerhebung durch eine freiwillig zu beantwortende Umfrage verstößt nicht gegen diese Vorschrift.

Die Speicherung der Daten der Interessenten ist gemäß § 28 Abs. 1 Satz 1 Nr. 2 BDSG auch zulässig, solange die Betroffenen keinen Widerspruch eingelegt haben. Das ideelle oder finanzielle Interesse der Umweltschutzorganisation an der Speicherung von potentiellen Kundendaten ist als berechtigtes Interesse anzusehen. Ein schutzwürdiges Interesse der Betroffenen an dem Ausschluß der

Speicherung kann nicht generell angenommen werden. Da die Betroffenen bei der Zusendung von Informationsmaterial über das ihnen nach § 28 Abs. 3 BDSG zustehende Widerspruchsrecht aufgeklärt und gemäß § 33 BDSG von der Speicherung benachrichtigt werden, bestehen insoweit keine rechtlichen Bedenken.

Mit dem Arbeitskreis Deutscher Marktforschungsinstitute e. V., der sich in dieser Angelegenheit ebenfalls an uns gewandt hatte, konnte allerdings kein Konsens über die datenschutzrechtliche Bewertung der Umfrage erzielt werden. Nach Ansicht des Vereins sind derartige Umfragen unzulässig. Er befürchtet, daß künftig alle Unternehmen, Vereine usw. Interessenten ohne deren Einverständnis mit Umfragen ermitteln, deren Daten speichern und ungefragt Werbematerial übersenden. Unserer Ansicht nach ist diese Form der Werbung jedoch unter den oben dargestellten Voraussetzungen nicht zu beanstanden.

23. Schufa

23.1 Anfrageberechtigung bei telefonischer Anfrage

Im 10. TB (vgl. dort 24.) hatten wir auf Mißbrauchsfälle bei telefonischer Auskunftserteilung durch die Schufa hingewiesen. Vor Auskunftserteilung verlangt die Schufa von der anfragenden Stelle deren Schufa-Kennummer sowie ein Paßwort. Um Mißbrauchsmöglichkeiten bei telefonischer Auskunftserteilung künftig besser zu vermeiden, verlangt die Schufa nun von ihren Vertragspartnern ein häufiger wechselndes Paßwort. Das Paßwort wird in Abständen von drei Monaten bis einem Jahr gewechselt. Ein großer Vertragspartner in Hamburg wechselt das Paßwort sogar monatlich.

Mit der Schufa wurde zudem eine quantitative Verbesserung der Stichprobenverfahren, die die Schufa zur Prüfung des berechtigten Interesses durchführt, erörtert. Unter den Aufsichtsbehörden besteht Einigkeit, daß die Zahl der monatlichen Stichproben ein Promille erreichen sollte. § 29 Abs. 2 Satz 3 BDSG fordert die Aufzeichnung der Gründe für das Vorliegen eines berechtigten Interesses und der Art und Weise ihrer glaubhaften Darlegung im Einzelfall.

Die Schufa ist der Ansicht, daß die angestrebte Quote längst erreicht sei, da 1,5 % aller Auskünfte Selbstauskünfte seien. In diesen Fällen überprüfe der Betroffene selbst die Richtigkeit seines Datenbestandes und die Frage, ob Anfragen der letzten 12 Monate berechtigt waren. Zudem würden 70 % aller Anfragen durch nachträgliche Einmeldungen von entsprechenden Vertragsabschlüssen bestätigt, und so werde dem Erfordernis zur Darlegung des berechtigten Interesses hinreichend Rechnung getragen. Weitere Überprüfungen der Datenbestände der Schufa würden bei divergierenden Angaben sowohl von den Vertragspartnern als auch den Betroffenen selbst vorgenommen. Eine Erhöhung der Stichprobenkontrolle zur Verhinderung von Mißbrauchsfällen sei daher nicht notwendig.

Die Auffassung der Schufa können wir nicht teilen. Durch die in § 29 Abs. 2 BDSG enthaltene Protokollierungspflicht soll Zwang ausgeübt werden, daß die übermittelnde Stelle im Einzelfall tatsächlich prüft, ob ein berechtigtes Interesse gegeben ist. Die Praxis der Schufa, Auskunft bei Ankreuzen von Anfragegründen auf einem Formular oder bei telefonischer Mitteilung eines verschlüsselten Anfragemerkmals zu geben, ist nur dann mit dem BDSG vereinbar, wenn die Schufa als übermittelnde Stelle das berechtigte Interesse auch stichprobenweise selbst überprüft. Eine Überprüfung durch die Betroffenen oder mittelbar durch Nachmeldungen der Vertragspartner erfüllt nicht die gesetzlichen Anforderungen. Wir werden daher weiterhin mit den anderen Aufsichtsbehörden auf eine Erhöhung der Stichproben hinwirken.

23.2 Auskunft aufgrund mutmaßlicher Einwilligung

Im 9. TB (5.2.1.2) hatten wir kritisiert, daß die Schufa einem Vertragspartner auch in einem Fall Auskünfte gab, in dem ein Girokonto auf Guthabenbasis eingerichtet wurde, der Kunde die Schufa-Klausel nicht unterzeichnet hatte und sein Konto dann ungenehmigt überzog. Die Schufa hat uns dazu mitgeteilt, daß es sich dabei um einen Ausnahmefall handelte, dessen Sachlage sich erst nach Auskunftserteilung herausgestellt hatte. Die Kreditinstitute holen nur dann Auskünfte ein, wenn der Kunde die Schufa-Klausel unterzeichnet hat. Dementsprechend erteilt die Schufa bei Kreditanfragen durch Kreditinstitute nur bei Unterzeichnung der Klausel Auskunft.

23.3 Auslandsvertragsmodell

Das im 9. TB (vgl. dort 5.2.1.1.) dargestellte Vertragsmodell der Schufa für die Datenübermittlung in das Ausland hat nach Auskunft der Schufa in der Praxis bisher keine Relevanz. Ein grenzüberschreitender Datenverkehr habe bei der Schufa bisher – bis auf einen Fall in Österreich (siehe 8. TB, 4.1) – nicht stattgefunden.

24. Private bundesweite Schuldnerverzeichnisse

24.1 Rechtslage

Die Frage nach der Zulässigkeit privater bundesweiter Schuldnerverzeichnisse ist weiterhin ungeklärt. Der bereits im 9. TB kritisierte Gesetzentwurf der Bundesregierung (vgl. 4.14.4.4 und 5.6) ist auch in der vergangenen Legislaturperiode weder verabschiedet noch abgeändert worden.

Für die Verbreitung von Informationen aus den Schuldnerverzeichnissen ist nach wie vor keine ausreichende Rechtsgrundlage vorhanden. § 915 ZPO in der derzeitigen Fassung enthält keine Regelung der Zulässigkeit privater Schuldnerverzeichnisse. Die zu § 915 Abs. 4 Satz 3 ZPO vom Bundesminister der Justiz erlassene „Allgemeine Vorschrift zur Erteilung und Entnahme von Abschriften oder Auszügen aus den Schuldnerverzeichnissen" reicht als Rechtsgrundlage für die Verbreitung von Informationen nicht aus, da sie den

Anforderungen des Bundesverfassungsgerichts zum informationellen Selbstbestimmungsrecht nicht entspricht (vgl. 9. TB, 5.6.1).

24.2 Kreditschutz-Vereinigung (KSV)

Ungeachtet der aus unserer Sicht rechtlich unzulässigen privaten zentralen Schuldnerverzeichnisse bieten zunehmend mehr Unternehmen Auskünfte aus einem bundesweiten Register an. Seit Frühjahr 1991 verfügt die Kreditschutz-Vereinigung, die im Besitz der Bundes-Schufa ist, über die kompletten Daten der Schuldnerverzeichnisse aller deutschen Amtsgerichte. Der Sitz der Gesellschaft ist in Wiesbaden. Die KSV strebt an, als Anschlußpartner die Gruppen zu gewinnen, die von der Schufa nicht oder nur eingeschränkt bedient werden können, wie Inkassounternehmen, Versicherungsgesellschaften, Wohnungsvermieter, Einzel- und Großhandel, Gewerbe- und Produktionsbetriebe.

Abgesehen von der Rechtsgrundlage wirft der Auskunfteibetrieb der KSV eine Reihe von datenschutzrechtlichen Fragen auf. Zu nennen sind vor allem die Vermeidung von Identitätsverwechslungen aufgrund fehlender Geburtsdaten in den Schuldnerverzeichnissen und der Nachweis eines berechtigten Interesses für die Auskunft. Wir haben vorgeschlagen, die Frage der Zulässigkeit des Auskunfteibetriebes und die damit zusammenhängenden datenschutzrechtlichen Probleme mit allen Aufsichtsbehörden der Länder zu erörtern.

25. Versicherungswirtschaft

Die Lösung von Fragen im Bereich der zentralen Warn- und Hinweissysteme (vgl. zuletzt 10. TB, 25.3, 25.4) und die Entwicklung weiterer datenschutzrechtlich unbedenklicher Schweigepflicht-Entbindungsklauseln in Schadensfällen (vgl. zuletzt 10. TB, 25.7) wurden weiter vorangebracht.

Außerdem hat sich ein neuer Schwerpunkt der Tätigkeit der Datenschutzaufsichtsbehörde auf dem Gebiet der Versicherungswirtschaft ergeben. Zunehmend kooperieren die Unternehmen zum Beispiel mit Banken und Bausparkassen. In diesem Zusammenhang werden insbesondere auch personenbezogene Daten weitergegeben. Das Augenmerk ist daher künftig besonders auf eine datenschutzrechtlich unbedenkliche Ausgestaltung dieser sog. Allfinanz-Konzepte (siehe auch 25.3) zu richten.

25.1 Automationsentwicklung

Der Verband der Sachversicherer hatte zunächst erklärt, das zentrale Warn- und Hinweissystem in diesem Bereich müsse aus internen Gründen in Form eines Match-Code-Verfahrens neben dem Einsatz des phonetischen Strukturcode-Verfahrens beibehalten werden. Nunmehr wurde jedoch die Einstellung des Match-Code-Verfahrens beschlossen. Damit zeichnet sich die vollständige Vereinheitlichung aller zentralen Warn- und Hinweissysteme in der Versicherungswirtschaft ab. Diese Entwicklung ist aus datenschutzrechtlicher Sicht begrüßenswert (siehe zu den Verfahren 8. TB, 4.2.1.1).

Die Ausgestaltung des derzeitigen Match-Code-Verfahrens bei der zentralen Registrierstelle Rechtsschutz (vgl. 7. TB, 5.4.1.2) macht es praktisch unmöglich, den vorhandenen Bestand direkt auf das phonetische Strukturcode-Verfahren umzustellen. Dies ergibt sich aus der fehlenden Ermittlungsmöglichkeit der vollständigen personenbezogenen Daten infolge der Verkürzung des Datensatzes durch den Match-Code. Daher wird zunächst mit den Neumeldungen beim HUK-Verband eine Strukturcode-Datei aufgebaut, die bis zur Vernichtung aller Daten der Match-Code-Datei nach Ablauf der Löschungsfrist von 5 Jahren nur sicher aufbewahrt, jedoch nicht genutzt wird. Die Hinnahme einer derartigen zeitlichen Verzögerung war im Interesse einer künftigen sicheren und einheitlichen Verfahrensweise unumgänglich.

Die Einführung des Strukturcode-Verfahrens für das Meldeverfahren der Kfz-Versicherer ist für November 1992 vorgesehen.

25.2 Zentrale Registrierstelle Rechtsschutz

Entgegen der Ankündigung im 10. TB (vgl. dort 25.4) hat das Bundesaufsichtsamt für das Versicherungswesen die zunächst vorgelegte Neufassung des § 19 Abs. 2 der Allgemeinen Bedingungen für die Rechtsschutz-Versicherung (ARB) nicht genehmigt. Nach diesem Entwurf sollte die Kündigungsmöglichkeit für den Versicherungsnehmer und die Versicherung erst bestehen, wenn die Leistungspflicht für mindestens drei Versicherungsfälle in 12 Monaten vorliegt. Statt dessen wurde eine Neufassung genehmigt, die lediglich die vom Bundesgerichtshof in seinem Urteil vom 27. März 1991 (vgl. 10. TB, 25.4) beanstandete Ungleichbehandlung von Versicherung und Versicherungsnehmer ausräumt. Danach kann jetzt neben dem Versicherer auch der Versicherungsnehmer nach mindestens zwei Schadensfällen innerhalb von 12 Monaten kündigen. Eine Einschränkung des Rechts zur außerordentlichen Kündigung seitens des Versicherers ist damit unterblieben.

Die Bemühungen, die bestehende Datei auf eine rechtlich einwandfreie Grundlage zu stellen, ohne § 19 Abs. 2 ARB zur Beurteilung heranzuziehen, haben zu folgendem Formulierungsvorschlag in dem Merkblatt für die Versicherungskunden geführt:

„Zentrale Hinweissysteme der Fachverbände

Rechtsschutzversicherer

— außerordentliche und ordentliche Vertragskündigungen des Versicherers jeweils nach mindestens zwei Versicherungsfällen innerhalb von 12 Monaten

— ordentliche Kündigung des Versicherers nach mindestens 3 Versicherungsfällen innerhalb von 36 Monaten,

— ordentliche Kündigung des Versicherers bei konkreten Anhaltspunkten für Versicherungsmißbrauch."

Die Voraussetzungen für eine Eintragung in diese Warndatei wären damit vertretbar geregelt und für die Versicherungskunden klar beschrieben. Ob sich

dieser Vorschlag durchsetzen wird, bleibt abzuwarten. Das Bundesaufsichtsamt für das Versicherungswesen hat sich kritisch über die Möglichkeit der Einmeldung in die Datei bei konkreten Anhaltspunkten für Versicherungsmißbrauch geäußert.

Unabhängig davon ist jedoch darauf hinzuweisen, daß jedem Versicherungsnehmer bei Abschluß eines Vertrages eine Einwilligungserklärung zur Unterzeichnung vorgelegt wird. Sie gilt nur, wenn er die Möglichkeit hatte, in zumutbarer Weise vom Inhalt des vom Versicherer bereitgehaltenen Merkblattes zur Datenverarbeitung Kenntnis zu nehmen. Um umfassend über den Sinn und die Voraussetzungen zur Einmeldung in die zentralen Hinweissysteme der Fachverbände informiert zu sein, sollte jeder Versicherungsnehmer vor Abschluß eines Vertrages von dieser Möglichkeit Gebrauch machen.

Auf Betreiben der Aufsichtsbehörden hat sich der HUK-Verband zumindest zu einer Information in den „Altfällen" bereit erklärt. Den von einer Kündigung nach der alten – unwirksamen – Vorschrift des § 19 Abs. 2 ARB Betroffenen, die an die Zentrale Registrierstelle Rechtsschutz gemeldet wurden und sich über die weitere Speicherung beschweren, sollen die zugrunde liegenden Gesichtspunkte umfassend erläutert werden.

25.3 Allfinanz-Konzepte

Durch ein Schreiben des Bundesaufsichtsamtes für das Versicherungswesen wurden wir als Aufsichtsbehörde auf eine dort zur Genehmigung vorgelegte Einwilligungsklausel eines Versicherungsunternehmens aufmerksam. Darin war eine außerordentlich weitgehende, vom Versicherungsnehmer bei Vertragsabschluß zu unterzeichnende Einwilligung in Datenübermittlungen niedergelegt.

Die dem Bundesaufsichtsamt für das Versicherungswesen vorgelegte Erklärung war als Bestandteil der zwischen den Aufsichtsbehörden der Länder, dem Bundesaufsichtsamt für das Versicherungswesen und der Versicherungswirtschaft abgestimmten Einwilligungsklausel (vgl. zuletzt 7. TB, 5.4.2) geplant. Bei der Festlegung dieses Textes sind die Beteiligten von einer Verarbeitung der personenbezogenen Daten ausschließlich zur Durchführung der Versicherungsverträge bzw. zur Risikobeurteilung bei Vertragsschluß ausgegangen.

Der nunmehr vorgelegten Einwilligungsklausel – die aus nachstehenden Gründen bisher nicht gebilligt wurde – liegt die zunehmende Zusammenarbeit unterschiedlicher Unternehmen, wie etwa Versicherungen, Banken und Bausparkassen zugrunde. Im Rahmen von sog. Allfinanz-Konzepten sollen die mit Vertragsbeziehungen in Zusammenhang stehenden Erkenntnisse über Personen genutzt werden, um gezielte Kundenwerbung für andere an der Unternehmensgruppe beteiligte Branchen zu ermöglichen. Zu diesem Zweck wird beispielsweise in der Versicherungswirtschaft beabsichtigt, von dem Kunden bei Abschluß eines Versicherungsvertrages eine Einwilligung in die Weitergabe seiner personenbezogenen Daten an andere Branchen zu erhalten. Die personenbezogenen Daten beschränken sich dabei nicht etwa auf Angaben von

Namen und Adressen, sondern beinhalten darüber hinaus genaue Auskünfte über Vertragsinhalte, Auszahlungen von Lebensversicherungen, Vertragstreue u.ä.

Die Absicht, sensible Daten nun auch an Vermittler sowie an weitere Branchen zu übermitteln, bedeutet jedoch für den Versicherungsnehmer die Gefahr, daß Dritte Kenntnis von vertragsinternen Vorgängen erlangen. Seitens der Aufsichtsbehörden wird bei der Beurteilung der Zulässigkeit von Datenübermittlungen über die Grenzen des einzelnen Unternehmens hinaus nicht verkannt, daß es einerseits ein legitimes Anliegen ist, die über einen Versicherungsnehmer gewonnenen Erkenntnisse zur Erstellung gezielter Angebote anderer Branchen zu nutzen. Zugleich kann auch auf Seiten des Kunden durchaus Interesse an solcher Beratung bestehen. Dabei ist jedoch zu berücksichtigen, daß derartige Übermittlungen nach den Vorschriften des Bundesdatenschutzgesetzes nur zulässig sind, soweit der Betroffene gemäß § 4 Abs. 2 BDSG eingewilligt hat. Eine rechtswirksame Einwilligung setzt zumindest voraus, daß der Erklärende sich der Sachlage bewußt ist, d. h. er müßte darüber informiert sein, welchen Unternehmen welche Daten zu welchen Zwecken übermittelt werden sollen. Dies wird bei der vorgesehenen Erklärung in keiner Weise deutlich erkennbar.

Darüber hinaus bleibt der Versicherungsnehmer auch weitgehend darüber im Unklaren, daß er die Möglichkeit hat, die Passage folgenlos zu streichen. Vielmehr wird lediglich auf das vom Versicherer bereitgehaltene Merkblatt – das nicht jedem Kunden automatisch ausgehändigt wird – hingewiesen. Darin allerdings soll nach dem Willen des Versicherers die für den übrigen Vertrag folgenlose Streichungsmöglichkeit verdeutlicht werden.

Die Aufsichtsbehörden haben daher gefordert, daß eine hinreichend konkrete und differenzierte Formulierung der Einwilligungserklärung, die dem Betroffenen erkennbar macht, an wen welche Daten zu welchen Zwecken übermittelt werden, und die Möglichkeit zur folgenlosen Streichung in den Text selbst aufgenommen wird.

Seitens der Versicherungswirtschaft wurde die Zusage gegeben, ihre Vorstellungen zur Lösung der datenschutzrechtlichen Problematik einschließlich von Formulierungsvorschlägen den Aufsichtsbehörden zu übersenden.

25.4 Schweigepflicht-Entbindungsklauseln

Nachdem zwischen den Datenschutzaufsichtsbehörden und der Versicherungswirtschaft Einvernehmen über den Text der Schweigepflicht-Entbindungsklausel im Schadensfall in der Allgemeinen Haftpflicht-Versicherung hergestellt worden war (vgl. 10. TB, 25.7.1), konnten nunmehr die Verhandlungen über eine einheitliche Klausel bei der Reise-Rücktrittskosten-Versicherung im Schadensfall (vgl. 25.4.1) fortgeführt werden.

Darüber hinaus wurden Gespräche über den Umgang mit Altverträgen in der Lebens-, Unfall- und Krankenversicherung (vgl. 25.4.3), zur Information betroffener Stellen über neugefaßte Schweigepflicht-Entbindungserklärungen (vgl.

25.4.4) sowie über die Fassung dieser Klausel im Schadensfall in der Kfz-Haftpflichtversicherung (vgl. 25.4.2) geführt.

25.4.1 Reise-Rücktrittskosten-Versicherung

Der Deutsche Transportversicherer-Verband hat – wie angekündigt (vgl. 10. TB, 25.7.2) – folgenden Entwurf für eine Schweigepflicht-Entbindungserklärung im Schadensfall vorgelegt:

„Mir ist bekannt, daß der Versicherer zur Beurteilung seiner Leistungspflicht Angaben überprüft, die ich zur Begründung meines Anspruchs mache. Zu diesem Zweck befreie ich die Angehörigen von Heilberufen oder Krankenanstalten, die in den von mir vorgelegten Unterlagen genannt sind oder die an der Heilbehandlung beteiligt waren, von ihrer Schweigepflicht –, und zwar auch über meinen Tod hinaus.

Hinsichtlich einer bereits früher (längstens 1 Jahr vor Eintritt des Schadensfalls, bei unregelmäßig über längere Zeit auftretenden z. B. psychischen oder epileptischen Krankheiten 2 Jahre) von einem Arzt, Zahnarzt oder sonstigem Angehörigen eines Heilberufes durchgeführten Behandlung gilt diese Entbindung von der Schweigepflicht jedoch nur, soweit diese Angaben zur Überprüfung der Leistungspflicht erforderlich sind.

Diese Erklärung gebe ich für die von mir gesetzlich vertretene(n) Person(en) . . . – Name(n) der versicherten Person(en) – . . . ab, die die Bedeutung dieser Erklärung nicht selbst beurteilen kann(können)."

Dieser Text enthält die bisher geforderte Konkretisierung für unregelmäßig über längere Zeit auftretende Krankheiten.

25.4.2 Kfz-Haftpflicht-Versicherung

Von den Kfz-Haftpflicht-Versicherern werden zur Zeit unterschiedliche Schweigepflicht-Entbindungserklärungen im Schadensfall verwendet. Auf unsere Anregung hat der HUK-Verband einen Vorschlag für eine einheitliche Klausel für die Autohaftpflicht-Versicherung vorgelegt.

Dieser Text weicht allerdings im Wortlaut von dem der Allgemeinen Haftpflicht-Versicherung ab, so daß die Aufsichtsbehörden im Sinne einer Vereinheitlichung der Klauseln vorgeschlagen haben, die Formulierung anzugleichen. Da die zu beurteilenden Sachverhalte keinen abweichenden Text erforderlich machen, hat der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) zugesagt, nach Rücksprache mit den entsprechenden Gremien zu dem Vorschlag Stellung zu nehmen. Die Autoversicherer haben sich mittlerweile dafür ausgesprochen, den Text, der in der Allgemeinen Haftpflicht-Versicherung entwickelt wurde, wörtlich zu übernehmen.

25.4.3 Altverträge in der Lebens-, Unfall- und Krankenversicherung

Im Zusammenhang mit der Neufassung der Schweigepflicht-Entbindungsklauseln in Schadensfällen stellte sich die Frage nach der Praxis der Versicherungswirtschaft in den Fällen, in denen Versicherungsnehmer in der Lebens-, Unfall- und Krankenversicherung bereits bei Vertragsabschluß die alte – datenschutzrechtlich bedenkliche, mittlerweile neu gefaßte – Klausel unterzeichnet hatten. Seitens der Versicherungswirtschaft wurde zugesichert, daß interne Arbeitsanweisungen die Orientierung nur noch an den Zulässigkeitsvoraussetzungen der neuen Klausel sicherstellen. Wünschenswert wäre darüber hinaus jedoch eine Information des Versicherungsnehmers über diese Tatsache im Versicherungsfall, z. B. durch Übersendung der neuesten Fassung mit den übrigen Unterlagen.

25.4.4 Information der Ärzte über Neufassungen

Angesichts der nahezu vollständig abgeschlossenen Neufassungen der Schweigepflicht-Entbindungserklärungen wurde seitens der Aufsichtsbehörden das Problem der Information der davon Betroffenen aufgeworfen. Ein Arzt oder sonstiger Angehöriger eines Heilberufes macht sich wegen Verletzung von Privatgeheimnissen nach § 203 Strafgesetzbuch strafbar, wenn er unbefugt ein fremdes Geheimnis offenbart, das ihm in dieser beruflichen Eigenschaft bekannt geworden ist. Die Befugnis zur Bekanntgabe gesundheitlicher Befunde gegenüber Versicherungen kann sich aus einer vom Versicherungsnehmer unterzeichneten Schweigepflicht-Entbindungserklärung ergeben.

Die Befreiung von der ärztlichen Schweigepflicht hat jedoch lediglich den in dieser Klausel jeweils festgelegten Umfang. Ein Arzt macht sich daher auch dann strafbar, wenn er mehr bekanntgibt, als er nach dem erklärten Willen des Patienten offenbaren darf. Diese Grenze kann er nach Auffassung der Aufsichtsbehörde jedoch nur dann einhalten, wenn er über den Inhalt der unterzeichneten Schweigepflicht-Entbindungserklärung informiert ist.

Praxis der Versicherungen ist zum Teil, bei Gesundheitsabfragen den mit der Heilbehandlung befaßten Personen lediglich mitzuteilen, daß eine derartige Erklärung unterzeichnet wurde. Dieses Verfahren reicht nach Auffassung der Aufsichtsbehörde keinesfalls aus, um dem Arzt oder sonstigen Angehörigen eines Heilberufes eine sichere Befugnis zur Offenbarung von Gesundheitsdaten zu verschaffen. Vielmehr muß ihm deutlich sein, welchen Umfang seine Auskunft haben darf, damit er die Grenze zur Strafbarkeit nicht überschreitet. Die Vertreter der Versicherungswirtschaft haben zugesagt, Vorschläge zu unterbreiten, auf welche Weise Ärzte und andere betroffene Stellen über die Neufassung von Schweigepflicht-Entbindungserklärungen unterrichtet werden.

25.5 Gruppenversicherungsverträge

Bereits im Jahre 1990 wurde zwischen den Aufsichtsbehörden und der Versicherungswirtschaft eine Absprache über Gruppenversicherungsverträge getroffen. Danach legen Vereine, die ihren Mitgliedern die Teilnahme an Gruppenversicherungsverträgen ermöglichen wollen, diesen mit der Beitrittserklärung zugleich eine Einwilligungserklärung zur Datenübermittlung vor, deren

Unterzeichnung freiwillig ist (vgl. ausführlich 9. TB, 5.3.2). Darin wurde erklärt, daß das Mitglied mit der Weitergabe seines Namens und seiner Anschrift an den Versicherer zum Zwecke des Abschlusses eines Gruppenversicherungsvertrages einverstanden ist.

Diejenigen Personen, die zum Zeitpunkt des Abschlusses eines Rahmenvertrages bereits Vereinsmitglieder waren, erhalten ein sog. Avisschreiben, mit dem der Besuch eines Versicherungsvertreters angekündigt wird. Sollten sie mit dem Besuch nicht einverstanden sein, werden auch keine Daten an die Versicherungsgesellschaft übermittelt. Darüber hinaus wird auch Neumitgliedern ein Avisschreiben übersandt, denen bei Abschluß eines Versicherungsvertrages eine Erklärung zur Spende der jeweils anfallenden Risikoanteile aus der Überschußbeteiligung an den Verein vorgelegt werden soll.

Bei einer Versicherungsgesellschaft ist nunmehr das Problem aufgetreten, daß diese sich von den Vereinen nicht nur den Namen und die Anschrift, sondern auch das Geburtsjahr übermitteln läßt. Die Aufsichtsbehörden sehen eine über die Einwilligungserklärung hinausgehende Übermittlung von Daten als unzulässig an, weil der Betroffene über den Umfang der Datenweitergabe im Unklaren bleibt. Es stellt sich daher die Frage, welche praktischen Möglichkeiten zur problemlosen Einbeziehung des Geburtsjahres bestehen. Seitens der Aufsichtsbehörde wurde vorgeschlagen, das Geburtsjahr in die Avisschreiben aufzunehmen und diese Schreiben auf Neumitglieder auszudehnen. Unter diesen Umständen wären die Vereinsmitglieder umfassend über den Umfang der Datenübermittlung informiert. Die Versicherungwirtschaft hat zugesagt, sich kurzfristig zu diesem Vorschlag zu äußern.

25.6 Datenübermittlungen in das Ausland

Im 10. TB (25.6) wurde über die Weitergabe von personenbezogenen Daten in das Ausland im Falle von Kfz-Schadensfällen im Ausland oder unter Beteiligung von Ausländern auf dem Gebiet der Bundesrepublik Deutschland berichtet. Aufgrund weiterer Informationen seitens der Versicherungswirtschaft konnte überprüft werden, daß diese Übermittlung personenbezogener Daten in das Ausland zur Durchsetzung gegenseitiger Ansprüche der Unfallbeteiligten erforderlich ist. Für die Zulässigkeit dieses Verfahrens nach den Vorschriften des Bundesdatenschutzgesetzes ist es notwendig, daß die Daten ausschließlich zum Zwecke der Schadenabwicklung verwendet werden. Seitens des HUK-Verbandes wurde dies für die dort eingehenden Daten zugesichert. Darüber hinaus wurde erklärt, daß auch für die strenge Zweckbindung im Ausland – ggf. durch entsprechende Hinweise – Sorge getragen werde.

Insbesondere im Hinblick auf den Entwurf der EG-Richtlinie zum Datenschutz (vgl. 1.7) wird künftig zu beobachten sein, zu welchen Zwecken und in welchem Umfang die Versicherungswirtschaft den Austausch personenbezogener Daten mit dem Ausland vornimmt.

26. Handels- und Wirtschaftsauskunfteien

26.1 Kein Vertragsmodell

Im 10. TB (26.2) wurde dargestellt, daß die Handels- und Wirtschaftsauskunfteien trotz ihrer früher geäußerten Bedenken ein Vertragsmodell für den grenzüberschreitenden Datenverkehr erneut rechtlich prüfen wollten. Leider haben die Handels- und Wirtschaftsauskunfteien über ihren Verband nun vortragen lassen, daß ihre bisher geltend gemachten Bedenken gegen das Vertragsmodell weiter bestehen und derartige vertragliche Regelungen mit Mitgliedern oder Kunden in Drittländern nicht akzeptiert werden können.

Die Handels- und Wirtschaftsauskunfteien erkennen weder eine Notwendigkeit noch eine Verpflichtung an, bei einem Datenexport in Länder mit schwächeren oder fehlenden Datenschutzgesetzen das von den Aufsichtsbehörden vorgeschlagene Vertragsmodell einzuführen. Als Begründung wird angegeben, das Vertragsmodell verstoße gegen geltendes Recht. Den Aufsichtsbehörden ginge es darum, in Ausübung ihrer nationalen Eingriffsbefugnisse auf die Ausgestaltung von Exportvereinbarungen einzuwirken und auf diese Weise zu einer extraterritorialen Erstreckung des nationalen Datenschutzrechts zu gelangen.

Es wird vorgetragen, daß vertragliche Regelungen die Geschäftsverbindungen zu den ausländischen Kunden oder Mitgliedern beeinträchtigen würden. Gerade in den Ländern, in denen die Vorkehrungen des deutschen Datenschutzes nicht bekannt seien, bestehe kein Verständnis für die Notwendigkeit und den Sinn dieser Regelungen. Zudem könnte durch Vertragsmodelle auch der beabsichtigte Datenschutz nicht gewährleistet werden. Die Behörden des Empfängerlandes seien nicht an Verträge gebunden. Die Verträge könnten jederzeit ohne Kenntnis der Betroffenen geändert werden.

Schließlich wird vorgetragen, die Vertragsmodelle seien vor dem Hintergrund der geplanten EG-Datenschutzrichtlinie sinnlos. Nach Inkrafttreten der Datenschutzrichtlinie könnten die Aufsichtsbehörden innerhalb der EG keinen Datenexport unterbinden unabhängig davon, ob in dem jeweiligen Mitgliedsland ein Datenschutzgesetz vorhanden sei.

Wir sind der Ansicht, daß die vom Verband vorgetragenen Begründungen gegen ein Vertragsmodell nicht überzeugend sind. Insbesondere vor dem Hintergrund des Richtlinienentwurfs der EG (siehe 1.7) sind die Argumente der Handels- und Wirtschaftsauskunfteien nicht nachvollziehbar. Der Richtlinienentwurf versucht, den Datenschutz in der EG auf ein allgemein hohes Niveau festzulegen. Sowohl für die Zulässigkeit der Datenübermittlung auf EG-Ebene als auch in ein Drittland wird künftig ein bestimmtes Schutzniveau vorgeschrieben sein. Das Argument des Verbandes der Handels- und Wirtschaftsauskunfteien, daß die Mitgliedsstaaten nach Erlaß der Richtlinie den freien Verkehr personenbezogener Daten zwischen Mitgliedsstaaten nicht aus Gründen des Schutzes der Privatsphäre unterbinden dürften, ist daher unzutreffend.

Bis zum Erlaß der EG-Richtlinie ist nach wie vor ein Vertragsmodell zum Ausgleich des unterschiedlichen Datenschutzstandards – trotz unzureichender Kontrollrechte – als Übergangslösung vertretbar (vgl. 9. TB, 5.2.1.1 und 5.4.2).

26.2 Keine Erhöhung der Stichproben

Im 10. TB (vgl. 26.1) wurde mitgeteilt, daß die Handels- und Wirtschaftsauskunfteien sich bereit erklärt hatten, eine qualitative und quantitative Veränderung des Kontrollverfahrens zu erwägen, um Probleme bei der Kontrolle des berechtigten Interesses zu verhindern. Nach § 29 Abs. 2 Satz 3 BDSG sind Auskunfteien verpflichtet, bei jeder erteilten Auskunft die Gründe für das Vorliegen eines berechtigten Interesses und die Art und Weise ihrer glaubhaften Darlegung von der übermittelnden Stelle aufzuzeichnen. In der Praxis wurden häufig nur vorformulierte Angaben (Bonität, Forderung, usw.) sowie Datum und Empfänger der Auskunft aufgezeichnet. Selten wurde mehr als nur der Firmenname vermerkt, so daß eine Individualisierung der Person, die die Anfrage stellte, oft nicht mehr möglich war.

Die Mitglieder des Verbandes der Handels- und Wirtschaftsauskunfteien haben sich nun erfreulicherweise bereit erklärt, durch Einführung eines mit den Aufsichtsbehörden abgestimmten Formulars die Stichprobenkontrollen zu verbessern. Auf dem Formular wird entweder eine präzise Umschreibung des der Auskunft zugrunde liegenden Vorganges oder ein entsprechendes zentrales Dokument als Nachweis für das Vorhandensein eines berechtigten Interesses vom Auskunftsempfänger vermerkt.

Leider besteht aber keine Bereitschaft der Mitglieder des Verbandes, die Anzahl der Stichprobenkontrollen von ein Promille auf zwei Promille zu erhöhen und die Stichproben auf die absolute Mindestzahl von 12 im Jahr festzulegen. Der Verband trägt dazu vor, daß die Stichprobenkontrollen kaum zur Aufdeckung von mißbräuchlichen Anfragen führen. Die Mitarbeiter der Auskunfteien seien schon jetzt darauf geschult, den geringsten Hinweisen auf fehlende Anfrageberechtigungen nachzugehen und in Zweifelsfällen die Auskunft nicht zu erteilen.

Wir bedauern diese Entscheidung des Verbandes und halten weiterhin die Erhöhung der Stichprobenkontrolle zur ständigen Überprüfung der Anfrageberechtigung für unbedingt notwendig.

27. Kartengestützte Zahlungsverfahren

Aufgrund von Eingaben haben wir uns im Berichtsjahr intensiv mit kartengestützten Zahlungsverfahren und deren Datenschutzproblemen auseinandergesetzt, insbesondere mit electronic-cash und Lastschriftverfahren. Bei jedem kartengestützten Zahlvorgang – sei es der Kauf von Konsumgütern, die Benutzung öffentlicher Verkehrsmittel oder die Begleichung einer Hotelrechnung – werden zahlreiche personenbezogene Daten gespeichert, die für andere Zwecke genutzt werden können. Sperrdateien geben Auskunft über Seriosität

und Solvenz von Kunden. Das Kaufverhalten kann zu Kundenprofilen verdichtet werden und ist daher für die werbende Wirtschaft von Interesse.

Datenschutzrechtliche Aspekte von kartengesteuerten Zahlungsverfahren waren u.a. Gegenstand von mehreren Gesprächen, die wir – in Abstimmung mit den obersten Aufsichtsbehörden – mit Vertretern des Zentralen Kreditausschusses für den Bankbereich, der in Hamburg ansässigen Mineralölgesellschaften für den Tankstellenbereich und einem Modehaus für den dortigen Zahlungsverkehr geführt haben.

Während beim Lastschriftverfahren der Personenbezug der Daten unstrittig ist, da der Kunde durch seine Unterschrift selbst den Namen preisgibt, bestanden unterschiedliche Ansichten darüber, inwieweit bei electronic-cash personenbezogene Daten verarbeitet werden. Der Zentrale Kreditausschuß hielt die vom Handel und bei den Netzbetreibern gespeicherten Daten nicht für personenbezogen, weil weder Handel noch Netzbetreiber die Möglichkeit hätten, von Bankleitzahl und Kontonummer auf den Namen des Kontoinhabers zu schließen. Da die für eine Herstellung des Personenbezugs notwendigen Angaben – Name und Anschrift – entweder in den Autorisierungssystemen des Kreditgewerbes oder erst bei der bezogenen Bank vorgehalten würden und dort in jedem Fall den strengen Anforderungen des Bankgeheimnisses unterlägen, sei dem Handel und den Netzbetreibern eine Deanonymisierung nur mit einem unverhältnismäßig großen Aufwand möglich.

Demgegenüber sind wir der Ansicht, daß eine Person nicht erst durch Namen und Anschrift, sondern auch durch andere Merkmale wie Bankleitzahl und Kontonummer eindeutig bestimmt wird. Mit der Verbreitung elektronischer Zahlungssysteme erhält die Kontonummer langfristig eine ähnliche Identifikationswirkung wie die Telefonnummer. Bankleitzahl und Kontonummer werden gerade deshalb gespeichert, um möglichen strittigen Fällen nachgehen zu können. Da die Datenverarbeitung als Gesamtvorgang der Herstellung des Personenbezugs dient, sind die gespeicherten Daten personenbezogen.

27.1 Electronic-cash

Electronic-cash ist in der Bundesrepublik seit 1989 im Einsatz. Zwar sind die bei den Händlern aufgestellten Kassenterminals aufgrund einer Entscheidung des Bundeskartellamtes auch für Kreditkarten nutzbar, dennoch ist das neue Verfahren hauptsächlich auf die Eurocheque-Karte abgestimmt.

Electronic-cash setzt sich aus der Autorisierung der Eurocheque-Karte und der Zahlungsabwicklung zusammen. Bei der Autorisierung, die online über Autorisierungszentralen des Kreditwesens erfolgt, wird geprüft, ob die Karte möglicherweise gesperrt ist und ob der Kaufbetrag den noch freien Verfügungsrahmen übersteigt. Ferner wird die vom Kunden eingegebene persönliche Identifikationsnummer (PIN) verifiziert; eine Echtheitsüberprüfung der Karte findet zumeist nicht statt. Die Inhalte der Autorisierungsanfrage und -antwort werden in einem Transaktionssatz gespeichert.

Bei fehlgeschlagener Autorisierung wird die Ursache am Kassenterminal angezeigt. Insbesondere wird dem Händler durch den Fehlercode 13 offenbart, daß der Kaufbetrag durch den freien Verfügungsrahmen nicht gedeckt ist. Bei erfolgreicher Autorisierung wird aus den Transaktionssätzen eine Lastschriftdatei erstellt, die entweder online oder über Datenträgeraustausch an die Händlerbank zwecks Einzug der Forderungen im bankenüblichen Lastschriftverfahren übermittelt wird.

Die Online-Verbindung vom Kassenterminal zu den Autorisierungsstellen der Kreditwirtschaft wird über Netzbetreiber abgewickelt, wobei im Mineralölbereich, der sich durch geschlossene Warenwirtschaftssysteme auszeichnet, große Konzerne als eigenständige Netzbetreiber auftreten. Da electronic-cash den Scheckverkehr elektronisch nachvollzieht, müssen zumindest bis zur Zahlungsabwicklung personenbezogene Daten über den Kaufvorgang gespeichert werden: Während die Netzbetreiber die Transaktionssätze 90 Tage über den Kauftag hinaus speichern und anschließend mikroverfilmen, bewahren die Tankstellen-Einzelhändler die Kassenbelege mit Kontonummer und Bankleitzahl längerfristig auf.

Die Speicherung und Übermittlung von Daten für Autorisierungszwecke ist gem. § 28 Abs. 1 BDSG zulässig, da sie dazu dienen, einen unzulässigen Gebrauch der Karte auszuschließen. Zweifel sind hinsichtlich des Differenzierungsgrads der Fehlermeldungen angebracht. Insbesondere bestehen datenschutzrechtliche Bedenken dagegen, daß mit dem Fehlercode 13 dem Händler eine „Limitüberschreitung" offenbart wird, obwohl bereits eine allgemeine und damit weniger diskriminierende Meldung ausreichen würde, um einen Mißbrauch zu verhindern. Die Zusammenfassung dieses Codes mit anderen Fehlermeldungen würde völlig genügen. Der Zentrale Kreditausschuß erklärte sich bereit, den Fehlercode 13 künftig so zu formulieren, daß Mißverständnisse und Diskriminierungen möglichst vermieden werden.

Soweit die Transaktionssätze für die Abwicklung des Zahlungsvorgangs benötigt werden, ist gegen ihre Speicherung nichts einzuwenden. Fragwürdig ist in diesem Zusammenhang allerdings, daß einzelne Mineralölkonzerne, die zugleich Netzbetreiber sind, neben dem Kaufbetrag und -zeitpunkt auch die Artikelbezeichnung und Umsatzmenge personenbezogen speichern. Dies ist vom Erforderlichkeitsgrundsatz nicht gedeckt und beeinträchtigt schutzwürdige Interessen der Betroffenen, da sich für die gesamte Dauer der Speicherung das individuelle Kaufverhalten nachvollziehen läßt. Wir haben daher die entsprechenden Mineralölkonzerne aufgefordert, den Transaktionssatz nach Ablauf der 90-Tage-Frist entweder ganz zu löschen oder zu anonymisieren.

27.2 Lastschriftverfahren

Im April 1990 hat ein großes Modehaus ein eigenes, ebenfalls auf der EC-Karte basierendes bargeldloses Zahlungssystem eingeführt, dem mittlerweile weitere Einzelhandelsunternehmen gefolgt sind. Beim Lastschriftverfahren wird auf eine zentrale Autorisierung und somit auch auf eine Eingabe der PIN-Nummer

verzichtet. Statt dessen authentifiziert sich der Kunde lediglich durch seine Unterschrift. Durch Abgleich mit händlereigenen Sperrdateien wird geprüft, ob die EC-Karte beispielsweise aufgrund mißbräuchlicher Nutzung gesperrt ist. Die Lastschrift wird über Datenträgeraustausch mit der Händlerbank eingelöst.

Während bei electronic-cash die Banken bis zur Garantiesumme für nicht gedeckte Kaufbeträge haften, verbleibt beim Lastschriftverfahren das Risiko beim Handel. Der Händler erhält jedoch bei Widerruf der Abbuchung von der Kundenbank Name und Anschrift des Kunden, um seine Ansprüche diesem gegenüber direkt geltend machen zu können. Das Einverständnis zu einer derartigen Übermittlung erteilt der Kartenbenutzer bereits mit seiner Unterschrift unter den Kaufbeleg.

Im Dezember 1991 hat sich der Zentrale Kreditausschuß für die Einführung eines weiteren Lastschriftverfahrens ausgesprochen (POZ-System). Diese Entscheidung ist vor dem Hintergrund von Akzeptanzschwierigkeiten bei electronic-cash zu sehen, die unter anderem darauf zurückgeführt werden können, daß nur 30% aller EC-Karteninhaber überhaupt ihre PIN-Nummer kennen. Bei diesem Verfahren werden Konzepte von electronic-cash und Lastschriftverfahren des Handels kombiniert: Einerseits soll der Händler – vergleichbar mit electronic-cash – online die Autorisierungszentralen des Kreditwesens nutzen können, andererseits wird die Lastschrift wie bisher über Datenträgeraustausch bei der Händlerbank eingelöst.

Da – anders als bei electronic-cash – bei dem vom Einzelhandel eingeführten Lastschriftverfahren keine Online-Autorisierung der Karte stattfindet, führen viele Unternehmen Sperrdateien mit Daten über nicht zugelassene EC-Karten. Problematisch sind solche Dateien vor allem dann, wenn keine nachvollziehbaren Kriterien darüber bestehen, unter welchen Umständen Daten in dieser Datei gespeichert werden, und wenn der Betroffene nicht über die Speicherung informiert wird. Da gegen eine Speicherung mit dessen Kenntnis und Einwilligung jedoch nichts einzuwenden ist, wurde mit einem in Hamburg ansässigen Modehaus abgesprochen, daß der Kunde bereits beim Kauf über die Übermittlung von Sperrdateien an andere Unternehmen informiert wird und per Unterschrift die Einwilligung für das Verfahren erteilen kann.

Die datenschutzrechtliche Bewertung von Sperrdateien ist auch auf das neue, vom Kreditwesen konzipierte Lastschriftverfahren übertragbar: Speicherung und Abgleich einer zentralen Sperrdatei befreien nicht von der Erfordernis der Information und Einwilligung des Kunden.

Der Handel benötigt beim Lastschriftverfahren zur Geltendmachung seiner Forderung gegenüber dem Kunden differenzierte Zahlungsdaten. Da nach Begleichung der Forderung jedoch kein Grund für die weitere personenbezogene Speicherung besteht, ist es datenschutzrechtlich geboten, die Daten anschließend zu löschen.

27.3 Rechte der Betroffenen

Die Speicherung von Daten im Rahmen des elektronischen Zahlungsverkehrs löst Benachrichtungspflichten nach § 33 BDSG aus. Auf eine Benachrichtigung kann nur unter den Voraussetzungen des § 33 Abs. 2 BDSG verzichtet werden. Um einer einzelfallbezogenen Benachrichtigungspflicht zu entgehen, müssen die beteiligten Unternehmen die Betroffenen über ihre Datenverarbeitung möglichst verständlich und vollständig aufklären. Obwohl die Vertreter der Kreditwirtschaft eine solche Information im Sommer 1991 zugesagt haben, wurde die Zusage bislang noch nicht umgesetzt.

Manche der am elektronischen Zahlungsverkehr beteiligten Stellen tun sich mit dem Auskunftsrecht gemäß § 34 BDSG schwer. Unter Hinweis darauf, daß die bei electronic-cash gespeicherten Daten nicht personenenbezogen seien, sind die Auskünfte häufig sehr allgemein gehalten; die tatsächlich gespeicherten Daten werden nicht genannt. Im besten Fall erteilen Handelsunternehmen und Netzbetreiber dem Kunden Auskünfte über die Art der gespeicherten Daten, nicht jedoch über die konkreten, dem Kunden zuzuordnenden Daten.

Eine solche Auskunftspraxis widerspricht dem Datenschutzrecht und muß geändert werden. Das Recht des Betroffenen auf eine vollständige und konkrete Auskunft über die zu seiner Person gespeicherten Daten ist zu gewährleisten, indem ihm auf Antrag tatsächlich alle von den beteiligten Stellen über ihn gespeicherten Daten mitgeteilt werden. Allerdings kann das Unternehmen von ihm verlangen, durch Nennung der Kontonummer, des Kauftermins und möglicherweise weiterer Hilfsangaben (z.B. Ort des Kaufs) das Auffinden seiner Daten zu erleichtern.

Falsche Daten müssen berichtigt, unzulässig gespeicherte Daten gelöscht werden (§ 35 BDSG). Ein Löschungsanspruch wegen unzulässiger Speicherung besteht auch bei Daten, die nicht erforderlich sind. Hierzu gehören bei electronic-cash vor allem solche Daten, die zwar personenbezogen gespeichert, aber nicht personenbezogen benötigt werden, z.B. Artikelnummern und Mengenangaben. Bei Lastschriftverfahren werden die personenbezogenen Daten über die gekauften Artikel dann nicht mehr benötigt, wenn die Forderung gegenüber dem Kunden unwiderruflich beglichen wurde.

Systemfehler oder Manipulationshandlungen können im elektronischen Zahlungsverkehr materielle Schäden, insbesondere eine dem Grund oder der Höhe nach fehlerhafte Kontobelastung verursachen. Da derartige Schäden Folgen unrichtiger oder unzulässiger automatisierter Datenverarbeitung sind, können die Betroffenen Schadenersatzansprüche gegenüber den beteiligten Unternehmen geltend machen. Dabei liegt die Beweislast, ob der Schaden Folge eines von der speichernden Stelle zu vertretenden Umstandes ist, gemäß § 8 BDSG bei den Unternehmen.

Darüber hinaus sollte der Kunde gegenüber der Bank seinen Verzicht auf eine Teilnahme an bestimmten kartengestützten Zahlungssystemen erklären können, ohne dabei von anderen Systemen ausgeschlossen zu sein. Der Zentrale

Kreditausschuß hat zugesagt, derartige Überlegungen bei der Konzeption des im Dezember 1991 beschlossenen neuen Lastschriftverfahrens möglichst zu berücksichtigen, solange nicht technische Sachzwänge dem entgegenstehen.

28. Meldepflicht nach § 32 BDSG

Die Novellierung des Bundesdatenschutzgesetzes hat im wesentlichen an der Meldepflicht nichts geändert. Wie bereits in den Vorjahren (s. auch 6. TB, 5.7.1) muß die Aufsichtsbehörde leider davon ausgehen, daß vielen Betrieben, die eine Tätigkeit nach § 32 Abs. 1 BDSG aufnehmen, die Meldepflicht nicht bekannt ist und sie daher dieser nicht nachgekommen sind. Zu den klassischen meldepflichtigen Tätigkeiten gehören z.B. Akten-, Datenträger- und Schriftgutvernichtung, Mikroverfilmung, Markt- und Meinungsforschung, Auftragsdatenverarbeitung in Rechenzentren z.B. für Lohnabrechnung, Datenübermittlung durch Auskunfteien.

Wir werden weiterhin die veröffentlichten Handelsregistereintragungen sichten und Firmen anschreiben, um eine etwaige Meldepflicht festzustellen. Außerdem wird die Handelskammer Hamburg zukünftig neuen Firmen mit ihrem bisherigen Begrüßungsschreiben ein Merkblatt zum Datenschutz und zur Meldepflicht zusenden. Ein derartiges Verfahren haben die Wirtschafts- und Ordnungsämter für den Fall einer Gewerbeanmeldung trotz unserer intensiven Bemühungen leider abgelehnt.

An dieser Stelle muß auch auf die Bußgeldvorschriften hingewiesen werden. Danach handelt ordnungswidrig, wer eine Meldung nach § 32 BDSG nicht oder nicht rechtzeitig erstattet.

29. Arbeitnehmerdatenschutz

29.1 Psycho-Tests bei Bewerberauswahl

Im 10. TB (28.2) hatten wir auf einen psychologischen Bewerbertest einer Personalberatungsfirma aufmerksam gemacht, der aus 200 zum Teil sehr persönlichen Fragen besteht.

Bei dem Personalberatungsunternehmen handelt es sich um die Firma U-Man International Hamburg, die in der Presse wiederholt im Rahmen der Auseinandersetzung um die Scientology Erwähnung fand. Anfang 1992 führten wir bei der Firma eine Prüfung durch. Wir haben festgestellt, daß die Bewerberdaten personenbezogen automatisiert verarbeitet werden, ohne daß eine Löschungsfrist vorgesehen wäre.

Im Anschluß an die Prüfung haben wir die Firma auf die Rechtswidrigkeit der Fragebögen hingewiesen und sie aufgefordert, auf den Psycho-Test zu verzichten. Auch haben wir die Firma zur Löschung bzw. Anonymisierung der gespeicherten Daten aufgefordert. Zur Begründung haben wir im wesentlichen auf die von der Rechtsprechung entwickelten Grundsätze zum Fragerecht des Arbeit-

gebers verwiesen, welches bei solchen ausforschenden Psycho-Tests ohne Bezug zum Arbeitsplatz deutlich überschritten wird.

Die Firma hat daraufhin die Löschung der gespeicherten Daten in der automatisierten Datei und in den Akten unmittelbar nach Erledigung des Auftrages zugesagt. Zu einem Verzicht auf den rechtswidrigen Psycho-Test konnte sich die Firma jedoch nicht entschließen. Dies haben wir zum Anlaß genommen, erneut auf die Unzulässigkeit des Tests hinzuweisen. Wir haben dabei betont, daß ein möglichst wirksamer Schutz von Bewerbern vor rechtswidrigen Ausforschungen ihrer Persönlichkeit im Bewerbungsverfahren es erforderlich macht, auf konkrete Beispiele unzulässiger Bewerbertests öffentlich hinzuweisen.

In diesem Zusammenhang möchten wir hervorheben, daß etwaige Einwilligungen der Bewerber in solche ausforschenden Psycho-Tests an deren arbeitsrechtlicher Unzulässigkeit nichts ändern. Unzulässige Tests und Bewerberbefragungen erweitern die Informationsbasis des Arbeitgebers über die arbeitsrechtlich anerkannten Daten hinaus. Danach darf der Arbeitgeber nur solche Fragen stellen, die einen Bezug zum Arbeitsplatz erkennen lassen. Auch über eine Einwilligung kann sich der Arbeitgeber keinen Zugang zu Informationen verschaffen, die über diesen insbesondere von der Rechtsprechung festgelegten Rahmen hinausgehen. Die weitergehenden Informationsabfragen sind ihm prinzipiell verwehrt.

Auch soweit Arbeitgeber diese Daten in Akten speichern, verstoßen sie gegen das informationelle Selbstbestimmungsrecht der Bewerber, die für die Vernichtung dieser Unterlagen sorgen können. Dagegen besteht insoweit bisher leider nach dem Bundesdatenschutzgesetz weder ein Auskunftsrecht der Betroffenen noch ein Aufsichtsrecht für uns (vgl.1.6.1).

Wir befürchten, daß die Dunkelziffer bei unzulässigen Psycho-Tests recht hoch sein dürfte. Eine bundesweite Umfrage, die wir bei den Aufsichtsbehörden der Länder für den Datenschutz im nicht-öffentlichen Bereich durchgeführt haben, hat keine weiteren Erkenntnisse gebracht. Wir schließen daraus, daß eine intensivere datenschutzrechtliche Durchleuchtung dieses Problemfeldes unbedingt geboten erscheint. Ein Schritt in diese Richtung muß sicherlich darin liegen, bei den potentiellen Verwendern solcher Tests, also bei den Arbeitgebern, verstärkte Aufklärungsarbeit zu leisten.

Die Firma U-Man International ist inzwischen in Hamburg nicht mehr erreichbar („unbekannt verzogen"). Unsere Überprüfung konnte auf diese – unerwartete – Weise abgeschlossen werden.

29.2 Personaldatenschutz von Auszubildenden

Die Handelskammer Hamburg hatte im Berichtszeitraum nach dem Berufsbildungsgesetz die Ausbildungsdauer der bei ihr registrierten Auszubildenden zu kürzen. Dies hatte zwangsläufig eine entsprechende Verkürzung der Berufsschulpflicht und mithin eine Anpassung der Lehrinhalte zur Folge. Um die erforderlich gewordene Anpassung sachgerecht zu gestalten, kam es den Berufsschulen darauf an, Daten insbesondere über die neue Ausbildungsdauer zuverlässig zu erhalten.

Von Berufsschulen war daher der Wunsch geäußert worden, die Handelskammer möge Name, Anschrift, Ausbildungsberuf sowie Ausbildungsdauer der bei ihr registrierten Auszubildenden mitteilen.

Wir haben in Abstimmung mit der Behörde für Schule, Jugend und Berufsbildung die Übermittlung dieser Personaldaten von Auszubildenden durch die Handelskammer an die Berufsschulen gebilligt.

Die Behörde für Schule, Jugend und Berufsbildung hat in diesem Zusammenhang darauf hingewiesen, daß es sich bei der dualen Berufsausbildung um ein abgestimmtes Verhalten der Partner eines ganzheitlichen Bildungsprozesses handelt. Die Datenübermittlung ist besonders für eine zeitlich hinreichende Vorbereitung der Unterrichtsorganisation erforderlich (vgl. § 14 HmbDSG). Wir haben Wert darauf gelegt, daß die Auszubildenden – dem Grundsatz der Transparenz entsprechend – über die Datenübermittlung informiert werden.

Im Gegensatz dazu trugen wir in einem anderen Bereich Bedenken gegen Datenübermittlungen durch die Handelskammer vor. Wir hatten eine Eingabe zum Anlaß genommen, uns prinzipiell mit dem Prüfungsverfahren von Auszubildenden auseinanderzusetzen. Aus den entsprechenden Anmeldungsbögen zur Abschlußprüfung, über die im wesentlichen Einvernehmen hergestellt werden konnte, geht hervor, daß die Handelskammer die Ergebnisse der Abschlußprüfung regelmäßig an die Ausbildungsbetriebe übermittelt.

Für den Fall, daß der Prüfling nicht besteht, ist die Übermittlung in § 23 Abs. 1 der Prüfungsordnung vorgesehen. Für den Fall des Bestehens allerdings sieht die Prüfungsordnung keine Regelung vor.

Die Handelskammer sieht die Rechtsgrundlage für die Datenübermittlung in § 45 Berufsbildungsgesetz. Wir konnten uns einer solchen weiten Auslegung nicht anschließen und haben deshalb vorgeschlagen, die Datenübermittlung von einer Einwilligung der Betroffenen abhängig zu machen. Eine Einigung mit der Handelskammer konnte in dieser Frage jedoch leider nicht hergestellt werden.

30. Sonstige Probleme aus dem nichtöffentlichen Bereich

30.1 Datenverarbeitung bei der Scientology Kirche Hamburg e. V.

Auf Grund mehrerer Beschwerden von Betroffenen haben wir die Datenverarbeitung der Scientology Kirche Hamburg e. V. überprüft. Die Beschwerden betrafen überwiegend die Speicherung von personenbezogenen Daten in Interessentenlisten. Es wurde auch die Befürchtung geäußert, die Organisation habe personenbezogene Daten in „Gegnerdateien" gespeichert. Vor Ort ergab sich der folgende Sachverhalt:

Die von Interessenten durchgeführten Persönlichkeitstests werden automatisch ausgewertet. Die Testantworten und Testergebnisse werden jedoch nicht dauerhaft gespeichert.

Neben diesem Testauswertungsverfahren gibt es mehrere automatisierte Dateien bei der Organisation. Im wesentlichen handelt es sich dabei um eine Mitarbeiterdatei, eine Mitgliederdatei und eine Interessentendatei, die auf dieselbe Adreßdatei zurückgreifen. Außerdem gibt es eine davon getrennte Datei über mögliche Interessenten.

In der Mitarbeiterdatei hatte die Organisation früher neben allgemeinen Personal- und Abrechnungsdaten zunächst die Erfassung und Speicherung zusätzlicher Merkmale erwogen, die Rauschgiftkonsum, Schulden, Vorstrafen, Vertragsbruch und Ergebnisse von Persönlichkeitstests betrafen. Von einer derartigen Datenverarbeitung hatte die Organisation jedoch schließlich von sich aus abgesehen. Sie hat mitgeteilt, daß die dafür vorgesehenen Felder der Datei nun vollständig gelöscht würden.

Die Speicherung und Nutzung solcher Merkmale, die die Herstellung eines umfassenden Persönlichkeitsprofils des Arbeitnehmers ermöglicht, ist auch bei Einwilligung der Mitarbeiter unzulässig (siehe entsprechend 29.1). Es liegt bei den Mitarbeitern, auch die Löschung dieser sehr sensiblen Daten in den Akten der Organisation zu erreichen, soweit die Daten dort aufgenommen worden sind.

In der Adreßdatei sind Daten von Mitgliedern und Interessenten gespeichert, die z. B. ein Buch erworben haben. Soweit Mitglieder eine Einverständniserklärung in die Datenverarbeitung abgegeben haben, bestehen für die Dauer der Mitgliedschaft keine Bedenken gegen die Speicherung.

Es wurde auch die Speicherung von Mitgliedern festgestellt, für die keine Einverständniserklärung vorgelegt werden konnte, sowie von ehemaligen Mitgliedern. Bei ihnen werden jedoch regelmäßig nur die Adreßangaben gespeichert. Die Organisation geht auch selbst davon aus, daß sich die Speicherung auf Adreßdaten beschränken muß, wenn keine Einverständniserklärung vorliegt oder die Mitgliedschaft beendet ist.

Die Organisation hat uns mitgeteilt, daß sie inzwischen den Mitgliederbestand in der Datei insgesamt auf die erforderlichen Einverständniserklärungen anhand der Akten überprüft habe.

Einige von uns überprüfte Datensätze enthielten außerdem ein Enddatum der Mitgliedschaft, z. B. aus dem Jahr 1985. Eine unbefristete Speicherung nach Ablauf der Mitgliedschaft ist bedenklich, da sie zur Wahrung berechtigter Interessen der Organisation nicht erforderlich ist. Insoweit sind Fristen von höchstens fünf Jahren angebracht, nach deren Ablauf bei fehlender positiver Reaktion die Mitgliedsdaten zu löschen sind. Schon vorher sind die Daten der ehemaligen Mitglieder auf deren Verlangen zu löschen; diese Löschungen werden nach Angaben der Organisation auch vorgenommen.

Einige Mitgliederakten, die zum Vergleich mit den Datensätzen herangezogen wurden, enthielten neben Nachweisen über Kurse auch die Testauswertungsbögen eines Persönlichkeitstests. Auch bei Einverständniserklärung in die Datenverarbeitung bestehen Bedenken gegen die aktenmäßige Erfassung der

in den Tests enthaltenen sehr sensiblen Daten. Es ist wiederum Sache des einzelnen, seine Rechte insoweit unmittelbar wahrzunehmen.

Bei den Buchkäufern werden das Datum des Kaufes und die Anschrift erfaßt. Es wurde festgestellt, daß diese Angaben auch dann noch gespeichert wurden, wenn der Kauf schon mehrere Jahre zurücklag und danach kein weiteres Interesse an der Organisation mehr bekundet wurde. Eine derart langfristige Datenspeicherung ist nicht erforderlich und daher unzulässig. Hier ist eine kürzere Frist als bei früheren Mitgliedern von höchstens drei Jahren vertretbar.

Die Daten von Interessenten und von möglichen Interessenten sind zu löschen bzw. gemäß § 35 Abs. 3 BDSG zu sperren, wenn der Zusendung von Informationsmaterial widersprochen wird. Demgemäß verfährt die Organisation nach ihren Angaben regelmäßig. Allerdings haben wir bei der stichprobenweisen Überprüfung einen Fall gefunden, in dem der Betroffene trotz ausdrücklicher Bitte um Einstellung der Zusendung von Material noch weiter angeschrieben wurde. Aus Eingaben sind uns weitere derartige Fälle bekannt. Die Organisation hat eine Löschung in solchen Fällen zugesichert.

Eine automatisierte Datei über Gegner der Organisation konnten wir bei unserer Prüfung nicht feststellen. Im Presse- und Rechtsamt der Organisation befindet sich eine alphabetisch sortierte Hängeregistratur, in der Informationen über Politiker, Personen, die sich über die Organisation geäußert haben, Zeitungen usw. aufbewahrt werden. In den einzelnen Akten sind unter anderem chronologisch Zeitungsartikel, Schriftverkehr mit Personen und Transkripte von Rundfunk- und Fernsehinterviews enthalten. Nach dem Bundesdatenschutzgesetz ist diese Sammlung nicht zu beanstanden. Es ist Sache der Betroffenen, die eine Löschung erreichen wollen, für die Durchsetzung ihres informationellen Selbstbestimmungsrechts nach Art. 2 Abs. 1 und Art. 1 GG in Verbindung mit zivilrechtlichen Ansprüchen zu sorgen. Die Organisation hat hierzu erklärt, Akteneinsicht auch über die gesetzlichen Bestimmungen hinaus zu gewähren.

Wir werden die Organisation auch zukünftig bei Anhaltspunkten für Verstöße gegen den Datenschutz überprüfen. Das schwerwiegende Problem, daß die Verarbeitung von Daten in Akten im nicht-öffentlichen Bereich bisher nicht kontrolliert werden kann, ist nur durch den Gesetzgeber mit einer Änderung des Bundesdatenschutzgesetzes oder durch das Bundesverfassungsgericht lösbar (siehe 1.6.1). Sonst sind die Betroffenen nur auf eine freiwillig gewährte Akteneinsicht angewiesen, wie sie die Organisation zugesagt hat.

30.2 Mieterdatenschutz und Selbstauskunft

Anläßlich einer Eingabe befaßten wir uns mit der seit einigen Jahren verstärkt zu beobachtenden Praxis der Vermieter, von Mietinteressenten eine Selbstauskunft über ihre persönlichen und wirtschaftlichen Verhältnisse zu verlangen.

Da die erhobenen Daten in der Regel in Akten oder in nicht-automatisierten internen Dateien geführt und nicht an Dritte übermittelt werden, ist das BDSG

nur eingeschränkt anwendbar. Die Kontrollbefugnisse der Aufsichtsbehörde sind dementsprechend begrenzt. Zwar gelten die Vorschriften über das Datengeheimnis und die Datensicherheit. Eine darüber hinausgehende inhaltliche Überprüfung der Fragebögen kann dagegen nicht stattfinden.

Dies ändert nichts an der Tatsache, daß hier zum Teil erheblich in das Recht der Wohnungssuchenden auf informationelle Selbstbestimmung eingegriffen wird. Nach der Rechtsprechung des Bundesverfassungsgerichts ist das Recht des einzelnen, über Preisgabe und Verwendung seiner persönlichen Daten selbst zu bestimmen, auch im Privatrecht zu beachten. Das Fragerecht des Vermieters wird durch das Selbstbestimmungsrecht des Mieters begrenzt und besteht nur insoweit, als der Vermieter ein berechtigtes und schutzwürdiges Interesse an der Beantwortung der Fragen für das Mietverhältnis hat.

Zulässig sind z. B. Fragen nach dem Geburtsdatum, Beruf, Anzahl und Alter der zum Haushalt gehörenden Personen, Haustieren, Einkommensverhältnissen sowie der Abgabe einer eidesstattlichen Versicherung. Dagegen sind Fragen nach der Familienplanung, Mitgliedschaft in einem Mieterverein, Rechtsschutzversicherung und Vorstrafen unzulässig. Falls es nicht im Einzelfall aus besonderen Gründen einen Anlaß gibt, z. B. Zweifel an der Zahlungsfähigkeit, sind Angaben über Vermögensverhältnisse, Lebens- und sonstige Versicherungen, Personalausweis-/Paßnummer sowie den Geburtsort nicht erforderlich. Dies gilt auch für Fragen zum Arbeitgeber und zum bisherigen Vermieter, die die Einholung von Auskünften bei diesen ermöglichen sollen.

Auch wenn die Wohnungssuchenden rechtlich nicht verpflichtet sind, diese Fragen zu beantworten, werden sie doch faktisch dazu gezwungen, um als Mieter überhaupt in die engere Wahl zu kommen. Will oder kann ein Mietinteressent eine unzulässige Frage nicht wahrheitsgemäß beantworten, bleibt ihm nur ein Ausweg: Er darf lügen, ohne Nachteile befürchten zu müssen. Wahrheitswidrige Antworten auf unzulässige Fragen berechtigen den Vermieter selbst dann nicht zur späteren Anfechtung oder fristlosen Kündigung des Mietvertrages, wenn die Selbstauskunft eine solche Klausel enthielt.

Festzuhalten bleibt, daß die Regelungen des BDSG zur Datenverarbeitung in Akten und nicht-automatisierten Dateien lückenhaft sind und im Hinblick auf den Stellenwert des informationellen Selbstbestimmungsrechts verfassungsrechtlichen Bedenken begegnen (siehe 1.6.1).

30.3 Einsichtnahme in Mitgliederlisten von Parteien

An uns ist die Frage herangetragen worden, ob und inwieweit Mitglieder von Parteien Einsicht in die Mitgliederlisten nehmen können oder nicht.

Bisherige Praxis ist es offenbar, daß nicht jedem Mitglied die Einsichtnahme möglich ist. Insbesondere dann, wenn ein Mitglied Wahlen anfechten oder außerordentliche Mitgliederversammlungen durchführen will, kann die Verweigerung der Einsicht in das Mitgliederverzeichnis eine Behinderung der innerparteilichen Demokratie darstellen. Allerdings kollidieren die Anforderungen an die demokratischen Grundsätze der Parteien (Art. 21 GG) mit dem Grundrecht auf informationelle Selbstbestimmung der Mitglieder, deren persönliche Daten bei einer Einsichtnahme bekannt werden.

Durch eine Satzungsänderung oder eine Änderung des Parteiengesetzes, mit der die Modalitäten der Einsichtnahme in Mitgliederlisten geregelt werden können, würde der Eingriff in das Grundrecht auf informationelle Selbstbestimmung durch Offenbarung der Mitgliederliste normenklar festgelegt werden. Dabei wäre allerdings auch ein Widerspruchsrecht für die Mitglieder vorzusehen, die mit einer solchen Einsichtnahme nicht einverstanden sind. Die Überlegungen hierzu sind noch nicht abgeschlossen.

Geschäftsverteilung (Stand: 1. Dezember 1992)

Der Hamburgische Datenschutzbeauftragte
Baumwall 7, 2000 Hamburg 11

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

			Durchwahl
Dienststellenleiter:	Dr. Hans-Hermann Schrader	D	-2044-
Stellvertreter:	Peter Schaar		-2231-
Vorzimmer:	Eva-Maria Reupke		-2045-

D 1 - Geschäftsstelle

			Durchwahl
Leiter:	Detlef Malessa	D 1	-2223-
Sachbearbeiterin:	Annelies Franke	D 10	-2063-
Mitarbeiterinnen:	Eva-Maria Reupke	D 11	-2045-
	Irene Heinsohn	D 12	-2047-

D 1: Allgemeine Verwaltungsangelegenheiten
Tätigkeitsberichte
Konferenz der Datenschutzbeauftragten
Öffentlichkeitsarbeit
Geheimschutzangelegenheiten

D 10: Systemverwaltung
Bibliothek
Register nach § 24 HmbDSG
Bearbeitung von Eingaben

D 11: Vorzimmerdienst
Textverarbeitung
Eingabenverwaltung

D 12: PC-Textverarbeitung
Registratur
Postverteilung
Verwaltung von Senats-/Bürgerschaftsdrucksachen

D 2 - Referat

			Durchwahl
Leiter:	Matthias Burba	D 2-1	-2046-
	Ulrich Werner	D 2-2	-2581-
Sachbearbeiter:	Detlef Malessa	D 21	-2223-

D 2-1: Grundsatzfragen des Datenschutzes
Novellierung der Datenschutzgesetze
Verfassungsschutz
Justizverwaltung
Staatsanwaltschaft
Strafvollzug
Ausbildungsleiter für die Juristenausbildung

D 2-2: Polizei und Feuerwehr
Meldewesen
Ausländerwesen
Personenstandswesen
Straßenverkehrsverwaltung
Verkehrsordnungswidrigkeiten

D 21: Bau-, Vermessungs- und Wohnungswesen
Eingabenbearbeitung im Referatsbereich ohne Polizei, Justizverwaltung und Staatsanwaltschaft

D 3 - Referat

			Durchwahl
Leiter:	Peter Schaar	D 3	-2231-
Referent:	Uwe Schläger	D 30	-2564-
Referent:	Ulrich Kühn	D 31	-2564-
Sachbearbeiter:	Dietmar Nadler	D 32	-2236-

D 3: Telekommunikation
Online-Datenbanken
technische Assistenz für die Bereiche
— Polizei/Meldewesen
— Verfassungsschutz
— Justiz
— Wissenschaft und Forschung
— Kultur
datenschutzrechtliche Betreuung der Bereiche
— Statistik
— Wahlen
— Medien
— Umweltschutz

D 30: LAN
MS-DOS
Host-PC-Kopplung
Electronic-Cash
technische Assistenz für die Bereiche
— Sozialwesen/PROSA
— Gesundheitswesen
— Archivwesen
datenschutzrechtliche Betreuung des Bereichs Stadtentwicklung

D 31: Überwachungstechniken
UNIX
technische Assistenz für die Bereiche
— Schulwesen
— Wirtschaft

D 32: Richtlinien zur Datensicherung und Datenverarbeitung
IuK-Gesamtplan
Speichertechnik
BS 2000
MVS
technische Assistenz für die Bereiche
— Bauwesen
— Personalwesen
datenschutzrechtliche Betreuung der Bereiche
— Finanzen
— Organisation
— Bürgerschaft

D 4 – Referat

			Durchwahl
Leiter:	Dr. Hans-Joachim Menzel	D 4	–2558–
Sachbearbeiter:	Achim Kruppke	D 41	–2563–

D 4: Gesundheitswesen mit medizinischer Forschung
(öffentlicher und nicht-öffentlicher Bereich)
Kultur

D 41: Arbeits- und Sozialwesen

D 5 – Referat

			Durchwahl
Leiter:	Matthias Kock	D 5	–2562–
Sachbearbeiter:	Achim Kruppke	D 51	–2563–

D 5: Arbeitnehmer-Datenschutz
(öffentlicher und nicht-öffentlicher Bereich)
Archivwesen
Wirtschaft und Landwirtschaft
Wissenschaft und Forschung

D 51: Schulwesen

D 6 – Referat

			Durchwahl
Leiterinnen:	Helga Naujok	D 6-1	–2556–
	Elisabeth Duhr	D 6-2	–2541–
Sachbearbeiterin:	Evelyn Seiffert	D 61	–2468–

Aufsichtsbehörde nach § 38 Bundesdatenschutzgesetz

D 6-1: Versicherungswirtschaft einschließlich Wahrnehmung des Vorsitzes im Arbeitskreis Versicherungswirtschaft
Bauen und Wohnen, insbesondere Mietangelegenheiten
Transport und Verkehr einschließlich HVV
Handel, Industrie, gewerbliche Dienstleistungen und freie Berufe

D 6-2: Auskunfteien, Wirtschafts- und Handelsauskunfteien
SCHUFA
Markt- und Meinungsforschung
Kreditwirtschaft
Versandhandel
Werbung
Adreßhandel
Datenbankbetreiber, Mailboxen und Netzanbieter
Grenzüberschreitender Datenverkehr im öffentlichen und nicht-öffentlichen Bereich, insbesondere Datenschutz der Europäischen Gemeinschaften

D 61: Beratung und Betreuung von Unternehmen, Vereinen, Verbänden usw. insbesondere bei der Auftragsdatenverarbeitung, dem Bildschirmtext und der sonstigen Datenverarbeitung
Beratung von Bürgern und Bearbeitung von Eingaben insbesondere bei sonstigen Datenschutzangelegenheiten im nicht-öffentlichen Bereich

Stichwortverzeichnis

Abfallwirtschaftliche Planung ... 5.5
Abgabenordnung (AO) ... 10.1
Abhören von Wohnungen ... 1., 19.1
Abteilungsrechner ... 3.9
Abwasserdaten ... 5.3
Aktendatenschutz ... 1.6.1, 30.
Akteneinsicht ... 5.2, 6.7.1, 7.3, 9.1, 30.1
Aktenvorlageersuchen ... 12.5
Allfinanz-Konzepte ... 1.2, 25., 25.3
Amts- und Berufsgeheimnisse ... 10.1
Andere Personen ... 17.2.3
Anfrageberechtigung ... 23.1
Anhaltemeldungen ... 17.5
Anmeldefehlversuche ... 3.5
Anrufbeantworter ... 4.5
Ansteckungsgefahr (PHW) ... 17.2.4
Anwendungsbereich des HmbDSG ... 1.4.1
Arbeitsdatei Innere Sicherheit (APIS) ... 17.2.3
Arbeitsdateien ... 17.2.1
Arbeitslosigkeit ... 6.2
AZR-Nummer ... 15.1.1
ärztliche Schweigepflicht ... 10.4, 21.10, 21.11
Aufenthaltsgenehmigung ... 15.1.1
Aufsichtsbehörde ... 1.6.2
Auftragsdatenverarbeitung ... 3.2.3
Aufzeichnung des gesprochenen Wortes ... 17.7, 19.1
Ausbau von Festplatten ... 3.6
Auskunft ... 19.4
Auskunftspflicht ... 6.10
Auskunftsrecht ... 18.1
Auskunftsverweigerungsrecht ... 10.1
Ausländerzentralregister (AZR) ... 15.1.1
Auslandsvertragsmodell ... 23.3
Auszubildende ... 29.2
Auswahlentscheidungen ... 18.3
Automation des Meldewesens ... 13.2
Automationsvorhaben siehe Projekte
automatisierte Datenverarbeitung ... 1.1, 3.
automatisiertes Melderegister ... 13.1
Automatisierung Verfassungsschutz ... 18.3

Baugenehmigungsverfahren ... 12.4
Beamtengesetz ... 7.2
Beanstandungen ... 1.9.7
Beihilfe ... 21.7
Benutzerkennungen ... 3.5
Benutzerprofile ... 4.6.1, 4.6.2

Berufsordnung Hamburger Ärzte ... 21.8, 21.10, 21.11
Berufsschulen ... 29.2
Beschäftigte ... 18.2
Beschäftigtendaten ... 1.2, 7.2
Beschlagnahme von Patientenkartei ... 10.4
Beteiligung des HmbDSB ... 1.1, 19.3
Betriebspraktika von Schülern ... 9.3
Betriebsprüfungsdienst ... 10.2
Betriebssystem SINIX ... 3.9
Betriebssystem UNIX ... 3.9
Betriebssystemebene (shell) ... 3.9
Bewerber ... 7.4, 7.8
Bewerberauswahl ... 29.1
Bezirksversammlung ... 6.7.1
Bildaufnahmen ... 19.1
Bildschirmtext-Staatsvertrag ... 4.6.1
Bodendaten ... 5.4
Bulletin Board Systems (BBS) ... 4.6.1
Bundesdatenschutzgesetz, Auswirkungen ... 1.6
Bundeskriminalamt (BKA) ... 17.2.1, 17.2.2
Bundeszentralregister ... 15.2
Bürgernähe ... 1.8
Bürgerschaft ... 1.4.3, 1.9.2, 1.9.5, 6.7.2, 12.5
bürgerschaftliche Anfragen ... 1.9

Datenerhebung beim Betroffenen ... 16.1
Datenerhebung durch verdeckte technische Mittel ... 1.2, 17.7
Datenerhebung in Wohnungen ... 1., 17.7, 19.1
Datenlöschung ... 3.6
datenschutzrechtliche Verantwortung ... 13.2, 17.2.1
Datenträgerkontrolle ... 4.2
Datenträgervernichtung ... 3.6
Datenübermittlung ... 19.4
Datenübermittlungen ins Ausland ... 25.6
Datenübertragungsdienst nach X.25 ... 4.4
Datenverarbeitungszentrale (DVZ) ... 3.2.1, 3.8
Datex-P ... 4.4
defekte Festplatten ... 3.6
Demonstrationen ... 17.6, 17.8
Deputierte ... 6.7.1
Dienstanweisungen ... 3.9, 14., 19.5, 21.3
Dienstanweisung für Standesbeamte ... 14.
Dienstvorschrift zum Sozialdatenschutz ... 6.4
Digitalisierung des Behördennetzes ... 3.1.3, 4.3
Drogenkriminalität ... 17.4.3

EG-Datenschutz-Richtlinie (Entwurf) ... 1.7
EG-Richtlinie über den freien Zugang zu Umweltinformationen ... 5.1

eidesstattliche Versicherung 19.4
Eignungsuntersuchung 7.3
Eingaben 1.8.1
Einwilligung 12.3, 21.10, 21.11, 23.2, 25.2, 25.3, 29.1
Einwohnerzentralamt 13.1
Electronic-cash 27.1
Elektronikschrottverordnung 3.6
Elektronische Post 4.6.1
Entsorgung von Datenträgern 3.6
Erkennungsdienst und Daktyloskopie 17.2.1
erkennungsdienstliche (ed-) Behandlung 16.1

Fachbehörden (Zuständigkeit bei IuK-Verfahren) 3.2.3
Fachbereich Informatik 4.2
Falldateien 17.2.1
Fangschaltungsbeschluß des Bundesverfassungsgerichts 1.,4.1
Fehlbelegungsabgabe-Verfahren 12.2
Fehlsubventionierung 12.2.2
Fernmeldegeheimnis 4.1, 4.6.1
Fernsteuerungsprogramme 3.4
Fernwartung 1.2, 3.3, 21.3.2
Flächenbezogenes Informationssystem 12.1
Finanzamtsvorsteher 10.3
Fragerecht des Arbeitgebers 29.1
Frauenanteil ..... 2.
Freedom of Information 1.3, 5.1
Freigaberichtlinie 3.9
Freitodgefahr (PHW) 17.2.4

Gebrauchssteuerung der Datenverarbeitung 4.3
Gebührendaten ..... 4.2, 4.6.
Gebührenrechner in TK-Anlagen 4.2
Gefahrenabwehr 17.4.3, 17.7, 17.8, 18.1, 19.1
Gemeinsame Datenverarbeitungsstelle der Krankenversicherung Hamburg (GDKV) 21.6
Gemeinschaftspraxen 21.8. 21.10
Gerichte 1.9.8
Gesetz über das Bundeskriminalamt (BKA-Gesetz) 17.2.1
Gesetz über die Datenverarbeitung der Polizei (PolDVG) 17.7, 19.1
Gesetz zur Bekämpfung der organisierten Kriminalität 17.7, 19.1
Gesetzesvorbehalt 4.1
Gesundheitsberichterstattung 21.4
Gesundheitsdaten ..... 1.2, 7.8, 21.
Gesundheits-Strukturgesetz 6.1, 21.2
Gesundheitswesen (Gesetz) 1.5.2
gläserner Mitarbeiter 3.4
Glasfaser-Backbone 4.3
Großkundenabonnement 7.7
Grundrecht auf Datenschutz 1.3

Grundrecht auf Unverletzlichkeit der Wohnung 1., 1.3. 19
Gruppenversicherungsverträge 25.5

Hacking in Sprachinformationssystemen 4.5
Haftdatei 17.2.1
Hamburg Handbuch 7.6
Hamburger Verkehrsverbund 7.7
Hamburgisches Abwassergesetz (Entwurf) 5.3
Hamburgisches Archivgesetz 1.5.1
Hamburgisches Behördennetz 4.3
Hamburgisches Bodenschutzgesetz (Entwurf) 5.4
Hamburgisches Datenschutzgesetz (Novellierung) 1.1, 1.4
Hamburgisches Meldegesetz 1.5.2
Hamburgisches Statistikgesetz 1.5.1. 8
Hamburgisches Verfassungsschutzgesetz (Entwurf) 1.5.2. 16.1
Hamburgisches Vermessungsgesetz (Entwurf) 1.5.2. 12.1. 12.4
Handelskammer Hamburg 29.2
Handels- und Wirtschaftsauskunfteien ..... 26.
Hochschule für bildende Künste 11.1.2
Hospitationen von Schülern 9.3
HuK-Verband 17.2.2

Identitätsfeststellung 16.1
Informationsanspruch nach dem UIG 5.2.2
Informationsfreiheit 1.3
Informationssystem der Polizei (INPOL) 15.2, 17.2.1. 17.2.2, 17.3, 17.7
Informationszugangsrecht zu Umweltinformationen 5.1, 5.2, 5.3
Infrastrukturansatz 3.1.2
Innenministerkonferenz 17.2.1, 17.2.3. 17.2.4
Interessentenwerbung 22.2
IuK-Drucksache 3.1.1
IuK-Infrastruktur 3.1
IuK-Plan 3.2.2, 13.2
IuK-Politik des Hamburger Senats 3.1.1
IuK-Technik ..... 3.

Jugendliche mit Datenschutzrechten 1.4.2
Justizmitteilungsgesetz 19.2

Kammerbeitrag für Ärzte 21.9
Kfz-Diebstahl 17.2.2, 17.4.3
Kfz-Haftpflicht-Versicherung 25.4.2
Kfz-Kennzeichen 17.7
Kfz-Sachfahndung 17.2.2
Kinder in polizeilichen Dateien 17.4
Kommunikationsnetze 3.1.3
Konkurs 19.4

Kontakt- und Begleitpersonen ... 17.2.3
Kontrollbefugnisse der Landesdatenschutzbeauftragten ... 10.1
Kontrollmitteilungen ... 10.1
Kontrollrechte nach dem BDSG ... 1.6.2
Kontrollzuständigkeit bei den Gerichten ... 1.9.8
Kontrollzuständigkeit bei freiem Träger ... 6.8
Krankenversicherungskarte ... 21.2
Kreditschutz-Vereinigung (KSV) ... 24.2
Kriminalakten ... 17.4.2
Kriminalaktennachweis ... 17.2.1
Kriminelle Vereinigung ... 17.7
Kundenwerbung ... 25.3

Ladendiebstahl ... 17.4.3
Landesamt für Informationstechnik (LIT) ... 3.2.1
Landesbetrieb Stadtreinigung ... 5.5
Landesmedienanstalten ... 4.6.2
Landesversicherungsanstalt ... 7.5
Längerfristige Observation ... 17.7
Lastschriftverfahren ... 27.2
Lauschangriff ... 1., 19.1
Lebens-, Unfall- und Krankenversicherung ... 25.4.3
Leitstelle Meldewesen ... 13.1
Liegenschaftskataster ... 12.1, 12.4
LIT ... 3.2.1
Lokale Netze (LAN) ... 4.3
Löschung von Festplatten ... 3.6
Löschungsvorschriften für Videoaufnahmen ... 17.8

Mailbox-Systeme ... 4.6.1
Match-Code-Verfahren ... 25.1
Medienprivileg ... 4.6.1
medizinische Risikofaktoren ... 7.3
Medizinischer Dienst ... 21.6
Meldepflicht nach BDSG ... 28.
Melderegister ... 11.2, 13.1
Melderegisterauskunft ... 13.1
Melderegisterzugriff der Polizei ... 17.3
Meldeverfahren der Kfz-Versicherer ... 25.1
Merkblatt bei Allfinanz ... 25.3
Message Handling Systems (MHS) ... 4.6.1
Mietenausgleichszentrale (MAZ) ... 12.2.1
Mietenspiegel ... 12.3
Mieterdatenschutz ... 30.2
Mietpreisüberhöhungen ... 6.9
Mikrophone ... 19.1
Mikroverfilmung ... 16.2
Ministerium für Staatssicherheit (Stasi) ... 7.4
Mitarbeiterkontrolle ... 3.4

Mitgliederlisten von Parteien ... 30.2
Mitwirkungspflicht bei Sozialleistungen ... 6.6, 6.10
Modernisierung der Verwaltung ... 3.1.1

nachrichtendienstliche Mittel ... 18.1
Netzwerkdiagnoseprogramme ... 3.4
Neue Medien ... 4.
NS-Zeit ... 11.2

Oberfinanzdirektion ... 10.3
Observation ... 17.7
Öffentlichkeitsarbeit ... 1.8.2
Ordnungsmäßigkeit der Datenverarbeitung ... 4.2
Ordnungswidrigkeitengesetz ... 16.1
Organisationskontrolle ... 3.9
organisierte Kriminalität ... 19.1
OrgKG und Lauschangriff ... 19.1

Parlamentarischer Untersuchungsausschuß ... 12.5
Paßfoto ... 16.1
Paßnummer ... 15.1.1
Paßwörter ... 3.5, 3.8
Paßwortrichtlinie ... 3.8
Patientendaten ... 10.4, 21.
Personalakte ... 7.2
Personalärztlicher Dienst ... 7.3
Personalausweisfoto ... 16.1
Personalausweisgesetz ... 16.1
Personalausweisregister ... 16.1, 16.2
Personalinformationssystem ... 7.1
Personalräte ... 1.9
Personen- und Sachfahndung ... 17.2.1
Personenbezogene Hinweise (PHW) ... 17.2.4
Personenkennzeichen ... 15.1.1
Personenschutzsender ... 17.7, 19.1
Personenstandsgesetz ... 14.
Pflegeheime ... 6.5
Phonetisches Strukturcode-Verfahren ... 25.1
PHW Ansteckungsgefahr ... 17.2.4
PHW Freitodgefahr ... 17.2.4
PIOS-Dateien ... 17.2.1, 17.3
Polizeiliche Beobachtung ... 17.7.
polizeiliche Erkenntnisdaten ... 17.1.2
polizeiliche Vorgangsdaten ... 17.1.1
polizeiliche Zentralstelle ... 17.2.1
polizeilicher Abgleichsdatenbestand ... 17.1.2
polizeiliches Auskunftsystem (POLAS) ... 17.3
Postkontrolle der Korrepondenz von Strafgefangenen ... 20.
Postwurfsendungen ... 22.1

private PC ... 1.2, 3.7, 9.2, 10.2, 17.1.1, 19.5, 20.4, 21.1
Prognose für polizeiliche Speicherung ... 17.4.2
Prognoseentscheidung ... 17.8
Projekt Automation Standesämter (PASTA) ... 14.
Projekt Bauaufsicht mit Computerunterstützung (BACom) ... 12.4
Projekt Computerunterstützte Vorgangsbearbeitung bei der Polizei (COMVOR) ... 1.9.6, 17.1
Projekt Jugendamts-Automation (PROJUGA) ... 6.3
Projekt Personalwesen (PROPERS) ... 1.1, 1.9.6, 7.1
Projekt Qualitätssicherung in der Chirurgie (Quasic) ... 21.5.1
Projekt Qualitätssicherung Geburtshilfe ... 21.5.2
Projekt Sozialhilfe-Automation (PROSA) ... 1.1, 1.9.6, 6.2
Prostituierte in polizeilichen Dateien ... 17.5
Protokollierung ... 19.4, 19.5, 21.3.2
Psycho-Tests bei Bewerbern ... 29.1

Qualitätssicherung im Krankenhaus ... 21.1, 21.5

Rasterfahndung ... 17.7, 19.1
Rationalisierung durch Einsatz von DV-Technik ... 3.1.1, 13.2
Rechte der Betroffenen bei ec-cash ... 27.3
Referatsarbeitskartei (RAK) ... 18.3
Registereinsicht ... 18.1
Registerfunktion ... 16.2
Reise-Rücktrittskosten-Versicherung ... 25.4.1
Remote-Control-Software ... 3.4
Rentenversicherung ... 7.5
Risikoanalysen ... 1.1

Sachakten beim Staatsschutz ... 17.6
SAGA ... 12.5
Satellitenkommunikation ... 4.6
SCHUFA ... 23.
Schulärztliche Untersuchung ... 9.1
Schuldfähigkeit ... 17.4.2
Schuldnerverzeichnis ... 19.4, 25.
Schülerdaten ... 9.2
Schulgesetz ... 1.5.2, 9.1
Schweigepflicht-Entbindungserklärung ... 6.6, 21.10, 21.11, 25., 25.4
Schwerpunkte des Datenschutzes ... 1.1, 1.2
Scientology Kirche Hamburg e.V. ... 30.1
Selbstauskunft ... 30.2
Senatsamt für den Verwaltungsdienst ... 3.2.2, 3.9
Serienstraftaten ... 17.4.3
Shell-Berechtigung bei UNIX-Systemen ... 3.9
Sicherheitsmängel bei PC ... 19.5
Sicherheitsüberprüfung von Beschäftigten ... 18.2

Sozialdatenpool ... 6.1
Sozialdienststellen ... 21.7
Sozialgesetzbuch ... 6.1
Sozialhilfe ... 6.2
Speicherfristen ... 15.2
Speicherfristen für APIS ... 17.2.3
Speicherfristen für Kinder ... 17.4.1
Spontanversammlung ... 17.8
Sprachinformationssysteme ... 4.5
Spurendokumentationsdateien (SPUDOK) ... 17.2.1
Staatsangehörigkeit ... 6.2
Staatsanwaltschaft ... 19.5
Staatsarchiv ... 1.5.1
Staatsschutzabteilung des Landeskriminalamtes ... 17.6
Stadtreinigung ... 5.6
Standardpaßworte ... 3.5
Standesamt ... 14.
Standleitungen ... 4.4
Stasi, Ministerium für Staatssicherheit ... 7.4
Statistik ... 6.2, 8.
Steuerfahndung ... 10.1, 10.4
Steuergeheimnis ... 10.1
Stichprobenkontrollen bei Auskunfteien ... 26.2
Stichprobenkontrollen bei SCHUFA-Anfragen ... 23.1
Strafprozeßordnung ... 16.1, 17.7, 17.8, 19.1
Straftaten von erheblicher Bedeutung ... 17.2.3, 17.7, 17.8
Strafunmündige in polizeilichen Daten ... 17.4.1
Strafverfolgung ... 17.4.3, 17.7, 17.8, 19.1
Studenten ... 11.1.1
Studienplatzbewerber ... 11.1.2
Superuser-Status (UNIX) ... 3.9
Systemadministration (UNIX) ... 3.9
Systementscheidung ... 18.3

Technikfolgenabschätzung ... 3.2.1
Technische Mittel zur Datenerhebung ... 17.7, 19.1
Teledienstunternehmen-Datenschutzverordnung (UDSV) ... 4.1
Telefon-Fangschaltungen ... 1., 4.1
Telekom-Datenschutzverordnung (TDSV) ... 4.1, 4.6.1
Telekommunikationsanlage des Fachbereichs Informatik ... 4.2
Telekommunikationsdienste ... 4.6.1
Telekommunikationsnetz der Hamburger Verwaltung ... 4.3, 4.4
Transportkontrolle ... 4.2

Übermittlung an private Stellen ... 17.2.2
Überwachung der Benutzer ... 3.4
Überwachung der Datenübertragung ... 3.4

U-Man International Hamburg ... 29.1
Umweltinformationen ... 5.1, 5.2
Umweltinformationsgesetz (UIG) ... 5.2
unbefugte Offenbarung ... 10.3
Universität Hamburg ... 4.2, 7.5
UNIX-Anlagen beim Schuldnerverzeichnis des Amtsgerichts ... 19.4
UNIX-Anlagen im Landesbetrieb Krankenhäuser ... 21.3.2
UNIX-Anlagen im Senatsamt für den Verwaltungsdienst ... 3.9
Unterausschuß Datenschutz ... 1.9.2
Unterrichtung des HmbDSB ... 1.1, 21.1
Untersuchungsausschuß ... 12.5
Unverletzlichkeit der Wohnung ... 19.1
unwiderrufliche Löschung ... 3.6

V-Leute ... 17.7
Verbindungsdaten ... 4.1, 4.2
verdeckte Ermittler ... 17.7, 19.1
verdeckte Datenerhebung ... 17.7, 19.1
Verfassungsschutz ... 18., 18.2, 18.3
Verfassungsschutzgesetz ... 1.5.2, 18.1, 18.2
Verhaltens- und Leistungskontrolle ... 3.4
Verkauf von Arztpraxen ... 21.10
Verkehrsordnungswidrigkeiten ... 16.1
Verkehrszentralregister ... 16.1
Verletzung von Privatgeheimnissen ... 25.4.4
Vermessungsgesetz ... 1.5.2, 12.1, 12.4
Vermißte ... 17.4.3
Vermißtendatei ... 17.2.4
Veröffentlichung von Mitarbeiterdaten ... 7.6
Veröffentlichung von Sozialdaten ... 6.7.2
Verpflichtungsgesetz ... 9.3
Verrechnungsstellen, ärztliche ... 21.11
Versammlungsgesetz ... 17.8
Verschlüsselung ... 21.3.2
Versicherungsnummer ... 15.1.1
Versicherungswirtschaft ... 25.
Versorgungsamt ... 6.6
Vertragsmodell Auskunfteien ... 26.1
Verwaltungszusammenarbeit ... 1.9.8
Videoaufnahmen bei Versammlungen ... 17.8
Videodat ... 4.6.2
Videotext ... 4.6.2
Voice-Mailbox-Systeme ... 4.5
Volkszählungsurteil ... 11.1.1, 15.1.1, 19.2
Vorgezogener Datenschutz ... 1.1

Wanzen ... 19.1
Warn- und Hinweissysteme bei Versicherungen ... 25.
Wohnungsabhören ... 1., 19.1
Wohnungseinbruch ... 17.4.3

X.25 ... 4.4
X.400 ... 4.6.1

Zeichnungsvorbehalt ... 10.3
Zentrale Registrierstelle Rechtsschutz ... 25.1, 25.2
Zentrales Verkehrs-Informationssystem (ZEVIS) ... 17.3
Zentralstellenfunktion des BKA ... 17.2.1, 17.2.2
ZEVIS ... 17.3
Zeugnisverweigerungsrecht ... 10.4
Zielrufnummern ... 4.1, 4.2
Zugangsberechtigung über Paßwörter ... 3.5
Zugangsschutz ... 19.5
Zugriffskontrolle ... 3.9
Zusammenarbeit ... 1.9
Zuständigkeiten für die IuK-Technik ... 3.2
Zuwendungsgeber und -empfänger ... 7.9
Zweckbindung ... 18.1