BÜRGERSCHAFT
DER FREIEN UND HANSESTADT HAMBURG **Drucksache 13/1412**

13. Wahlperiode **16. 03. 88**

Der Hamburgische Datenschutzbeauftragte

An die
Frau Präsidentin der Bürgerschaft

Betr.: Sechster Tätigkeitsbericht
des Hamburgischen Datenschutzbeauftragten

Gemäß § 20 Absatz 2 Satz 2 des Hamburgischen Datenschutzgesetzes übersende ich der Bürgerschaft meinen sechsten Tätigkeitsbericht.*

Dem Senat leite ich meinen Tätigkeitsbericht gleichzeitig zu.

Schapper

* Verteilt nur an die Abgeordneten der Bürgerschaft

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

Anlage zur Drs
LC 13/1412

Der Hamburgische Datenschutzbeauftragte

6. Tätigkeitsbericht 1987

Sechster Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten

Zugleich Tätigkeitsbericht der Aufsichtsbehörde für den nicht-öffentlichen Bereich

vorgelegt zum 1. Januar 1988

Herausgegeben vom Hamburgischen Datenschutzbeauftragten
Claus Henning Schapper
Millerntorplatz 1 · 2000 Hamburg 4 · Tel.: 34 97 40 20

Druck: Lütcke & Wulff, Hamburg 1

GLIEDERUNG

		Seite
1.	**Zur Lage des Datenschutzes**	1
1.1	**Zum Stand der Gesetzgebung**	1
1.1.1	Novellierung des Bundesdatenschutzgesetzes	1
1.1.2	Die neuen Sicherheitsgesetze	4
1.1.3	Gesetz zur Strukturreform im Gesundheitswesen	8
1.1.4	Die Lage in Hamburg	9
1.2	**Volkszählung 1987**	9
1.3	**Verhältnis zur Verwaltung**	10
2.	**Entwicklung der Dienststelle**	12
2.1	**Ausstattung**	12
2.2	**Eingaben**	13
3.	**Beobachtung der automatisierten Datenverarbeitung**	13
3.1	**Kompromittierende Abstrahlung**	13
3.2	**Optische Speichertechnik**	14
3.3	**Schriftgutvernichtung**	18
3.4	**Umsetzung der ADV-Richtlinien bei zentralen ADV-Verfahren der FHH**	19
3.4.1	Gebäudevorerhebung	20
3.4.2	Personalamtsverfahren	24
3.5	**Verarbeitung personenbezogener Daten auf Personalcomputern (PC)**	26
3.5.1	Spezifische Risiken des PC-Einsatzes	26
3.5.2	Zuständigkeit für die Sicherstellung des Datenschutzes gem. § 16 HmbDSG	27
3.5.3	„Vorläufige Hinweise" des Senatsamtes für den Verwaltungsdienst — Organisationsamt —	27
3.6	**TEMEX**	28
4.	**Einzelne Probleme des Datenschutzes im öffentlichen Bereich**	30
4.1	**Sozialwesen**	30
4.1.1	Räumliche Verhältnisse und namentlicher Aufruf in den Sozialdienststellen der Bezirksämter	31
4.1.2	Amtsvormundschaft und Amtspflegschaft bei nichtehelichen Kindern	32
4.1.3	Durchführung des Unterhaltsvorschußgesetzes	33
4.1.4	Offenbarung von Sozialdaten auf Aufenthaltsgestattungen für Asylbewerber	33
4.1.5	Einmalige Leistungen gem. § 21 BSHG	34
4.1.6	Offenbarung von Sozialdaten auf Überweisungsträgern	34
4.1.7	Vordrucke	35
4.2	**Personalwesen**	36
4.2.1	Führung und Verwaltung von Personalakten	36
4.2.2	Bewerberfragebogen und Führungszeugnis	37
4.2.3	Personalstrukturdatei	38
4.2.4	Ortszuschlag	39
4.2.5	Persönlichkeitstest bei Bewerbern für den Strafvollzugsdienst	40
4.2.6	Lehrerindividualdatei	41

4.3	**Statistik**	43
4.3.1	Landesstatistikgesetz	43
4.3.2	Hochschulstatistik	43
4.3.2.1	Stand der Gesetzgebung	43
4.3.2.2	Verlaufsstatistik	44
4.3.2.3	Erhebung der Statistikdaten an den Hamburger Hochschulen	44
4.3.3	Jugendhilfestatistik	46
4.3.3.1	Rechtsgrundlage	46
4.3.3.2	Durchführung der Erhebung	47
4.4	**Volkszählung 1987**	48
4.4.1	Beurteilung des bisherigen Ablaufs der Zählung	48
4.4.2	Unzureichende Beteiligung	50
4.4.3	Verarbeitung von Volkszählungsdaten	51
4.4.3.1	Unvollständiges Datenverarbeitungskonzept	51
4.4.3.2	Unzureichendes Freigabeverfahren	52
4.4.3.3	Zeitpunkt und Verfahren der Trennung von Hilfs- und Erhebungsmerkmalen	53
4.4.3.4	Speicherung der Arbeitsstättenanschrift	55
4.4.3.5	Reidentifizierbarkeit von Daten	56
4.4.4	Einzelprobleme bei der Durchführung der Volkszählung	56
4.4.4.1	Zählerauswahl und -bestellung	56
4.4.4.2	Durchführung der Erhebung in Einrichtungen und Anstalten	58
4.4.4.3	Datenübermittlungen von der und an die Meldebehörde	59
4.4.4.4	Beschwerden über den Zählereinsatz und das Zählerverhalten	62
4.4.4.5	Erinnerungs- und Mahnverfahren	63
4.4.4.6	Wiederholungsbefragung	64
4.5	**Archivwesen**	66
4.6	**Gewerbewesen — Automation des Gewerberegisters**	67
4.6.1	Rechtsgrundlagen und gegenwärtige Praxis	67
4.6.2	Konzept einer Automatisierung des Gewerberegisters	67
4.6.3	Probleme des Datenschutzes	67
4.7	**Einsichtsrecht in Umweltakten**	69
4.8	**Bauwesen**	73
4.9	**Steuerwesen**	74
4.9.1	Steuerdaten-Abrufverordnung	74
4.9.2	Kontrollmitteilungsverordnung	75
4.9.3	Verwaltungsvorschriften zur Landeshaushaltsordnung	75
4.10	**Einwohnerwesen**	76
4.10.1	Paß- und Personalausweiswesen	76
4.10.1.1	Hamburgisches Personalausweisgesetz	76
4.10.1.2	Erste Erfahrungen mit dem maschinenlesbaren Personalausweis	77
4.10.2	Meldewesen	77
4.10.2.1	Maschineller Abgleich des kirchlichen und staatlichen Meldebestandes	77

4.11	**Polizei**	78
4.11.1	Übergangslösungen	78
4.11.2	Einsatz von Personalcomputern	81
4.11.3	Datenverarbeitung beim polizeilichen Staatsschutz	82
4.11.3.1	Datenschutzrechtliche Prüfung bei der Fachdirektion 7	82
4.11.3.2	Speicherung von Volkszählungsgegnern	86
4.11.3.3	Übermittlung polizeilicher Erkenntnisse an den Verfassungsschutz	86
4.11.4	Erfassung von Angehörigen arabischer Staaten	88
4.11.5	Personenfeststellungsverfahren	89
4.11.6	Aufarbeitung des „Hamburger Kessels" durch die Gerichte	90
4.11.7	Löschung von Daten über Suizidversuche	91
4.11.8	Polizei in der Zentralambulanz für Betrunkene (ZAB)	91
4.11.9	Personengebundene Hinweise (PHW)	91
4.12	**Verfassungsschutz**	93
4.12.1	Auskunftsrechte der Bürger	93
4.12.2	Speicherung von Volkszählungsgegnern	94
4.13	**Justiz**	94
4.13.1	Justizmitteilungsgesetz	95
4.13.2	Novellierung der Strafprozeßordnung	95
4.13.3	Neues Informationssystem der Staatsanwaltschaften	96
4.13.4	Einsicht in Gerichtsakten zu Forschungszwecken	96
4.13.5	Gerichtsakten zu Prüfungszwecken	97
4.13.6	Öffentliche Bekanntmachungen von Entmündigungen	97
4.13.7	Grundbuchämter	98
4.13.8	Schuldnerverzeichnis	99
4.14	**Strafvollzug**	100
4.14.1	Bereichsspezifische Rechtsgrundlagen	100
4.14.1.1	Strafvollzugsgesetz	100
4.14.1.2	Jugendstrafvollzugsgesetz	100
4.14.1.3	Untersuchungshaft	100
4.14.2	Eingaben	100
4.15	**AIDS**	101
4.15.1	AIDS in polizeilichen Informationssystemen	101
4.15.2	AIDS im Strafvollzug	104
4.15.3	Dateien der Blutspendedienste	104
4.15.4	AIDS-Test bei Bewerbern für den öffentlichen Dienst	104
4.15.5	Gesundheitsämter als AIDS-Beratungsstellen	104
4.15.6	Prävalenz-Studie über HIV-Infektionen bei Schwangeren	105
4.16	**Gesundheitswesen**	106
4.16.1	Krankenhaus	106
4.16.1.1	Entwurf eines hamburgischen Krankenhausgesetzes	106
4.16.1.2	Dienstanweisung über die Führung und Herausgabe von Krankenakten und Röntgenbildern	107

4.16.1.3 Auskunft an der Krankenhauspforte ... 107
4.16.1.4 Ergebnisse aus der Prüfung des AK Altona ... 108
4.16.1.5 Übermittlung von Patientendaten von den Krankenhäusern an Krankenkassen 108
4.16.2 Gesundheitsämter ... 109
4.16.2.1 Zentralkartei ... 110
4.16.2.2 Gutachterwesen ... 110
4.16.2.3 Medizinalkartei ... 111
4.16.2.4 Überwachung des BTM-Verkehrs, Suchterkennung ... 112
4.16.2.5 Geburts- und Todesbescheinigungen ... 112
4.16.2.6 Sozial- und Jugendpsychiatrischer Dienst ... 113
4.16.3 Entwurf eines hamburgischen Maßregelvollzugsgesetzes ... 114
4.16.4 Schweigepflichtentbindung im Verfahren nach dem Schwerbehindertengesetz 115
4.17 **Wissenschaft und Forschung** ... 116
4.17.1 UKE-Studien über gesundheitliche Folgeschäden durch Holzschutzmittel ... 116
4.18 **Schulwesen** ... 117
4.18.1 Bereichsspezifische Datenschutzbestimmungen im Schulgesetz ... 117
4.19 **Verkehrswesen** ... 117
4.19.1 ZEVIS-Fahrzeugregisterverordnung ... 117
4.19.2 Automation des Kraftfahrzeug-Zulassungswesens ... 118

5. Einzelne Probleme des Datenschutzes im nicht-öffentlichen Bereich ... 121
5.1 **Versandhandel** ... 121
5.1.1 Interne Bonitätsprüfung ... 121
5.1.2 Gespräch mit dem Bundesverband des Deutschen Versandhandels ... 122
5.1.2.1 Werbeaktionen des Versandhandels ... 122
5.1.2.2 Verhältnis des Versandhandels zur SCHUFA ... 123
5.2 **Kreditwirtschaft / SCHUFA** ... 123
5.2.1 Neues SCHUFA-Verfahren: Kartellrechtliche Entwicklung ... 123
5.2.2 Neues SCHUFA-Merkmal bei Rückständen nach Kündigung eines Kredits ... 126
5.2.3 Probleme der Selbstauskunft (Auskunft an den Betroffenen) ... 126
5.2.4 Verbreitungsverbot für SCHUFA-Daten bei nicht feststehender Identität ... 127
5.2.5 SCHUFA-Klausel bei Guthaben-Konten ... 128
5.3 **Automatisierung des Zahlungsverkehrs** ... 128
5.4 **Versicherungswirtschaft** ... 131
5.4.1 Zentrale Dateien der Versicherungsverbände ... 131
5.4.1.1 Sonderwagnisdatei der Lebensversicherer ... 131
5.4.1.2 Zentrale Registrierstelle Rechtsschutz ... 132
5.4.1.3 Meldeverfahren der Kraftfahrzeug-Versicherer ... 132
5.4.1.4 Meldeverfahren der Unfallversicherer ... 135
5.4.1.5 Sachschadendatei ... 136
5.4.2 Einwilligungsklausel nach dem BDSG ... 138
5.4.3 Schweigepflicht-Entbindungsklausel ... 140

5.4.4 Datenübermittlungen im Zusammenhang mit Vertrauensschadenversicherungen ... 142

5.4.5 Auskunftsstelle über den Versicherungsaußendienst e.V. (AVAD) ... 144

5.4.5.1 Stand der Automation ... 144

5.4.5.2 Auskünfte über Versicherungsmakler ... 145

5.5 **Handels- und Wirtschaftsauskunfteien** ... 145

5.5.1 Angebot von bonitätsgeprüften Adressen ... 145

5.5.2 Automation bei Auskunfteien ... 145

5.6 **Arbeitnehmer-Datenschutz** ... 146

5.6.1 Frage- und Auskunftsrechte des Arbeitnehmers ... 146

5.6.2 Auskünfte an und durch einen Branchenauskunftsdienst ... 147

5.6.3 Personaldatenverarbeitung und Rechte des Betriebsrates ... 149

5.7 **Sonstige Probleme** ... 150

5.7.1 Überwachungstätigkeit — Registermeldungen ... 150

5.7.2 Auskünfte von Fluggesellschaften an Dritte ... 151

Abkürzungsverzeichnis

ADV	=	Automatische Datenverarbeitung
APIS	=	Arbeitsdatei PIOS Innere Sicherheit
AVAD	=	Auskunftsstelle über den Versicherungsaußendienst e.V.
BAG	=	Bundesarbeitsgericht
BAföG	=	Bundesausbildungsförderungsgesetz
BAJS	=	Behörde für Arbeit, Jugend und Soziales
BaKred	=	Bundesaufsichtsamt für das Kreditwesen
BauGB	=	Baugesetzbuch
BAV	=	Bundesaufsichtsamt für das Versicherungswesen
BB	=	Betriebsberater
BBauG	=	Bundesbaugesetz
BBG	=	Bundesbeamtengesetz
bDSB	=	betrieblicher Datenschutzbeauftragter
BetrVG	=	Betriebsverfassungsgesetz
BDSG	=	Bundesdatenschutzgesetz
BfD	=	Bundesbeauftragter für den Datenschutz
BfI	=	Behörde für Inneres
BGB	=	Bürgerliches Gesetzbuch
BGBl	=	Bundesgesetzblatt
BGH	=	Bundesgerichtshof
BGS	=	Bundesgrenzschutz
BKA	=	Bundeskriminalamt
BKK	=	Betriebskrankenkasse
BND	=	Bundesnachrichtendienst
BSB	=	Behörde für Schule und Berufsbildung
BseuchG	=	Bundesseuchengesetz
BT	=	Bundestag
BTM	=	Betäubungsmittel
Btx	=	Bildschirmtext
BV	=	Berufsunfähigkeitsversicherung
BVerfG	=	Bundesverfassungsgericht
BVerfSchG	=	Bundesverfassungsschutzgesetz
BZRG	=	Bundeszentralregister
CR	=	Computer und Recht
DB	=	Der Betrieb
DRS	=	Drucksache

DS	=	Datenschutz
DSB	=	Datenschutzbeauftragter
DTV	=	Deutscher Transportversicherer-Verband
DV	=	Datenverarbeitung
DVO	=	Durchführungsverordnung
DVZ	=	Datenverarbeitungszentrale
EC-Karte	=	Eurocheque-Karte
EDV	=	Elektronische Datenverarbeitung
GDV	=	Gesamtverband der Versicherungswirtschaft
GewO	=	Gewerbeordnung
GG	=	Grundgesetz
GVBl	=	Gesetz- und Verordnungsblatt
HBauO	=	Hamburgische Bauordnung
HEW	=	Hamburgische Electricitäts-Werke GmbH
HGW	=	Hamburger Gaswerke GmbH
HHA	=	Hamburger Hochbahn AG
HmbBG	=	Hamburgisches Beamtengesetz
HmbDSB	=	Hamburgischer Datenschutzbeauftragter
HmbDSG	=	Hamburgisches Datenschutzgesetz
HmbPersVG	=	Hamburgisches Personalvertretungsgesetz
HmbSOG	=	Hamburgisches Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung
HmbVerfSchG	=	Hamburgisches Verfassungsschutzgesetz
HUK-Verband	=	Verband der Haftpflicht-, Unfall-, Auto- und Rechtsschutzversicherer e.V.
HVV	=	Hamburger Verkehrsverbund
HWW	=	Hamburger Wasserwerke GmbH
IMK	=	Konferenz der Innenminister
IuK	=	Information und Kommunikation
JVA	=	Justizvollzugsanstalt
KAN	=	Kriminalaktennachweis
KBA	=	Kraftfahrtbundesamt
KGSt	=	Kommunale Gemeinschaftsstelle für Verwaltungsvereinfachung
KpS	=	Kriminalpolizeiliche personenbezogene Sammlung
LDSG	=	Landesdatenschutzgesetz
LID	=	Lehrerindividualdatei
MAD	=	Militärischer Abschirmdienst

ME	=	Musterentwurf eines einheitlichen Polizeigesetzes des Bundes und der Länder
MiStra	=	Mitteilungen in Strafsachen
MittVw	=	Mitteilungen für die hamburgische Verwaltung
MiZi	=	Mitteilungen in Zivilsachen
NADIS	=	Nachrichtendienstliches Informationssystem
NJW	=	Neue Juristische Wochenschrift
NRW	=	Nordrhein-Westfalen
OECD	=	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OFD	=	Oberfinanzdirektion
OWiG	=	Ordnungswidrigkeitengesetz
PB	=	Polizeiliche Beobachtung
PC	=	Personal Computer
PIN	=	Identifizierungsnummer
PIOS	=	Inpol-Anwendungen Personen, Institutionen, Objekte und Sachen
PIS	=	Personalinformationsystem
POLAS	=	Polizeiliches Auskunftssystem
POS	=	Point of Sale
RVO	=	Reichsversicherungsordnung
RZ	=	Rechenzentrum
SCHUFA	=	Schutzgemeinschaft für allgemeine Kreditsicherung
SGB	=	Sozialgesetzbuch
SOG	=	s. HmbSOG
SPUDOK	=	Spurendokumentation
StGB	=	Strafgesetzbuch
StPO	=	Strafprozeßordnung
StV-Btx	=	Staatsvertrag über Bildschirmtext
StVG	=	Straßenverkehrsgesetz
StVollzG	=	Strafvollzugsgesetz
TB	=	Tätigkeitsbericht
TEMEX	=	Telemetry Exchange
VDVM	=	Verband der Versicherungsmakler
VE	=	Vorentwurf
VV	=	Verwaltungsvorschrift
VZ-Urteil	=	Volkszählungsurteil

WoBindG	=	Wohnungsbindungsgesetz
WRV	=	Weimarer Reichsverfassung
ZAG	=	Gesetz über die Zusammenarbeit der Dienste und der Polizei
ZAW	=	Zentralausschuß der Werbewirtschaft e.V.
ZEVIS	=	Zentrales Verkehrsinformations-System
ZKA	=	Zentraler Kreditausschuß
ZPO	=	Zivilprozeßordnung

Paragraphenangaben ohne Zusatz beziehen sich auf das
Hamburgische Datenschutzgesetz (HmbDSG)

1. Zur Lage des Datenschutzes

1.1 Zum Stand der Gesetzgebung

1.1.1 Novellierung des Bundesdatenschutzgesetzes

Am 1. Januar 1988 konnten wir ein Jubiläum feiern: Das Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz — BDSG) ist zehn Jahre alt geworden. Seit dem 1. Januar 1978 ist nicht mehr wie ehedem die Verarbeitung personenbezogener Daten immer dann erlaubt, wenn sie nicht — ausnahmsweise — verboten war; sie ist verboten, sofern sie nicht ausdrücklich erlaubt ist — nach dem Willen des Gesetzgebers gilt dies allerdings nur, wenn die Datenverarbeitung in Dateien erfolgt. Davon abgesehen sind die Erlaubnistatbestände des BDSG so allgemein gehalten und so weit gefaßt, daß sie die Datenverarbeitung in keiner Weise eingeschränkt haben und auch ihrer Ausdehnung — selbst wenn modernste Technik genutzt wird — nicht im Wege stehen. Übermittlungen beispielsweise sind von Behörde zu Behörde zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden oder der empfangenden Stelle liegenden Aufgaben erforderlich sind (§ 10 BDSG); an nicht öffentliche Stellen dürfen personenbezogene Daten ferner dann übermittelt werden, wenn der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden (§ 11 BDSG).

Nach heutigem Rechtsverständnis entsprechen die zitierten Vorschriften — wie noch manche andere — nicht den verfassungsrechtlichen Anforderungen. Das Bundesverfassungsgericht hat mit dem Volkszählungsurteil vom 15. 12. 1983 klargestellt, daß die Verwendung personenbezogener Daten auf den gesetzlich bestimmten Zweck begrenzt und daß ein — amtshilfefester — Schutz gegen Zweckentfremdung durch Weitergabe und Verwertungsverbote erforderlich ist. Das BVerfG hat darüber hinaus festgestellt, daß jeder das Recht hat, grundsätzlich selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen und daß Einschränkungen dieses (Grund-)rechts einer verfassungsmäßigen Grundlage, also eines Gesetzes bedürfen. Das Recht auf informationelle Selbstbestimmung ist bei jeder Erhebung und jeder weiteren Verwendung personenbezogener Daten zu beachten, und auch auf die Form der Verarbeitung kommt es nicht an.

Der Gesetzgeber hat also die Aufgabe, die vielen Mängel des Datenschutzgesetzes zu beseitigen und ebenso zahlreiche Gesetzeslücken zu schließen. Da das VZ-Urteil schon mehr als vier Jahre alt ist, sind viele Kritiker der Meinung, daß der vom BVerfG für solche Fälle gewährte Übergangsbonus mittlerweile verbraucht ist. Übereinstimmung dürfte aber darüber bestehen, daß die Übergangsfrist mit dem Ende dieser Wahlperiode des Bundestages abläuft.

Geht es nach dem Bundesinnenminister, wird es indessen tragfähige Grundlagen für die Informationstätigkeit des Staates und der Wirtschaftsunternehmen auch weiterhin nicht geben. Gemessen an den Grundsätzen des BVerfG, gemessen aber auch an den Notwendigkeiten, die sich aus der technischen Entwicklung der Informationsverarbeitung in den letzten zehn Jahren ergeben, und auch — soweit man hierauf noch etwas geben will — an den eigenen Erklärungen der Bundesregierung, sie wolle den Datenschutz im Interesse der Bürger verbessern und die Datenverarbeitung transparenter gestalten, verdient der Referentenentwurf für eine Novellierung des BDSG, den Minister Zimmermann kürzlich der Öffentlichkeit präsentiert hat, die Note Ungenügend. Verglichen mit dem Entwurf, den die Bundesregierung Anfang 1986 im Bundestag eingebracht und den nicht nur die Konferenz der Datenschutzbeauftragten heftig kritisiert hatte, enthält der neue Entwurf zwar einige elegantere Formulierungen, die die Lesbarkeit des Gesetzestextes erhöhen mögen, inhaltlich aber nur wenige Verbesserungen, ganz im Gegenteil eine Reihe von Erleichterungen für die Datenverarbeitung, die den Datenschutz nicht fördern.

Einzuwenden ist gegen den Entwurf vor allem:

— Es bleibt bei der Beschränkung auf die Datenverarbeitung in Dateien, die schon in der neuen Gesetzesbezeichnung zum Ausdruck kommt und den gesamten Entwurf prägt. Demgegenüber umfaßt das Recht auf informationelle Selbstbestimmung jeden Umgang mit personenbezogenen Daten. Die Einbeziehung der Datennutzung bleibt weitgehend wirkungslos, weil nur die Nutzung unmittelbar aus Dateien gewonnener Daten geregelt wird. Die zunehmende Verknüpfung von Akten-, Text- und Datenverarbeitung wird ebensowenig berücksichtigt wie z.B. neue Formen der Bildverarbeitung, etwa durch Videoaufzeichnungen. Im übrigen ist auch der neue Dateibegriff zu eng.

  Neue Vorschriften im Verwaltungsverfahrensgesetz, die die Verarbeitung personenbezogener Daten außerhalb von Dateien regeln, gleichen die Nachteile des auf Dateien bezogenen Anwendungsbereichs des BDSG nicht aus, zumal der Bundesbeauftragte für den Datenschutz ihre Einhaltung nur in sehr begrenztem Umfang kontrollieren darf. Außerdem sind vom Anwendungsbereich des Verwaltungsverfahrensgesetzes große und wichtige Verwaltungsbereiche und -tätigkeiten (z.B. Finanzverwaltung, Post, Strafverfolgung) ausgenommen. Auch im nicht-öffentlichen Bereich bleibt die Datenverarbeitung außerhalb von Dateien ungeregelt. Aber auch hier ist es dem Betroffenen nicht zu vermitteln, daß seine Daten, die in Akten aufbewahrt werden, nicht vom Gesetz geschützt sind, zumal, wenn der Empfänger die übermittelten Daten automatisiert weiterverarbeitet.

— Es bleibt dabei, daß die Datenerhebung nicht geregelt wird, obwohl gerade sie den Bürger unmittelbar belastet. Kein ausreichender Ersatz ist die Erhebungsvorschrift im Verwaltungsverfahrensgesetz, in der zudem die Verpflichtung der erhebenden Stelle, den Erhebungszweck ausdrücklich festzulegen, fehlt.

  Gerade im nicht-öffentlichen Bereich haben Datenerhebungen, z.B. Nachbarschafts- und Arbeitgeberbefragungen durch Auskunfteien oder die Beschaffung von Anschriften durch Versicherungen immer wieder zu Problemen geführt. Bisher haben sich die Aufsichtsbehörden häufig mit der Ansicht durchgesetzt, daß eine rechtswidrige Erhebung auch die anschließende Speicherung rechtswidrig mache. Diese Argumentation wird den Auskunfteien und Versicherungen aber kaum mehr entgegengehalten können, wenn der Gesetzgeber die Erhebung weiterhin nicht dem Gesetz unterwirft.

— Es bleibt bei der weitgehenden Ausklammerung „interner Dateien". Es ist aber verfassungsrechtlich bedenklich, die interne Datenverarbeitung von jeglicher Kontrolle durch die Betroffenen, die Datenschutzbeauftragten und die Aufsichtsbehörden freizustellen.

— Es bleibt dabei, daß die Homecomputer aus der Geltung des Bundesdatenschutzgesetzes schlicht herausgenommen werden sollen. Diese „Lösung" wird der vielschichtigen datenschutzrechtlichen Problematik nicht gerecht, die sich aus der rapiden Zunahme dieser Kleinrechner, ihrer vielfältigen Verwendungsmöglichkeiten und der damit verknüpften erheblichen Gefahren für die informationelle Selbstbestimmung ergeben. Immer häufiger werden private Kleinrechner auch für dienstliche Zwecke am Arbeitsplatz oder auch zu Hause oder sowohl für private als auch für dienstliche Zwecke genutzt.

— Die im Entwurf vorgesehene Herausnahme der den Kirchen zugeordneten caritativen und erzieherischen Einrichtungen würde dazu führen, daß der staatliche Gesetzgeber auf einem wichtigen Gebiet nicht hinnehmbare Datenschutzdefizite in Kauf nehmen würde. Auch wenn die Kirchen eigene Datenschutzbestimmungen erlassen haben, sie können verbindliche Wirkung gegenüber Dritten nicht entfalten, die ihre Einrichtungen zwar nutzen, der Kirche aber nicht angehören.

— Wie das geltende Gesetz läßt der Entwurf jede Datenverarbeitung zu, wenn die Einwilligung des Betroffenen vorliegt, ohne daß besondere Regelungen den Betroffe-

nen davor schützen, daß er durch soziale, wirtschaftliche und psychische Zwänge (etwa als Mieter, Patient oder Arbeitsuchender) in seiner Entscheidungsfreiheit unangemessen eingeschränkt wird.

— Mit einem Gefährdungshaftungstatbestand, der nur für die automatisierte Datenverarbeitung gilt und der voraussetzt, daß Daten verfälscht und zugleich datenschutzrechtliche Vorschriften verletzt worden sind, ist praktisch nichts anzufangen.

— Der zunehmende Ausbau von Datenverarbeitungsnetzen und der vermehrte Einsatz von Kleincomputern erfordern weitere gesetzliche Maßnahmen zur Gewährleistung der Transparenz und der Kontrollierbarkeit dieser Datenverarbeitungsformen. Die unveränderte Übernahme von § 6 und dessen Anlage vernachlässigt den Einfluß neuer Technologien auf die automatisierte Datenverarbeitung.

— Auch die Regelung für automatisierte Abrufverfahren weist erhebliche Mängel auf. Die inhaltlichen Anforderungen an die Zulassung solcher Verfahren müssen präzisiert werden. Die Risiken, die in der möglichen Selbstbedienung des Datenempfängers liegen, müssen zumindest durch wirksame Kontrollmechanismen gemindert werden. Im öffentlichen Bereich ist die Einführung von Online-Verfahren unter den Vorbehalt einer Rechtsvorschrift zu stellen.

— Der Katalog erlaubter Zweckänderungen ist zu weit; soweit zweckfremde Datenspeicherungen und -nutzungen zugelassen werden, müssen sie dem Betroffenen mitgeteilt oder in anderer Weise offengelegt werden. Das gilt vor allem für Datenübermittlungen, sofern damit eine Zweckänderung verbunden ist. Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, müssen von der Befugnis zur Zweckentfremdung ausgenommen bleiben.

— Die Übermittlungsvorschriften sind gegenüber dem Vorentwurf erheblich verschlechtert worden. Erfolgt eine Datenübermittlung an eine andere öffentliche Stelle auf deren Ersuchen, wird der übermittelnden Behörde nicht einmal die Prüfung auferlegt, ob das Ersuchen zu den Aufgaben des Empfängers gehört. Bei Übermittlungen an nicht-öffentliche Stellen soll genügen, daß „kein Grund zu der Annahme besteht, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat". Obwohl mit der Übermittlung an nicht-öffentliche Stellen in aller Regel eine Zweckänderung verbunden ist, soll ein so schwerwiegender Eingriff also schon dann zugelassen werden, wenn eine nur kursorische Prüfung eventuell entgegenstehender schutzwürdiger Interessen stattgefunden hat.

— Das Recht des Bürgers auf Auskunft über seine Daten muß Herkunft und Empfänger umfassen, auch wenn diese Informationen nicht in Dateien gespeichert sind. Das Auskunftsrecht darf ferner nicht dadurch geschmälert werden, daß Nachrichtendienste ohne Verpflichtung zur Interessenabwägung im Einzelfall und ohne Begründung die Auskunft verweigern dürfen.

— Die Kontrollbefugnis des Bundesbeauftragten für den Datenschutz (BfD) wird — gemessen auch an der gegenwärtigen Kontrollpraxis — insgesamt dadurch verschlechtert,

  - daß ihm eine Kontrolle der Einhaltung „anderer Vorschriften" über den Datenschutz bei einer Datenverarbeitung außerhalb von Dateien nur noch dann möglich ist, wenn durch eine Eingabe des Betroffenen oder auf andere Weise Anhaltspunkte für eine Rechtsverletzung vorliegen,
  - daß in solchen Fällen systematische Kontrollen des BfD entgegen der bisherigen Praxis ausgeschlossen sind, weil die Kontrolle auf den Einzelfall beschränkt wird,
  - daß die Formulierung, die Kontrolle der Behörden finde „unbeschadet ihrer fachlichen Beurteilung und Verantwortlichkeit" statt, von den kontrollierenden Stellen so verstanden werden könnte, als ob eine Datenverarbeitung künftig nicht mehr inhaltlich, z.B. nicht mehr auf ihre Erforderlichkeit, überprüft werden kann,

- daß die Datenerhebung selbst dann nicht mehr kontrollierbar ist, wenn sie zur Datenspeicherung führt, weil sie nicht mehr im BDSG geregelt wird und auch nicht als Datenverarbeitung oder -nutzung gilt,
- daß personenbezogene Daten durch besonderes Gesetz von der Kontrolle ausgenommen werden können, obwohl es nach dem Volkszählungsurteil keine kontrollfreien Räume geben darf,
- daß personenbezogene Daten, die bei Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses nach dem G 10 anfallen, der Datenschutzkontrolle grundsätzlich entzogen sind, obwohl das Bundesverfassungsgericht durch Beschluß vom 20. Juni 1984 die Kontrolle durch Datenschutzbeauftragte zur Voraussetzung für die Zulässigkeit solcher Maßnahmen erklärt hat.

— Unbefriedigend sind vor allem die Datenschutzvorschriften für den nicht-öffentlichen Bereich. Sie orientieren sich nicht am Grundsatz der Zweckbindung und räumen verfassungsrechtlich bedenkliche Verarbeitungsprivilegien ein.

- Datenübermittlungen werden — gegenüber dem geltenden Recht — in mehrfacher Hinsicht erleichtert. Besonders bedenklich ist die Regelung des Adreßhandels. Es kann nicht davon ausgegangen werden — wie der Entwurf es tut —, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Übermittlung nicht habe, wenn Vertragsdaten, beispielsweise aus einem Arbeitsverhältnis, für Zwecke der Werbung oder der Markt- oder Meinungsforschung übermittelt werden sollen. Die einseitige Vermutung zugunsten der Werbung oder der Markt- und Meinungsforschung sollte ersatzlos gestrichen werden. Auch mit der Widerspruchslösung ist nichts anzufangen, weil sie offen läßt, was getan werden muß, um dem Betroffenen in der Praxis die Ausübung dieses Rechtes zu ermöglichen.
- Der Empfänger übermittelter Daten muß strenger an den Übermittlungszweck gebunden werden. Zweckfremde Nutzungen dürfen nicht schon dann zulässig sein, wenn der Nutzer keinen Grund zur Annahme sieht, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Verarbeitung hat.
- Die Auskunft an den Betroffenen über seine Daten muß auch im nicht-öffentlichen Bereich den Speicherungszweck umfassen; gleiches gilt für die Benachrichtigung über die erstmalige Speicherung von Daten. Über Herkunft und Empfänger ist auch dann Auskunft zu erteilen, wenn diese Angaben nicht in Dateien gespeichert sind. Auf eine Benachrichtigung sollte nur dann verzichtet werden können, wenn die Kenntnis des Betroffenen durch einen ausdrücklichen Hinweis sichergestellt ist.
- Welche Regelungen erforderlich sind, um die vielfältigen Probleme bei der Direktwerbung zu lösen, habe ich in meinem 4. Tätigkeitsbericht auf den Seiten 164 und 165 ausgeführt. Ich halte diese Vorschläge nach wie vor für aktuell. Wichtig ist ferner, daß die Rechte der Betroffenen gegenüber den Auskunfteien gestärkt werden. Auch hierzu habe ich in meinem 4. Tätigkeitsbericht mehrere Anregungen gegeben (S. 164). Schließlich erinnere ich an die schon mehrfach erhobene Forderung nach bereichsspezifischen Regelungen für die Verarbeitung von Arbeitnehmerdaten (s. hierzu S. 162 und 163 meines 4. Tätigkeitsberichts).

1.1.2 Die neuen Sicherheitsgesetze

Außer dem Entwurf für eine Novellierung des BDSG hat der Bundesinnenminister zwei weitere Referentenentwürfe vorgelegt, deren einer vor allem die Informationstätigkeit des Bundesamtes für Verfassungsschutz und seine Zusammenarbeit mit den Landesämtern neu regeln will (Bundesverfassungsschutzgesetz — BVerfSchG), während der andere gesetzliche Grundlagen für den Informationsaustausch zwischen Polizeibehörden und Nachrichtendiensten schaffen will (Verfassungsschutzmitteilungsgesetz — VerfSchMiG). Letzterer tritt an die Stelle des vielgescholtenen ZAG-Entwurfs, der aber im Vergleich mit seinem Nachfolger als ein Ausbund an Rechtsstaatlichkeit erscheint.

Mit der Zielsetzung, nicht „leichtfertig Risiken für die innere Sicherheit entstehen" zu lassen und nicht „unverantwortlich die Arbeit der Polizei un der Nachrichtendienste einzuengen", verstoßen beide Entwürfe in massiver Weise gegen den Grundsatz der Verhältnismäßigkeit ebenso wie gegen das Zweckbindungsgebot. Der Bundesverfassungsschutzgesetz-Entwurf stellt ausdrücklich fest, daß bei der Erfüllung der Aufgaben des Bundesamtes für Verfassungsschutz die im BDSG bzw. im VerwVerfG vorgesehenen Regelungen über die Zweckbindung keine Anwendung finden sollen. Der Verfassungsschutzmitteilungsgesetz-Entwurf versucht nicht einmal den Anschein zu erwecken, als wolle er aus dem Trennungsgebot für die informationelle Zusammenarbeit zwischen Polizei und Verfassungsschutz die gebotenen Konsequenzen ziehen; im Gegenteil: Aus einem Prinzip der Machthemmung wird ein Instrument möglichst effektiver Zusammenarbeit entwickelt.

Beide Gesetzentwürfe verfolgen ganz unverhohlen das Ziel, die bisherige Praxis des Datenaustauschs insbesondere zwischen den Sicherheitsbehörden und der Datenverarbeitung beim Verfassungsschutz festzuschreiben oder gar auszuweiten, soweit es — vorgeblichen — Sicherheitsinteressen dienen könnte. Sämtliche Einschränkungen der von den Nachrichtendiensten heute in Anspruch genommenen Befugnisse, wie sie in den Vorentwürfen — wenn auch nur in rudimentärer Form — enthalten waren, sind aus den neuen Entwürfen herausgestrichen worden. Insbesondere der von den früheren Entwürfen unternommene, wenn auch im Ansatz steckengebliebene Versuch, Datenübermittlungen an die Nachrichtendienste auf Erkenntnisse aus den Bereichen Spionage und Terrorismus zu beschränken, wird unter Berufung auf die Koalitionsvereinbarung wieder aufgegeben, in der es heißt: „Terrorismus- und Spionagebekämpfung sowie die Abwehr verfassungsfeindlicher Bestrebungen sind gleich wichtig." Hatten die Datenschutzbeauftragten in ihrer Stellungnahme vom April 1986 zu dem Vorentwurf für eine Novellierung des Bundesverfassungsschutzgesetzes kritisch angemerkt, daß seine Vorschriften schon deshalb wesentlich präziser gefaßt werden müßten, weil die Arbeit des Verfassungsschutzes vorwiegend unter Ausschluß der Öffentlichkeit und der Kontrolle der betroffenen Bürger stattfinden, will der Bundesinnenminister mit den neuen Entwürfen umgekehrt eine „Normenflut" vermeiden: „Generalklauseln sind unverzichtbar."

Nun noch einige Bemerkungen zu einzelnen Vorschriften der beiden Entwürfe, die an die gegen die Vorentwürfe vorgebrachte Kritik anknüpfen (s. 4. TB, S. 76-88); zunächst zu dem BVerfSchGE:

— Auf die klarstellende, die Trennung im organisatorischen Sinne absichernde Bestimmung, daß das BfV einer polizeilichen Dienststelle nicht angegliedert werden darf, darf nicht verzichtet werden.

— Da sich der zulässige Umfang der Informationsverarbeitung maßgeblich nach den Aufgaben der datenverarbeitenden Stelle bemißt, bedarf es einer möglichst genauen gesetzlichen Beschreibung der Aufgaben des BfV. Die bisher verwendeten und nach den BVerfSchGE unverändert bleibenden Begriffe wie „Bestrebungen gegen die freiheitlich-demokratische Grundordnung" oder „Gefährdung auswärtiger Belange" sind unpräzise.

  Unklar bleibt weiterhin, unter welchen Voraussetzungen „beeinflußte" Organisationen beobachtet werden dürfen und wieweit hierbei die Beobachtung auf Einzelpersonen ausgedehnt werden darf. Für den einzelnen muß feststellbar sein, wann er die Schwelle von der Ausübung der Grundrechte zur verfassungsfeindlichen Bestrebung überschreitet.

— Die Mitwirkung der Verfassungsschutzbehörden an der Überprüfung von Personen durch andere Stellen muß im Verfassungsschutzgesetz abschließend geregelt werden. Sofern über die Sicherheitsüberprüfung hinaus eine Mitwirkung an anderen Verfahren wie etwa bei Einbürgerungen, Asylverfahren, Ordensverleihung oder der Überprüfung von Bewerbern für den öffentlichen Dienst für unabdingbar gehalten wird, sind diese im Gesetz ausdrücklich zu nennen.

— Der Informationsaustausch der Verfassungsschutzbehörden untereinander bedarf einer aufgabenbezogenen Einschränkung. Er ist nur zulässig, soweit Informationen für die jeweilige Aufgabenerfüllung der einzelnen Verfassungsschutzbehörden erforderlich sind. So dürfen beispielsweise die aus einer Telefonüberwachung gewonnenen Daten auch zwischen Verfassungsschutzbehörden nur unter den engen Voraussetzungen des § 7 Abs. 3 G 10 ausgetauscht werden.

— Es ist zu begrüßen, daß nunmehr einige nachrichtendienstliche Mittel beispielshalber im Gesetz aufgezählt werden. Darüber hinaus sollte aber — auch zum Zwecke der Datenschutzkontrolle — die interne Festlegung der zulässigen Mittel und die Dokumentation ihres Einsatzes im einzelnen vorgeschrieben werden. Ferner muß sichergestellt werden, daß angesichts der Schwere des mit der Anwendung nachrichtendienstlicher Mittel verbundenen Eingriffs in das Persönlichkeitsrecht sich ihr Einsatz grundsätzlich nur gegen konkret verdächtige Personen richten darf. Entsprechend den Regelungen über die Post- und Telefonüberwachung sind schließlich Verwertungsbeschränkungen und eine Verpflichtung zur nachträglichen Unterrichtung des Betroffenen vorzusehen.

— Die Streichung des im Vorentwurf enthaltenen Satzes, daß das BfV die Polizei auch nicht im Wege der Amtshilfe um Maßnahmen ersuchen darf, zu denen es selbst nicht befugt ist, verstärkt den Verdacht, daß insbesondere die Grenzpolizeibehörden gleichsam als verlängerter Arm des Verfassungsschutzes spezielle Informationen für deren Zwecke erheben sollen — ohne jegliche Notwendigkeit für die eigene Aufgabenerfüllung, wie es der heutigen Praxis entspricht. Den hiergegen vorgebrachten verfassungsrechtlichen Bedenken wird offenbar keine Beachtung geschenkt.

— Die Regelung über die Speicherung, Veränderung und sonstige Nutzung personenbezogener Daten darf nicht — wie vorgesehen — auf Dateien beschränkt bleiben, zumal bei den Verfassungsschutzbehörden ein Großteil der das Persönlichkeitsrecht der Bürger maßgeblich berührenden Daten in Akten geführt wird und komplexe Aktensammlungen bereits heute gezielt und mit Hilfe automatisierter Verfahren erschlossen werden können.

  Wenigstens bei der Beobachtung verfassungswidriger Bestrebungen ohne Gewaltbezug sollte die personenbezogene Speicherungsbefugnis davon abhängig gemacht werden, daß der Extremismusbezug in der Person des zu Speichernden vorliegt.

— Wie es der Vorentwurf noch vorgesehen hatte, sollten Daten über Minderjährige unter 16 Jahren überhaupt nicht — also auch nicht in nicht automatisierten Dateien — gespeichert werden dürfen.

— Die den Behörden des Bundes eingeräumte Befugnis, von sich aus dem Verfassungsschutz die ihnen bekannt gewordenen Informationen über Tatsachen zu übermitteln, deren Kenntnis für die Erfüllung seiner Aufgaben erforderlich erscheint, geht entschieden zu weit und birgt in dieser uneingeschränkten Form die Gefahr in sich, daß ein Klima allgemeiner Verdächtigungen entsteht. Auch vermag der Bürger, der in Kontakt mit einer Verwaltungsbehörde tritt, nicht zu erkennen, was diese wann und bei welcher Gelegenheit an die Verfassungsschutzbehörde übermittelt.

— Auch die für alle öffentlichen Stellen festgelegte Verpflichtung, dem Verfassungsschutz auf Ersuchen die zur Erfüllung seiner Aufgaben erforderlichen Auskünfte zu erteilen, geht nach wie vor zu weit. Ebensowenig hinnehmbar ist die weiterhin vorgesehene pauschale Ermächtigung der Verfassungsschutzbehörde, in alle amtlich geführten Register Einsicht zu nehmen.

— Angesichts des weitreichenden Auftrages der Verfassungsschutzbehörden zur Sammlung von Informationen bedürfen die dabei angefallenen personenbezogenen Erkenntnisse einer besonders strengen Abschottung nach außen. Dem trägt der Entwurf nicht hinreichend Rechnung, der es für eine Weiterleitung verfassungs-

schutzbehördlicher Erkenntnisse an andere öffentliche Stellen genügen läßt, daß die Daten dort für Zwecke der öffentlichen Sicherheit benötigt werden.

Die Übermittlung von Daten des Verfassungsschutzes an Dienststellen der Stationierungsstreitkräfte muß angesichts der unübersehbaren Folgewirkungen und wegen der fehlenden Geltung deutschen Datenschutzrechts an besonders enge Voraussetzungen geknüpft werden. Zumindest hat in jedem Fall eine Abwägung mit den schutzwürdigen Belangen des Betroffenen zu erfolgen.

Die Weitergabe von Erkenntnissen an private Stellen muß auf die Fälle der Sicherheitsüberprüfung und der Spionage- bzw. Terrorismusabwehr beschränkt werden.

— Die auf automatisierte Dateien beschränkte Verpflichtung, Errichtungsanordnungen zu erstellen, muß auf alle Datensammlungen ausgedehnt werden. Die Unterrichtung des Datenschutzbeauftragten vor Aufnahme des Dateibetriebes ist vorzusehen.

Zum Verständnis des Verfassungsschutzmitteilungsgesetzes muß zunächst noch einmal verdeutlicht werden, daß Ziel des — verfassungskräftigen — Trennungsgebotes nicht nur die rein organisatorische Schaffung zweier unterschiedlicher Behörden für Aufgaben der Polizei und des Verfassungsschutzes ist. Seine materiell-inhaltliche Bedeutung besteht vielmehr darin, daß durch die Verteilung polizeilicher Befugnisse auf die eine und nachrichtendienstlicher Befugnisse auf die andere der beiden Behörden auch eine Bündelung der mit diesen unterschiedlichen Befugnissen gewonnenen Informationen vermieden werden soll. Diese Zielsetzung einer Machthemmung darf bei der Regelung der informationellen Zusammenarbeit zwischen Polizei und Nachrichtendiensten nicht unterlaufen werden, sie muß sich vielmehr in einer grundsätzlich strengen Zweckbindung niederschlagen.

Demgegenüber verpflichtet das VerfSchMiGE die Polizeibehörden und die Nachrichtendienste, sich gegenseitig über alle Angelegenheiten des Verfassungs- und Staatsschutzes zu unterrichten. Nach der Gesetzesbegründung ist in dem Begriff des Verfassungsschutzes die Aufgabe des sog. Staatsschutzes mitenthalten, die eine spezifische Ausprägung u.a. im sog. strafrechtlichen Verfassungsschutz (Bereich der Staatsschutzdelikte) erhalten habe. Bei diesem Ansatz hat der Verfassungsschutz Anspruch darauf, sämtliche vom Staatsschutz gesammelten Erkenntnisse zu erhalten, und umgekehrt ist es nicht viel anders. Damit sind das Trennungsgebot, soweit ihm eine materiell-inhaltliche Bedeutung zugemessen wird, und zugleich auch das Zweckbindungsprinzip praktisch aufgehoben. Vorsichtshalber ist aus dem BVerfSchMiGE auch der im ZAG-Entwurf noch enthaltene Satz herausgestrichen worden, wonach die Vorschriften über die organisatorische Trennung von Polizei und Nachrichtendiensten sowie über den Ausschluß polizeilicher Befugnisse für die Nachrichtendienste unberührt bleiben.

Staatsschutzdelikte i.S.d. BVerfSchMiGE können Straftaten jeder Art (z.B. Sachbeschädigung, Beleidigung, Nötigung in Form von Sitzstreiks) sein, die aufgrund ihrer Zielsetzung, des Motivs des Täters oder seiner Verbindung zu einer Organisation gegen die freiheitlich demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes oder die auswärtigen Belange des Bundesrepublik gerichtet sind. Jeder, der eine Bagatellstraftat begeht, muß also damit rechnen, zum Staatsfeind erklärt zu werden, wenn der Staatsschutz einen extremistischen Hintergrund (z.B. Volkszählungsboykott) annimmt. Weil der Staatsschutz seine Erkenntnisse an den Verfassungsschutz weiterzugeben hat, ist der Betroffene damit zugleich zum Verfassungsfeind geworden.

Da der BMI „strikt darauf geachtet hat, daß Datenschutz und innere Sicherheit ausgewogen und gleichrangig beachtet werden", versteht es sich von selbst, daß die Begrenzung der „Spontanübermittlungen" auf Spionage- und Terrorismusfälle, wie sie noch im ZAG-Entwurf vorgesehen war, wieder abgeschafft wird. Ebenso konsequent war es, auch die im ZAG-Entwurf vorgeschlagenen Einschränkungen für die Weitergabe von Informationen, die die Polizei unter Einsatz spezieller strafprozessualer Befugnisse

(zur Post- und Telefonkontrolle sowie zur Durchsuchung von Wohnungen) gewonnen hat und die nach der StPO besonderen Zweckbindungen unterliegen, zu streichen. Diese Daten dürfen also nicht nur, sie müssen wie alle anderen Daten, die die Polizei mit besonderen Methoden der Datenerhebung (z.B. durch polizeiliche Beobachtung oder unter Einsatz technischer Mittel) gewonnen hat, unter der alleinigen Voraussetzung, daß die empfangende Behörde die Daten für die Erfüllung ihrer Aufgaben benötigen könnte, z.B. an den Verfassungsschutz weitergegeben werden. Das kann auch im automatisierten Verfahren durch unmittelbaren Abruf geschehen, wenn nur der zuständige Minister oder sein Vertreter zugestimmt haben.

Kritikern, die davon sprechen, daß durch diesen Gesetzentwurf ein schrankenloser Datenaustausch zwischen den Sicherheitsbehörden ermöglicht wird, möchte ich nicht widersprechen.

1.1.3 Gesetz zur Strukturreform im Gesundheitswesen

Einschneidende Änderungen in der Informationsverarbeitung bei den gesetzlichen Krankenkassen stehen bevor, wenn der Referentenentwurf des BMA für ein Gesundheitsreformgesetz in der jetzt vorliegenden Fassung in Kraft treten sollte.

Der Entwurf sieht eine umfassende Speicherung von Patientendaten auf Leistungskonten der Versicherten vor. Begründet wird die Notwendigkeit dieser gewaltigen Datensammlungen mit den Schlagworten Transparenz, Wirtschaftlichkeit und Stärkung der Eigenverantwortung; Ziel ist die Eröffnung umfassender Kontrollmöglichkeiten die sich nicht nur auf Ärzte und sonstige Leistungserbringer, sondern auch auf die Patienten erstrecken sollen.

Ich halte die geplante versichertenbezogene Totalerfassung der Abrechnungsdaten für unverhältnismäßig und nicht vereinbar mit dem Grundrecht auf informationelle Selbstbestimmung. Sie schafft die ärztliche Schweigepflicht im Verhältnis Arzt-Krankenkasse praktisch ab.

Die Einführung von Leistungskonten erscheint mir auch nicht geeignet, die Erfüllung der berechtigten Forderungen der Krankenkassen nach verstärkten Kontrollmöglichkeiten zur Verhinderung von Abrechnungsbetrügereien und nach Erhöhung der Qualität und Wirtschaftlichkeit der Leistungserbringung sicherzustellen.

Abrechnungskontrollen können bei Millionen von Versicherungsfällen nur stichprobenartig erfolgen. Dafür ist eine Totalerfassung aber nicht erforderlich. Es besteht deshalb die Gefahr einer unzulässigen Vorratsdatensammlung. Wirtschaftlichkeitskontrollen lassen sich auch ohne personenbezogene Daten durchführen, so daß als stichhaltiges Argument für die Totalerfassung letzlich allein die Möglichkeit übrig bleibt, die Patienten auf gesundheitsschädigendes und unwirtschaftliches Verhalten zu kontrollieren. Dieser sozialpolitisch fragwürdige Ansatz vermag die Einschränkung von Grundrechten aber nicht zu tragen.

Für datenschutzrechtlich tolerierbar halte ich die auf Leistungserbringer bezogene Verarbeitung von Abrechnungsdaten und für Stichproben eine Zusammenführung mit versichertenbezogenen Daten. In diesen Fällen ist der Personenbezug der Daten nur zur Ermittlung der Qualität der ärztlichen Leistung oder zur Verifizierung der Abrechnung von Interesse. Bei der Güterabwägung kann man deshalb unterstellen, daß das öffentliche Interesse an der Funktionsfähigkeit des kassenärztlichen Versorgungssystems das Geheimhaltungsinteresse des Betroffenen überwiegt.

Zu Bedenken gibt auch Anlaß, daß der Entwurf einen weiteren Schritt in Richtung auf ein allgemeines Personenkennzeichen hin macht, indem er die Kennzeichnung jedes Abrechnungsbelegs mit der Sozialversicherungsnummer vorsieht. Der Geheimhaltungsschutz des Sozialgesetzbuchs, dem die Nummer grundsätzlich unterliegt, wird bei einer so weit verbreiteten Verwendung ausgehöhlt. Die Gefahr, daß andere Verwender der Versicherungsnummer unberechtigt auf die Patientendaten zugreifen, ist nicht auszuschließen.

1.1.4 Die Lage in Hamburg

Die Justizbehörde hat einen Entwurf zur Novellierung des Hamburgischen Datenschutzgesetzes in die Behördenabstimmung gegeben. Der Entwurf weicht in der Behandlung grundsätzlicher Fragen deutlich von dem oben erörterten Referentenentwurf aus dem Bundesinnenministerium ab. Er orientiert sich sehr viel stärker an dem von den sog. A-Ländern, also unter Beteiligung von Hamburg im Jahre 1986 im Bundesrat eingebrachten (Alternativ)-Entwurf zur Novellierung des BDSG und den damit weitgehend übereinstimmenden neuen Datenschutzgesetzen von Hessen und Bremen sowie dem Entwurf, den z.Z. der nordrhein-westfälische Landtag berät. Bei aller Kritik, die an einzelnen Vorschriften zu üben sein wird, gegen die Konzeption des Entwurfs habe ich wenig einzuwenden.

Die Koalitionspartner haben sich vorgenommen, das SOG zu novellieren. Einen neuen Entwurf habe ich bislang noch nicht erhalten. Wohl aber hatte ich Gelegenheit, zu dem Entwurf eines Krankenhausgesetzes, der auch einen Abschnitt über die Informationsverarbeitung enthält, Stellung zu nehmen (4.16.1.1.). Weitere Entwürfe sind z.Z. nicht in Sicht. Zu der Notwendigkeit, auf den verschiedensten Fachgebieten bereichsspezifische Datenschutzregelungen zu treffen, habe ich mich in den Vorjahren mehrfach geäußert und tue es auch in diesem Bericht wieder. Auch wegen der Konsequenzen, die sich ergeben, wenn nicht spätestens bis zum Ende dieser Wahlperiode gesetzliche Regelungen eben für die Informationstätigkeit der Polizei und des Verfassungsschutzes vorliegen, verweise ich auf die Ausführungen in meinem letzten TB (1.2, S. 2; 5.8.1, S. 67) und im Polizeiteil dieses Berichts (4.11.1).

1.2 Volkszählung 1987

Die Durchführung der Volkszählung bildetete erwartungsgemäß einen Schwerpunkt meiner Kontrolltätigkeit im Berichtsjahr und nimmt in dem vorliegenden Bericht erheblichen Raum ein (siehe Abschnitt 4.4).

Ich habe 1986 unter Hinweis auf die mit der Durchführung der VZ zu erwartenden Probleme angeregt, den Katalog der bei der als Totalerhebung durchgeführten VZ erfragten Merkmale auf einen „unverzichtbaren Kernbestand" zu reduzieren. Dies hätte die Vorteile gehabt,

— die mit der VZ verbundenen Kosten zu verringern,

— die Datenaufbereitung zu beschleunigen und

— die Akzeptanz der Zählung zu verbessern und damit den Konflikt um die VZ zu entschärfen.

Der Senat hat diesen Vorschlag aufgegriffen, ist damit aber bei der Bundesregierung nicht durchgedrungen.

Der Ablauf der Zählung bestärkt mich in meiner seinerzeit geäußerten Ansicht. Obwohl die Datenaufbereitung noch längst nicht abgeschlossen ist, läßt sich heute schon feststellen, daß

— die Kosten der VZ weit über den Voranschlägen liegen,

— sich die Datenaufbereitung gegenüber den ursprünglichen Planungen verzögert,

— die Auskunftsbereitschaft zumindest in Hamburg hinter den Erwartungen der Statistiker zurückbleibt (mehr als ein halbes Jahr nach dem Zählungsstichtag fehlen immer noch etwa 10% der Fragebögen).

Ich habe immer wieder darauf hingewiesen, daß neben einer verfassungsrechtlich einwandfreien gesetzlichen Grundlage den von den mit der Durchführung der Zählung befaßten Stellen zu treffenden Datensicherungsmaßnahmen große Bedeutung zukommt. Leider hat die amtliche Statistik hier einiges versäumt.

Bei der Durchführung der Erhebung ist es zu einer Vielzahl von vermeidbaren Mängeln und z.T. schwerwiegenden Verstößen gegen das Gesetz über eine Volks-, Berufs-, und

Arbeitsstättenzählung (Volkszählungsgesetz 1987 — VZG 1987) gekommen, die ein positives Urteil über den Ablauf der Zählung nicht zulassen.

Ich habe mich bislang zweimal veranlaßt gesehen, die Durchführung der Volkszählung 1987 durch das Statistische Landesamt Hamburg gem. § 21 HmbDSG gegenüber dem Senat förmlich zu beanstanden.

Die Beanstandungen bezogen sich auf folgende Punkte:

— Für die Vorbereitung der Gebäudevorerhebung und der Arbeitsstättenzählung wurden mehr Daten als zulässig an das Statistische Landesamt übermittelt und andere als die zugelassenen Quellen herangezogen.

— Das automatisierte Verfahren zur Verarbeitung der Volkszählungsdaten wurde nur unzureichend getestet und war nicht ordnungsgemäß freigegeben.

— Die Hilfsmerkmale und die Erhebungsmerkmale wurden bei der Gebäudevorerhebung nicht rechtzeitig getrennt und gelöscht.

— Die im Rahmen des automatisierten Erinnerungs- und Mahnverfahrens verarbeiteten Daten bleiben zu lange gespeichert.

— Das Statistische Landesamt konnte nicht davon abgebracht werden, auch bei Übereinstimmung von Wohn- und Arbeitsstättenanschrift die Anschrift der Arbeitsstätte dauerhaft zu speichern.

— Der Datenschutzbeauftragte wurde vom Statistischen Landesamt fortlaufend nur unzureichend informiert.

Diese Mängel, die nur einen kleinen Ausschnitt aus den insgesamt aufgetretenen Fehlern darstellen, lassen die Schlußfolgerung zu, daß die Statistiker mit der Durchführung derartiger Totalerhebungen überfordert sind und eine datenschutzrechtlich einwandfreie Zählung auch künftig nicht sichergestellt werden könnte. Ich halte aus diesen Gründen eine Wiederholung derartiger statistischer Großerhebungen — zumindest in der Form und in dem Umfang der VZ 1987 — auch aus Sicht des Datenschutzes nicht für angebracht.

Die Auseinandersetzung um die Volkszählung hat das Mißtrauen breiter Kreise der Bevölkerung gegen jegliche statistische Erfassung vergrößert. Die Folgen davon treffen nicht nur die Statistiker selbst, die nur unter großen Schwierigkeiten zu zuverlässigen Daten kommen, sondern auch die Nutzer der Statistik, die durch das Fehlen entsprechender Angaben in ihrer Aufgabenerfüllung behindert werden.

Der Konflikt hat jedoch auch eine positive Seite: viele Bürger reagieren heute sensibler auf die Speicherung und Verarbeitung ihrer Daten. Sie stellen Fragen über die Notwendigkeit der Datenerhebung und die Zwecke, die damit verfolgt werden. Und sie machen auch zunehmend von den ihnen zustehenden Rechten — z.B. dem durch die Datenschutzgesetze verbürgten Auskunftsrecht — Gebrauch. Dies kann ich als Datenschutzbeauftragter nur begrüßen.

1.3 Verhältnis zur Verwaltung

In meinem letzten Tätigkeitsbericht habe ich der Besorgnis Ausdruck gegeben, daß das Verständnis für datenschutzrechtliche Belange in der Verwaltung wieder verloren zu gehen drohe. In seiner Stellungnahme zu meinem 5. TB (Drs. 12/572) hat der Senat die Meinung geäußert, daß es sich bei den von mir dargestellten Vorgängen um Einzelfälle handele und sich eine Pauschalwertung verbiete. Diesen Einzelfällen werde der Senat „mit dem entschiedenen Bemühen, künftiges Fehlverhalten abzustellen, nachgehen". Eine allgemein nachlassende Sensibilität für datenschutzrechtliche Belange vermochte der Senat ebenfalls nicht zu erkennen. Vielmehr verfügten die Mitarbeiter der Hamburger Verwaltung „regelhaft über das erforderliche Problembewußtsein".

Leider muß ich dem widersprechen. Auch im vergangenen Jahr hat es eine Vielzahl von Verstößen gegen das Hamburgische Datenschutzgesetz und gegen andere

Datenschutzvorschriften gegeben, die meine im vorigen Berichtsjahr geäußerten Befürchtungen bestätigen:

— Im Rahmen von Überweisungaufträgen der Sozialämter wird den kontoführenden Instituten nach wie vor offenbart, daß der Kontoinhaber Sozialhilfeempfänger ist. Dies kann im Einzelfall schwerwiegende Konsequenzen für die Betroffenen haben, angefangen damit, daß in einzelnen Fällen das Girokonto gekündigt wird. Diese Praxis wird fortgeführt, obwohl ich den Senat auf das Problem wiederholt aufmerksam gemacht und ihm unter Hinweis auf ein in Nordrhein-Westfalen eingeführtes datenschutzrechtlich einwandfreies Verfahren auch eine Lösung angeboten habe.

— Durch den Aktenfund in einer Eidelstedter Lagerhalle und andere Vorfälle wurde offenbar, der Mehrzahl der Hamburger Behörden ist nicht bewußt, daß der Schutz personenbezogener Daten erst dann endet, wenn die Daten gelöscht bzw. die Datenträger vernichtet worden sind. Die Behörden sind dafür verantwortlich, auf welche Weise sie sich nicht mehr benötigter Datenträger, z.B. Akten, entledigen. Auch hierauf habe ich lange vor den spektakulären Vorfällen hingewiesen und ein Verfahren vorgeschlagen, mit dem eine einwandfreie Vernichtung ausgesonderten Schriftgutes gewährleistet worden wäre, auch dies leider ohne Erfolg.

— Auch 1987 ist es in mehreren Fällen zu einem Bruch des Adoptionsgeheimnisses gekommen. So hat das Einwohnerzentralamt Daten von in Adoptivpflegschaft befindlichen Kindern der Erhebungsstelle Volkszählung übermittelt und nicht einmal mitgeteilt, daß es sich dabei um gesperrte Daten handelte. Die Erhebungsstelle hat die Daten in die Begehungslisten der Zähler aufgenommen. Die Zähler haben die geschützten Daten Dritten, z.B. Nachbarn der Betroffenen offenbart, obwohl die Adoptiveltern aufgrund der strengen gesetzlichen Vorschriften davon ausgehen durften, daß das Adoptionsgeheimnis sorgsam gehütet wird.

— Der polizeiliche Staatsschutz hat auch in Hamburg Personen, deren Protest gegen die Volkszählung sich darin erschöpft hat, die Kennziffern auf den Fragebögen abzuschneiden oder bloß dazu aufzufordern, in seinem Informationssystem „APIS" gespeichert und sie auf diese Weise als „Staatsfeinde" gebrandmarkt. Wenn sie die eigenen Richtlinien beachtet hat, muß die Polizei sich von der Annahme hat leiten lassen, daß hier Straftäter am Werke waren, die auf unsere freiheitlich demokratische Grundordnung oder den Bestand unseres Staates zielten. Die Speicherung erfolgte, obwohl Innenbehörde und Datenschutzbeauftragter vorher Übereinstimmung erzielt haben, daß „Volkszählungsboykotteure" in APIS nichts zu suchen haben. Bei der Prüfung, die ich im vergangenen Frühjahr und Sommer beim Staatsschutz durchgeführt habe, habe ich leider feststellen müssen, daß in vielen anderen Fällen, in denen es um ähnlich „gravierende" Vorwürfe ging, Eintragungen in APIS erfolgten. Nicht genug damit: Einige Betroffene habe ich auch im nachrichtendienstlichen Informationssystem „Nadis" entdeckt.

Ich kann mit meinem Tätigkeitsbericht immer nur einen kleinen Ausschnitt aus den mir bekanntgewordenen Mängeln und Fehlleistungen darstellen. Dennoch möchte ich nicht behaupten, daß die Mehrzahl der Mitarbeiter der Verwaltung bewußt in unzulässiger Weise in das Recht der Bürger, grundsätzlich selbst über ihre Daten zu bestimmen, eingreift. Ich halte es aber nach wie vor für dringend geboten, daß die Verantwortlichen dem feststellbaren Rückgang an Sensibilität beim Umgang mit personenbezogenen Daten entschlossen entgegentreten.

Der Senat ist mit seiner am 24. März 1987 verteilten Stellungnahme meinem Vorschlag nicht gefolgt, jeden einzelnen Mitarbeiter anzusprechen, und ihn etwa in Form einer Beilage zur Gehaltsmitteilung zu sensibilisieren. Er hat aber — im März 1987 — zugesagt, diese Information mit einem „demnächst zu verteilenden, mit dem HmbDSB abgestimmten Rundschreiben an die Behörden" zu gewährleisten und in den „Mitteilungen für die Verwaltung" zu veröffentlichen.

Ein Schreiben mit Hinweisen für die Behörden ist diesen erst Anfang 1988 zugegangen. Die Umsetzung durch die Behörden, d.h. die Unterrichtung des einzelnen Mitarbeiters, steht noch aus.

Zwar hat es einige Fortschritte bei der Unterrichtung der Behörden über notwendige Datensicherungsmaßnahmen bei der Nutzung von Personalcomputern gegeben (vgl. 3.6.3). Zugleich mußte ich aber bei der Prüfung zweier Groß-ADV- Verfahren (Gebäudevorerhebung und Personalabrechnungsverfahren) feststellen, daß hier — also in einem Bereich, bei dem ich aufgrund des Eigeninteresses der Verwaltung bisher immer davon ausgegangen war, daß die Ordnungsmäßigkeit der Datenverarbeitung einigermaßen gegeben sei — massiv gegen die vom Senat erlassenen Richtlinien verstoßen wurde. Es spricht leider vieles dafür, daß es sich hierbei nicht um Einzelfälle handelt (vgl. 3.4).

Auf meine Kritik haben Senat und Verwaltung — wie ich meine — nicht immer in angemessener Weise reagiert. So wurde mir immer wieder eine aktuelle und vollständige Unterrichtung und eine frühzeitige Beteiligung versprochen. Ich mußte jedoch feststellen, daß der gute Vorsatz häufig nicht in die Praxis umgesetzt wurde. So ist der Senat in seiner Stellungnahme zu der von mir vorgebrachten Beanstandung, das Statistische Landesamt habe mir wichtige Anordnungen entgegen § 8 der Durchführungsverordnung zum VZG nicht unverzüglich zur Kenntnis gegeben, ohne weiteres von den Tatsachenfeststellungen der betroffenen Behörde ausgegangen, obwohl diese unübersehbar von meiner Sachverhaltsdarstellung abgewichen ist, und dies, ohne mir noch einmal Gelegenheit zur Richtigstellung zu geben. Auf diese Weise war es dem Senat möglich, schuldhafte Fehlleistungen des Statistischen Landesamtes nicht feststellen zu müssen und damit eine Form der Beteiligung des HmbDSB zu decken, die darin bestand, mir zwar Entwürfe zu Dienstanweisungen zuzuleiten und mir Gelegenheit zur Stellungnahme zu geben, meine Kritik und Alternativvorschläge jedoch nicht zu berücksichtigen, mich darüber nicht zu informieren und mir die datenschutzrechtlich bedenkliche Endfassung der Verfügungen erst mit mehrmonatiger Verzögerung zuzusenden, und auch erst aufgrund wiederholter Mahnungen und Erinnerungen.

Ich kann also nicht umhin festzustellen, daß die schon im vergangenen Jahr von mir gerügte Unbekümmertheit bei der Datenverarbeitung von hamburgischen Dienststellen sich jedenfalls nicht abgeschwächt hat. Trotzdem bin ich der Auffassung, daß es der Verwaltung gut anständen und auch der Aufgabenerfüllung förderlich wäre, wenn die Behörden die Gewährleistung des Datenschutzes — wie es ja auch das Gesetz vorsieht — zu ihrer eigenen Angelegenheit machten. Die Verwaltung ist zur Erfüllung ihrer Aufgaben auf die Mitarbeit des Bürgers angewiesen. Der Bürger ist hierzu aber nur bereit, wenn er darauf vertrauen kann, daß mit seinen Daten sorgsam umgegangen wird. Mit einem sparsamen, sensibleren und rechtlich einwandfreien Umgang mit personenbezogenen Daten könnte die Verwaltung auch einen nicht unbedeutenden Beitrag zur Stärkung des allgemeinen Rechtsbewußtseins leisten, dessen Niedergang ansonsten häufig öffentlich beklagt wird.

2. Entwicklung der Dienststelle

2.1 Ausstattung

Die personelle Ausstattung meiner Dienststelle ist nach wie vor unzureichend (vgl. 5. TB, 2.1, S. 5). Der Hamburgische Datenschutzbeauftragte liegt mit seinem Personalbestand (11 Stellen) deutlich hinter dem der meisten anderen Landesbeauftragten für den Datenschutz zurück. Zum Vergleich sei hier nur auf die Situation in den anderen Stadtstaaten hingewiesen: Dem Bremer Datenschutzbeauftragten stehen jetzt insgesamt 12 Stellen zur Verfügung, während in Berlin sogar 16 Stellen vorhanden sind, obwohl der Berliner Datenschutzbeauftragte nur für die datenschutzrechtliche Kontrolle des öffentlichen Bereiches zuständig ist.

Ich habe deshalb zum Haushaltsplan 1988 folgende neue Stellen beantragt:

— Um einen qualifizierten Informatiker mit der notwendigen Berufserfahrung für den Hamburgischen Datenschutzbeauftragten gewinnen zu können, ist die Zuweisung einer Regierungsdirektorenstelle erforderlich.

— Ein jüngerer Jurist könnte dazu beitragen, daß die erforderliche Kontrolldichte im Bereich der hamburgischen Verwaltung erhöht wird. Derzeit stehen hierfür lediglich zwei Juristen zur Verfügung, von denen einer auch im nicht-öffentlichen Bereich aushelfen muß.

— Nach den Erfahrungen, die sowohl der Hamburgische Datenschutzbeauftragte als auch andere Datenschutzbeauftragte gesammelt haben, ist es erforderlich, der Datenverarbeitung bei den Sicherheitsbehörden besondere Aufmerksamkeit zu widmen. Das hierfür zuständige Referat ist für eine Reihe weiterer, ebenso sensibler Bereiche verantwortlich, so daß vor allem für die Prüfung der umfangreichen Datenverarbeitung bei der Polizei keine hinreichende Personalkapazität zur Verfügung steht. Eine Sachbearbeiterstelle, die von einem Bewerber mit Erfahrung im Umgang mit polizeilichen Informationssystemen besetzt werden könnte, würde hier für eine wesentliche Verbesserung der Situation sorgen.

  Ferner muß ich an dieser Stelle davon berichten, daß ich Anfang September 1987 meine Diensträume im Millerntor-Hochhaus wegen einer Asbestverunreinigung verlassen mußte. Es ist derzeit immer noch ungewiß, wann die dortigen Räumlichkeiten wieder bezogen werden können. Zur Zeit sind die Mitarbeiter in zwei verschiedenen Dienstgebäuden untergebracht. Die Akten mußten am alten Platz verbleiben und waren mehrere Monate lang nicht zugänglich. Unter diesen Bedingungen ist ein geordneter Dienstbetrieb nicht möglich.

2.2 Eingaben

Im Berichtszeitraum erreichten mich 421 Eingaben. Davon entfielen 295 auf den öffentlichen und 126 auf den nicht-öffentlichen Bereich. Weil die hierfür benötigten Unterlagen nicht zugänglich sind, ist es mir leider nicht möglich, eine weitere Aufteilung der Eingaben nach Unterbereichen — wie in den letzten Jahren — vorzunehmen.

3. Beobachtung der automatisierten Datenverarbeitung

3.1 Kompromittierende Abstrahlung

Bei der Diskussion über die Sicherheit der Verarbeitung von Volkszählungsdaten ist auch auf das Problem der „kompromittierenden Abstrahlung" hingewiesen worden. Damit ist die ungewollte Aussendung von Signalen durch Geräte der elektronischen Datenverarbeitung gemeint, die — wie beim Betrieb aller elektronischen Geräte — als eine Art Abfallprodukt entstehen und die, wenn sie aufgefangen und ausgewertet werden, Informationen über das aktuelle Geschehen auf diesen Anlagen geben können.

Die Intensität der Abstrahlung und ihre Auswertbarkeit sind bei den verschiedenen Komponenten von EDV-Systemen höchst unterschiedlich. Die Strahlungsintensität ist bei Druckern und Bildschirmen beträchtlich größer als bei den sonstigen EDV-Geräten. Ohne großen technischen Aufwand lassen sich indes nur die von Bildschirmen abgegebenen Signale auswerten (zu den technischen Einzelheiten vgl. 9. TB des BfD, S. 73 f.).

Bei einem Mehrzweckrechenzentrum wie der Datenverarbeitungszentrale der Hamburger Verwaltung (DVZ) vermischen sich die von den verschiedenen Geräten abgegebenen Strahlungen, so daß eine Entbündelung — als Voraussetzung für eine Auswertung — einem potentiellen Angreifer kaum möglich sein dürfte, zumal dann, wenn aufgrund der Entfernung zum Ausspähungsobjekt die Intensität der empfangenen Signale sehr gering ist.

Das Senatsamt für den Verwaltungsdienst hält für die Abwehr des mit der kompromittierenden Abstrahlung verbundenen Mißbrauchsrisikos über die getroffenen Maßnahmen hinaus keine besonderen Vorkehrungen für notwendig. Ich habe dem nicht widersprochen.

3.2 Optische Speichertechnik

Wie kürzlich zu lesen war, sollen einer Marktuntersuchung zufolge in der Bundesrepublik Deutschland jährlich 140 Milliarden Blatt Papier einschließlich DV-Ausdrucke als Informationsträger genutzt werden. Davon werden nach Schätzung von Herstellerfirmen, die Organisationsmittel zur Papierablage produzieren, mehr als 40 % abgelegt, und zwar zu einem großen Anteil aufgrund gesetzlicher Bestimmungen sieben, zehn oder gar dreißig Jahre lang. Der Raumbedarf für diese Papierberge ist groß, ihre Verwaltung personalaufwendig und teuer. Die endlich notwendig werdende Beseitigung ist ein spezielles Problem, auf das ich unter Nr. 3.3 besonders eingehen will. Jedenfalls sind wir dem „papierlosen Büro" nicht näher gekommen.

Mit dem Anschwellen der Papierflut begann schon vor Jahrzehnten der Einzug des Mikrofilms in seinen verschiedenen Ausprägungen (Rollfilm, Jacket, Mikroplanfilm, Filmlochkarte) in die Büros und Archive. Der Mikrofilm ist heute als leistungsfähiges und kostengünstiges Speichermedium zur Archivierung von analogen Informationen (kaufmännisches und behördliches Schriftgut, Dokumentationen, Vorgangsablage) nicht mehr wegzudenken. Die wesentlichen Vorteile der Mikrofilm-Technologie im Vergleich zur Papierablage sind der geringe Bedarf an Platz und an Registraturmitteln, der Schutz vor unbefugter Belegentnahme und der Wegfall von Rücksortierungsarbeiten.

Datenschutzrechtliche Probleme treten bei der Mikroverfilmung insbesondere dann auf, wenn die Verfilmung nicht im eigenen Haus, sondern durch ein Service-Unternehmen erledigt werden soll. So ist es zum Beispiel bedenklich, wenn Krankenhäuser ihre Patientenakten durch gewerbliche Auftragnehmer verfilmen lassen wollen, weil die personellen und/oder technischen Voraussetzungen im Krankenhaus nicht vorhanden sind oder die Arbeiten durch Privatfirmen kostengünstiger angeboten werden. Mit der Übergabe der Patientenakten an den Gewerbebetrieb werden Patientendaten an dessen Mitarbeiter offenbart. Ich habe Zweifel, ob das Personal der Verfilmungsbetriebe dem ärztlichen Hilfspersonal zuzurechnen ist, so daß die Offenbarung nicht befugt wäre und damit gegen § 203 StGB verstieße. Ich habe deshalb angeregt, in Hamburg z.B. für die Krankenhäuser des Landesbetriebes die Regelung zu treffen, daß die Verfilmung von Krankenunterlagen unter ärztlicher Aufsicht im Krankenhaus durch eigenes oder fremdes Personal erfolgen sollte.

Inzwischen erfordert eine neue Form der optischen Speichertechnik unsere Aufmerksamkeit: Ich meine die digitalen optischen Speichersysteme. Sie zeichnen sich nicht nur durch eine enorme Steigerung des Speichervolumens aus (und zwar sowohl gegenüber der Mikrofilmtechnik als auch gegenüber den magnetischen Datenträgern). Das Hauptcharakteristikum der digitalen optischen Speichersysteme ist die Integration von Archivfunktionen (Speicherung und Rückgriff) mit dem Informationsmanagement. Die digitale Speicherungsform macht die archivierte Information verfügbar für eine automatisierte Auswertung und Weiterverarbeitung.

Nun werden auf dem Markt durchaus unterschiedliche Systeme angeboten, es gibt die WORMs, die CD-ROMs, CD-PROMs, Laserdiscs usw. Und jedes System, ja jede einzelne Anwendung hat ganz spezielle Komponenten, so daß es sich verbietet, verallgemeinernde Aussagen zu machen. Das gilt vor allem für die datenschutzrechtliche Bewertung. Ich möchte daher an einem konkreten Beispiel aufzeigen, wo datenschutzrechtliche Probleme auftreten können. Das Beispiel stammt übrigens nicht aus dem öffentlichen Bereich. Mir sind bisher auch keine Pläne der hamburgischen Verwaltung zur Einführung digitaler optischer Speichersysteme bekannt, aber in anderen Bundesländern haben auch öffentliche Stellen solche Systeme bereits in Betrieb genommen (z.B. die Augenklinik des Universitätskrankenhauses in München, die Parlamentsdokumentation der Landesverwaltung Nordrhein-Westfalen). Es dürfte nur eine Frage der Zeit sein, daß auch in der hamburgischen Verwaltung solche Systeme eingeführt werden.

Das Beispiel:

Ein Anwender hat ein optisches Speichersystem (hardware und software) erworben, um die Abrechnungsakten der Mitarbeiter (separater Teil der Personalakten) auf dieses System zu übernehmen. Nach der Übernahme auf das System sollen die Papierunterlagen vernichtet werden (Raumersparnis!); sie können vernichtet werden, weil das optische System den Anforderungen an eine ordnungsgemäße Speicherbuchführung im Sinne des Steuerrechts genügt. Der Anwender bat um eine Stellungnahme zu der Frage, ob die Anwendung unter das Datenschutzgesetz fällt.

Zur Erfassung der Dokumente für das Speichersystem werden die Papierseiten der Abrechnungsakten mit einem Scanner abgetastet. Eine Seite wird dabei Zeile für Zeile horizontal in Bildpunkte aufgelöst, ähnlich dem Verfahren, mit dem ein Fernsehbild erzeugt wird. Im hier eingesetzten sogenannten „High resolution mode" gemäß CCITT wird z.B. ein DIN-A 4-Dokument in ungefähr 4.000.000 Bildpunkte (pixels) aufgeteilt. Der Scanner (Digitalisierer) unterscheidet für jeden einzelnen Bildpunkt den Zustand „schwarz" oder „weiß" bzw. den entsprechenden Primärcode „1" oder „0". Auf diese Weise wird der bildhafte Inhalt des Dokuments in einen Datenstrom von 4.000.000 bits umgewandelt. Diese Codiertechnik wird „bit-map-scanning" genannt.

Der so gewonnene Bitstrom wird durch ein Kompressionsverfahren (in diesem Fall wird das vom CCITT empfohlene „modifizierte Huffmann-Code-Verfahren eingesetzt) drastisch reduziert, wodurch erheblicher Speicherplatz eingespart wird. Auch nach erfolgter Datenkompression übersteigt die Menge der zu speichernden Informationen jedoch in praktischer und wirtschaftlicher Hinsicht die Möglichkeiten konventioneller Speichermedien. Ein solches System läßt sich daher nur mit einer optischen Speicherplatte (DOR = Digital Optical Record) realisieren. In dem hier besprochenen Beispiel wird die WORM-Technik eingesetzt, d.h. die optische Speicherplatte kann einmal beschrieben und beliebig oft gelesen werden (write once, read many). Das zu speichernde Informationsmuster besteht aus „Pits", die in die Speicherschicht durch einen Laserstrahl eingeschmolzen werden. Beim Lesevorgang werden die gespeicherten „Pits" in die entsprechende binäre Darstellung (0 oder 1) zurückgewandelt. Mit dem hier beschriebenen optischen Speichersystem können nicht nur Bitströme (Faksimile-Dokumente) sondern auch alphanumerische Daten (Zeichen) verarbeitet werden, die über die Tastatur an einem Eingabe-(scan-)Platz eingegeben oder per DFÜ-Verbindung von einem zentralen EDV-System übertragen werden. Das Gesamtsystem wird vom Hersteller mit folgenden Funktionen angeboten:

— Archivieren

— Abfragen

— Wiederauffinden und -darstellen sowie Übertragen von

  — Original-(Faksimile-)Dokumenten und

  — alpha-numerischen Massen-(Historien-)Daten.

Damit können — als eigenständiges System (stand alone) oder im DFÜ-Verbund mit zentralen Groß-EDV-Systemen —

— alpha-numerische Massenspeicherung

— Archivierung von Dokumenten

— integrierte Aktenverarbeitung

EDV-mäßig organisiert werden.

Die zu beurteilende konkrete Anwendung wird als stand-alone-System betrieben. Von den möglichen Funktionen sind realisiert das Archivieren, das Abfragen, das Wiederauffinden und -darstellen von Original-(Faksimile-)Dokumenten. An alpha-numerischen Daten wird nur die Personalnummer der Mitarbeiter erfaßt. Der Zugriff auf die Dokumente ist nur über die Personalnummer möglich.

Maßgebend für die Frage, ob die Anwendung unter das Datenschutzgesetz (sei es HmbDSG bei einem öffentlichen Anwender, sei es BDSG bei einem nicht-öffentlichen Anwender) fällt, ist § 1 Abs. 2 Satz 1 HmbDSG bzw. BDSG. Die Anwendung fällt unter das Datenschutzgesetz, wenn personenbezogene Daten in einer Datei verarbeitet werden.

Die Daten sind von einem Datenträger (Seiten in Akten) auf einen anderen Datenträger (Optische Speicherplatte) übernommen worden, um auf Dauer zum Zwecke der weiteren Verwendung aufbewahrt zu werden. Das Speichern ist eine Phase der Datenverarbeitung (§ 4 Abs. 3 Nr. 1 HmbDSG bzw. § 2 Abs. 2 Nr. 1 BDSG).

Gespeichert sind einzelne Blätter der Personal-Abrechnungsakten

— als Faksimile-Wiedergabe („Primärdokument") und

— als codierte, vom System automatisiert auswertbare Beschreibung des Primärdokuments („Sekundärdokument").

Das Primärdokument ist in digitaler Form auf der optischen Speicherplatte unveränderbar und lesbar gespeichert. Es kann inhaltlich nicht automatisiert ausgewertet werden, sondern es kann nur als Faksimile-Wiedergabe auf einem Bildschirm angezeigt und über einen Faksimile-Drucker ausgedruckt werden.

Welche Daten das „Sekundärdokument" enthält, ist abhängig von der jeweiligen Anwendung. Parallel zum Scannen der Papierdokumente werden von einer Erfassungskraft über die Eingabe-Tastatur nach bestimmten Regeln das Dokument beschreibende Merkmale (Spezifikationen) eingegeben. Es muß eine Dokumentenidentifikation eingegeben werden, damit das System die Abspeicherung und das Wiederauffinden der Dokumente organisieren kann. Darüber hinaus können weitere Spezifikationen (Deskriptoren) zu jedem Dokument eingegeben werden. Bei einer Personalaktenanwendung könnten z.B. als Deskriptoren der Name, eine Dokumentenbezeichnung (z.B. Gehaltsabrechnung, Gehaltsvereinbarung usw.), ein Schlüsselwort (Angestellter, Arbeiter usw.) und ein Datum (Erstellungsdatum, Wirksamkeitsdatum usw.) sinnvoll sein.

Die Daten des Sekundärdokuments werden zusammen mit den für die Organisation der Archivierung und Wiedergabe benötigten System-Managementdaten dem Steuerungs- und Suchprogramm des Systems (dem „Retrieval-System") übergeben. Zum Abrufen eines Dokuments muß der Benutzer dem System entweder die Dokumentenidentifikation mitteilen (dann arbeitet das System mit einer durchschnittlichen Zugriffszeit von 150 Millisekunden im wahlfreien Zugriff), oder der Benutzer gibt dem System logisch verknüpfte Suchbegriffe ein (dann wählt das Retrieval-System alle Dokumente mit den entsprechenden Spezifikationen aus und zeigt dem Benutzer die Identifikationen der betreffenden Dokumente an). In beiden Fällen kann sich der Benutzer die entsprechenden Dokumente am Bildschirm ansehen oder auf dem Faksimile-Drucker ausgeben lassen.

Bei der zu beurteilenden Anwendung sind Dokumente mit Einzelangaben zu jeweils einer bestimmten Person (Mitarbeiter) gespeichert, auf die (nur!) über die Personalnummer zugegriffen werden kann. Daß es sich bei den gespeicherten Daten um personenbezogene Daten handelt, ist unzweifelhaft. Ob aber die so gestaltete Datenspeicherung den Dateibegriff der Datenschutzgesetze erfüllt, war zweifelhaft.

In meiner Stellungnahme bin ich zu dem Ergebnis gekommen. daß zwar eine gleichartig aufgebaute Sammlung von Daten vorliegt, daß der Dateibegriff der geltenden Datenschutzgesetze (HmbDSG, BDSG) gleichwohl nicht erfüllt ist. Der Dateibegriff setzt ja bekanntlich voraus, daß die Daten bei der Anlegung der Sammlung nach bestimmten Merkmalen erfaßt und geordnet worden sind und nach anderen bestimmten Merkmalen umgeordnet und ausgewertet werden können. Bei der zu beurteilenden Datenverarbeitung ist bei der Erfassung nur die Personalnummer eingegeben worden. Die Daten, die in den Primärdokumenten enthalten sind, stehen zur automatisierten Auswertung und Umordnung nicht zur Verfügung. Die Datensammlung kann danach nicht „nach anderen bestimmten Merkmalen" umgeordnet oder ausgewertet werden.

Anders wäre eine Anwendung zu beurteilen, bei der außer der Personalnummer als Dokumentenidentifikation noch weitere Spezifikationen (wie z.B. der Name des Mitarbeiters, der Beschäftigungsstatus, ein Datum usw.) eingegeben worden wären. Dann könnte die Datensammlung nach anderen Merkmalen (als der Personalnummer) umgeordnet und ausgewertet werden, wobei besondere datentechnische Voraussetzungen für das Umordnen nicht erfüllt zu sein brauchten. Bei automatisiert lesbaren Dateien steht nämlich der Umordnungsmöglichkeit nicht entgegen, wenn die Datei in veränderter Form nicht auf demselben sondern nur auf einem anderen Datenträger wiedergegeben werden kann (z.B. auf Magnetband oder aber auf WORM-Platten gespeicherte Daten).

Es ist also das Datenschutzgesetz nicht anwendbar, weil der Dateibegriff nicht erfüllt ist. Dieses Ergebnis kann angesichts der Tatsache, daß bei der zu beurteilenden Anwendung personenbezogene Daten automatisiert verarbeitet werden, nicht befriedigen. Erklärtes Ziel des Datenschutzes ist es, durch den Schutz personenbezogener Daten insbesondere bei der automatisierten Datenverarbeitung der Beeinträchtigung schutzwürdiger Belange der Betroffenen entgegenzuwirken. An diesem Beispiel zeigt sich, daß sowohl die Definition des Dateibegriffs als auch die Beschränkung des Schutzes auf in Dateien verarbeitete Daten problematisch ist. Das Herausfallen aus dem Datenschutzgesetz hat zur Folge, daß den Betroffenen die Datenschutzrechte, nämlich das Recht auf Auskunft, auf Berichtigung, auf Sperrung und auf Löschung nicht zustehen. Wenn, wie bei der beschriebenen Anwendung geplant, die Papier-Dokumente nach Erfassung mit dem Scanner vernichtet werden, haben die Betroffenen aber auch nicht die Möglichkeit, die entprechenden Unterlagen durch Einsicht in die Personal-Abrechnungsakte zu überprüfen. Hier klafft also offensichtlich eine Lücke, die zur Zeit vielleicht durch eine Vereinbarung zwischen dem Anwender und der Personalvertretung — wenn auch eher notdürftig — geschlossen werden könnte. Offen bleibt, welche Rechte Betroffene bei einer ähnlichen Anwendung haben sollen, wenn die Betroffenen nicht Mitarbeiter datenverarbeitender Stellen sind, sondern z.B. Kunden einer Firma, Objekte von Auskunfteien, Bürger gegenüber einer Behörde.

Die Entstehung des BDSG beruht auf der Erkenntnis, daß mit der automatisierten Datenverarbeitung eine erhöhte Gefährdung des informationellen Selbstbestimmungsrechts einhergeht. Zur Entstehungszeit der Datenschutzgesetze war automatisierte Datenverarbeitung noch geprägt von der Datenverarbeitung in Dateien, auf die die Legaldefinition des § 2 Abs. 3 Nr. 3 BDSG zugeschnitten ist. Mit der Weiterentwicklung der Datenverarbeitungstechnik hat sich sehr bald gezeigt, daß neue Formen der automatisierten Datenhaltung und -verarbeitung denkbar sind und inzwischen auch eingesetzt werden, die nicht unter den Dateibegriff nach der geltenden Definition fallen, die aber gleichwohl ein Risiko für die Betroffenen darstellen. Es ist kein rationaler Grund dafür ersichtlich, daß in solcher Form verarbeitete personenbezogene Daten aus dem Schutz der Datenschutzgesetze herausfallen sollen. Die Datenschutzbeauftragten

streben daher seit langem — neben der Preisgabe des Dateibezugs — eine entsprechende Neudefinition des Dateibegriffs an.

Hessen und Bremen haben inzwischen mit ihren neuen Datenschutzgesetzen diesen Erkenntnissen Rechnung getragen und neue Definitionen eingeführt. Danach ist eine Datei „eine Sammlung von Daten, die durch automatisierte Verfahren ausgewertet werden kann (automatisierte Datei) oder eine gleichartig aufgebaute Sammlung von Daten, die nach bestimmten Merkmalen geordnet und ausgewertet werden kann (nicht automatisierte Datei)". Zwar bliebe auch dann, wenn diese Definition der beschriebenen konkreten Anwendung zugrunde gelegt werden könnte, sehr zweifelhaft, ob die beschriebene Datensammlung unter diesen Dateibegriff fiele, denn sind die gespeicherten Daten durch ein automatisiertes Verfahren auswertbar? Aber auf diese Frage käme es gar nicht mehr an, weil die genannten neuen Datenschutzgesetze die Verarbeitung personenbezogener Daten schlechthin regeln und lediglich in einzelnen Bestimmungen auf die Speicherung in Dateien abstellen. Dieses Beispiel zeigt m.E., welche Bedeutung der Definition des Dateibegriffs bzw. der Ausweitung der Anwendung der Datenschutzgesetze auf jegliche Verarbeitung personenbezogener Daten zukommt. Es bleibt abzuwarten, ob bei weiteren Novellierungen (z.B. des BDSG und des HmbDSG) eine zufriedenstellende Lösung gefunden wird.

3.3 Schriftgutvernichtung

140 Milliarden Blatt beschriftetes Papier fallen jährlich in der Bundesrepublik an (s. Nr. 3.2), dazu Magnetbänder, Disketten, Karboncassetten, Mikrofilmmaterial. Auch wenn dieses Material eine gewisse Zeit lang gebraucht wird und/oder aufgrund gesetzlicher Bestimmungen aufzubewahren ist, so kommt doch irgendwann der Tag, an dem man sich von diesem Material trennen möchte. Es gab Zeiten, da stellte Altpapier ein verwertbares Gut dar, man konnte es verkaufen. Heute muß in der Regel für den Abtransport und die Vernichtung bezahlt werden. Der Wunsch, sich möglichst ohne großen Aufwand von nicht mehr benötigtem Material zu trennen, ist naheliegend und verständlich. Leider ist die billigste Methode nicht immer die beste — jedenfalls dann gewiß nicht, wenn sie rechtlich unzulässig ist. Wirtschaftlichkeitsüberlegungen machen unzulässiges Verwaltungshandeln nicht zulässig. Nur wenn mehrere gesetzlich zulässige Lösungen möglich sind, ist für Wirtschaftlichkeitsüberlegungen Raum.

Warum regen sich Bürger und Medien auf, wenn z.B. Lohnsteuerkarten, Sozialhilfe-, Gerichts- und Steuerakten für Neugierige, für aus Langeweile herumstöbernde Jugendliche oder auch nach Diebesgut suchende (potentielle) Straftäter leicht zugänglich gelagert sind, wenn Passanten die Akten nur von der Straße aufsammeln müssen, weil sie von einem ungesicherten Fahrzeug heruntergefallen sind, oder wenn auf dem Winterhuder Marktplatz Personalausweise herumliegen, die wenige Tage vorher von den ehemaligen Inhabern beim Einwohneramt abgegeben worden waren? Was ist dabei, wenn Besucher von Gerichten und Behörden beim Warten und Herumgehen im Treppenhaus oder im Dachgeschoß auf Stapel von Akten stoßen, die zwar vielleicht schon acht oder auch zehn Jahre alte Vorgänge enthalten, die aber — der Mensch lebt meist länger — doch noch sehr interessant sein können?

Nun — es gibt das Steuergeheimnis, das Sozialgeheimnis und noch viele andere Berufs- oder besondere Amtsgeheimnisse und schließlich das allgemeine Datengeheimnis. Die Geltung all dieser Vorschriften zum Schutz des informationellen Selbstbestimmungsrechts endet nicht an dem Tag, an dem der Besitzer das Interesse an den Unterlagen verliert. Der Schutz endet erst, wenn das Risiko entfallen ist, d.h. mit der vollständigen Vernichtung der Unterlagen bzw. der Löschung der Daten. Derjenige, der Unterlagen zu sichern hat, damit die darin enthaltenen Daten nicht unbefugt offenbart werden, hat auch noch die Aussonderung und Vernichtung der Unterlagen derart zu organisieren, daß kein Unbefugter die Unterlagen in Besitz nehmen oder darin enthaltene Daten zur Kenntnis nehmen kann.

Diese Sicherungspflicht bis zur endgültigen Vernichtung der Unterlagen besteht nicht etwa nur für Unterlagen, die den Dateibegriff des § 4 Abs. 4 Nr. 3 des geltenden

HmbDSG erfüllen. Das Steuergeheimnis, das Sozialgeheimnis und alle anderen Berufs- und Amtsgeheimnisse sind von der Verwaltung zu wahren, ohne daß es darauf ankommt, ob die betreffenden Informationen in Dateien gespeichert werden. Die Sicherungspflicht trifft direkt jede Stelle der Verwaltung, die jeweils selbst die Verantwortung für die Einhaltung der Vertraulichkeit innerhalb ihres Zuständigkeitsbereichs trägt. Diese Pflicht besteht bereits angesichts der geltenden Gesetze (z.B. § 30 Abgabenordnung, § 35 Sozialgesetzbuch I, § 203 StGB, § 30 Verwaltungsverfahrensgesetz, § 5 HmbDSG), es bedarf zu ihrer Begründung keiner weiteren Regelungen, so daß nicht etwa mit dem erforderlichen Handeln noch gewartet werden kann, bis das Senatsamt für den Verwaltungsdienst, die Finanzbehörde oder — wie manche glauben — der Hamburgische Datenschutzbeauftragte den Stellen fertige Handlungsanweisungen zur Verfügung stellt.

Wie meine Umfrage bei allen Hamburger Behörden und öffentlichen Stellen vom April 1987 zur Praxis der Schriftgutvernichtung gezeigt hat, ist bislang diesem Problem nicht die nötige Aufmerksamkeit gewidmet worden. Zum großen Teil genügt die Organisation der Sammlung und Vernichtung von Unterlagen mit personenbezogenen Daten nicht den gesetzlichen Anforderungen, weil sie nicht gewährleistet, daß eine unbefugte Offenbarung der zwar nicht mehr benötigten, aber immer noch vertraulichen Daten ausgeschlossen ist.

Aufgrund dieser Erkenntnis sind im Senatsamt für den Verwaltungsdienst Überlegungen angestellt worden, ob durch eine umfassende Darstellung der zu beachtenden Aspekte, der möglichen Maßnahmen und eines Mustervertrages über die Auftragsvergabe an gewerbliche Akten- und Schriftgutvernichter („Hinweise zur Schriftgutvernichtung") den öffentlichen Stellen Hilfestellung geleistet werden kann. Es hat mit Vertretern der Finanzbehörde und der Bezirksämter Gespräche geführt, um zum einen die zu berücksichtigenden tatsächlichen Verhältnisse „vor Ort" zu ermitteln und zum anderen nach praktikablen Lösungen zu suchen. Ich war an diesen Gesprächen beratend beteiligt und habe einen Mustervertrag entworfen, in den die einschlägigen datenschutzrechtlichen Anforderungen an eine Schriftgutvernichtung durch gewerbliche Auftragnehmer eingeflossen sind.

Leider ist es aus Gründen, die ich nicht kenne, bis heute — also mehr als ein halbes Jahr, nachdem ich dem Senatsamt meinen Vorschlag übersandt hatte — noch nicht zu einer Formulierung der „Hinweise zur Schriftgutvernichtung" gekommen, und auch nach meiner Umfrage vom April 1987 sind erneut vertrauliche Unterlagen auf „offenem Markt" oder in ungesicherten Treppenhäusern usw. von Unbefugten aufgelesen worden. So positiv der Ansatz des Senatsamtes für den Verwaltungsdienst zu werten ist, so unbefriedigend ist die langsame Umsetzung dieses Gedankens. Auf keinen Fall können jedoch die für ihr Schriftgut selbst verantwortlichen Stellen sich damit exkulpieren, daß ihnen die in Aussicht gestellten Hinweise noch nicht zur Verfügung stehen. Ich sehe mich daher gezwungen, zukünftige erneute Verstöße gegen das Datenschutzgesetz oder gegen andere dem Datenschutz dienende Bestimmungen durch Organisationsmängel bei der Schriftgutvernichtung zu beanstanden.

3.4 Umsetzung der ADV-Richtlinien bei zentralen ADV-Verfahren der Freien und Hansestadt Hamburg

In meinem 5. TB (S. 6 ff.) habe ich über meine Beobachtung berichtet, daß im Bereich der dezentralen Datenverarbeitung die ADV-Richtlinien des Senatsamtes für den Verwaltungsdienst kaum Beachtung finden. Ich habe dies u.a. darauf zurückgeführt, daß die dezentralen ADV-Anwender meist „von Haus aus" keine „Datenverarbeiter" sind, daß ihnen oft das Problembewußtsein für Fragen des Datenschutzes und der Datensicherung fehlt und daß sie nicht in den zwischen Senatsamt für den Verwaltungsdienst und ADV-Gruppen bestehenden Informationsfluß integriert sind. Schließlich war zu berücksichtigen, daß die für die Groß-ADV entwickelten Regelungen nicht ohne weiteres auf die dezentrale Datenverarbeitung übertragbar sind. Über den Fortgang meiner Verhandlungen mit dem Senatsamt für den Verwaltungsdienst zur Verbesserung der

Situation im Bereich der dezentralen Datenverarbeitung berichte ich unter Nr. 3.5 in diesem TB.

Im jetzt abgelaufenen Berichtsjahr bin ich der Frage nachgegangen, ob wenigstens im Bereich der zentralen ADV-Verfahren, also der „Groß-ADV", für den die DS-Richtlinie, die DS-Rahmenregelungen, die Freigaberichtlinie und die Dokumentationsrichtlinie erlassen worden sind, diese Vorschriften eingehalten werden. Das Ergebnis war wenig ermutigend: Meine Prüfung der Gebäudevorerhebung (s. auch Nr. 4.4.3.2 in diesem Bericht) im Statistischen Landesamt und in der Datenverarbeitungszentrale hat gezeigt, daß die Richtlinien — jedenfalls bei diesem Verfahren — nur eine untergeordnete Rolle spielen. Bei meiner im Berichtsjahr begonnenen Prüfung der beim Personalamt eingesetzten ADV-Verfahren ist, wenn die Prüfung z.Z. auch noch nicht abgeschlossen ist, immerhin schon so viel erkennbar, daß bei diesem komplexen und bedeutenden Verfahren die Umsetzung der Richtlinien in die Praxis ebenfalls nicht gelungen ist. Es gibt Anhaltspunkte dafür, daß diese Ergebnisse nicht lediglich zufällig gefundene Ausnahmen sind. Vielmehr muß ich davon ausgehen, daß nur ein geringer Teil der ADV-Verfahren der hamburgischen Verwaltung getreu den Regelungen der Richtlinien betrieben wird.

Wesentlicher Bestandteil einer DV-Organisation, die den Anspruch erhebt, den Anforderungen des § 8 Abs. 1 HmbDSG bzw. des § 6 Abs. 1 BDSG zu genügen, sind verbindliche technisch-organisatorische Regelungen. Mit den vom Senatsamt für den Verwaltungsdienst erlassenen ADV-Richtlinien liegen für die hamburgische Verwaltung solche verbindlichen Regelungen vor, die auch geeignet erscheinen, ein hohes Maß an Datensicherheit und Datenschutz zu gewährleisten. Allerdings kann die angestrebte Sicherheit nur erreicht werden, wenn alle Regelungen von allen Beteiligten eingehalten werden. Die Regelungen stellen ein Gesamtkonzept dar, aus dem nicht Teile beliebig ausgeklammert werden können, ohne daß die Sicherheit der Datenverarbeitung gefährdet wird. Die Einhaltung der Richtlinien von allen Stellen der hamburgischen Verwaltung muß daher gefordert werden. Falls sich in besonders gelagerten Einzelfällen erweisen sollte, daß bestimmte von den Richtlinien vorgeschriebene Maßnahmen tatsächlich nicht oder nicht mit angemessenem Aufwand realisiert werden können, so müssen die nicht realisierbaren Maßnahmen durch andere ersetzt werden, damit insgesamt der geforderte Sicherheitsstandard eingehalten wird. Dies müßte auch in den Richtlinien zugelassen werden. Insofern müßten die Richtlinien überarbeitet werden. Durch mehr oder weniger stillschweigende Duldung von Verstößen gegen verbindliche Regelungen wird jedenfalls das gesamte organisatorische Sicherungskonzept in Frage gestellt.

3.4.1 Gebäudevorerhebung

Die Prüfung des Verfahrens Gebäudevorerhebung (GVE) ergab hinsichtlich der Anwendung der DV-Richtlinien folgendes:

Bei der Verfahrensentwicklung hat keine Hauptuntersuchung stattgefunden, es ist keine Problemanalyse und kein Rahmenkonzept erstellt worden, ganz zu schweigen von einer Detailplanung, d.h. die „Richtlinien für die Organisation der automatischen Informationsverarbeitung in der hamburgischen Verwaltung" sind nicht angewendet worden.

Die Behörde für Inneres hat dazu nachträglich vorgetragen, das Konzept für das Verfahren GVE sei bereits 1982/83 entwickelt und dargestellt worden, so daß für die jetzt durchgeführten Arbeiten zur GVE 1987 ein durchdachtes und datenschutzrechtlich einwandfreies Konzept zur Verfügung gestanden habe und lediglich ein entsprechender Hinweis in der Dokumentation versäumt worden sei. Dagegen läßt sich zweierlei einwenden:

(1) Wenn tatsächlich ein fertiges Konzept vorhanden war, ist nicht verständlich, warum sich die Erstellung der Datenflußbeschreibung für die GVE 1987 über Monate hingezogen hat und warum erst am Ende der Verarbeitung die „Verfahrensfreigabe"

erfolgte. Auch deutet die von der Behörde für Inneres benutzte Formulierung „..wurden als Konzept für ein planvolles Vorgehen die in einem Datenflußplan zusammengefaßten Erfahrungen, die bei Planung und Durchführung der GVE 1982/83 gewonnen wurden, zugrunde gelegt" darauf hin, daß bei der GVE 1982/83 ebenfalls keine korrekte Verfahrensentwicklung und Freigabe erfolgte, jedenfalls aber das damalige Verfahren verändert worden ist. Schließlich bleibt unklar, warum 1986 so viele Arbeiten im DVZ-Test durchgeführt wurden, wenn auf ein fertiges und bewährtes Konzept zurückgegriffen werden konnte.

(2) Das Verfahren GVE für die abgesetzte VZ 1983 wurde vor dem „Volkszählungsurteil" des BVerfG vom 15. Dezember 1983 auf einer anderen formal- und materiellrechtlichen Grundlage entwickelt. Aus den vorgelegten Unterlagen geht nicht hervor, inwieweit geprüft wurde, ob das „übernommene" Verfahren aus den Jahren 1982/83 den vom BVerfG und im VZG 1987 formulierten Grundsätzen entspricht.

Das Verfahren GVE wurde — ohne daß in einer Planungsphase das beabsichtigte Vorgehen festgelegt worden wäre — schrittweise entwickelt und ausprobiert, und zwar mit echten Daten. Anhand von Ausdrucken „fehlerhafter" Fälle wurde jeweils der nächste Schritt überlegt und durchgeführt. Planung, Programmierung, Test und Produktion waren nicht eindeutig voneinander getrennt. Bei solcher Vorgehensweise bleibt eine Grundvoraussetzung für eine ordnungsgemäße Entwicklung und Anwendung von Programmen/Verfahren, mit denen personenbezogene Daten verarbeitet werden, zwangsläufig auf der Strecke: die Forderung, echte Daten ausschließlich mit ausgetesteten und freigegebenen Verfahren zu verarbeiten.

Der Einsatz eines Verfahrens zur Produktion setzt eine ordnungsgemäße Freigabe des gesamten Verfahrens oder zumindest abgrenzbarer, in sich geschlossener Teile von Verfahren, hier z.B. Teil GVE des Verfahrens Volkszählung 1987, voraus (vgl. Freigaberichtlinie Nr. 1.1 bis 1.3.3). Nach den in der DVZ vorgefundenen Dokumenten wurden Programme, die als Standardprogramme — wie z.B. „SORT" — als außerhalb des Verfahrens freigegeben angesehen werden können, zur Produktion eingesetzt ab 1. Juli 1986, die „Freigabeerklärung" des Verfahrens GVE datiert dagegen vom 24. September 1986.

Nach Nr. 2.7.1 der DS-Rahmenregelungen ist der Test mit „echten" Daten grundsätzlich unzulässig. Ausnahmen bedürfen nach Nr. 2.7.2 der DS-Rahmenregelungen der vorherigen schriftlichen Zustimmung der fachlich zuständigen Stelle. Der Rechenstelle, in der die Originaldaten verarbeitet werden sollen, ist eine Durchschrift der Genehmigung zu übersenden, das Senatsamt für den Verwaltungsdienst ist zu informieren, die Datensicherungsregelungen für die Produktion sind entsprechend anzuwenden.

Die Verwendung von Originaldaten im Testbetrieb ist eine gravierende Schwachstelle im Gesamtsystem der Datensicherung gegen unberechtigten Zugriff. Deshalb hat die DVZ darauf zu achten, daß — sollte eine programmierende Stelle ausnahmsweise mit echten Daten testen wollen — die erforderlichen Ausnahmegenemigungen für einen genau umrissenen Auftrag vorliegen. Aus den von der programmierenden Stelle im Statistischen Landesamt ausgestellten Testaufträgen war für die DVZ eindeutig zu erkennen, daß Originaldaten als Eingabedatenbestände in den „Test" einfließen sollten. Das statistische Landesamt hat nicht nur ausnahmsweise Originaldaten im DVZ-Test verarbeiten lassen. Die Einbringung von im Test erstellten Ausgabedatenbeständen in spätere Produktionsläufe läßt darauf schließen, daß hiermit die besonderen für die Produktion geltenden Sicherungsvorkehrungen pragmatisch umgangen werden sollten. Dies ist ein Verstoß gegen Wortlaut und Sinn von Nr. 2.7 der DS-Rahmenregelungen. Auch die DVZ hat gegen diese Bestimmung verstoßen. Gem. Nr. 2.7.2 Satz 2 ist der Rechenstelle eine Durchschrift der schriftlichen Ausnahmegenehmigung der fachlich zuständigen Stelle zu übersenden. Da eine solche schriftliche Genehmigung nicht vorlag, hätte die DVZ die entsprechenden Aufträge nicht ausführen dürfen.

Bei dem geprüften Verfahren hatte die programmierende Stelle weitgehend freie Hand auch bei der Verarbeitung von Originaldaten: Zunächst, d.h. bis Herbst 1986, war die

programmierende Stelle sogar befugt, der DVZ Produktionsaufträge zu erteilen. Damit war die funktionale Trennung der Bereiche Programmierung und Verfahrensanwendung (Nr. 1.2 DS-Rahmenregelungen) nicht gewährleistet.

Beim Test wurden Ausgabedatenbestände — ebenfalls mit echten Daten — erzeugt, die dann in die eigentliche Produktion eingingen. In einem von mir geprüften Produktionsauftrag wird ausdrücklich darauf verwiesen, daß ein Eingabedatenbestand im DVZ-Test erstellt wurde. Diesen Produktionsauftrag hätte die DVZ auf keinen Fall ausführen dürfen. Schon die dauerhafte, vom Statistischen Landesamt verfügte „Sperrung" von Datenbeständen, die im DVZ-Test erzeugt werden, ist problematisch. Dadurch wird verhindert, daß die Datenträger, auf denen sich die Dateien befinden, überschrieben werden. Da es sich im konkreten Fall sogar um Originaldaten mit Personenbezug handelte, besteht die Gefahr, daß hier „schwarze" Dateien entstehen, die sich einer datenschutzrechtlichen Kontrolle weitgehend entziehen und zu einem späteren Zeitpunkt entweder im vorgeblichen Testbetrieb oder in der Produktion ausgewertet werden.

Ich habe bei der Prüfung festgestellt, daß wiederholt Fremdmagnetbänder unter Produktionsbedingungen mit echten Daten beschrieben wurden, die dann auf Anweisung der programmierenden Stelle von der DVZ an das Statistische Landesamt gesandt wurden (Auftragserteilung auf einem Formular mit der Überschrift „Verarbeitung/Ausgabe von Testmagnetbändern"). Da die auf den dem Statistischen Landesamt übersandten Bändern gespeicherten Daten keinen Personenbezug aufweisen, liegt hier zwar kein Verstoß gegen das Datenschutzrecht vor. Der Vorgang offenbart jedoch eine Schwachstelle im DVZ-Sicherheitssystem, der ich im Zusammenhang mit anderen Prüfungen bereits nachgehe.

DVZ-Test- und Produktionsaufträge wurden wiederholt aufgrund fernmündlicher Anweisung durch das Statistische Landesamt von der DVZ abgewickelt und die schriftlichen Aufträge erst nach Abwicklung nachgereicht.

Die Ausführung von Aufträgen aufgrund telefonischer Auftragserteilung ist unzulässig. Selbst wenn Tage oder Wochen später ein ordnungsgemäßer schriftlicher Auftrag folgt, hat die DVZ hiermit gegen Nr. 2.6 DS-Rahmenregelungen verstoßen. Danach müssen Aufträge für Produktionsarbeiten schriftlich erteilt und von Bediensteten unterzeichnet werden, die dazu berechtigt und in das Verzeichnis der Auftragsberechtigten aufgenommen worden sind. Bei (fern-)mündlicher Auftragserteilung ist eine Prüfung der Auftragsberechtigung durch die DVZ und auch eine lückenlose Kontrolle durch den Hamburgischen Datenschutzbeauftragten nicht möglich. Ich habe in der DVZ nicht einmal schriftliche Aufzeichnungen über die mündliche Auftragserteilung gefunden. Ich kann deshalb nicht beurteilen, ob die Aufträge tatsächlich von den dazu befugten Mitarbeitern des Statistischen Landesamtes erteilt wurden. Die nachträglich der DVZ zugesandten schriftlichen Auftragsbestätigungen sind entsprechend den Unterschriftsbefugnissen unterzeichnet worden.

Die Stellungnahme des Senats zu diesen Feststellungen, die Bestandteil meiner Beanstandung der GVE (s. Nr. 4.4.3) waren, konnte mich nun keineswegs davon überzeugen, daß in Zukunft die Einhaltung der Richtlinien mit Nachdruck durchgesetzt wird. Der Senat beantwortete nämlich meine Beanstandung insoweit mit folgenden Ausführungen:

(1) Das bei der Gebäudevorerhebung eingesetzte Verfahren besteht aus einer Folge von Programmen, die — verteilt über einen Zeitraum von mehreren Monaten — nacheinander abgewickelt wurden.

    Dabei sind die einzelnen Produktionsaufträge, die sich auf die Ausführung von einem oder mehreren Programmen als Teil des Gesamtverfahrens bezogen, stets nur für bereits ordnungsgemäß freigegebene Programme erteilt worden.

    Produktionsläufe mit nicht freigegebenen Programmen hat es nicht gegeben. Insofern hat weder das Statistische Landesamt noch die Datenverarbeitungszentrale gegen die Freigaberichtlinien verstoßen.

(2) Ein Verstoß gegen Nr. 2.7 der DS-Rahmenregelungen liegt nicht vor, da im Verlauf des Verfahrens „Gebäudevorerhebung" DVZ-Tests stets von der für die Produktionsaufträge verantwortlichen Stelle in Auftrag gegeben wurden. In keinem Fall handelte es sich um Tests durch den Programmierer, wofür eine Ausnahmegenehmigung durch die fachlich zuständige Stelle hätte eingeholt werden müssen.

(3) Das Verfahren „Gebäudevorerhebung" ist in einer Reihe von Arbeitsschritten in Abstimmung zwischen der fachlich zuständigen Stelle und der Produktionssteuerung in der Datenverarbeitungszentrale abgewickelt worden. Zur Beschleunigung des Gesamtablaufs sind in einigen wenigen Fällen auch mündliche Aufträge von Auftragsberechtigten ausgeführt und dokumentiert worden. Da in jedem Fall unverzüglich ein schriftlicher Auftrag folgte, sind die Notizen über die mündlichen Aufträge vernichtet worden.

(4) Der Senat folgt dem Datenschutzbeauftragten insofern, als er es für erforderlich hält, die internen Richtlinien strikter zu befolgen als es hier geschehen ist. Wenn z.B. ausnahmsweise mündliche Aufträge ausgeführt werden, müssen diese auch nach — unerläßlicher — schriftlicher Bestätigung prüfungsfähig dokumentiert bleiben.

Mit diesen Feststellungen wird insbesondere die Bedeutung einer Verfahrensfreigabe nicht angemessen berücksichtigt. Die Verfahrensfreigabe ist durchaus nicht identisch mit der Summe der Programmfreigaben, sie ist etwas anderes, und zwar ein „Mehr". Unter 3.4.2 wird dies näher ausgeführt werden.

Die Antwort des Senats stellt die Grundprinzipien einer sicheren und ordnungsgemäßen Datenverarbeitung infrage. Diese Grundprinzipien sind die Funktionstrennung hinsichtlich der am Verfahren Beteiligten sowie die strikte Trennung von Entwicklung und Test von der Produktion. Sie sind auch das „Herzstück" der ADV-Richtlinien des Senatsamtes für den Verwaltungsdienst. Wenn der Senat auf meine Beanstandungen zum Ablauf der Tests beim Verfahren GVE und zur Verwendung von im DVZ-Test erzeugten Ausgabedatenbeständen für die Produktion antwortet (s. oben (2), ein Verstoß gegen Nr. 2.7 der DS-Rahmenregelungen liege nicht vor, da DVZ-Tests stets (!) von der für die Produktionsaufträge verantwortlichen Stelle in Auftrag gegeben wurden, und in keinem Fall habe es sich um Tests durch den Programmierer gehandelt, wofür eine Ausnahmegenehmigung der fachlich zuständigen Stelle hätte eingeholt werden müssen, so stellt dies eine Wertung dar, die dem Sachverhalt nicht entspricht: Das gesamte Testgeschehen ist mit den einschlägigen Richtlinien nicht in Einklang zu bringen. Begriffe wie Testdaten, Funktionstest, Abnahmetest kommen in diesem Testgeschehen nicht vor. Da ist es kaum verwunderlich, wenn — angeblich ohne „Unrechtsbewußtsein" - im Testbetrieb erzeugte Datenausgaben als Eingabedatenbestände in die Produktion einfließen. Es ist aber unzulässig, im Test erzeugte Datenbestände für andere als Testzwecke zu verwenden, d.h. es ist unzulässig, diese Datenbestände für die Produktion zu verwenden, auch wenn sie im Auftrag oder mit Genehmigung der fachlich zuständigen Stelle ausnahmsweise mit echten Daten in einem DVZ-Test erzeugt wurden.

Auch die unter (1) zitierte Antwort des Senats ist dem beanstandeten Sachverhalt nicht angemessen: Der Hinweis auf vorliegende Programmfreigaben liegt neben der Sache, weil ich die fehlende Verfahrensfreigabe gerügt hatte.

Zwar hat sich der Senat meiner Beurteilung, gegen seine Richtlinien sei im Verfahren GVE verstoßen worden, in seiner Stellungnahme nicht angeschlossen (s.o. (1) bis (3)). Dennoch hatte ich mir wegen seiner abschließenden Feststellung, er folge mir darin, daß die internen Richtlinien strikter als hier geschehen zu befolgen seien (s.o. (4)), Hoffnung gemacht, er werde nunmehr mit Nachdruck auf Einhaltung der Richtlinien drängen. In dieser Hoffnung fühlte ich mich noch bestärkt durch die ergänzenden Ausführungen des Staatsrates der Behörde für Inneres, mit denen er mir die Antwort des Senats auf meine Beanstandungen übermittelt hatte:

„Die Feststellungen des Senats zum Datenverarbeitungsverfahren beziehen sich nur auf die Frage, ob es in der Vergangenheit Verstöße gegen datenschutzrechtliche Bestimmungen (Datenschutzrahmenregelungen, Freigaberichtlinie, Dokumentations-

richtlinie) gegeben hat. Sie entbinden die beteiligten Diensstellen nicht von der Aufgabe zu prüfen, welche zusätzlichen Sicherungen über die bestehenden Regelungen hinaus wegen der besonderen Sensibilität der Volkszählungsdaten erforderlich sind. Dies gilt insbesondere hinsichtlich der internen Abschottung in der Datenverarbeitungszentrale sowie des Verfahrens bei der Freigabe von Programmen beziehungsweise von Programmteilen. Nach dem Ergebnis des von Ihnen am 28.4.1987 mit Vertretern des Senatsamtes für den Verwaltungsdienst, der Finanzbehörde und der Behörde für Inneres geführten Gesprächs besteht kein Zweifel, daß die Probleme einvernehmlich gelöst werden."

Inzwischen hat sich gezeigt, daß eine „einvernehmliche Lösung der Probleme" jedenfalls nicht in allen Punkten gefunden wurde, s. dazu Nr. 4.4.3.2.

3.4.2 Personalamtsverfahren

Die Entwicklung des jetzigen Programmsystems begann nach Einrichtung der Besoldungs- und Versorgungsstelle (BVSt) im Jahre 1962 schrittweise. Heute werden mit den Programmen des Personalamtsverfahrens die Bezüge von über 65.000 Versorgungsempfängern und etwa 115.000 aktiven Beschäftigten berechnet und angewiesen. Für Angestellte, Arbeiter, Beamte, den Personenkreis nach Art. 131 GG, sonstige Beschäftigte und Versorgungsempfänger werden Löhne und Gehälter, Steuern und Sozialabgaben errechnet, gezahlt, verbucht. Dabei werden Pfändungen und Abtretungen ebenso wie vermögenswirksame Anlagen von Teilen der Bezüge, BHW-Beiträge u.a. berücksichtigt. In allen Berechnungen und Buchungen gibt es darüber hinaus die Möglichkeit der rückwirkenden Neuberechnung, d.h. es können auch historische Daten verarbeitet werden.

Natürlich ist ein solches Verfahren außerordentlich komplex und wegen ständig sich ändernder Gesetze, Tarife, Beitragsregelungen usw. häufigen Änderungen unterworfen. Die Programme sind in Assembler, einer maschinenorientierten Sprache, geschrieben. Programme in dieser Sprache können sehr effektiv sein und sich durch kurze Laufzeiten im Rechenzentrum auszeichnen. Sie sind aber nicht besonders wartungsfreundlich und für Außenstehende nur schwer nachvollziehbar. (Seit langem besteht daher für die hamburgische Verwaltung die Regelung, daß Programme nur mit einer besonderen Genehmigung durch das Senatsamt für den Verwaltungsdienst in Assembler geschrieben werden dürfen.) Die Einarbeitung eines neuen Mitarbeiters in Assembler-Programme ist grundsätzlich zeitaufwendig und schwierig, um so mehr, wenn die Programme auch noch so komplex und fachlich anspruchsvoll sind wie die des Personalamtsverfahrens. Ein derartiges Verfahren zu prüfen, ist für interne Kontrollorgane (Innenrevisoren, DV-Revisor) und erst recht für externe Kontrollorgane (Rechnungshof, HmbDSB) mit erheblichem zeitlichen Aufwand verbunden und erfordert eine hohe fachliche Kompetenz. Um den Aufwand in angemessenen Grenzen zu halten, habe ich meine Prüfung des Verfahrens, mit der ich Mitte 1987 angefangen habe, von Anfang an ganz bewußt auf wenige — datenschutzrechtlich bedeutsame — Schwerpunkte beschränkt:

(1) Prüfung in organisatorisch-technischer Hinsicht, und zwar als summarische Prüfung und Beurteilung der Ordnungsmäßigkeit des Gesamtverfahrens (Zulässigkeit, Prüfbarkeit, Sicherheit) und als Prüfung ausgewählter Details unter primär technisch-organisatorischen Aspekten,

(2) Prüfung der rechtlichen Grundlagen der Datenverarbeitung am Beispiel des Verfahrens für die Angestellten der FHH.

Die Prüfung wurde erschwert durch den Umstand, daß eine allgemeine Verfahrensbeschreibung im Sinne der Dokumentationsrichtlinie nicht vorhanden ist. Dieser Teil der Dokumentation ist aber ebenso wichtig wie etwa die Programmdokumentation. Er soll Aufschluß geben über

— die mit dem Verfahren zu erfüllende Aufgabe,

— die beteiligten Stellen und ihre Funktionen,

— die Auftragsberechtigten und den Umfang der jeweiligen Berechtigungen,

— den Verfahrensablauf (Gliederung und Termine),

— den Aufbau des Programmsystems und

— die zu verarbeitenden Daten.

Die allgemeine Verfahrensbeschreibung ist wesentliche Voraussetzung für die Prüfbarkeit eines Verfahrens, und zwar sowohl für die fachlich zuständige Stelle als auch für externe Prüfer.

Die fachlich zuständige Stelle soll in der allgemeinen Verfahrensbeschreibung eine Darstellung des fachlichen Konzepts vorfinden, das sie nach rechtlicher Zulässigkeit, fachlicher Richtigkeit und Angemessenheit der Organisation zu beurteilen hat. Ist das Konzept in Ordnung, soll es der fachlich zuständigen Stelle, der programmierenden Stelle und Kontrollorganen (DV-Revisor, Rechnungshof, Datenschutzbeauftragter) als Maßstab für Prüfungen von Testergebnissen und als Maßstab für die Prüfung der Ordnungsmäßigkeit der Datenverarbeitung dienen.

Da eine allgemeine Verfahrensbeschreibung für das Personalamtsverfahren bis heute nicht erstellt worden ist, kann es nicht überraschen, daß das Verfahren als Ganzes bis heute nicht freigegeben ist (es werden nur jeweils Programme freigegeben). Mit der Verfahrensfreigabe soll die Übernahme der Verantwortung für die Anwendung eines Verfahrens durch die für eine bestimmte Verwaltungsaufgabe fachlich zuständige Stelle dokumentiert werden (vgl. hierzu auch 4.4.3.2). Die fachlich zuständige Stelle bringt mit der formellen Freigabe zum Ausdruck, daß das vorgesehene Verfahren den rechtlichen (Zulässigkeit), sonstigen fachlichen (Richtigkeit, Vollständigkeit) und organisatorischen (Sicherheit, Wirtschaftlichkeit, Pünktlichkeit, Benutzerfreundlichkeit) Anforderungen der Aufgabe entspricht. Weil eine allgemeine Verfahrensbeschreibung fehlt, war es mir noch nicht möglich, die Zulässigkeit des Verfahrens in jeder Hinsicht zu beurteilen. Zulässig ist die Datenverarbeitung einer öffentlichen Stelle dann, wenn sie zur rechtmäßigen Aufgabenerfüllung im Zuständigkeitsbereich dieser Stelle (der „speichernden Stelle") erforderlich ist. Da die Aufgabe der BVST und die Aufgaben, zu deren Erfüllung das Personalamtsverfahren tatsächlich eingesetzt wird, aber noch nicht im Zusammenhang und übersichtlich dargestellt sind, was bei Beachtung der Dokumentationsrichtlinie hätte geschehen sein müssen, müssen sie erst noch ermittelt und dargestellt werden.

Erst nach der Verfahrensfreigabe darf ein Verfahren zur Produktion eingesetzt werden. Die Integrität der Programme ist zu sichern. Nach notwendigen Programmänderungen ist grundsätzlich eine erneute Freigabe des Verfahrens oder — falls selbständige Verfahrensteile definiert sind — des Verfahrensteils erforderlich. Die Freigabe hat nach der Freigaberichtlinie in einem formellen Verfahren zu erfolgen. Kennzeichnend für dieses Verfahren sind getrennte Tests der fachlich zuständigen Stelle (Abnahmetest) und der programmierenden Stelle (Funktionstest), getrennte Testdatenbestände sowie getrennte Bibliotheken.

Für das Personalamtsverfahren wird die Freigaberichtlinie bisher nicht angewendet. Zwar stammt die Richtlinie erst aus dem Jahre 1982 und das Personalamtsverfahren war bei ihrer Einführung fast zwanzig Jahre in Betrieb. Dennoch ist es datenschutzrechtlich von Bedeutung, daß fünf Jahre nach Inkrafttreten der Freigaberichtlinie (1. 1. 83) dieses Verfahren noch betrieben wird, ohne wenigstens nachträglich und nach dem derzeitigen Stand freigegeben worden zu sein und ohne Anwendung des vorgeschriebenen Testverfahrens.

In dem Text, mit dem die Freigaberichtlinie seinerzeit eingeführt wurde (MittVw 1982 S. 70), wird unter Nr. 2 bestimmt: Die Richtlinie gilt für alle Verfahren, die nach dem 1. 1. 83 für die Erledigung von Aufgaben der FHH angewendet werden. Nach Nr. 3 des Vortextes können unter besonderen Voraussetzungen, deren Vorliegen beim Personalamtsverfahren unterstellt werden mag, für eine Übergangszeit Abweichungen im Einvernehmen mit dem Senatsamt für den Verwaltungsdienst zugelassen werden. Sollte

es eine solche einvernehmliche, abweichende Regelung geben (mir ist sie jedenfalls nicht bekannt), so kann nach nunmehr fünf Jahren seit Inkrafttreten der Richtlinie m.E. keine „Übergangs"-Regelung mehr zulässig sein.

Programme für das Personalamtsverfahren werden — wie ich festgestellt habe — für die fachlich zuständige und die programmierende Stelle zusammen in einem gemeinsamen Test getestet. Der Test wird von einer eigens dafür gebildeten Funktionseinheit „Testbuchhaltung" mit einem von dieser selbst erstellten und fortgeschriebenen Testdatenbestand durchgeführt. Die Freigabe der Programme erfolgt auf einem Vordruck, der von dem Muster in der Freigaberichtlinie abweicht. Ich habe mir noch kein abschließendes Urteil darüber gebildet, ob das vom Personalamt praktizierte Freigabeverfahren als geeignete Lösung im Sinne der Ordnungsmäßigkeit der Datenverarbeitung zu beurteilen ist. Festzustellen ist aber, daß dieses Verfahren gegen die z.Z. geltende verbindliche Richtlinie verstößt.

Die Überprüfung des Personalamtsverfahrens wird fortgesetzt.

3.5 Verarbeitung personenbezogener Daten auf Personalcomputern (PC)

Der verstärkte Einsatz von Personalcomputern in der Verwaltung bringt Probleme für die Gewährleistung des Datenschutzes mit sich, auf die ich bereits in meinen letzten beiden Tätigkeitsberichten (4. TB, 3.3, S. 13 ff. und 5. TB, 3.1, S. 6 ff.) eingegangen bin.

3.5.1 Spezifische Risiken des PC Einsatzes

Die zusätzliche Flexibilität , die die kleinen Rechner im Vergleich zur klassischen Groß-DV bieten, wird mit dem Preis zusätzlicher spezifischer Risiken bezahlt:

Zentrale, allgemein hochentwickelte Schutzmechanismen die im Großrechnerbereich der übliche Standard sind, entfallen weitgehend.

Die organisatorische und personelle Funktionstrennung zwischen Entwicklung, Anwendung und Betrieb ist zumeist aufgehoben zugunsten einer direkten, alleinigen Verfügbarkeit des Gerätes, des Betriebssystems, der Programme und der Datenträger für den Benutzer. Ein tragendes Prinzip der Datensicherung, das „Vier-Augen-Prinzip", wird bei der PC-Nutzung zumeist nicht angewandt.

Leicht transportable Datenträger mit immer größerer Speicherkapazität erschweren die gesetzlich vorgeschriebene Abgangskontrolle, d.h. Maßnahmen, die verhindern sollen, daß bei der Datenverarbeitung tätige Personen unbefugt Datenträger entfernen.

Während durch hochentwickelte Test-, Freigabe-, und Katalogisierungsverfahren bei Großrechnersystemen im allgemeinen sichergestellt wird, daß nur zugelassene und geprüfte Programme für die DV eingesetzt werden, ist der Nutzbarkeit beliebiger, in bezug auf Qualität und Leistungsumfang nicht immer überschaubarer eigener und erworbener Programme auf PC's kaum eine Grenze gesetzt. Dadurch wird die Ordnungsmäßigkeit der DV in Frage gestellt.

Dem Nutzer von PC's ist es möglich, „eigene" Datenbestände fast beliebig anzulegen, aus fremden Quellen zu übernehmen, diese zu verknüpfen und mit einfachsten Mitteln auszuwerten, z.B. mit preiswerten, auf PC's lauffähigen Datenbanksystemen.

Bisher waren nur wenige Mitarbeiter mit entsprechenden Vorkenntnissen mit der DV befaßt. Die PC-Anwender in den Fachbereichen verfügen demgegenüber häufig weder über entsprechende Kenntnisse noch über das notwendige Problembewußtsein. Im umgekehrten Verhältnis zu den gestiegenen technischen Möglichkeiten, die sich aus dem PC-Einsatz ergeben, stehen die technisch unterstützten Sicherungs- und Kontrollmechanismen. So verfügt das am weitesten verbreitete PC-Betriebssystem standardmäßig weder über wirkungsvolle Zugriffs-, Benutzer- und Eingabekontrollsysteme noch über Logprotokollierung oder Verschlüsselung. Zwar versucht eine Vielzahl von freien Anbietern diese Marktlücke zu füllen. Standard-Produkte auf dem Gebiet Datensicherungssoftware für PC's , die allen Anforderungen genügen, sehe ich z.Z. jedoch noch nicht.

3.5.2 Zuständigkeit für die Sicherstellung des Datenschutzes gem. § 16 HmbDSG

Gem. § 16 HmbDSG haben die Behörden sicherzustellen, daß die Datenschutzvorschriften eingehalten werden. Insbesondere haben sie dafür zu sorgen, daß die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, überwacht wird (ADV-Revision). Der Senat hat von der ihm durch § 16 Satz 3 HmbDSG eingräumten Möglichkeit Gebrauch gemacht, die ADV-Revision einer anderen als der datenverarbeitenden Behörde zuzuweisen, weil die Überwachung besondere Fachkenntnisse hinsichtlich der verwendeten Datenverarbeitungssysteme erfordert. Durch Zuständigkeitsanordnung vom 25. Mai 1982 hat er diese Aufgabe dem Senatsamt für den Verwaltungsdienst zugewiesen.

Die mit den IuK-Entscheidungen des Senats (vg. 4. TB, 3.1, S. 9) angestrebte vergrößerte Entscheidungskompetenz der Behörden für die einzelnen Automationsvorhaben stellt auch in bezug auf die zu treffenden Datensicherungsmaßnahmen die behördliche Eigenverantwortung vor neue Aufgaben. Wenn — wie dies offenbar angestrebt wird — die ADV-Revision, soweit es sich um autonome Anlagen handelt, auf die Fachbehörden verlagert werden soll, so muß dies selbstverständlich mit einer Übertragung qualifizierter personeller Ressourcen und mit einer größeren Bereitschaft der Fachbehörden einhergehen, die Belange des Datenschutzes schon in der Projektierung von ADV-Vorhaben zu berücksichtigen.

3.5.3 „Vorläufige Hinweise"
des Senatsamtes für den Verwaltungsdienst — Organisationsamt —

Ich habe wiederholt angeregt, von zentraler Stelle Rahmenregelungen für den Einsatz dezentraler DV-Anlagen in der Hamburger Verwaltung zu erlassen (vgl. 5. TB, 3.1.3, S. 10), die von den Fachbehörden auszufüllen wären. Das Senatsamt für den Verwaltungsdienst (Organisationsamt) hat inzwischen mit mir abgestimmte vorläufige Hinweise für die Verarbeitung personenbezogener Daten auf Personalcomputern (PC's) in der Verwaltung herausgegeben. Nach einer Schilderung der mit dem PC-Einsatz zusammenhängenden zusätzlichen Risiken (vgl. 3.5.1) werden Maßnahmen dargestellt, die zur Gewährleistung des Datenschutzes bei der Nutzung von PC's zu ergreifen sind. Ausgehend davon, daß die einschlägigen Rechtsvorschriften wie HmbDSG, BDSG, Sozialbesetzbuch auch für autonome Anwendungen gelten, wird darauf hingewiesen, daß es nach § 16 HmbDSG den Behörden obliege, den Datenschutz in ihrem Bereich sicherzustellen. Da sich Schutzmaßnahmen in jedem Fall auch nach der Schutzwürdigkeit der Daten zu richten hätten, dürften personenbezogene Daten auf dem PC nicht schlechter geschützt werden als auf dem Großrechner.

Bei der Verarbeitung personenbezogener Daten auf PC werden im einzelnen folgende Maßnahmen vorgeschlagen:

Die Verantwortlichkeiten der Benutzer, ggf. auch der Stellen, die die Anlagen betreiben oder die Programme entwickeln, seien klar zu regeln. Die Datenschutz- und Datensicherungsmaßnahmen seien entsprechend den konkreten Bedingungen der Aufgaben und der Aufgabenerfüllung festzulegen.

Es sei vorzusehen, revisionsfähige Unterlagen (z.B. Logprotokoll oder Logbuch, Inventarisierung der Datenträger, Zuordnung von Benutzern zu Benutzergruppen, Art und zeitliche Befristung von Berechtigungen, Programmdokumentation) zu führen.

Soweit realisierbar, sollten die Funktionen Entwicklung, Systemverantwortung und Benutzung aufbauorganisatorisch getrennt werden. Schon bei der Entwicklung sei zu klären, welcher Benutzer welche Daten für die Aufgabenerfüllung benötige. Wenn eine Funktionstrennung nicht oder nur unzureichend zu gewährleisten sei, erhalte die interne Datenschutzkontrolle besonderes Gewicht.

Information und Schulung der Beteiligten seien zu gewährleisten.

Es sei zu prüfen, wieweit die organisatorischen Maßnahmen zur Datensicherung von technischen und baulichen Maßnahmen flankiert werden müssen. Beispielhaft nennt das Senatsamt

— Räumliche Abschottung (Zugang, Verwahrung von Daten und Programmen),

— Zugangsprüfung (Schlüssel, Karten, Passwords, Benutzerkennung, Benutzungsprofile),

— Versiegelung von Programmen, Freigabe von Verfahren, strikte Menüsteuerung,

— Beschränkung auf Festplatten,

— Verschlüsselte Speicherung sensibler Daten.

Die datenschutzrechtlichen Anforderungen sollen bereits in die Konzeptentwicklung einbezogen werden. Auch beim Ausbau technischer Infrastruktur für nicht vorweg bekannte Anwendungen sei zu bedenken, ob später die Verarbeitung personenbezogener Daten in Frage kommen könnte und deshalb hierfür technische Grundvoraussetzungen gesichert werden müßten.

Im Einzelfall wird vom Organisationsamt eine Schwachstellenanalyse zur Klärung von Schutzwürdigkeit und Gefährdungsrisiko der Daten empfohlen. Die Anforderungen seien im Zusammenhang zu sehen. Entscheidend sei das Gesamtkonzept für einen Aufgabenbereich. Die Risiken müßten jeweils konkret bewertet werden. Nach der Abstufung von Schutzwürdigkeit und Risiken bestimmen sich die Beurteilungsspielräume und die erforderlichen Maßnahmen. Wenn technische Lösungen ausschieden, könnten u.U. organisatorische Alternativen in Betracht gezogen werden.

In Zweifelsfällen empfiehlt das Organisationsamt die Einschaltung des Hamburgischen Datenschutzbeauftragten. Generell legt das Organisationsamt den Behörden nahe, sich bei der Speicherung und Verarbeitung personenbezogener Daten auf PC zurückzuhalten. Zu beachten sei auch das Risiko, daß am Rande an sich unkritischer PC-Anwendungen aus unzureichendem Problembewußtsein „nebenbei" personenbezogenen Daten mit erhoben, gespeichert und verarbeitet werden. Im Zweifel, wenn die erforderlichen Maßnahmen nicht zu gewährleisten seien, sei von der Speicherung und Verarbeitung personenbezogener Daten auf einem PC abzuraten.

Ich sehe in diesen vorläufigen Hinweisen einen Schritt in Richtung auf einen sensibleren Umgang mit personenbezogenen Daten, soweit diese auf PC's verarbeitet werden. Gleichwohl ist nicht geklärt, welchen Grad an Verbindlichkeit diese Hinweise haben und wie die Fachbehörden den gesetzten Rahmen ausfüllen.

Die vorläufigen Hinweise stehen — obwohl sich an verschiedenen Stellen Überschneidungen ergeben — neben den bisherigen verwaltungsinternen Datensicherungsvorschriften (DS-Richtlinie, DS-Rahmenregelungen, Freigaberichtlinie und Dokumentationsrichtlinie, vgl. hierzu auch Abschnitt 3.4), ohne daß das Verhältnis der Hinweise zu diesen Regelungen geklärt ist. M.E. besteht die dringende Notwendigkeit, die vorhandenen Regelungen so zu überarbeiten, daß sowohl die neueren Entwicklungen im Großrechnerbereich als auch der Einsatz von dezentralen Anlagen eingefangen werden.

Ich habe Grund zu der Annahme, daß die empfohlene Zurückhaltung bei der Verarbeitung personenbezogener Daten auf PC's nicht von allen Behörden geteilt wird.

3.6 TEMEX

In meinem letzten Bericht (5. TB Seite 17, 18) hatte ich angekündigt, die weitere Entwicklung des TEMEX-Dienstes der Deutschen Bundespost in Hamburg aufmerksam zu verfolgen und weiter darüber zu berichten.

Am 3. 11. 1987 ist nun der Betriebsversuch für Hamburg (es laufen Betriebsversuche in zehn weiteren Städten) eingeschaltet worden. Das TEMEX-Netz für den hamburgischen Betriebsversuch kann wie folgt beschrieben werden:

An die TEMEX-Hauptzentrale im Fernmeldeamt 6 in der Binderstaße sind vier TEMEX-Zentralen und fünf TEMEX-Konzentratoreinrichtungen sternförmig angeschlossen. Die TEMEX-Zentralen befinden sich in den Stadtteilen Uhlenhorst (Anschlußbereich —

AsB — 22), Bergedorf (AsB 721), Altstadt (AsB 32) und Blankenese (AsB 86). TEMEX-Konzentratoreinrichtungen stehen zur Verfügung in Hamm (AsB 21), Lohbrügge (AsB 738), Harburg (AsB 77), Heimfeld (AsB 790) und Rotherbaum (AsB 44). Diese regionale TEMEX-Netz-Insel ist nicht mit den in anderen Städten geschaffenen regionalen TEMEX-Inseln verbunden und wird dies auch nicht bei einer bundesweiten Einführung des TEMEX-Dienstes als Regeldienst. Typische Fernwirkanwendungen sind nämlich in der Regel regional strukturiert, weil die Dienstleistungsanbieter überwiegend Leistungen mit begrenztem Wirkbereich anbieten. In Anlehnung an diesen Bedarf sind die TEMEX-Gesamtsysteme als regionale Inseln ausgelegt. Gleichwohl können Fernwirkleitstellen von Dienstleistungsanbietern auch dann betrieben werden, wenn sie sich außerhalb des regionalen Bereichs der zuständigen TEMEX-Hauptzentrale befinden. Die Anbindung der Fernwirkleitstellen an die TEMEX-Hauptzentrale oder eine TEMEX-Zentrale erfolgt über die von der Post angebotenen DATEL-Dienste (Direktrufverbindung, Datex-L-Verbindung, Fernsprechverbindung). Die TEMEX-Endgeräte und Endeinrichtungen (Sensoren, Notrufmelder, Zähler usw.) sind über Telefonanschlußleitungen mit der nächsten Ortsvermittlungsstelle, bei der eine TEMEX-Zentrale eingerichtet ist, verbunden. TEMEX-Zentralen sind an die TEMEX-Hauptzentrale über feste Verbindungen (Fernsprechleitungen mit höherer Übertragungsgeschwindigkeit) angeschlossen.

Im Rahmen der öffentlichen Veranstaltung zur Einschaltung des Betriebsversuchs in Hamburg wurden Beispiele für die Möglichkeiten des neuen Dienstleistungsangebots der Post demonstriert:

— Das Öffnen einer durch Sensor überwachten Tür löste eine entsprechende Meldung auf dem Bildschirm der Fernwirkleitstelle aus, der die Überwachung der Tür übertragen war.

— Nach Absetzen eines entsprechenden, per TEMEX übertragenen Befehls in der Fernwirkleitstelle wurde durch Schließen eines entsprechenden Kontaktes eine Lampe in einem von der Fernwirkleitstelle betreuten Objekt (Gebäude usw.) eingeschaltet.

— Nach Absetzen eines entsprechenden Befehls in der Fernwirkleitstelle wurde von einem an TEMEX angeschlossenen Zähler der momentane Zählerstand übermittelt und auf dem Bildschirm in der Fernwirkleitstelle angezeigt.

— Eine Dame in einem Altersheim in Bergedorf betätigte „ihre" Notrufklingel und löste damit eine Meldung in „ihrer" Fernwirkleitstelle in einem anderen Stadtteil aus. Die Fernwirkleitstelle, die eine entsprechende Notrufanwendung als Dienstleistung betreibt, veranlaßte darauf per TEMEX das Aufleuchten eines Signallämpchens im Zimmer der alten Dame zum Zeichen, daß ihr Notruf gehört worden war, und informierte gleichzeitig den Notarzt, der sich alsbald im Notarztwagen zu der alten Dame auf den Weg machte.

Diese Beispiele veranschaulichen drei der vier Grundtypen von TEMEX-Anwendungen, nämlich Fernanzeigen (Öffnen der Tür, Notrufsignal), Fernmessen (Ablesen des Zählerstandes), Fernschalten (Einschalten der Lampen). Für die vierte typische Anwendung, das Ferneinstellen, wurde in der Demonstration kein Beispiel geboten. Denkbar ist z.B. die Übermittlung bestimmter Informationen aufgrund von erhaltenen Meßwerten durch eine Fernwirkleitstelle, wie es bei einem Parkleitsystem realisiert werden könnte.

Demnächst ist die Einberufung eines Begleitgremiums durch die Deutsche Bundespost geplant. In diesem Begleitgremium werden Vertreter der Post, der Diensteanbieter und der Datenschutzbeauftragten insbesondere datenschutzrechtliche Aspekte, die mit TEMEX oder mit Dienstleistungen unter Einsatz von TEMEX in Zusammenhang stehen, untersuchen. An diesem Begleitgremium werde ich mich beteiligen. Daneben wird der Betriebsversuch durch das Fraunhofer-Institut wissenschaftlich begleitet. Das Institut wird aus statistischen Auswertungen Empfehlungen an die Deutsche Bundespost ableiten.

Ich plane, im nächsten Berichtszeitraum wenigstens ein konkretes Dienstleistungsangebot mit TEMEX-Anwendung näher zu untersuchen, da es — wie ich schon in meinen früheren Berichten ausgeführt habe — weniger die TEMEX-Technik ist, die datenschutzrechtliche Probleme aufwirft, als vielmehr die Gesamtumstände und vertraglichen Bedingungen einer TEMEX-Anwendung.

4. Einzelne Probleme des Datenschutzes im öffentlichen Bereich

4.1 Sozialwesen

In einer Zeit, in der die Sozialhilfe sich für eine ständig steigende Zahl von Bürgern als das „letzte Netz" der sozialen Sicherung bewähren muß, ist es besonders wichtig, daß niemand aus der Sorge heraus, irgend jemand aus seinem sozialen Umfeld könne von seiner Hilfsbedürftigkeit erfahren, davon abgehalten wird, sein Recht geltend zu machen und Sozialhilfe zu beantragen. Deshalb müssen Hilfeempfänger darauf vertrauen können, daß die Vorschriften zum Schutz ihrer zum Teil sehr sensiblen Daten von der Verwaltung strikt beachtet werden.

Leider stelle ich aber immer wieder fest, daß die Verwaltung noch weit davon entfernt ist, dem Sozialdatenschutz den erforderlichen Stellenwert einzuräumen. Die Ursachen dafür sind vielfältig und können hier nur skizziert werden.

Es war und ist in der Sozialverwaltung üblich, daß vorhandene Daten über Leistungsempfänger und ggf. auch deren Angehörige anderen Sozialleistungsträgern auf Anfrage zur Verfügung gestellt werden. Zur Begründung wird in vielen Fällen auf § 69 SGB X verwiesen, wonach die Offenbarung personenbezogener Daten u.a. zulässig ist für die Erfüllung sozialgesetzlicher Aufgaben. Häufig wird dabei nicht berücksichtigt, daß die Befugnis zur Informationsverarbeitung nur so weit reicht, wie dies für die gesetzliche Aufgabenerfüllung im Einzelfall erforderlich ist. Der Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen muß darüber hinaus — gemessen an der konkreten Aufgabe — verhältnismäßig sein. Aus dem Grundsatz der Verhältnismäßigkeit folgt z.B., daß Akten nicht komplett weitergegeben werden dürfen, wenn dem Empfänger die Kenntnis von Teilen der Akte ausreichen würde.

Seit Inkrafttreten der Vorschriften über den Sozialdatenschutz (SGB X) sind inzwischen sieben Jahre verstrichen. Nunmehr ist es an der Zeit, von alten Denk- und Organisationsmustern Abschied zu nehmen, wonach im Zweifel verwaltungsökonomischen Gesichtspunkten eine höhere Bedeutung beigemessen wird als dem Recht der Hilfeempfänger auf Schutz ihrer Sozialdaten. Als Beispiel für ein Verwaltungshandeln, das längst hätte aufgegeben werden müssen und an dem immer noch zäh festgehalten wird, nenne ich die Angabe von Sozialdaten auf Überweisungsträgern (vgl. 4.1.6) und die Weitergabe von Betroffenen-Daten in Aktendeckeln statt in verschlossenen Briefumschlägen.

Wünschenswert wäre in diesem Zusammenhang auch ein kritischer Umgang mit Verwaltungsanweisungen, die naturgemäß nicht alle datenschutzrechtlichen Probleme, wie sie im konkreten Einzelfall für eine Einstellung, die die Interessen der Betroffenen nicht hinreichend beachtet, entstehen können, berücksichtigen. Soweit Verstöße gegen das Sozialgeheimnis auf Unsicherheit bei der Anwendung gesetzlicher Vorschriften zurückzuführen sind, liegt dies sicher auch daran, daß bisher erst ein verschwindend geringer Teil der Sachbearbeiter in Sozialdienststellen in Fragen des Datenschutzes aus- bzw. fortgebildet wurde.

Eine weitere Ursache ist das durchaus berechtigte Bestreben der Verwaltung zu verhindern, daß Sozialleistungen zu Unrecht beansprucht werden. Dies hat aber dazu geführt, daß von den Betroffenen in der Regel mehr Informationen und Nachweise gefordert werden, als für die Entscheidung über den jeweils konkreten Antrag erforderlich ist. Dieses Mißtrauen gegenüber Hilfeempfängern, das sich auch in vielen Vor-

drucken, mit denen Daten erhoben werden, wiederfindet, steht in deutlichem Widerspruch zu der Tatsache, daß in Hamburg jährlich nur etwa 150 Strafanzeigen wegen mißbräuchlicher Inanspruchnahme von Sozialleistungen erstattet werden.

Um Mißverständnissen vorzubeugen: Meine Kritik richtet sich nicht in erster Linie gegen die „vor Ort" tätigen Sachbearbeiter. Deren Arbeitspensum hat inzwischen ein solches Ausmaß erreicht, daß häufig schlicht die Zeit fehlt, Fragen des Datenschutzes im Einzelfall zu prüfen. Letztlich sind Senat und Bürgerschaft aufgerufen, trotz der angespannten Haushaltslage die Sozialdienststellen in personeller, organisatorischer und räumlicher Hinsicht so auszustatten, daß die in diesem Bereich tätigen Mitarbeiter nicht ständig Gefahr laufen, mit dem Gesetz in Konflikt zu kommen und die betroffenen Hilfeempfänger und deren Angehörige darauf vertrauen können, daß ihre Daten bei der Verwaltung so geschützt sind, wie es das Gesetz verlangt.

4.1.1 Räumliche Verhältnisse und namentlicher Aufruf in den Sozialdienststellen der Bezirksämter

Im Berichtszeitraum habe ich in verschiedenen Sozialämtern die räumlichen Verhältnisse und den organisatorischen Ablauf bei der Bedienung des Publikums geprüft. Anlaß war u.a. die Beschwerde eines Bürgers, der mir mitteilte, daß er auch auf mehrfach vorgetragene Bitte kein Einzelgespräch mit seinem Sachbearbeiter gewährt bekommen habe. Da immer mindestens zwei Beratungen in einem Zimmer stattgefunden hätten, kenne er inzwischen die Lebensgeschichte mehrerer Hilfeempfänger. Der Petent trug weiter vor, er habe bereits mehrfach die Möglichkeit gehabt, die auf dem Schreibtisch seines Sachbearbeiters gestapelten Personalausweise der Hilfeempfänger an sich zu nehmen, wenn sich sein Sachbearbeiter vom Schreibtisch entfernt habe. Es sei nicht auszuschließen, daß sein Personalausweis einmal in falsche Hände gelange.

Von mehreren Bürgern wurde ich gebeten, darauf hinzuwirken, daß der namentliche Aufruf in den Wartezonen der Sozialämter unterbleibt.

Eine Hilfeempfängerin beschwerte sich z.B. darüber, daß ein junger Mann, dessen Annäherungsversuche sie in der Wartezone des Sozialamtes abgewehrt habe, sich beim Aufruf ihren Namen notiert und sie danach mehrfach telefonisch belästigt habe.

Meine Prüfungen vor Ort ergaben, daß die räumlichen Verhältnisse Einzelgespräche im wesentlichen nicht zulassen. Die Büros sind größtenteils mit zwei Sachbearbeitern, teils noch zusätzlich mit einem Mitarbeiter besetzt. Ein leeres Zimmer, in dem auf Wunsch von Hilfeempfängern Einzelgespräche stattfinden könnten, steht einigen Sozialämtern nicht zur Verfügung. Allerdings waren einige Räume krankheits- oder urlaubsbedingt nicht besetzt, so daß hier durchaus eine Ausweichmöglichkeit bestand, die aber nicht genutzt wurde. Der Ablauf in den Sozialämtern ist wie folgt organisiert:

Besucher geben bei Ankunft im Sozialamt dem für sie zuständigen Sachbearbeiter ihren Personalausweis ab, unabhängig davon, ob gerade Beratungen stattfinden oder nicht. Die Ausweise werden auf dem Schreibtisch gestapelt, die Besucher in der Reihenfolge, in der sie ihren Ausweis abgegeben haben, durch namentlichen Aufruf in der Wartezone ins Büro gebeten. Dieses Verfahren trägt lt. Auskunft der Sozialamtsleiter dazu bei, eine gerechte Reihenfolge der Bearbeitung zu sichern.

Zusammenfassend kann festgestellt werden: Die derzeitigen räumlichen Verhältnisse und organisatorischen Abläufe in den Sozialämtern gewährleisten den Rechtsanspruch der Betroffenen auf Schutz ihrer Sozialdaten nicht. Die Offenbarung von Sozialgeheimnissen an Unbefugte ist zum Teil vorprogrammiert. Ich habe dem Senatsamt für Bezirksangelegenheiten vorgeschlagen, in den Wartezonen der Sozialämter (ähnlich wie im Arbeitsamt und in vielen Arztpraxen) ein Zahlen-System einzuführen. Dies hätte den Vorteil, daß

— der namentliche Aufruf unterbliebe,

— Störungen der Beratungsgespräche durch Hilfeempfänger, die ihren Ausweis abgeben, vermieden würden,

— das Risiko des Diebstahls/Vertauschens von Ausweisen entfiele.

Sollten sich Hilfeempfänger durch dieses Verfahren zu „Nummern" herabgewürdigt fühlen, könnte dies nach meinem Verständnis durch eine freundliche — namentliche — Begrüßung durch den jeweiligen Sachbearbeiter aufgefangen werden. Mein Vorschlag wurde vom Senatsamt für Bezirksangelegenheiten aufgegriffen. Ein Modell-Versuch in zwei Hamburger Sozialämtern soll auch Erkenntnisse darüber bringen, ob der Verzicht auf den namentlichen Aufruf von den Betroffenen als Verbesserung empfunden wird.

Meinen Prüfungsbericht hat das Senatsamt für Bezirksangelegenheiten außerdem zum Anlaß genommen, alle Bezirksämter noch einmal aufzufordern, Bürgern auf Wunsch Einzelgespräche zu gewähren. Aus zahlreichen Gesprächen mit Sachbearbeitern verschiedener Sozialämter ist mir aber bekannt, daß sich diese Anweisung auch bei gutem Willen praktisch nicht umsetzen läßt, solange die räumliche und personelle Situation in den Sozialämtern nicht verbessert wird.

4.1.2 *Amtsvormundschaft und Amtspflegschaft bei nichtehelichen Kindern*

Ein Amtspfleger machte mich auf das an Hamburger Jugendämtern praktizierte Verfahren bei der Beschaffung von Informationen über das Einkommen von Vätern nichtehelicher Kinder aufmerksam, das nachstehend kurz geschildert werden soll:

Sofern der Vater eines nichtehelichen Kindes, das unter Amtspflegschaft oder -vormundschaft steht, seiner Unterhaltsverpflichtung nicht nachkommt, wird ohne Einwilligung des Betroffenen, häufig sogar ohne sein Wissen, sein Einkommen von Amts wegen ermittelt. Bei den damit zusammenhängenden Anfragen an Sozialleistungsträger und Arbeitgeber offenbart der Amtspfleger, daß der Betroffene Vater eines nichtehelichen Kindes ist, und legt für den Empfänger der Anfrage die Schlußfolgerung nahe, daß der Betroffene seiner gesetzlichen Unterhaltsverpflichtung nicht nachkommt.

Die Behörde für Arbeit, Jugend und Soziales hat sich meiner Auffassung angeschlossen, daß diese Praxis rechtswidrig ist.

Unstreitig ist die Geltendmachung von Unterhaltsansprüchen gem. § 1706 BGB Aufgabe des Amtspflegers bzw. — sofern die Mutter des Kindes noch minderjährig ist — des Amtsvormundes. Um einen Unterhaltsanspruch in angemessener Höhe geltend machen zu können, ist es notwendig, das Einkommen des Unterhaltspflichtigen zu kennen, da dessen Lebensstellung gem. § 1615 c BGB bei der Bemessung des Unterhalts zu berücksichtigen ist. Sofern der Unterhaltsverpflichtete seiner Auskunftspflicht gem. § 1605 BGB i.V.m. § 1615 a BGB nicht nachkommt, steht dem Amtspfleger als gesetzlichem Vertreter des Kindes in diesem Bereich wie jedem privaten Unterhaltsberechtigten das Verfahren gem. § 74 Nr. 2 a SGB X offen. Danach ist eine Offenbarung von Daten durch die in § 35 SGB I genannten Stellen (u.a. die oben erwähnten Leistungsträger) zulässig, wenn folgende Voraussetzungen erfüllt sind:

Obwohl der Betroffene aufgefordert, gemahnt, ihm eine angemessene Frist gesetzt und er auf die in § 74 SGB X enthaltene ersatzweise Offenbarungsbefugnis hingewiesen wird, erfüllt er seine Auskunftspflicht nicht oder nicht vollständig. Diese Verfahrensschritte müssen jeder Anfrage bei einem Leistungsträger vorausgegangen sein, da § 1605 BGB nicht die Pflicht des Betroffenen normiert, Einkommensverhältnisse bzw. -veränderungen unaufgefordert darzulegen. Die Anfrage ist auf die zur Erfüllung der Aufgabe (Geltendmachung des Unterhaltsanspruchs) notwendigen Daten zu beschränken.

Die Behörde für Arbeit, Jugend und Soziales hat zugesagt, für die Zukunft sicherzustellen, daß die Verfahrensregularien des § 74 Nr. 2 SGB X von den Amtspflegern in jedem Einzelfall streng beachtet werden. Die Behörde ist aber bisher nicht bereit, die ihrer Aufsicht unterstehenden Amtspfleger anzuweisen, auf Anfragen bei Arbeitgebern künftig zu verzichten. Die Rechtslage ist unumstritten: Nach bürgerlichem Recht gibt es keine Auskunftspflicht des Arbeitgebers, wie sie das Sozialrecht für andere Fälle

(z.B. § 116 BSHG, § 6 UVG) normiert. § 1605 BGB gibt dem Unterhaltsberechtigten auch nicht das Recht, sich beim Arbeitgeber unmittelbar über das Arbeitseinkommen des Unterhaltspflichtigen zu erkundigen.

Schließlich läßt sich auch aus § 74 SGB X eine Befugnis des Unterhaltsberechtigten (hier: des Amtspflegers), sich mit einem Auskunftsersuchen an den Arbeitgeber zu wenden, meines Erachtens nicht herleiten. Die BAJS vertritt demgegenüber die Auffassung, daß die Vorschrift einer analogen Anwendung zugänglich sei. Eine Gesetzeslücke sehe ich nicht. Der Amtspfleger kann (ebenso wie der Privatpfleger) als Vertreter des nichtehelichen Kindes den Zivilrechtsweg (Auskunftsklage) beschreiten, wenn ihm die für einen Unterhaltsprozeß erforderlichen Daten nicht bekannt sind. Die Diskussion mit der BAJS ist noch nicht abgeschlossen.

4.1.3 Durchführung des Unterhaltsvorschußgesetzes

Nach dem Unterhaltsvorschußgesetz (UVG) haben Kinder alleinstehender Mütter und Väter unter bestimmten Voraussetzungen Anspruch auf Unterhaltsvorschuß oder -ausfalleistung. Nach § 6 Abs. 1 UVG ist der unterhaltspflichtige Elternteil, bei dem das Kind nicht lebt, dem Jugendamt zu den Auskünften verpflichtet, die zur Durchführung des UVG erforderlich sind. Zur Durchführung des UVG ist u.a. die Kenntnis der wirtschaftlichen Verhältnisse des unterhaltspflichtigen Elternteils erforderlich, denn nur anhand dieser Daten kann die Höhe des geschuldeten Unterhalts und damit die Höhe des zu zahlenden Unterhaltsvorschusses bestimmt werden.

In einem mir bekanntgewordenen Fall hatte sich ein Jugendamt an das Arbeitsamt Hamburg gewandt, um von dort Auskünfte über das Einkommen des unterhaltspflichtigen Vaters eines nichtehelichen Kindes zu bekommen. Mit dieser Anfrage hat das Jugendamt Tatsachen über die persönlichen Verhältnisse des Kindes und des Vaters bekanntgegeben, die unter den Schutz des Sozialgeheimnisses fallen und nach § 69 Abs. 1 Nr. 1 SGB X nur offenbart werden dürfen, soweit dies zur Erfüllung der Aufgaben des Jugendamtes nach dem Sozialgesetzbuch erforderlich ist.

Unstreitig handelt es sich bei der Festsetzung der Höhe des zu zahlenden Unterhaltsvorschusses um eine solche Aufgabe: Das UVG gilt gem. Art. II, § 1 SGB I, als besonderer Teil des Sozialgesetzbuches. Das Jugendamt hat zwar zunächst den Unterhaltspflichtigen aufgefordert, seiner Auskunftspflicht nach § 6 Abs. 1 UVG nachzukommen. Es hat ihm aber keine Frist gesetzt und ihn auch nicht darauf hingewiesen, daß es bei fruchtlosem Fristablauf die erforderlichen Auskünfte beim Arbeitsamt einholen werde. Nur unter dieser Voraussetzung aber wäre unter dem Gesichtspunkt der Verhältnismäßigkeit der geschilderte Eingriff in das informationelle Selbstbestimmungsrecht des Betroffenen gerechtfertigt gewesen. Die BAJS hat zugesagt, künftig entsprechend zu verfahren.

4.1.4 Offenbarung von Sozialdaten auf Aufenthaltsgestattungen für Asylbewerber

Durch eine Beschwerde wurde ich darauf aufmerksam, daß in Hamburg alle Aufenthaltsgestattungen von Asylbewerbern, die Sozialhilfe beziehen, mit einem Stempel versehen werden, aus dem sich das zuständige Sozialamt sowie der Zeitraum, für den Sozialhilfe geleistet worden ist, ergibt. Die Behörde für Arbeit, Jugend und Soziales hat eingeräumt, daß die Sozialdienststellen mit diesem Verfahren gegen § 35 SGB I verstoßen, wonach Leistungsträger personenbezogene Daten als Sozialgeheimnis zu wahren haben. Eine Einwilligung der Betroffenen liegt in diesen Fällen ebensowenig vor wie eine gesetzliche Offenbarungsbefugnis gem. §§ 68 ff. SGB X. Die Behörde begründete diese unbefugte Offenbarung von Sozialdaten damit, daß die Angaben zur Vermeidung von Doppelleistungen erforderlich seien, da die Aufenthaltsgestattung keine Meldeanschrift enthalte. Ohne den Hinweis des Sozialhilfeträgers könne sich ein Asylbewerber ohne weiteres bei mehreren Sozialämtern melden und Leistungen beziehen, ohne daß dies kontrollierbar wäre.

Bei inländischen Mitbürgern werde das Problem des möglichen Mißbrauchs von Sozialhilfeleistungen über die Meldeanschrift (Vorlage des Personalausweises bei

Antragstellung) gelöst. Die Behörde schlug vor, künftig nur noch den Stempel des zuständigen Bezirksamtes ohne den Zusatz „Sozialamt" zu benutzen. Um ggf. Rückfragen zu ermöglichen — z.B. für welchen Zeitraum bereits Sozialhilfe geleistet worden sei — sei es außerdem erforderlich, die Telefonnummer des zuständigen Sachbearbeiters anzugeben. Die Telefonnummer lasse keinen Rückschluß darauf zu, daß es sich um eine Sozialdienststelle handele.

Ich halte es für datenschutzrechtlich vertretbar, Aufenthaltsgestattungen mit dem Stempel des Bezirksamtes zu versehen. Aus dem Datum „Bezirksamt" läßt sich für Dritte meines Erachtens nicht ohne weiteres ableiten, daß die Aufenthaltsgestattung in einer Sozialdienststelle gestempelt wurde. Die Angabe der Telefonnummer halte ich dagegen für bedenklich, auch wenn sie allein noch kein Sozialgeheimnis offenbart. Es ist aber für jeden, der die Behörden-Nr. nicht ohnehin schon kennt, sehr leicht feststellbar, daß sich dahinter ein Sozialamt verbirgt.

Offenbart ist ein Sozialgeheimnis aber schon dann, wenn es in irgendeiner Weise an einen Dritten gelangt. Unerheblich ist, ob das Offenbaren ausdrücklich oder konkludent erfolgt. Die Behörde hat sich meinen rechtlichen Bedenken leider nicht angeschlossen. Offenbar haben sich auch in diesem Fall verwaltungspraktische Erwägungen (Arbeitserleichterungen) durchgesetzt.

4.1.5 Einmalige Leistungen gem. § 21 BSHG

Bei der Bearbeitung einer Eingabe habe ich davon erfahren, daß in der Fachlichen Weisung der Behörde für Arbeit, Jugend und Soziales zu § 21 BSHG u.a auf bestehende Lieferverträge zwischen dem Beschaffungsreferat der BAJS und verschiedenen Lieferanten hingewiesen wird. Sofern ein Antragsteller die Voraussetzungen zur Gewährung einer einmaligen Leistung gem. § 21 BSHG erfüllt, wird vom Sozialamt ein Bestellschein an die Lieferfirma gesandt, auf dem Name und Anschrift des Hilfeempfängers vermerkt sind. Damit wird dem Lieferanten offenbart, daß der Empfänger der Ware Sozialhilfe erhält.

Da in diesem Fall weder die gesetzlichen Offenbarungstatbestände der §§ 68 bis 77 SGB X greifen, noch eine Einwilligung der betroffenen Hilfeempfänger eingeholt wird, ist die geschilderte Praxis rechtswidrig.

Die Petentin hatte sich zunächst beim Bezirksamt Altona über die Weitergabe ihrer Daten an die Lieferfirma beschwert. Ihr war zu einem Zeitpunkt, als sie schon nicht mehr Hilfeempfängerin war, von einem Möbelhaus ein Kauf auf Raten mit der Begründung verweigert worden, daß sie Sozialhilfeempfängerin sei. Das Bezirksamt Altona teilte ihr auf ihre Beschwerde mit, ein Fehlverhalten von Mitarbeitern des Sozialamtes könne nicht festgestellt werden. Es seien auch keine Sozialdaten an Dritte weitergegeben worden. Aus der Angabe der Lieferanschrift auf dem Bestellschein des Sozialamtes sei keinesfalls zu schließen, daß der Empfänger der Ware Sozialhilfe beziehe. Was sonst soll ein Lieferant aus der Bestellung eines Sozialamtes — lieferbar an eine Privat-Adresse — wohl schließen?

Die BAJS hat sich inzwischen meiner Rechtsauffassung angeschlossen. Künftig wird, wenn ein Antragsteller die Voraussetzungen zur Gewährung einer einmaligen Leistung gem. § 21 BSHG erfüllt, ein Bestellschein vom Sozialamt nur dann an die Lieferfirma gesandt, wenn der Hilfeempfänger vorher seine ausdrückliche Einwilligung gem. § 67 SGB X dazu gegeben hat. Wird die Einwilligung nicht erteilt, wird die Hilfe als Geldleistung und nicht als Sachleistung erbracht.

4.1.6 Offenbarung von Sozialdaten auf Überweisungsträgern

Im letzten Tätigkeitsbericht (5. TB, 5.14) hatte ich beanstandet, daß die Hamburgischen Sozialhilfedienststellen bei der Übersendung von Sozialhilfeleistungen auf Konten der Empfänger als Verwendungszweck „Sozialamt" auf dem Überweisungsträger angeben. Da die gesetzlichen Offenbarungsbefugnisse der §§ 68 bis 77 SGB X die damit verbundene Mitteilung, daß der Konteninhaber Sozialhilfe erhält, nicht abdecken und

auch eine Einwilligungserklärung des Betroffenen gem. § 67 SGB X nicht vorliegt, ist sie aus meiner Sicht rechtswidrig.

Die Behörde für Arbeit, Jugend und Soziales (BAJS) hat inzwischen zur Lösung des Problems vorgeschlagen, künftig auf den Überweisungsträgern folgende Angaben zu verwenden: Kürzel für den Leistungsträger, Aktenzeichen und Leistungszeitraum. Bei einem (fiktiven) Hilfeempfänger namens Fritz Wagner, geb. 1. 1. 1947, wohnhaft in Barmbek-Uhlenhorst, würde demnach bei einer Hilfe zum Lebensunterhalt für die Zeit vom 1. 3. bis zum 1. 4. folgender Verwendungszweck angegeben werden: BU SO 21 WAG 1/1/47/1. 3-1. 4. Es ist offensichtlich, daß das Kürzel „BU SO" keine hinreichende Anonymisierung des Datums „Sozialamt" darstellt.

Die BAJS stützt ihren Vorschlag auf § 69 Abs. 1 SGB X, wonach ein Leistungsträger Sozialdaten offenbaren darf, soweit dies für die Erfüllung seiner Aufgaben nach dem Sozialgesetzbuch erforderlich ist. Ich halte weder das Kürzel des zuständigen Bezirksamtes mit dem Zusatz „SO" noch die Angabe des Geburtsdatums für erforderlich im Sinne des § 69 Abs. 1 SGB X. Im übrigen bin ich nach wie vor der Auffassung, daß der Hilfeempfänger selbst eine Überweisung der „FHH-Finanzbehörde" auch ohne das Kürzel seines Bezirksamtes und „SO" - insbesondere bei laufender Hilfe zum Lebensunterhalt — durchaus als Sozialhilfe des für ihn zuständigen Sozialamtes erkennen kann.

Das von der BAJS immer wieder vorgebrachte Argument der Verfahrensvereinfachung kann eine Durchbrechung des Sozialgeheimnisses — auch im Hinblick auf den besonderen Stellenwert, den der Gesetzgeber dem Schutz von Sozialdaten eingeräumt hat — nicht rechtfertigen.

Ich habe der BAJS mitgeteilt, daß ich in der vorgeschlagenen Lösung keine wirkliche Verbesserung des Schutzes für die Betroffenen erkenne. Die BAJS hat es danach nicht mehr für nötig gehalten, weiter nach einer rechtlich einwandfreien Lösung zu suchen. Es soll auch in Zukunft bei der bisherigen rechtswidrigen Praxis bleiben.

4.1.7 Vordrucke

Sozialdaten werden in der Regel vom Betroffenen mit Hilfe von Vordrucken erhoben. Formularmäßig werden in vielen Fällen auch Daten von anderen Personen/Stellen bei Sozialleistungsträgern abgefragt. Ich habe im Berichtsjahr verschiedene Vordrucke geprüft und erhebliche Mängel festgestellt, die mich zu folgenden Hinweisen veranlassen:

— Werden Daten beim Betroffenen aufgrund einer Rechtsvorschrift erhoben, dann ist er auf sie, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen (§ 9 Abs. 2 HmbDSG/BDSG).

— Es dürfen nur die unbedingt notwendigen Daten erhoben und gesammelt werden. Auch dürfen sie nicht beliebig, sondern nur zu dem Zweck verwendet werden, für den sie erhoben wurden. Eine Ausnahme besteht nur, wenn zur anderweitigen Verwendung eine ausdrückliche gesetzliche Ermächtigung oder eine „informierte" Einwilligung des Betroffenen vorliegt.

— Die Prüfung, ob die Erhebung und ggf. Weitergabe von Daten vom Gesetz erlaubt ist, darf nicht pauschal erfolgen, sondern muß am Einzelfall orientiert sein. Das gilt für die Frage der Erforderlichkeit ebenso wie für die Beurteilung, ob schutzwürdige Belange des Betroffenen unverhältnismäßig beeinträchtigt werden.

— Personen oder Stellen, denen Sozialdaten befugt offenbart werden, haben diese in demselben Umfang geheimzuhalten wie die Sozialleistungsträger. Der Empfänger der Daten sollte auf diese Verpflichtung in jedem Einzelfall ausdrücklich hingewiesen werden.

Bereits vorhandene Vordrucke sind — soweit dies nicht bereits geschehen ist — auf die beschriebenen datenschutzrechtlichen Mindestanforderungen hin zu überprüfen und ggf. zu ändern.

4.2 Personalwesen

4.2.1 Führung und Verwaltung von Personalakten

Mehrere Eingaben von Bediensteten der FHH haben mich veranlaßt, Datenschutzproblemen bei der Personalaktenführung nachzugehen und insbesondere die „Anordnung über die Führung und Verwaltung der Personalakten" vom 30. 11. 1971 (Mitteilung der Verwaltung 1971, S. 280) zu überprüfen.

Eine bereichsspezifische gesetzliche Grundlage, wie sie das Volkszählungsurteil des Bundesverfassungsgerichts fordert, wird z.Z. nur auf Bundesebene vorbereitet. Das Senatsamt für den Verwaltungsdienst — Personalamt — , mit dem ich die Gesamtproblematik erörtert habe, wirkt an diesem Gesetzgebungsverfahren mit. Es verfolgt dabei nach eigenen Angaben das Ziel, das bislang herrschende Prinzip der „Vollständigkeit" der Personalakten durch das Prinzip der „Erforderlichkeit" der Datenspeicherung zu ersetzen. Ich begrüße den Versuch, die Datenspur der öffentlich Bediensteten auf diese Weise zu verwischen.

Ein Bundesgesetz für die Personalaktenführung — auch als Rahmengesetz — läßt der Bürgerschaft, aber auch dem Senat Spielraum für eigene Regelungen. Obwohl ich Verständnis dafür habe, daß zunächst die Bundesgesetzgebung abgewartet werden soll, halte ich es angesichts des unsicheren Zeithorizontes für angemessen, bereits aufgetretene Probleme in Hamburg schon jetzt einer (Zwischen-)Lösung zuzuführen.

Nach Ziff. 3 Abs. 2 der Anordnung über die Führung und Verwaltung der Personalakten dürfen Personalakten „grundsätzlich nur einem eng begrenzten Personenkreis mit besonderer dienstlicher Verantwortung für Personalangelegenheiten zugänglich gemacht werden". Dies sind nach § 3 HmBG „Dienstvorgesetzte", also nur Senatoren, Staatsräte, Bezirksamtsleiter und Bedienstete „mit Leitungsfunktion", denen die Wahrnehmung der Befugnisse des Dienstvorgesetzten übertragen wurde, Ziff. 2.2 bis 2.5 der Verwaltungsvorschrift zu § 3 HmbBG. Damit ist auch nach Überzeugung des Senatsamtes für den Verwaltungsdienst eine Überlassung von Personalakten an Fachvorgesetzte grundsätzlich nicht zulässig. Das gilt auch für die Bewerberauswahl bei Stellen-Besetzungen. Aufgrund verschiedener Anfragen aus einzelnen Fachbehörden gehe ich davon aus, daß gerade hier die Trennung von Dienst- und Fachvorgesetzten in den Behörden nicht immer verwirklicht ist. So wurden z.B. in der Baubehörde Abschnittsleitern nicht nur die Personalakten von Bewerbern aus der Behörde zur Verfügung gestellt, sondern auch Auskünfte über Krankmeldungen gegeben. Auf meine Anregung hat das Personalamt die Leiter der Personalabteilungen in den Fachbehörden, Senats- und Bezirksämtern auf das Erfordernis einer Trennung von Dienst- und Fachvorgesetztenfunktion ausdrücklich hingewiesen. Mit Schreiben vom 5. 1. 1988 teilte mir die Baubehörde jetzt mit, daß das Recht auf Einsicht in die Personalakte in Zukunft ausdrücklich auf die Behördenleitung, die Personalabteilung und die Amtsleiter beschränkt bleibt und „nicht weiter delegierbar ist". Ohne schriftliche Einwilligung werde die Personalakte eines verwaltungsinternen Bewerbers nicht mehr angefordert bzw. vorgelegt. Ich hoffe, daß diese Regelung von anderen Behörden übernommen wird.

Die Beschränkung des Rechts auf Einsicht in Personalakten gilt auch für Gehaltspfändungen. Da die Mitteilung von Pfändungen materiell Teil der Personalakte ist, darf der Fachvorgesetzte hiervon grundsätzlich keine Kenntnis erhalten. Dies hat das Bundesverwaltungsgericht in einem Urteil vom 28. 8. 1986 (2 C 51.84) aus der Fürsorgepflicht des Dienstherrn (§ 79 Bundesbeamtengesetz) abgeleitet. Für die Entscheidung über tatsächlich in Betracht kommende dienstrechtliche Konsequenzen kann im Einzelfall allerdings der Fachvorgesetzte herangezogen und in notwendigem Umfang informiert werden.

Nach Ziff. 30 Abs. 1 der Anordnung zur Personalaktenführung ist bei Widersprüchen von Bediensteten gegen personalrechtliche Entscheidungen dem Senatsamt die vollständige Personalakte vorzulegen. Auch wenn es Fälle gegeben haben mag, bei

denen andere Vorgänge in der Personalakte die Entscheidung über den Widerspruch beeinflußten, erscheint bei vielen in sich geschlossenen Widerspruchssachen eine Vorlage der vollständigen Personalakte nicht erforderlich. Dies gilt etwa bei Beihilfe-, Reisekosten-, (Sonder-)Urlaubs-Streitigkeiten. Das Senatsamt für den Verwaltungsdienst ist meiner Anregung gefolgt und verzichtet hier in Zukunft grundsätzlich auf die Vorlage der Personalakte. Bei Bedarf fordert das Senatsamt sie gesondert an.

Die Überlassung von Personalakten an Personalstellen anderer Hamburger Behörden ist nach Ziff. 31 (1) der Anordnung auch ohne Kenntnis des Betroffenen vorgesehen, wenn dies der „Vorbereitung oder Durchführung von Entscheidungen in Personalangelegenheiten" dient. Gegen diesen heimlichen Aktenaustausch habe ich Bedenken. Zur Durchsetzung eines übergreifenden Personalplanungskonzeptes ist die Versetzung oder Anordnung eines Beamten nach §§ 29 Abs. 1, 30 Abs. 1 HmbBG zwar nicht von der Zustimmung des Betroffenen abhängig. Zur Vorbereitung solcher Maßnahmen ist dann auch die Versendung der dafür notwendigen Teile der Personalakten (und nicht der ganzen Akte) ohne Zustimmung möglich. Dies schließt aber eine Information des Betroffenen über die Aktenversendung und insbesondere über den Empfänger keineswegs aus. Es sind keine berechtigten öffentlichen Interessen erkennbar, die insofern eine Einschränkung des informationellen Selbstbestimmungsrechts des Bediensteten rechtfertigen. Der Amtshilfegrundsatz des Art. 35 Abs. 1 GG wird durch eine Information des Betroffenen nicht tangiert.

4.2.2 Bewerberfragebogen und Führungszeugnis

Seit 1985 existieren Muster-Entwürfe eines „Fragebogens für Bewerber" und eines „Fragebogens für Einzustellende" vom Senatsamt für den Verwaltungsdienst. Diese Fragebogen sollen — nach dem vorgeschriebenen Mitbestimmungsverfahren — die derzeit noch verwendeten Fragebogen in den einzelnen Behörden ablösen. Die alten Fragebogen z.B. der Gesundheitsbehörde und der staatlichen Krankenhäuser verstoßen mit einem Teil der Fragen gegen datenschutzrechtliche und arbeitsrechtliche Grundsätze. Die neuen Musterentwürfe wurden mit mir abgestimmt.

Bedenken hatte ich gegen die Frage nach anhängigen Ermittlungs-, Straf- und Disziplinarverfahren geltend gemacht. Eine solche Frage wird von Ziff. 5 der Verwaltungsvorschriften zu § 6 HmbBG (Mitteilung der Verwaltung 1981 S. 19) und von Ziff. 6.1 der Durchführungsbestimmungen zum BZR-Gesetz (Mitteilung der Verwaltung 1985, S. 163) gefordert. Hierzu teilte ich dem Senatsamt folgende Rechtsauffassung mit: Die Interessen des Bewerbers, ohne rechtskräftige Schuldfeststellung keine Nachteile zu erleiden (Wahrung der rechtsstaatlichen Unschuldsvermutung), sind abzuwägen mit der Rechtspflicht der Behörden, nur „geeignete" Bewerber einzustellen. Ein Interessenausgleich könnte so aussehen, daß erst nach einer i.ü. positiven Entscheidung über die Bewerbung, also nicht im „Fragebogen für Bewerber", sondern im „Fragebogen für Einzustellende" nach anhängigen Verfahren gefragt wird. Parallel zur Anordnung über Mitteilungen in Strafsachen (Ziff. 15, 29) ist die Frage jedoch auf gerichtliche Verfahren (also nicht Ermittlungsverfahren) und Disziplinarverfahren sowie weiter auf Vorsatztaten zu beschränken. Für Bewerber um Angestellten- oder Arbeiterstellen ist das Auskunftsverlangen darüber hinaus auf bestimmte Deliktstypen zu begrenzen, die für den konkreten Arbeitsplatz von Bedeutung sind. Dies bedingt eine behördenspezifische Ausgestaltung der Frage. Hat die/der Einzustellende die so eingeschränkte Frage nach schwebenden Verfahren bejaht, ist mit ihr/ihm ein Gespräch über Tatvorwurf und voraussichtliches Strafmaß zu führen. Bei geringfügigem Schuldvorwurf ist zu berücksichtigen, daß § 32 Bundeszentralregistergesetz (BZRG) den Inhalt eines Führungszeugnisses auf schwerer wiegende Verurteilungen beschränkt und der Betroffene sich i.ü. als „nicht vorbestraft" bezeichnen darf. Ein Urteil über die „Eignung" eines Bewerbers ist nur durch eine Gesamtabwägung im Einzelfall zu erreichen. Unzulässig ist eine automatische Ablehnung bei einer Bejahung der Frage nach anhängigen Verfahren. Als eine Alternative zu diesem differenzierten Interessenausgleich sehe ich nur die wirklich freiwillige Beantwortung der Frage nach anhängigen Verfahren. Da eine

Nichtbeantwortung in der Praxis jedoch den Schluß auf ein Vorliegen schwebender Verfahren nahelegt, wäre es zur Gewährleistung einer echten Freiwilligkeit konsequent, auch eine falsche Antwort „nein" anzubieten und zu akzeptieren.

Nicht im „Fragebogen für Bewerber" selbst, aber als weitere Bewerbungsunterlage fordert Ziff. 6 der Hamburger Durchführungsbestimmung zum BZRG von allen Bewerbern für den öffentlichen Dienst die Vorlage eines Führungszeugnisses. Während Beamte grundsätzlich für alle (hoheitlichen) Aufgaben der FHH und unabhängig von konkreten Arbeitsplätzen eingestellt werden, werden Angestellte und Arbeiter für die Erfüllung bestimmter Aufgaben gesucht und angestellt. Dies gilt auch dann, wenn als Arbeitgeber der Angestellten wie bei den Beamten die FHH und nicht mehr die einzelne Beschäftigungsbehörde erscheint. Die Bewerbungsregeln richten sich bei Angestellten und Arbeitern auch in diesem Fall nach den arbeitsrechtlichen Grundsätzen. Als ein solcher Grundsatz ist anerkannt, daß das Fragerecht des Arbeitgebers bei Bewerbungen auf solche Vorstrafen begrenzt ist, die für die Erfüllung der in Aussicht genommenen Aufgabe bedeutsam sind. Diese Arbeitsplatzbezogenheit der Frage nach Vorstrafen wird jedoch unterlaufen durch die Vorlage eines allgemeinen Führungszeugnisses. Denn dieses differenziert nach §§ 32 ff. BZRG nicht nach bestimmten Deliktstypen oder Arten von Rechtsgutverletzungen. Ich ziehe hieraus den Schluß, daß bei Bewerbungen um Einstellung als Arbeitnehmer die Forderung nach Vorlage eines Führungszeugnisses weder arbeitsrechtlich noch datenschutzrechtlich zulässig ist.

In seiner Antwort vom 25. 11. 1987 erklärt sich das Senatsamt für den Verwaltungsdienst — Personalamt — bereit, nach schwebenden Verfahren erst nach einer im übrigen positiven Einstellungsentscheidung zu fragen, d.h. nicht mehr im „Fragebogen für Bewerber", sondern im Fragebogen für „Einzustellende". Bei Angestellten und Arbeitern soll in Zukunft auf die Vorlage eines Führungszeugnisses verzichtet werden. Nicht akzeptiert hat das Personalamt die Beschränkung der Formularfrage auf Vorsatzarten und den Verzicht auf Fragen nach schwebenden Ermittlungsverfahren. Der zukünftige Arbeitgeber müsse von staatsanwaltschaftlichen (nicht polizeilichen) Ermittlungen, die auch schwere Taten betreffen und länger dauern könnten, ebenso Kenntnis erhalten wie von Fahrlässigkeits-Vorwürfen, die ebenfalls erhebliche Rechtsgutverletzungen beinhalten könnten. Andererseits kündigte das Personalamt an, die Formularfrage nach anhängigen Verfahren auf solche zu beschränken, die voraussichtlich zu einer Strafe von mindestens 90 Tagessätzen oder 3 Monaten Freiheitsentzug führen werden, der Grenze, unterhalb derer eine Aufnahme ins Führungszeugnis nicht stattfindet.

Angesichts des — statistisch gesehen — sehr unsicheren Ausgangs auch staatsanwaltschaftlicher Ermittlungsverfahren und der in der Anordnung über Mitteilungen in Strafsachen (MiStra) nicht ohne Grund vorgenommenen grundsätzlichen Differenzierung in vorsätzliche und fahrlässige Taten halte ich nach wie vor einen Verzicht auf Fragen nach jeglichen Ermittlungsverfahren und Gerichtsverfahren wegen fahrlässiger Tatvorwürfe für angemessen, um der rechtsstaatlichen Unschuldsvermutung besser gerecht zu werden. Die vom Personalamt eingeräumten Änderungen bedeuten jedoch einen wesentlichen Schritt in die richtige Richtung. Es kommt mir darauf an, wenigstens diese neuen Regelungen, insbesondere die „bereinigten" Bewerberfragebogen in den Ämtern und Behörden zügig einzusetzen.

4.2.3 Personalstrukturdatei

Im Oktober teilte mir das Senatsamt für den Verwaltungsdienst — Personalamt — mit, daß es die Personalstellen der Behörden und Ämter um eine Übermittlung von Personaldaten an die Datenverarbeitungszentrale bitten werde, um die „Personalstrukturdatei" zu ergänzen. Die Personalstrukturdatei wird „gespeist" aus den Abrechnungsdateien der Besoldungs- und Versorgungsstelle und enthält zu den einzelnen Merkmalen auch den Namen und die Kennziffer des Bediensteten. Die Historik der Daten reicht über die der Abrechnungsdateien hinaus. Genutzt wird die Personalstrukturdatei zu gesamthamburgischen Personalstrukturanalysen, aber auch zu behördenspezifischen Auswertungen.

Ich habe die beabsichtigte Nacherfassung zum Anlaß genommen, das Personalamt um nähere Auskunft zu Organisation und Zweck der Personalstrukturdatei zu bitten. Zum einen bedarf es meines Erachtens einer klaren Regelung der Kompetenzen. Wie verträgt sich eine zentrale Gesamtpersonaldatei mit der dezentralen Personalverwaltung durch die einzelnen Behörden? Zum anderen meine ich, daß reine Strukturanalysen auch ohne direkten Personenbezug durch Namen und Kennziffer auskommen. Um historische Längsschnittanalysen vornehmen zu können, würde nach meiner Auffassung ein matchcode aus Teilen des Namens und der Kennziffer zur Verklammerung der Daten eines „Merkmalsträgers" ausreichen. Schon diese Art der Anonymisierung würde weitgehend vor Mißbräuchen schützen. Ich habe Bedenken dagegen, daß ohne eine entsprechende gesetzliche Grundlage und die mit den Gesetzesberatungen verbundene öffentliche Diskussion eine zuverlässige, sehr detaillierte, Jahrzehnte zurückreichende Datei mit Informationen über alle Hamburger Bedienstete entsteht, die für die verschiedensten, im vorhinein nicht bestimmten Zwecke von unterschiedlichen Stellen genutzt wird. Auf mein Auskunftsverlangen vom 11. November und die Bitte, die für den Herbst 1987 angekündigte Nacherfassung vorerst zurückzustellen, habe ich bis zum Jahreswechsel keine Antwort erhalten.

4.2.4 Ortszuschlag

In meinem letzten Tätigkeitsbericht (5. TB, 5.2.3) habe ich Probleme bei der Ortszuschlagsberechnung für öffentliche Bedienstete aufgezeigt. Dabei ging es im wesentlichen um die Formularfrage nach der Adresse des Arbeitgebers des Ehegatten. Gehört nämlich der Ehegatten-Arbeitgeber ebenfalls zum öffentlichen Dienst, so wird der Ortszuschlag der Stufe 2 (Mehrbetrag) nur anteilig gewährt, § 40 Abs. 5 Bundesbesoldungsgesetz. Nach den Verwaltungsvorschriften des Bundes zu § 40 BBesG tauschen die beiden Beschäftigungsbehörden bzw. öffentlichen Arbeitgeber der Ehegatten Vergleichsmitteilungen mit den für die Ortszuschlagsberechnung notwendigen personenbezogenen Daten der Eheleute aus.

Unmittelbar nach Erscheinen meines letzten TB erreichte mich eine Beschwerde, der die Kopie einer Vergleichsmitteilung der Behörde für Schule und Berufsbildung an einen privaten Arbeitgeber beigefügt war. Die Mitteilung enthält neben persönlichen Daten des Behördenbediensteten und seiner beim Mitteilungsempfänger beschäftigten Ehefrau die Frage: „Zahlen Sie familienbezogene Bestandteile (Ortszuschlag o.ä.)?" Die Vergleichsmitteilung wurde also vorsorglich, „auf Verdacht", abgesandt und offenbarte dem privaten Arbeitgeber Alter, Heiratsdatum, Dienstalter, Beamtenstatus und Beschäftigungsdauer des Ehegatten der eigenen Arbeitnehmerin. Auf meine Kritik an diesem Verfahren entwickelte die Schulbehörde einen Musterbrief, mit dem der Arbeitgeber des Ehegatten in Zweifelsfällen nun ohne Mitteilung personenbezogener Daten gefragt wird, ob er zum öffentlichen Dienst i.S.d. § 40 BBesG gehört. Das Senatsamt für den Verwaltungsdienst — Personalamt — wies aus Anlaß dieses Falles in einem Schreiben vom 1.4.1987 alle Behörden und Ämter darauf hin, daß nur Arbeitgeber des öffentlichen Dienstes Vergleichsmittlungen erhalten dürfen.

§ 40 Abs. 2 Nr. BBesG sieht einen erhöhten Ortszuschlag vor, wenn ein Beamter eine andere Person (meist sein Kind) in „seine" Wohnung aufgenommen hat und ihr Unterhalt gewährt und „für den Unterhalt der aufgenommenen Person Mittel zur Verfügung stehen", die einen bestimmten Betrag nicht übersteigen. Beansprucht noch ein Dritter (z.B. der Lebensgefährte des Beamten) aus demselben Grund den erhöhten Ortszuschlag, wird dieser nur anteilig gewährt. Um die Kriterien „seine" Wohnung, Mittel für den Unterhalt und die Ortszuschlagsbeanspruchung durch einen Dritten zu klären, verwenden die Behörden sehr unterschiedliche eigene Zusatzfragebogen. In diesen wird zum Teil nach den genauen Eigentums- bzw. Besitzverhältnissen an der Wohnung und nach dem Arbeitgeber des Dritten auch für den Fall gefragt, daß der Dritte gar keinen erhöhten Ortszuschlag beansprucht. Für die der aufgenommenen Person „zur Verfügung stehenden Mittel" legen Schulbehörde und Arbeits- und Sozialbehörde neben anderen Einkünften den Unterhaltsanspruch gegen den geschiedenen Ehegatten,

nicht den tatsächlich gezahlten Unterhalt, zugrunde. Als Belege werden „Haushaltsbescheinigungen, Mietvertrag oder Eigentumsnachweis, Unterhaltsurteil neuesten Datums bzw. Belege über die Einkommensverhältnisse des anderen Elternteils" und anderes gefordert. Petenten fühlten sich durch diese Regelungen genötigt, ggf. gerichtliche Auseinandersetzungen mit dem geschiedenen Ehegatten zu führen und durch die Nachweise zusätzliche Daten zu offenbaren, die von § 40 BBesG nicht gefordert werden.

Die Justizbehörde verfährt demgegenüber wesentlich „datenschutzfreundlicher". Sie fragt nur nach dem tatsächlich gezahlten „Unterhalt vom anderen Elternteil", läßt sich also nicht Unterlagen zur Berechnung des möglicherweise niedrigeren oder höheren Unterhaltsanspruchs vorlegen. Ich halte allein diese Praxis für gesetzeskonform: Mittel „stehen zur Verfügung", wenn sie gezahlt werden, nicht wenn sie erst eingeklagt werden müssen.

Ich habe mehrere Eingaben zum Ortszuschlag zum Anlaß genommen, dem für die Durchführungsbestimmungen zum Besoldungsgesetz zuständigen Senatsamt für den Verwaltungsdienst meine Befürchtung auszudrücken, daß das Bemühen der öffentlichen Hand um möglichst lückenlosen Schutz vor ungerechtfertigter Überzahlung den Datenschutz in der Praxis unterläuft. Die Komplexität der gesetzlichen Regelungen — allein § 40 BBesG nimmt ca. 100 Druckzeilen in Anspruch — fordert eine derartige Fülle von Einzeldaten und deren Belege, daß der Staat allein über die Ortszuschlags-Berechnung einen m.E. unangemessen tiefen Einblick in die privaten Verhältnisse seiner Bediensteten erhält. Ich habe in einem Gespräch mit dem Senatsamt für den Verwaltungsdienst zur Kenntnis genommen, daß die Bundesländer den Bundesgesetzgeber zu einer Vereinfachung des Bundesbesoldungsrechts aufgefordert haben — wenn auch eher aus verwaltungsökonomischen als aus datenschutzrechtlichen Gründen. Bis zu einer Gesetzesänderung sieht sich das Senatsamt aber an die mit Zustimmung des Bundesrates erlassenen Verwaltungsvorschriften zu § 40 BBesG gebunden, die allerdings die zum 1. 1. 1986 eingetretene Gesetzesänderung hinsichtlich einer aufgenommenen Person noch nicht berücksichtigen. Das Bundesrecht gilt gem. § 1 BBesG direkt auch für die Beamten der Länder.

In einem Rundschreiben an die Datenschutzbeauftragten des Bundes und der Länder habe ich einerseits das Bedürfnis nach einer Gesetzesvereinfachung formuliert und andererseits auf eine mögliche Beschränkung des Fragenumfangs für die Ortszuschlagsberechnung aufmerksam gemacht. Insbesondere den Datenschutzbeauftragten von Schleswig-Holstein hat dies zu einem gleichgerichteten Vorstoß gegenüber dem Kieler Finanzministerium veranlaßt. Neben der Verfolgung des Gesetzgebungsverfahrens scheint mir — auch parallel — eine Abstimmung der zuständigen Landesbehörden über den Fragen- und Nachweisumfang auf dem kleinsten gemeinsamen Nenner notwendig.

Kurz vor dem Jahreswechsel hat mir nun das Personalamt mitgeteilt, daß es der Behörde für Arbeit, Jugend und Soziales empfohlen hat, den oben erwähnten Zusatzfragebogen nicht mehr zu verwenden, und daß es zu den neugefaßten Bestimmungen des § 40 BBesG nun eigene Richtlinien erarbeitet. Dabei wird es nicht zuletzt um die Handhabung des Tatbestandsmerkmals „für den Unterhalt zur Verfügung stehende Mittel" gehen.

4.2.5 Persönlichkeitstests bei Bewerbungen für den Strafvollzugsdienst

Bei Bewerbungen für den mittleren allgemeinen Strafvollzugsdienst setzte die Justizbehörde den Persönlichkeitstest „MPI" (= Mandsley-Personality-Inventory) ein. Dieser Test mißt die „neurotische Tendenz" (z.B. Labilität, Nervosität, Kritiksucht) und „Extraversion" (Sorglosigkeit, Aktivität, Streben nach Einfluß und Geselligkeit) des Bewerbers anhand von 48 Fragen. Beispiel: „Sind Sie leicht verstimmt", „Grübeln Sie viel über Ihre Vergangenheit nach".

Persönlichkeitstests sind nach der Rechtsprechung nur zulässig, wenn sie einerseits geeignet sind festzustellen, ob ein Bewerber die Anforderungen eines konkreten

Arbeitsplatzes erfüllt, und wenn sie andererseits dafür auch erforderlich sind. Darüber hinaus ist zur Prüfung der Verhältnismäßigkeit der Nutzen des Tests mit der Beeinträchtigung des Bewerbers abzuwägen. Der Mensch soll grundsätzlich an seinem Verhalten gemessen werden und nicht durch eine Erforschung des Unbewußten. Nicht ausreichend zur Legitimation eines Persönlichkeitstests ist die „Einwilligung" des Bewerbers. Er wird i.d.R. weder darüber aufgeklärt, was genau bei ihm getestet wird, noch läßt es die Testmethode zu, die Bedeutung der einzelnen Fragen für das Testziel zu erläutern. Angesichts der gegenwärtigen Arbeitsmarktlage steht es dem Bewerber auch nicht wirklich frei, sich dem Test zu unterziehen oder nicht. Der Preis für eine Verweigerung ist regelmäßig die Ablehnung einer Bewerbung.

Die Eignung eines Tests setzt voraus, daß die Anforderungskriterien für einen bestimmten Arbeitsplatz bzw. eine bestimmte Laufbahn vorher festgelegt werden. Dies ist für den Bereich des Hamburger Strafvollzugs nicht geschehen. Aus dem allgemeinen Resozialisierungsziel des § 2 StrafVzG kann nicht mit der notwendigen Bestimmtheit auf einzelne psychische Anforderungen an Vollzugsbeamte geschlossen werden. Darüber hinaus ist der MPI-Test anhand von „Normalitätswerten" von englischen Durchschnittsbürgern im Jahre 1959 entwickelt worden. Eine Übertragung auf die heutige bundesrepublikanische Gesellschaft ist auch nach Meinung des Text-Autors selbst (Eysenck, Das „Mandsley-Personality-Inventory" als Bestimmer der neurotischen Tendenz und Extraversion, S. 4-7, 17) äußerst fragwürdig. Die den MPI-Test auswertende Psychologin der Justizbehörde geht schließlich selbst davon aus, daß die MPI-Fragen leicht durchschaubar sind und somit — zumindest in einer Prüfungssituation — eher die Anpassungsfähigkeit oder -bereitschaft des Bewerbers messen als seine wirkliche neurotische Tendenz.

Ist damit bereits die Eignung des MPI-Tests als Einstellungsprüfung für den mittleren Vollzugsdienst äußerst zweifelhaft, geht die Justizbehörde selbst auch nicht von seiner Erforderlichkeit aus: Aufgrund des Tests scheidet in der Praxis kein Bewerber endgültig aus dem Auswahlverfahren aus. Die Antworten werden lediglich als Hinweise gewertet, die in persönlichen Gesprächen revidiert werden können.

Eine Abwägung des relativ geringen Nutzens des MPI-Tests mit seiner belastenden Wirkung für den Betroffenen ergibt nach meiner Auffassung, daß der Einsatz des MPI-Tests unverhältnismäßig ist. Die Fragen reichen durchgehend in die Intimsphäre des Bewerbers, die Erforschung des Unbewußten entzieht der Testperson die Möglichkeit einer verantwortlichen willentlichen Verhaltenssteuerung. Hier ist die Grenze zur Behandlung des Menschen als Objekt und damit ein Verstoß gegen die Menschenwürde nicht weit. Aus diesen Gründen halte ich die Verwendung des MPI-Tests für datenschutzrechtlich nicht zulässig; sie verstößt mangels gesetzlicher Grundlage und ohne eine wirksame Einwilligung des Betroffenen gegen das informationelle Selbstbestimmungsrecht des Bewerbers. Ich habe der Justizbehörde deswegen empfohlen, den Test ab sofort aufzugeben. Darüber hinaus habe ich gegen die derzeit praktizierte unbegrenzte Aufbewahrung der Test-Antworten in Registraturakten der auswertenden Psychologin Bedenken geltend gemacht. Mit Schreiben vom 17. 8. 1987 teilte mir die Justizbehörde mit, daß das Strafvollzugsamt „mit Rücksicht auf die geltend gemachten datenschutzrechtlichen Bedenken und den geringen praktischen Nutzen" auf weitere MPI-Tests verzichtet.

4.2.6 Lehrerindividualdatei

Die „Modernisierung der Lehrerindividualdatei" (LID), die ich in meinem letzten Tätigkeitsbericht (Ziff. 5.2.2) ausführlicher dargestellt habe, ist ins Stocken geraten. Es konnte weder die Datenstrukturanalyse abgeschlossen noch eine endgültige Entscheidung über die weiter zu verfolgende Projektalternative getroffen werden.

Die Verzögerungen haben zumindest mittelbar auch datenschutzrechtliche Gründe: Die Gewerkschaft Erziehung und Wissenschaft sowie die pädagogischen Personalräte befürchten die Einrichtung eines umfassenden Personalinformationssystems mit weitreichenden Kontroll- und Dispositionsmöglichkeiten zu Lasten der Lehrer. Mit der

Begründung, daß die modernisierte LID in den Personalabteilungen angewendet werden solle, räumt die Schulbehörde nur dem Personalrat der Verwaltung, nicht aber den Personalräten der Lehrer das nach dem Personalvertretungsgesetz vorgesehene Mitbestimmungsrecht ein. Mit zwei Auswirkungen dieses Konfliktes hatte ich mich direkt zu befassen:

— Entgegen der früheren Praxis lehnte die Schulbehörde es aus datenschutzrechtlichen Gründen ab, den Lehrerpersonalräten weiterhin regelmäßig „Grundlisten" aus der LID zur Verfügung zu stellen. Diese Grundlisten enthalten unter anderem Namen, Geburtsdatum, Adresse, Telefonnummer, Lehrbefähigung und Unterrichtsstundenzahl aller Lehrer des Schultyps mit eigenem bzw. der Schultypen mit gemeinsamem Personalrat. In einem Gespräch am 24. April habe ich mit Vertretern der Schulbehörde und der Lehrerpersonalräte Verwendungszwecke der Grundlisten und denkbare Kompromisse erörtert. Nicht sinnvoll erschien mir, daß ausschließlich die Personalräte von der innerbehördlichen Nutzung der Listen ausgeschlossen werden sollten, während die Weitergabe an verschiedene Fachabteilungen nicht in Frage gestellt wurde. Ich habe mich deswegen bereit erklärt, die (frühere) Praxis der regelmäßigen Zusendung auch an die Personalräte für eine Übergangszeit zu akzeptieren. Dies sollte den Lehrern — z.B. auf den jährlich auszufüllenden LID-Erhebungsbogen — mitgeteilt werden. Die umstrittene Grundfrage nach dem Umfang der Mitwirkungsrechte der Personalräte kann und soll diese pragmatische Lösung allerdings nicht beantworten. Im Rahmen der Modernisierung der LID ist die Grundlisten-Weitergabe insgesamt neu zu überdenken — auch hinsichtlich technischer Möglichkeiten, nur wenige ausgewählte Daten auszudrucken. Das gilt für die Weitergabe von LID-Daten an Personalräte ebenso wie an die verschiedenen Fachabteilungen der Schulbehörde.

— In der Auseinandersetzung um ein Personalinformationssystem der Schulbehörde setzte die gewerkschafts-orientierte „Hamburger Lehrerzeitung" neben einem Aufruf zum Boykott der LID-Erhebungen auch das Auskunftsrecht nach § 14 HmbDSG als politisches Druckmittel ein. An der Aktion „Fragt Eure Daten ab" beteiligten sich seit Dezember 1986 ca. 650 Lehrerinnen und Lehrer. Die Schulbehörde antwortete auf die Aktionsankündigung mit der Einrichtung einer PC-gestützten Datei „Auskunftsersuchen zu gespeicherten Daten". Die Datei enthielt Name, Vorname, Personalnummer, Schulnummer, Eingangs- und Erledigungsdatum. Der Name erschließt die Beihilfe- und die Personalkartei, die Personalnummer die Daten aus der LID, die Schulnummer den letztjährigen LID-Erhebungsbogen. Bei der Zusammenstellung dieser Auskünfte selbst konnte die Datei nicht helfen; sie war nur als Erledigungskontrolle, zur Terminsüberwachung geeignet.

  Aus diesem Grund und vor dem Hintergrund möglicher Mißbrauchsrisiken (z.B. Auswertung „Protestpotential pro Schule/Schultyp"; Verknüpfungen mit LID) habe ich der Schulbehörde gegenüber Zweifel an der Notwendigkeit der Datei (§ 9 HmbDSG) geäußert und um Auskunft darüber gebeten, wann welche Daten wieder gelöscht werden. In ihrer Antwort am 30. Oktober stellt die Schulbehörde zunächst selbst die politische Auseinandersetzung um die LID in den Vordergrund, versichert dann aber, „daß die Datei reine Arbeitshilfe ist und darüber hinaus keinerlei Erkenntnis- und Verwendungszwecken dient". Sollte die Erforderlichkeit einer solchen Hilfe durch den Datenschutzbeauftragten bestritten werden, so käme das dem „Verbot der Benutzung moderner Technik in Massenverfahren gleich, zu deren Bewältigung solche Maschinen gerade gedacht sind". Inzwischen sei die Datei allerdings abgearbeitet und deswegen wieder gelöscht worden. Es liegt mir fern, die Einrichtung von Dateien als Arbeitshilfe grundsätzlich für nicht „erforderlich" im Sinne des § 9 HmbDSG zu erklären. Gerade bei der Nutzung der automatischen Datenverarbeitung sind jedoch auch Wirkungen in die Erforderlichkeitsprüfung mit einzubeziehen, die über den rein verwaltungsökonomischen Aspekt hinausgehen. Die bezüglich der Datensicherheit ohnehin problematische Speicherung personenbezogener Daten auf einem PC ist jedenfalls dann nach besonders strengen Maßstäben zu

beurteilen, wenn sie — zumindest aus Sicht der Betroffenen — als Waffe in einer politischen Auseinandersetzung erscheint. Nach dem Antwortschreiben der Schulbehörde bleibt der Eindruck, daß die Daten nicht vorgangsbezogen mit der jeweiligen Auskunftserteilung gelöscht wurden, sondern erst nach Erledigung aller Auskunftsbegehren. Am Schluß der Aktion ergab sich somit eine vollständige Liste aller Anfragenden. Die technische Hilfe ermöglichte also eine Übersicht über diejenigen Lehrerinnen und Lehrer, die sich an der Protestaktion der Gewerkschaft beteiligten und möglicherweise auch in der weiteren Auseinandersetzung wieder auftreten könnten. Die pädagogischen Personalräte kommen in einem Brief zu der „unerfreulichen Schlußfolgerung, daß es hierbei um die Einschüchterung der auskunftssuchenden Lehrerinnen und Lehrer geht". In einem derart gespannten Klima zwischen der speichernden Stelle und den Betroffenen ist nach meiner Auffassung sowohl die „Erforderlichkeit" der computergestützten Personen-Datei, als auch ihre Sicherheit und die Einhaltung des Löschungsgebotes strenger zu beurteilen als im Normalfall.

4.3 Statistik

4.3.1 Landesstatistikgesetz

Zu meiner bereits in den letzten Tätigkeitsberichten (4. TB, 4.3.5, S. 43 und 5. TB, 5.3.3, S. 46) erhobenen Forderung nach einem Landesstatistikgesetz hat die Behörde für Inneres leider immer noch nicht Stellung genommen. Nach einer jüngst abgegebenen Erklärung sind die entsprechenden Prüfungen noch nicht abgeschlossen.

Die mit der Durchführung der Volkszählung verbundenen Probleme (vgl. 4.4), insbesondere in bezug auf die notwendige Abschottung der Statistik von anderen Verwaltungsaufgaben (z.B. von der Vorbereitung von Wahlen und der Verwaltung von Zahlungsfällen bei Pflegekindern und Heiminsassen, die ebenfalls vom Statistischen Landesamt wahrgenommenen werden) und die bei der automatisierten Verarbeitung von Statistikdaten zu treffenden zusätzlichen Sicherungsmaßnahmen (vgl. BVerfGE 65,1, S. 48) unterstreichen die Notwendigkeit eines Landesstatistikgesetzes.

Die Verarbeitung von personenbezogenen Daten — auch für statistische Zwecke — stellt regelmäßig einen Eingriff in das Recht auf informationelle Selbstbestimmung dar, der einer normenklaren gesetzlichen Grundlage bedarf. Eine solche Grundlage fehlt immer noch, sofern es sich bei den vom Statistischen Landesamt durchgeführten Statistiken nicht um Bundesstatistiken handelt.

Da das Volkszählungsurteil des Bundesverfassungsgerichts nunmehr mehr als vier Jahre zurück liegt, hoffe ich, daß der Klärungsprozeß in der Innenbehörde forciert und zu einem unter Datenschutzaspekten befriedigenden Ergebnis kommen wird.

4.3.2 Hochschulstatistik

4.3.2.1 Stand der Gesetzgebung

Ich habe bereits in meinen früheren Tätigkeitsberichten darauf hingewiesen, daß das Hochschulstatistikgesetz nicht den im „Volkszählungsurteil" vom Bundesverfassungsgericht formulierten Grundsätzen entspricht:

— Es mangelt an der notwendigen Klarheit hinsichtlich der Erhebungsmerkmale.

— § 15 Abs. 2 HStatG erlaubt die Weitergabe von Einzeldaten an die fachlich zuständigen obersten Bundes- und Landesbehörden sowie an die von ihnen bestimmten Stellen und Personen; außerdem wird die Weiterleitung von Einzelangaben für wissenschaftliche Zwecke zugelassen, ohne daß Empfänger bestimmt werden.

— § 15 Abs. 3 HStatG läßt die Verwendung von personenbezogenen Daten, die im Rahmen der Hochschulstatistik erhoben worden sind, für verwaltungsinterne Zwecke der Hochschule zu.

— Es fehlen die vom Bundesverfassungsgericht geforderten organisatorischen und verfahrensmäßigen Vorkehrungen zur Vermeidung eines Mißbrauchs.

Die Erhebung, Speicherung und weitere Verarbeitung von personenbezogenen Daten der Hochschulstatistik erfolgen deshalb ohne eine den verfassungsrechtlichen Anforderungen entsprechende gesetzliche Grundlage. Um so bedauerlicher ist es, daß das Gesetzgebungsverfahren für ein neues Hochschulstatistikgesetz aufgrund von Meinungsverschiedenheiten zwischen Bund und Ländern ins Stocken geraten ist. Mit zunehmender zeitlicher Entfernung vom Volkszählungsurteil unterliegt die Rechtmäßigkeit der Erhebung jedoch immer schwerwiegenderen Zweifeln, da sich Bund und Länder wohl kaum noch auf einen „Übergangsbonus" bei der Umsetzung der Grundsätze des BVerfG berufen können, zumal das Gesetzgebungsverfahren allem Anschein nach seit 1985 ruht.

Die Behörde für Wissenschaft und Forschung und das Statistische Landesamt sind meiner Forderung, auf die Speicherung personenbezogener Daten für die Hochschulstatistik zu verzichten (3. TB, 3.6.5.2, S. 46), nicht nur nicht nachgekommen; sie haben ganz im Gegenteil die Verarbeitung der Daten von Studenten und Prüfungskandidaten sogar noch ausgeweitet, wie dies im nächsten Abschnitt dargestellt wird.

4.3.2.2 Verlaufsstatistik

In der Verlaufsstatistik werden die stichtagsbezogenen Daten verschiedener Semester mit anderen personenbezogenen Grunddaten verknüpft und ausgewertet. Dabei handelt es sich um einen weit tieferen Eingriff in das Recht auf informationelle Selbstbestimmung des Betroffenen, als dies bei einer reinen Stichtagserhebung der Fall ist. Um die Angaben, die jeweils zum Semesterbeginn erhoben werden, für eine Verlaufsstatistik zusammenführen zu können, unterbleibt eine Anonymisierung der Einzeldatensätze. Die statistischen Daten sind also — zumindest für die gesamte Studienzeit — personenbezogen gespeichert, auch wenn der Bezug nicht durch den Namen der Betroffenen, sondern durch Namensteile und weitere „unveränderliche" Merkmale hergestellt wird.

Konnte ich in meinem 3. und 4. TB noch feststellen, daß in Hamburg keine Verlaufsstatistiken über Studenten und Prüfungskandidaten geführt wurden, so muß ich konstatieren, daß mittlerweile auch die Hamburger Hochschulen Daten für die bundesweite Verlaufsstatistik zuliefern. Dies geschieht, obwohl ich wiederholt auf die besonderen Gefahren dieser Verarbeitungsform hingewiesen habe (s.o.) und obwohl die Verlaufsstatistik in den letzten Entwürfen für ein Hochschulstatistikgesetz nicht mehr enthalten ist. In der Begründung des Referentenentwurfs wird der Verzicht auf die Verlaufstatistik mit verfassungsrechtlichen Bedenken (Verwendung eines Personenkennzeichens oder eines entsprechenden Substituts) und mit der Entwicklung der statistischen und sozialwissenschaftlichen Forschungsmethoden in den letzten Jahren begründet, die es zweifelhaft erscheinen lassen, ob die Verlaufsstatistik noch verhältnismäßig ist.

Die Behörde für Wissenschaft und Forschung und das Statistische Landesamt sind über diese ihr bekannten Bedenken hinweggegangen. Die Verarbeitung personenbezogener Studenten- und Prüfungsdaten hat mit der Einführung der Verlaufsstatistik eine neue noch bedenklichere Qualität bekommen. Dies ist geschehen, obwohl keine gesetzliche Grundlage hierfür besteht und auch ein „Übergangsbonus" nicht in Anspruch genommen werden kann. Auf die Verlaufsstatistik muß also verzichtet werden und die entsprechenden Daten müssen gelöscht werden.

4.3.2.3 Erhebung der Statistikdaten an den Hamburger Hochschulen

Ich habe festgestellt, daß die Erhebung personenbezogener Daten für die Hochschulstatistik Bestandteil des Einschreibungsverfahrens an den Hamburger Hochschulen (Erstimmatrikulation bzw. Rückmeldung) ist. Die Immatrikulation ist z.B. gem. § 5 Abs. 2 der Immatrikulationsordnung der Fachhochschule Hamburg vom 5. 6. 1980 auf einem von der Fachhochschule vorgeschriebenen Formular zu beantragen. Gem. § 6 Abs. 4 Nr. 1 sind dem Immatrikulationsantrag die vollständig ausgefüllten, vom Studentensekretariat insbesondere für statistische Erhebungen zusätzlich ausgehändigten Fragebogen (Erhebungsbogen) beizufügen. Der vorliegende Rückmeldebogen für das Win-

tersemester 1987/1988 weist ausdrücklich darauf hin, daß der Erhebungsbogen für die Hochschulstatistik Bestandteil des Bogens ist.

Ähnliche Regelungen finden sich in

— der Immatrikulations- und Gasthörerordnung der Hochschule für Bildende Künste (§ 7 Abs. 2 Nr. 3),

— der vorläufigen Immatrikulations- und Gasthörerordnung der Hochschule für Musik und Darstellende Kunst (§ 15 Abs. 2 Nr. 2),

— der Immatrikulationsordnung der Hochschule für Wirtschaft und Politik (§ 3 Abs. 2),

— der Immatrikulationsordnung der Technischen Universität Hamburg-Harburg (§ 4 Abs. 2).

Obwohl es an der Universität Hamburg keine Immatrikulationsordnung gibt, werden auch hier die Angaben für die Hochschulstatistik im Rahmen der Immatrikulation erhoben.

Im einzelnen sehe ich folgende Probleme:

Die Immatrikulation und die Erhebung der Daten zur Hochschulstatistik werden in einem Verwaltungsakt zusammengefaßt, ohne daß — z.B. an der Universität — den Betroffenen deutlich wird, welche Angaben für welchen Zweck abgefragt werden.

Die Durchführung der Erhebung durch die Hochschulen und nicht durch von der übrigen Verwaltung abgeschottete Erhebungsstellen oder das Statistische Landesamt führt dazu, daß die Betroffenen den Hochschulen gegenüber auch solche Angaben offenbaren müssen, die ausschließlich für statistische Zwecke benötigt werden. Da die Immatrikulationsunterlagen — einschließlich der Statistik-Daten — zumindest an der Universität — für die Dauer des Studiums in der Verwaltung aufbewahrt werden, kommt es zu einer dauerhaften, gesetzlich nicht gedeckten Verletzung des Persönlichkeitsrechts der Betroffenen. Das Formular „Immatrikulationsantrag" der Universität ist so gestaltet, daß die nach § 12 Abs. 1 BStatG vorgeschriebene Trennung der Hilfsmerkmale von den Erhebungsmerkmalen nicht möglich erscheint. Die vorgeschriebene Löschung der Hilfsmerkmale ist aus diesem Grund ebenfalls nicht möglich.

Die Betroffenen werden auch nicht darüber informiert, daß ihre statistischen Angaben für Zwecke einer Verlaufsstatistik fortgeschrieben werden und somit ein über die statistische Momentaufnahme hinausgehendes Persönlichkeitsbild entsteht.

Ich halte die Praxis der Hamburger Hochschulen und die ihr zugrundeliegenden Vorschriften für eine unzulässige Vermischung von Verwaltung und Statistik. Nach den Feststellungen des Bundesverfassungsgerichts müssen Statistik und Verwaltung strikt voneinander getrennt werden, um zu vermeiden, daß einem Auskunftspflichtigen aus seinen Angaben für eine statistische Erhebung Nachteile entstehen, weil diese Daten auch für administrative Zwecke genutzt werden. Die im geltenden Hochschulstatistikgesetz noch vorgesehene kombinierte Nutzung der Erhebungsdaten für statistische Zwecke und Verwaltungszwecke entspricht diesem Grundsatz nicht.

Die Zusammenfassung von Immatrikulation und statistischer Erhebung in einem Verwaltungsakt stellt aus meiner Sicht eine unzulässige Vermischung verschiedener Zwecke dar. Zur Durchsetzung der Auskunftspflicht für die Hochschulstatistik stehen rechtmäßig nur die im Bundesstatistikgesetz enthaltenen Sanktionsmöglichkeiten zur Verfügung. Durch die Einbindung des Erhebungsbogens in die Immatrikulationsunterlagen kann die Einschreibung nur dann erfolgen, wenn der Student auch die für die Statistik geforderten Angaben preisgibt. Gerade angesichts der begründeten Zweifel an der Vereinbarkeit des Hochschulstatistikgesetzes mit dem Grundgesetz halte ich diese Praxis für äußerst bedenklich.

Sofern ausschließlich für statistische Zwecke erhobene Angaben in die Studentenakten eingegangen sind, ist auch dies i. S. einer strikten Trennung von Statistik und Ver-

waltung nicht zulässig. Ich habe deshalb die Universität Hamburg aufgefordert, die Erhebung von Daten für die Hochschulstatistik bis zum Immatrikulationstermin für das SS 1988 auf ein Verfahren umzustellen, wie es in der Novelle zum HStatG vorgesehen ist.

Auch an den anderen Hochschulen müssen die Durchführung der Statistik und die ihr zugrundeliegenden Immatrikulationsordnungen im Sinne des im Referentenentwurf für ein neues Hochschulstatistikgesetz vorgesehenen Verfahrens geändert werden. Dies bedeutet, daß auf eine gesonderte Erhebung von Daten für statistische Zwecke bei den Studenten und Prüfungskandidaten zugunsten einer reinen Sekundärstatistik verzichtet wird (vgl. 3. TB, 3.6.5.2, S. 46).

4.3.3 Jugendhilfestatistik

Aufgrund einer Eingabe habe ich die Jugendhilfestatistik datenschutzrechtlich überprüft.

Ich habe in meinen — auch der Behörde für Inneres zugeleiteten — Feststellungen schwerwiegende Bedenken gegen die Verfassungsmäßigkeit der Rechtsgrundlage dieser Statistik und gegen die Art der Durchführung beim Statistischen Landesamt Hamburg geäußert. Obwohl meine Bedenken dem Statistischen Landesamt seit dem Frühsommer bekannt waren, unterblieben Änderungen in der Durchführung der Erhebung weitgehend. Der Senat hat dies in seiner Antwort auf eine Kleine Anfrage (Drs. 13/647) damit begründet, meine Stellungnahme enthalte zwar datenschutzrechtliche Bedenken, jedoch keine konkreten Forderungen hinsichtlich der Erhebung.

Ich möchte bei dieser Gelegenheit noch einmal klarstellen: Es obliegt gem. § 16 HmbDSG den Behörden der FHH, für ihren Bereich die Ausführung des HmbDSG sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen. Wenn der Datenschutzbeauftragte darauf hinweist, daß ein Verwaltungshandeln datenschutzrechtlich bedenklich ist, so müssen die zuständigen Stellen unverzüglich Maßnahmen einleiten, um die aufgezeigten Mängel zu beseitigen, und dies selbstverständlich auch dann, wenn der Datenschutzbeauftragte konkrete Forderungen nicht erhoben hat.

Im einzelnen habe ich folgendes festgestellt:

4.3.3.1 Rechtsgrundlage

Ich bin der Auffassung, daß die gesetzliche Grundlage (§ 4 des Gesetzes über die Durchführung von Statistiken auf dem Gebiet der Sozialhilfe, die Kriegsopferfürsorge und der Jugendhilfe i.V.m. dem Gesetz über die Statistik für Bundeszwecke (Bundesstatistikgesetz — BStatG) für die Durchführung der Jugendhilfestatistik nicht den durch das Urteil des Bundesverfassungsgerichts zur Volkszählung 1983 formulierten Grundsätzen entspricht:

Die Hilfsmerkmale werden in dem Gesetz nicht bestimmt. Zwar gestattet das BStatG vom 22. 1. 1987 in § 26 Abs. 2 bei Erhebungen aufgrund bereits vor Inkrafttreten des neuen BStatG geltender Rechtsvorschriften unter bestimmten Voraussetzungen die Erhebung von Hilfsmerkmalen, auch wenn diese in der die Erhebung anordnenden Rechtsvorschrift nicht spezifiziert werden. Um die daran anknüpfenden Informations-, Trennungs- und Löschungsregelungen umsetzen zu können, muß jedoch nachprüfbar festgelegt werden, bei welchen Merkmalen es sich um Hilfsmerkmale handelt.

Es ist zu bezweifeln, ob die in § 4 des o.a. Gesetzes formulierten Erhebungsmerkmale hinreichend präzise bestimmt sind. Dieser Mangel ist besonders schwerwiegend, weil der Gesetzgeber mit dem zweiten Statistikbereinigungsgesetz vom 19. 12. 1986 durchaus die Gelegenheit gehabt hätte, eine datenschutzrechtlich einwandfreie bereichsspezifische Regelung zu treffen. Wenn dagegen von der Behörde für Inneres ins Feld geführt wird, der Gesetzgeber habe mit dem zweiten Statistikbereinigungsgesetz vorrangig andere Ziele verfolgt als die Anpassung von statistischen Rechtsvorschriften an Forderungen des Volkszählungsurteils, so entkräftet dies nicht meine Kritik.

4.3.3.2 Durchführung der Erhebung

Zur Durchführung der Erhebung hat die Behörde für Arbeit, Jugend, und Soziales dem Statistischen Landesamt die Anschriften der auskunftspflichtigen Träger und Einrichtungen übermittelt. Dies ist gem. § 5 Abs. 1 Nr. 3 des o.g. Gesetzes zulässig. Das Statistische Landesamt hat diese listenmäßig übermittelten Daten in einer Datei zusammengefaßt, die außer der Bezeichnung und Anschrift der Einrichtungen als Schlüssel auch eine Kennziffer für den Träger der Einrichtung und die laufende Nummer der Einrichtung enthält. Aus der Datei werden eine Adressenliste für die Rücklaufkontrolle und Adreßaufkleber für die zu befragenden Einrichtungen ausgedruckt. Die Rücklaufkontrolle erfolgt manuell durch handschriftlichen Vermerk auf der Adressenliste. Gegen dieses Verfahren habe ich keine Einwände.

Die den auskunftspflichtigen Trägern zugesandten Erhebungsunterlagen bestehen aus einem Erhebungsbogen, einem Erläuterungsblatt und einem Beilegeblatt „Rechtsgrundlage".

In dem an die Auskunftspflichtigen geschickten Anschreiben heißt es, der obere Teil des Erhebungsbogens mit Namen, Anschriften und Telefonnummern für Rückfragen werde nach Abschluß der Aufbereitungsarbeiten von den übrigen Angaben getrennt und vernichtet. Dateien mit den Angaben zu den Erhebungstatbeständen würden nach Abschluß der nächsten Erhebung vernichtet.

Der Fragebogen ist jedoch so gestaltet, daß eine Trennung — wie in dem Anschreiben zugesagt — nicht erfolgen kann, weil Vorder- und Rückseite bedruckt sind und ein Abtrennen des durch eine unterbrochene Linie gekennzeichneten oberen Teils der ersten Seite des Erhebungsbogens unweigerlich auch dazu führen würde, daß die Seite zwei des Fragebogens mit den entsprechenden Erhebungsmerkmalen nicht mehr ausgewertet werden könnte. Die Bfl hat dazu erklärt, daß der Erhebungsbogen für die Jugendhilfestatistik durch ein Versäumnis der Druckerei eine Fassung erhalten habe, die ein Abtrennen des Namens und Anschriftenabschnittes ohne den gleichzeitigen Verlust eines Teiles der Erhebungsmerkmale nicht zulasse. Da die Vorbereitung der Erhebung unter beträchtlichem Termindruck gestanden habe, hätten korrekt gestaltete neue Bögen aus Zeitgründen nicht mehr hergestellt werden können. Nach Auskunft des Statistischen Landesamtes ist dem Gebot der Beseitigung von Hilfsmerkmalen in der Weise Rechnung getragen worden, daß die Erhebungsunterlagen im Dezember 1987 insgesamt vernichtet wurden.

Der Teil mit den Angaben zu den Erhebungstatbeständen enthält als erste Zeile eine vom Statistischen Landesamt auszufüllende Kennziffer. Diese Kennziffer setzt sich nach Auskunft des Statistischen Landesamtes in Hamburg wie folgt zusammen:

— Stelle 1 bis 3 Kreis (wird in Hamburg nicht signiert, jedoch im automatisierten Verfahren mit Kreiskennung für Hamburg verarbeitet),

— Stelle 3 bis 6 Gemeinde (in Hamburg wird hier eine dreistellige Ortsteilkennziffer eingetragen),

— Stelle 7 bis 10 laufende Nummer der Einrichtung (diese laufende Nummer ist identisch mit der im Adressenmaterial vergebenen laufenden Nummer).

— Stellen 11 und 12 Kennziffer für Art der Einrichtung.

Ich bin der Auffassung, daß es sich bei dieser Kennziffer um ein Hilfsmerkmal i.S.v. § 16 BStatG handelt, dessen dauerhafte Speicherung gem. § 12 BStatG nicht zulässig ist.

Die 12stellige vom Statistischen Landesamt vergebene Fragebogenkennziffer und die Angaben zu den Erhebungstatbeständen werden aber in der Datenverarbeitungszentrale erfaßt und dauerhaft gespeichert. Eine Übermittlung von Einzelangaben an die Behörde für Arbeit, Jugend und Soziales oder an andere Stellen der hamburgischen Verwaltung erfolgt nach Angaben des Statistischen Landesamtes allerdings nicht.

Der Adreßbestand für die Abwicklung der Erhebung einschließlich des Schlüssels wird beim Statistischen Landesamt auf einem Personal-Computer gespeichert. Nach Auskunft der Bfl sollen nach Abschluß der Aufbereitungsarbeiten für die Jugendhilfestatistik die Adressen gelöscht werden. Bei der für das Jahr 1990 angesetzten nächsten Erhebung werde die BAJS um die Überlassung der Namen und Anschriften der dann bestehenden Träger und Einrichtungen der Jugendhilfe gebeten werden.

Auf demselben Personal-Computer werden lt. Auskunft des Statistischen Landesamtes außer dieser Adreßdatei noch verschiedene andere Adreßdateien für vom Statistischen Landesamt durchgeführte Statistiken, Versanddateien und Dateien über Zahlungsfälle von Pflegekindern und Heiminsassen geführt. Die entsprechenden Verfahren sind mit der Programmiersprache BASIC programmiert; die Daten werden auf Fest- und Wechselplattenlaufwerken gespeichert und sind nicht durch besondere Sicherungssoftware gegen einen unbefugten Zugriff gesichert.

Dazu bemerkt die Bfl, daß es für das eingesetzte System keine Sicherungssoftware gebe. Ausreichende Vorkehrungen gegen unberechtigte Datennutzungen seien jedoch durch eine Raumsicherung (Sicherheitsschlüssel) und durch das Unter-Verschluß-Halten des Schlüssels für die Anlage getroffen; im ganzen hätten lediglich drei Bedienstete des Statistischen Landesamtes Zugang zu der Anlage. Die getroffenen Maßnahmen reichten also aus. Diese Auffassung teile ich nicht. Ist die Verarbeitung von Statistik- und Verwaltungsdaten auf einem Rechner ohnehin problematisch, so verstärken sich meine Zweifel angesichts der eingesetzten Technik, die nicht dem heute hinsichtlich des Datenschutzes erforderlichen Mindeststandard entspricht (vgl. hierzu meine Ausführungen in Abschnitt 3.5).

4.4 Volkszählung 1987

Die folgende Darstellung der Durchführung der Zählung schließt an die in meinen letzten Tätigkeitsberichten enthaltenen Ausführungen (vgl. 5.TB, 5.3.1, S. 38) an. Im Mittelpunkt stehen diesmal die datenschutzrechtlichen Probleme, die im Zusammenhang mit der Durchführung der Erhebung aufgetreten sind. Einiges hierzu habe ich bereits weiter oben im Abschnitt zur Lage des Datenschutzes (vgl. 1.2) ausgeführt.

Der Beitrag weist schwerpunktmäßig auf Fehlleistungen der mit der Durchführung der Volkszählung befaßten Stellen hin, die mich zu förmlichen Beanstandungen gegenüber dem Senat veranlaßt haben:

- Die unzureichende Beteiligung und Information durch die Innenbehörde (4.4.2),
- unzulässige Übermittlungen von Meldedaten durch das Einwohnerzentralamt und von anderen Stellen an die Erhebungsstelle Volkszählung (4.4.4.3),
- das unzureichende Freigabeverfahren (4.4.3.2),
- die nicht rechtzeitige Trennung und Löschung von Erhebungsunterlagen (4.4.3.3),
- nicht rechtzeitige Löschung der Daten aus der Datenbank beim Erinnerungs- und Mahnverfahren (4.4.4.5),

4.4.1 Beurteilung des bisherigen Ablaufs der Zählung

Das Großprojekt der amtlichen Statistik — die Volkszählung 1987 — hat wie erwartet einen Großteil der Kapazitäten meiner Dienststelle absorbiert. Obwohl die Aufbereitung der VZ-Daten noch längst nicht abgeschlossen ist, muß ich konstatieren, daß es sowohl bei der Vorbereitung, bei der Datenerhebung beim Bürger und bei der weiteren Verarbeitung zu z.T. schwerwiegenden Verstößen gegen das Datenschutzrecht gekommen ist (vgl. auch 1.2), die ich gegenüber dem Senat gem. § 21 HmbDSG förmlich beanstandet habe.

Obwohl der Senat der in meiner ersten förmlichen Beanstandung vom 17. März 1987 vorgenommenen Bewertung nur zum Teil gefolgt war, hatte er doch eine strikte Beachtung der einschlägigen Datenschutzvorschriften zugesagt. Bedauerlicherweise ent-

sprach die Praxis häufig nicht dieser Zusicherung, so daß ich mich im November 1987 zu einer zweiten förmlichen Beanstandung veranlaßt gesehen habe.

Der im folgenden dargestellte Ablauf der Zählung in Hamburg ergibt leider ein Bild, das aus Sicht des Datenschutzes nicht sehr erfreulich ist. Ich komme um die Feststellung nicht herum, daß es dem mit der Durchführung der VZ befaßten Statistischen Landesamt offenbar immer noch an der notwendigen Sensibilität für Belange des Datenschutzes mangelt.

Aber auch der Senat hat sich in seinen Stellungnahmen zu meinen Beanstandungen in einer Weise geäußert, die mir nicht immer angemessen erscheint. Das betrifft vor allem die Frage, wie verbindlich Datenschutzvorschriften sind. Gerade im Hinblick darauf, daß gegen verschiedene Verwaltungsvorschriften wiederholt verstoßen wurde, macht deutlich, daß es bei der automatisierten DV zusätzlicher Rechtsvorschriften bedarf, die z.B. die Freigabe und Dokumentation von Verfahren verbindlich festlegen. Ich werde entsprechende Anregungen in die anstehende Diskussion über die Novellierung des HmbDSG einbringen.

Von besonderer Bedeutung für die Rechtmäßigkeit der weiteren Verarbeitung von VZ-Daten sind solche Mängel, die zur Folge haben, daß sich die im VZG 1987 vorgesehenen grundrechtssichernden Maßnahmen verzögern. Bereits jetzt muß ich feststellen, daß die bei der Durchführung der Volkszählung eingetretenen Verzögerungen nicht ohne Konsequenzen bleiben können.

Ich habe der Bfl mitgeteilt, daß m.E. eine weitere Verarbeitung der Erhebungsunterlagen der Gebäudevorerhebung im Hinblick auf die gesetzlich vorgeschriebene Trennung von Erhebungs- und Hilfsmerkmalen zum frühest möglichen Zeitpunkt (§15 Abs. 1 VZG 1987) auf schwerwiegende Bedenken stößt, da dieser Zeitpunkt bereits überschritten ist (vgl. 4.4.3.3). Auch beim automatisierten Erinnerungs- und Mahnverfahren habe ich beanstandet, daß Einwohnerdaten aus der Einwohnerdatenbank ERA nicht rechtzeitig gelöscht werden (vgl. 4.4.5.8).

Noch gravierender würden sich weitere Verzögerungen auswirken, die z.B. ein Zwangsgeldverfahren, das erst mehr als ein halbes Jahr nach dem Erhebungsstichtag einsetzt, aufgrund der organisatorischen Gegebenheiten und des Verarbeitungskonzeptes des Statistischen Landesamtes nahezu zwangsläufig bewirken würde. Wenn die Folge wäre, daß auch für die Haupterhebung die in § 15 Abs. 1 VZG 1987 geforderte Trennung von Erhebungs- und Hilfsmerkmalen und die in § 15 Abs. 2 VZG 1987 geforderte Vernichtung der Erhebungsvordrucke nicht rechtzeitig erfolgt, würde hiermit die Zulässigkeit der gesamten weiteren Verarbeitung der Volkszählungsdaten in Frage gestellt. Das Bundesverfassungsgericht hat in mehreren Entscheidungen (z.B. Kammerentscheidung v. 24. 9. 1987, 1 BvR97087) festgestellt, daß bei der Beurteilung der Rechtmäßigkeit des Verwaltungshandelns vermeidbare Verzögerungen außer Betracht zu bleiben haben. Die statistischen Ämter seien gehalten, die Aufbereitungsorganisation und die personellen und sachlichen Mittel in den Grenzen des vom Bürger vernünftigerweise erwartbaren Aufwandes an einer zügigen Aufbereitung auszurichten.

Ich bin der Auffassung, daß der Versuch, alle noch säumigen Auskunftspflichtigen zur Abgabe ihrer Fragebögen zu zwingen, zu weiteren erheblichen Verzögerungen führen würde. Diese Annahme gründet sich nicht nur auf den bisherigen Ablauf der Zählung in Hamburg; sie wird bestärkt durch andernorts gewonnene Erfahrungen. Ich erwarte auch nicht, daß sich aufgrund einer „harten Linie" — quasi als Äquivalent für den zusätzlichen personellen und sachlichen Aufwand — wesentlich brauchbarere Daten gewinnen lassen, da — auch dies bestätigen Erfahrungen aus anderen Erhebungsstellen — die Qualität der zwangsweise erhobenen Daten wohl noch mehr zu wünschen übrig läßt als die der „freiwillig" erteilten Auskünfte.

Ich habe den Innensenator darauf hingewiesen, daß als einzig gangbarer Weg, der eine von weiteren Rechtsverstößen unbelastete Durchführung der Volkszählung ermöglicht und dennoch zu einigermaßen brauchbaren Ergebnissen führt, nur die sofortige

Ersatzvornahme (§ 11 Abs. 1 VZG 1987) in Betracht kommt. Diese setzt — jedenfalls nach meiner Gesetzesinterpretation — nicht voraus, daß zuvor Zwangsmaßnahmen zur Durchsetzung der Auskunftspflicht versucht worden sind.

Bisher hat der Senat über das weitere Vorgehen, also darüber, ob Maßnahmen zur Durchsetzung der Auskunftspflicht ergriffen werden sollen, noch nicht abschließend entschieden.

4.4.2 Unzureichende Beteiligung

Bereits in meinem letzten TB (5.3.1, S. 45) mußte ich — damals in Zusammenhang mit der Zählerbenennung — feststellen, daß ich vom Statistischen Landesamt nur unzureichend und nicht rechtzeitig über die Verarbeitung personenbezogener Daten im Rahmen der VZ informiert wurde. Der Senat hatte daraufhin zugesagt, mich in Zukunft umfassend und aktuell zu unterrichten. Leider muß ich heute berichten, daß die Information meiner Dienststelle über die Verarbeitung personenbezogener Daten bei der VZ auch im Jahr 1987 sehr zu wünschen übrig ließ. Dies gilt auch für Fälle, in denen eine frühzeitige Unterrichtung in einer Rechtsvorschrift festgelegt ist.

§ 8 der Verordnung zu Durchführung des Volkszählungsgesetzes vom 2. 9. 1986 sieht vor, daß die vom Leiter des Statistischen Landesamtes zu treffenden Anordnungen zur ordnungsgemäßen Durchführung der Volkszählung dem Hamburgischen Datenschutzbeauftragten unverzüglich zur Kenntnis zu geben sind.

Die Behörde für Inneres hat mehrfach gegen diese Vorschrift verstoßen:

Trotz wiederholter Anmahnungen wurden mir

— die Dienstanweisung zur personellen Abschottung der Erhebungsstelle Volkszählung und über zusätzliche Maßnahmen zur Datensicherung vom 14. August 1987 und

— die Verfügung zur Löschung von Einwohnerdaten in der Datenbank ERA vom 1. September 1987

erst mit Schreiben vom 27. Oktober 1987, d.h. mit mehrmonatiger Verspätung übersandt.

Die unzureichende Information und die nur zögerliche und zudem teilweise nicht vollständige Beantwortung meiner Fragen durch die Behörde für Inneres in diesen und in verschiedenen anderen Fällen verstößt auch gegen das Hamburgische Datenschutzgesetz. Gem. § 20 Abs. 4 HmbDSG sind die Behörden dazu verpflichtet, den Hamburgischen Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen und ihm inbesondere Auskunft zu Fragen sowie Einsicht in alle Unterlagen und Akten zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen. Dazu gehört auch eine rechtzeitige und vollständige Unterrichtung über geplante Verarbeitungsschritte, zumal dann, wenn ich entsprechende Fragen gestellt habe.

Der Senat hat meine Beanstandung mit der Begründung zurückgewiesen, die nicht fristgerechte Beantwortung meiner Fragen sei darauf zurückzuführen, daß die Meinungsbildung unter Berücksichtigung der personellen Situation und der vielfältigen Aufgaben bei der Durchführung der Volkszählung nicht habe früher abgeschlossen werden können. Allein die Vielzahl der Fragen, die von den Medien, von einzelnen Bürgern oder Bürgerinitiativen und nicht zuletzt von Abgeordneten aufgeworfen würden oder gegenüber Gerichten beantwortet werden müßten, hätten die Leitung und das Personal der Erhebungsstelle in einem für den Fortgang der Arbeiten bedeutsamen Umfang in Anspruch genommen.

Der Senat hat weiter ausgeführt, daß die von mir angesprochenen Anweisungen des Leiters der Erhebungsstelle mit mir erörtert und abgestimmt worden seien. Eine schuldhafte Verzögerung bei der Information des Hamburgischen Datenschutzbeauftragten habe der Senat nicht festgestellt.

Dazu stelle ich folgendes fest:

Die vom Senat behauptete frühzeitige Abstimmung der Dienstanweisungen hat nicht stattgefunden. Zwar habe ich Vorentwürfe erhalten; ich habe diese jedoch kritisiert und Gegenvorschläge gemacht (vgl.4.4.3.2(3)), die aber nicht aufgegriffen wurden. Die endgültige Fassung der Dienstanweisungen habe ich erst mit mehrmonatiger Verspätung erhalten. Die desweiteren vom Senat gegebene Begründung für Antwortverzögerungen läßt darauf schließen, daß die Erhebungsstelle personell und organisatorisch mit der Abwicklung der Zählung überfordert war, was im Hinblick auf die vom Bundesverfassungsgericht aufgestellte Forderung nach einer zügigen Durchführung bedenklich erscheint.

Leider bin ich auch in anderen Fällen nicht rechtzeitig unterrichtet worden. So blieben trotz mehrmaliger Erinnerung meine der Bfl im Juli 1987 gestellten Fragen zur Wiederholungsbefragung lange Zeit unbeantwortet. Ende Oktober übersandte mir die Bfl — ohne auf meine Bedenken einzugehen und ohne auf meine Fragen zu antworten — einige vom Statistischen Bundesamt ausgearbeitete Unterlagen über die Wiederholungsbefragung. Telefonisch konnte ich dann in Erfahrung bringen, daß Hamburg das Bundeskonzept übernehmen würde (vgl.4.4.5.9).

Die Verwaltung scheint — zumindest in diesem Punkt — die Ausführungen des Bundesverfassungsgerichts nicht ernstzunehmen. Dieses mißt in seinem Volkszählungsurteil (BVerfGE 65,1 S.46) der rechtzeitigen Beteiligung unabhängiger Datenschutzbeauftragter bei der Volkszählung für einen effektiven Schutz des informationellen Selbstbestimmungrechts erhebliche Bedeutung zu.

4.4.3 Verarbeitung von Volkszählungsdaten

4.4.3.1 Unvollständiges Datenverarbeitungskonzept

Im VZ-Urteil hat das Bundesverfassungsgericht auch darauf hingewiesen, daß die Funktionsfähigkeit der amtlichen Statistik an den Wahrheitsgehalt der erhobenen Daten gebunden sei und dieses Ziel nur erreicht werden könne, wenn bei dem auskunftspflichtigen Bürger das notwendige Vertrauen in die Abschottung seiner für statistische Zwecke erhobenen Daten geschaffen werde, ohne welche seine Bereitschaft, wahrheitsgemäße Angaben zu machen, nicht herzustellen sei. „Eine Staatspraxis, die sich nicht um die Bildung eines solchen Vertrauens durch Offenlegung des Datenverarbeitungsprozesses und strikte Abschottung bemühte, würde auf längere Sicht zu schwindender Kooperationsbereitschaft führen, weil Mißtrauen entstünde."

Damit die Datenschutzbeauftragten kontrollieren können, ob bei der Verarbeitung der Volkszählungsdaten den verfassungsrechtlich gebotenen Anforderungen in wirksamer Weise Rechnung getragen wird, müssen sie das für die programmierenden Stellen verbindliche Datenverarbeitungskonzept kennen. Ich hatte deshalb schon frühzeitig vom Statistischen Landesamt Hamburg gefordert, mir ein umfassendes Datenverarbeitungskonzept zur Verfügung zu stellen. Mir wurde daraufhin mitgeteilt, die Datenverarbeitungsprogramme würden von verschiedenen Statistischen Landesämtern — das Statistische Landesamt Hamburg ist hieran nicht beteiligt — unter Federführung des Statistischen Bundesamtes erstellt. Aus diesem Grund könne das Statistische Landesamt Hamburg nur die Materialien an den Hamburgischen Datenschutzbeauftragten weiterleiten, die bereits vom Statistischen Bundesamt fertiggestellt worden seien.

Erst kurz vor dem Erhebungsstichtag wurde mir der erste Teil des Aufbereitungskonzeptes der Volkszählungsdaten 1987 zugestellt. Es handelte sich dabei um einen Datenflußplan zur manuellen Bearbeitung der Erhebungsformulare, einen Datenflußplan über die maschinelle Verarbeitung mit Erläuterungen und einige Datensatzbeschreibungen. Die mir jetzt vorliegenden Unterlagen zur maschinellen Datenaufbereitung beinhaltet die maschinelle Erfassung der Daten und die Plausibilitätskontrollen, läßt jedoch die Phase der Anonymisierung gem. § 15 VZG 1987 (Löschung der Hilfsmerkmale und Ordnungsnummern bzw.deren Ersatz durch rückgriffsfreie Nummern und Ersatz der genauen Anschriften durch die Blockseitennummern — vgl. auch 4.4.3.3) aus.

Das Statistische Landesamt meint, das Fehlen eines vollständigen DV-Konzeptes sei kein gravierender Mangel, weil für die Ausarbeitung der noch fehlenden Teile des Konzepts genügend Zeit zur Verfügung stehe. Dem ist entgegenzuhalten, daß gerade der Mangel an zusätzlichen „vertrauensbildenden Maßnahmen" zur verringerten Auskunftsbereitschaft und damit nicht zuletzt zu Verzögerungen beigetragen hat, die wiederum datenschutzrechtliche Bedenken auslösen (vgl. 4.4.1 und 4.4.3.3).

4.4.3.2 Unzureichendes Freigabeverfahren

(1) Bei der Prüfung des Verfahrens zur Vorbereitung der Gebäudevorerhebung habe ich festgestellt, daß auch die in § 8 Abs. 1 Hamburgisches Datenschutzgesetz geforderten technischen und organisatorischen Maßnahmen zur Datensicherung nicht in ausreichendem Maße gewährleistet waren (vgl. auch 3.4.1).

Vor allem hatte ich zu bemängeln, daß das bei der GVE eingesetzte Verfahren nicht ordnungsgemäß getestet und freigegeben wurde. Die Datenverarbeitungszentrale der Hamburger Verwaltung (DVZ) hatte Produktionsaufträge ausgeführt, ohne daß eine Freigabeerklärung für das Verfahren vorlag, und war damit ihrer Verpflichtung zur Prüfung der vom Statistischen Landesamt vorgelegten Unterlagen nicht nachgekommen. Im sog. „DVZ-Test" wurden personenbezogene Originaldaten verarbeitet; die DVZ hatte nicht geprüft, ob hierfür die nach den einschlägigen Verwaltungsvorschriften obligatorische Ausnahmegenehmigung vorlag. Ferner hatte die DVZ Aufträge aufgrund mündlicher Anweisung ausgeführt, obwohl nur bei schriftlichen Aufträgen die Auftragsberechtigung geprüft werden kann.

Es ist bedauerlich, daß die bestehenden Datensicherungsvorschriften gerade bei der Durchführung der Volkszählung so interpretiert wurden, daß hier nicht einmal der normalerweise geforderte Sicherheitsstandard bei der Datenverarbeitung gewährleistet war. Der Senat hatte aber zugesagt, daß in Zukunft die für die Datenverarbeitung allgemein geltenden Richtlinien auch bei der DVZ befolgt würden und daß zusätzliche Sicherungen wegen der besonderen Sensibilität der Volkszählungsdaten getroffen würden (vgl. hierzu auch 3.4).

Die inzwischen unter meiner Beteiligung ausgearbeiteten Dienstanweisungen für die Datenverarbeitungszentrale (DVZ) sehen bei der Verarbeitung von VZ-Daten insbesondere für die Phase der maschinellen Verarbeitung von Zählungsergebnissen und von Daten zur Durchführung der Zählung bis zur Fertigstellung des Urbestandes der VZ, d.h. bis zu der nach § 15 Abs. 3, 4 VZG 1987 vorgesehenen Anonymisierung der Daten zusätzliche, über das bei der sonstigen Verarbeitung übliche Maß hinausgehende Sicherungsmaßnahmen vor, mit denen ich einverstanden bin.

(2) Hingegen ist die Dienstanweisung zur personellen Abschottung der Erhebungsstelle VZ und über zusätzliche Maßnahmen zur Datensicherung im Hinblick auf die bei der Verarbeitung von Volkszählungsdaten erforderlichen Sicherheitsstandards, soweit diese von der Erhebungsstelle zu treffen sind, unzureichend und verstößt gegen § 8 Abs. 1 HmbDSG. Es ist ärgerlich, daß damit die vom Senat im Zusammenhang mit meiner Beanstandung der Gebäudevorerhebung gegebenen Zusagen hier nicht eingehalten werden.

Mein Formulierungsvorschlag für die im Wege der Verbundprogrammierung erstellten Verfahrensteile orientierte sich an den Richtlinien zur Freigabe von automatisierten Verfahren (- Freigaberichtlinie -, MittVw 1982, S. 70). Er sah vor, daß auf einen eigenen Abnahmetest dann verzichtet werden kann, wenn vom Statistischen Landesamt geprüft wurde, ob

— die im Rahmen des Verbundes vorhandenen Testfälle den in Hamburg geltenden Vorschriften entsprechen (Nr. 2 und 3 Freigaberichtlinie),

— die im Rahmen des Verbundes erarbeiteten Testergebnisse richtig sind und

— die getesteten Programm- und Betriebssystemversionen und die Programm- und Betriebssystemversionen des freizugebenden automatisierten Verfahrens übereinstimmen.

Damit wollte ich sicherstellen, daß — hier bezogen auf die Verbundprogrammierung — die in Hamburg geltenden Standards der Datensicherung — hier: Freigaberichtlinie — auch bei der Verarbeitung der VZ-Daten eingehalten werden. Von der BfI wurde die von mir vorgeschlagene Fassung mit der Begründung zurückgewiesen, daß sie zu einem erheblichen zusätzlichen Arbeitsaufwand geführt hätte, ohne daß damit ein entsprechender Gewinn verbunden wäre.

Ich habe Zweifel an der von der Behörde für Inneres geäußerten Annahme, daß die in den anderen Bundesländern durchgeführten Tests den Hamburger Anforderungen — jedenfalls im Hinblick auf die Notwendigkeit von Abnahmetests — entsprechen. Gerade deshalb entbindet das von der Behörde für Inneres bekundete Streben nach einem einheitlichen Verfahren der Bundesländer bei der Durchführung von Tests das Statistische Landesamt nicht von seinen Prüfungsverpflichtungen gem. Nr. 5.2 Freigaberichtlinie, die sich ausdrücklich auf die Verbundprogrammierung beziehen, d.h. auf eine Verfahrensentwicklung, bei der auch außerhamburgische Stellen mitwirken.

Der Senat hat zu meiner Beanstandung ausgeführt, die an der Verbundprogrammierung beteiligten Länder hätten verabredet, die Qualität der durchgeführten Tests sollten der Qualität der in Hamburg durchgeführten Abnahmetests entsprechen. Verfahrensteile würden an die anderen Verbundteilnehmer jeweils erst dann versandt und damit freigegeben, wenn sichergestellt sei, daß sie funktionstüchtig sind und den fachlichen, organisatorischen und rechtlichen Anforderungen entsprächen.

Eine derartige „Verabredung" reicht m.E. nicht aus und entbindet das Statistische Landesamt auch nicht von seinen in den Freigaberichtlinien festgelegten Prüfungsverpflichtungen.

Unzureichend ist es auch, daß in der Dienstanweisung wieder nur — entgegen meinen Forderungen und entsprechenden Zusagen der BfI — ein Abnahmetest (Test unter Beteiligung sowohl der programmierenden als auch der fachlich zuständigen Stelle) nur auf Programm-, nicht jedoch auf Verfahrensebene vorgesehen ist. Da — wie meine Prüfung des Verfahrens Gebäudevorerhebung ergeben hatte — zum großen Teil Standardprogramme eingesetzt werden, wird hiermit das Ziel einer ordnungsgemäßen Verfahrensfreigabe unterlaufen:

— Bei der Freigabe eines Sortierprogramms kommt es datenschutzrechtlich in erster Linie darauf an, welche Datenbestände nach welchen Merkmalen sortiert werden, was jedoch — nach dem Wortlaut der Dienstanweisung — nicht Gegenstand der Freigabe nach einem Abnahmetest ist.

— Bei einem Programm zur Zusammenführung von Daten aus verschiedenen Dateien steht ebenfalls im Mittelpunkt des Interesses die Frage, welche Daten aus welchen Dateien nach welchen Kriterien zusammengeführt werden.

Der Sinn eines Abnahmetests besteht aber gerade darin, das Zusammenwirken aller Programme in bezug auf die zu erfüllende Fachaufgabe zu beurteilen.

Ich habe deshalb auch diesen Teil der Dienstanweisung beanstandet. Der Senat hat zugesagt, die Formulierung der Dienstanweisung der bereits geübten Praxis anzupassen, was ich so interpretiere, daß meine Forderungen berücksichtigt werden.

4.4.3.3 Zeitpunkt und Verfahren der Trennung von Hilfs- und Erhebungsmerkmalen

(1) Nach § 15 Abs. 1 VZG 1987 sind die Hilfsmerkmale mit Ausnahme der Hilfsmerkmale Straße und Hausnummer sowie Name der Arbeits- oder Ausbildungsstätte und Name, Bezeichnung von Unternehmen und Arbeitsstätten unverzüglich nach Durchführung der Eingangskontrollen bei den Statistischen Ämtern der Länder von den Erhebungsmerkmalen zu trennen und gesondert aufzubewahren.

§ 15 Abs. 2 VZG 1987 sieht vor, daß die Erhebungsvordrucke einschließlich der Hilfsmerkmale zum frühestmöglichen Zeitpunkt, spätestens zwei Wochen nach Feststellung der amtlichen Bevölkerungszahl des Landes zu vernichten sind.

Zur Frage des frühestmöglichen Zeitpunkts der Trennung und Löschung der Erhebungsunterlagen hat das BVerfG, wie bereits erwähnt, festgestellt, daß bei der Beurteilung der Rechtmäßigkeit des Verwaltungshandelns vermeidbare wesentliche Verzögerungen der Datenaufbereitung außer Betracht zu bleiben hätten; die statistischen Landesämter seien gehalten, die Aufbereitungsorganisation und die personellen und sachlichen Mittel in den Grenzen des vom Bürger vernünftigerweise erwartbaren Aufwandes an einer zügigen Aufbereitung auszurichten (BvR 97087, S. 8).

(2) Meine Prüfungen haben ergeben, daß die Aufbereitungsorganisation und die personelle Ausstattung der Erhebungsstelle in Hamburg dieser Maxime nicht genügt. Bereits jetzt ist es zuwesentlichen Verzögerungen gekommen.

So verstößt eine Vernichtung der Erhebungsbögen der Gebäudevorerhebung (GVE) erst im Frühjahr 1988 gegen § 15 Abs.1 VZG 1987. Aufgrund der Gestaltung der Erhebungsbögen ist hier eine Trennung von Erhebungs- und Hilfsmerkmalen — anders als bei der Haupterhebung — technisch nicht möglich.

Bei einer sachgerechten Gestaltung der Erhebungsunterlagen wäre es möglich gewesen, die Trennung bereits 1987 vorzunehmen, da die GVE bereits im Frühjahr 1987 durchgeführt wurde. Das Bundesverfassungsgericht hat darauf hingewiesen, daß „die Gestaltung des Personenbogens den verfassungsrechtlichen Trennungsgeboten zu folgen hat, nicht umgekehrt" (1 BvR970/87, S. 7). Ich sehe keine Gründe, die Gestaltung der Erhebungsunterlagen bei der GVE anders zu beurteilen.

Meine Forderungen an das Statistische Landesamt haben sich deshalb immer daran orientiert, ein Verfahren zu finden, das dem grundrechtssichernden Trennungsgebot des § 15 Abs.1 VZG 1987 genügt und zugleich eine Auswertung der Erhebungsunterlagen durch das Statistische Landesamt ermöglicht. Ich war deshalb damit einverstanden, daß die Angaben aus dem Erhebungsteil der Gebäudebögen auf Wohnungsbögen der entsprechenden Gebäude übertragen und die Bögen unmittelbar danach — wie auch im Sicherungskonzept für die Erhebungsstelle Volkszählung vorgesehen — vernichtet, also Trennung und Löschung uno actu vorgenommen werden sollten, dies allerdings unter der Voraussetzung, daß der Vernichtungszeitpunkt nicht wesentlich hinter dem bei anderer Gestaltung der Erhebungsunterlagen möglichen Zeitpunkt der Trennung liegen dürfte. Das wäre natürlich nur dann zu erreichen gewesen, wenn mit der Übertragung der Erhebungsangaben aus der GVE auf die Wohnungsbögen unmittelbar nach dem Eingang der GVE-Unterlagen begonnen worden wäre. Davon konnte ich aufgrund von entsprechenden Aussagen der Bfl auch ausgehen.

So hat die Bfl in ihrer Stellungnahme gegenüber dem Verwaltungsgericht Hamburg v. 15. Mai 1987 zu dem Verfahren der Aufbereitung der Daten aus der GVE ausgeführt:

> „... Nach dem 25. Mai 1987 — wenn mit dem Rücklauf der ersten Wohnungsbogen gerechnet werden kann — werden die Gebäudebogen zwecks Übertragung der Erhebungsmerkmale aus der Gebäudevorerhebung in den dafür vorgesehenen Teil des Wohnungsbogens an die entsprechenden Zählungsdienststellen verteilt. ... Nach Übertragung der Erhebungsmerkmale aus dem Gebäudebogen in den Wohnungsbogen werden die Gebäudebogen sofort vernichtet."

Die Bfl teilte mir demgegenüber im Oktober mit, sie wolle mit der Vernichtung der GVE-Bögen warten, bis alle Wohnungsbögen im Statistischen Landesamt vorlägen, um die Richtigkeit der Angaben auf den Gebäudebögen hinsichtlich der Zahl der Wohnungen zu überprüfen. Die Vernichtung der GVE-Unterlagen wäre bei diesem Verfahren bis März/April 1988 hinausgeschoben worden. Dies wäre mit § 15 Abs. 1 VZG 1987 nicht vereinbar gewesen. Geboten war vielmehr die sofortige Vernichtung bzw. Löschung der Identifikationsangaben — sei es durch Schwärzung oder durch Vernichtung der Erhebungsbögen. Hierauf habe ich mit meiner Beanstandung vom November 1987 den Senat hingewiesen.

Der Senat hat in seiner Stellungnahme zu meiner Beanstandung festgestellt, er schließe sich jetzt meiner Rechtsauffassung an, nach der § 15 Abs. 1 VZG 1987 ohne Rücksicht auf eine konkrete Schutzbedürftigkeit im einzelnen die möglichst frühzeitige Trennung bzw. Löschung der Hilfsdaten fordere. Er werde daher durch entsprechende Anweisung sicherstellen, daß die wegen der Gestaltung der Erhebungsbögen nicht abtrennbaren Hilfsmerkmale unverzüglich unkenntlich gemacht würden.

(3) Die Trennungs- und Löschungsgebote des VZG 1987 beschränken sich nicht auf die papiernen Erhebungsunterlagen; sie beziehen die Phase der automatisierten Verarbeitung mit ein. Gem. § 15 Abs. 3 VZG 1987 sind die laufenden Nummern und Ordnungsnummern (insbesondere der Haushaltsheftnummern, über die Personen-, Wohnungs- und Haushaltsmantelbogen zusammengeführt werden können) zu löschen, sobald die Zusammenhänge zwischen Personen und Haushalt, Haushalt und Wohnung, Wohnung und Gebäude durch Nummern, die einen Rückgriff auf einzelne Personen ausschließen, festgehalten worden sind.

Gem. § 15 Abs. 4 VZG 1987 können die Hilfsmerkmale Straße und Hausnummer gemeinsam mit den Erhebungsmerkmalen auf die für die maschinelle Weiterverarbeitung bestimmten Datenträger übernommen werden. Der Name darf nicht gemeinsam mit den Erhebungsmerkmalen abgespeichert werden. Über die genaue Anschrift könnte eine Deanonymisierung von Daten, d.h. ihre Zuordnung zu einzelnen namentlich bezeichneten Personen, durchgeführt werden. Aus diesem Grund sieht § 15 Abs. 4 VZG 1987 vor, daß die Hilfsmerkmale Straße und Hausnummer zu löschen sind, sobald ihre Zugehörigkeit zu kleinräumigen Gliederungen festgelegt ist. Die unterste Ebene der kleinräumigen Gliederung, für die eine statistische Verwendung vorgesehen werden darf, ist die Blockseite.

Leider liegen mir bislang keine Informationen darüber vor, in welcher Weise und wann die geforderten Anonymisierungsmaßnahmen beim automatisierten Verfahren vorgenommen werden sollen (vgl. Tz. 4.4.3.1).

4.4.3.4 Speicherung der Arbeitsstättenanschrift

Ein besonderes Problem im Rahmen des Gesamtkomplexes „Anonymität von Volkszählungsdaten" stellt die Speicherung der in Frage 12 des Personenbogens erfragten Adresse der Arbeitsstätte dar. Bei der Anschrift der Arbeitsstätte handelt es sich um ein Erhebungsmerkmal, das nach dem VZG 1987 dauerhaft gespeichert werden darf. Bei Selbständigen, die ihr Gewerbe in dem Gebäude ausüben, in dem sich ihre Wohnung befindet (Frage 14 des Personenbogens, 1. Alt.), wird somit auch deren Wohnanschrift dauerhaft gespeichert.

Die Anschrift der Arbeitsstätte wird zum Zwecke der Feststellung der Pendlerbewegungen zwischen Wohnung und Arbeitsstätte erhoben, um damit zur Lösung verkehrsplanerischer Fragen beizutragen (Bundestagsdrucksache 10/2814, S.17). Die dauerhafte Speicherung der Anschrift der Arbeitsstätten ist in den beschriebenen Fällen nicht erforderlich, da keine Pendlerbewegungen stattfinden, weil auf dem Wohngrundstück gearbeitet wird.

Außerdem würde die dauerhafte Speicherung der Anschriften mit dem Löschungsgebot für Straße und Hausnummer nach § 15 Abs. 4 Volkszählungsgesetz 1987 kollidieren, denn die unterste Ebene der kleinräumigen Gliederung, deren dauerhafte Speicherung zulässig ist, ist die „Blockseite". Eine dauerhafte Speicherung der Arbeitsstättenanschrift mit genauer Straßen- und Hausnummernangabe würde in diesen Fällen zu einer dauerhaften Speicherung der Wohnanschrift der Betroffenen führen. Da die Zuordnung von Personen zu Gebäuden ebenfalls gespeichert wird, ergibt sich hieraus — indirekt — auch für alle anderen Personen, die in dem betreffenden Gebäude gezählt wurden, einzusätzliches vermeidbares Reidentifikationsrisiko.

Ich habe deshalb gegenüber dem Senat beanstandet, daß das Statistische Landesamt Hamburg — anders als die Statistischen Ämter anderer Bundesländer — auf die

maschinelle Speicherung der Anschrift der Arbeitsstätte auch in den beschriebenen Fällen nicht verzichten wollte, obwohl eine Speicherung nicht erforderlich ist und zudem für die Betroffenen ein größeres Reidentifizierungsrisiko mit sich bringen würde.

Inzwischen hat übrigens auch das Bundesverfassungsgericht — in einem Beschluß vom 18. Dezember 1987 — festgestellt, daß dem Gebot der möglichst frühzeitigen faktischen Anonymisierung nur dann hinreichend Rechnung getragen werde, wenn in diesen Fällen die Anschrift der Arbeitsstätte nicht — auch nicht kodiert — auf die für die maschinelle Weiterverarbeitung bestimmten Datenträger übernommen oder hierfür signiert werde (1 BvR 96287, S. 6). Das BVerfG führt weiter aus, der Verzicht auf diese Speicherung sei dabei den Statistischen Landesämtern nicht freigestellt, sondern von Verfassungs wegen zum Schutz des Rechts auf informationelle Selbstbestimmung geboten (a.a.O., S. 8).

Der Senat ist jetzt der mit meiner Beanstandung erhobenen Forderung gefolgt. Auch in Hamburg wird also bei der beschriebenen Konstellation auf die Speicherung der Arbeitsstättenanschrift verzichtet.

4.4.3.5 Reidentifizierbarkeit von Daten

In der Diskussion um die Volkszählung hat die sog. „Reidentifizierungsproblematik" zeitweilig eine große Bedeutung gehabt. Dabei wurde zum Teil die Frage gestellt, ob die vom Bundesverfassungsgericht in seinem Volkszählungsurteil geforderte möglichst frühzeitige faktische Anonymisierung bei der Verarbeitung der Volkszählungsdaten tatsächlich gewährleistet wird.

Die von Informatikern vorgenommenen Versuche und entsprechende methodische Überlegungen, die bereits in meinem 5. TB wiedergegeben sind (5.3.2, S. 45), machen jedoch deutlich, daß eine Deanonymisierung von Daten, d.h. die Zuordnung von ohne Namen gespeicherten Daten zu einzelnen Personen, auch dann möglich ist, wenn die Maßnahmen nach § 15 VZG 1987 eingehalten werden, also die genaue Anschrift durch die Blockseite und die Haushaltsheftnummern durch unverfängliche Ordnungsnummern ersetzt werden. Derartige Versuche setzen jedoch sowohl ein entsprechendes Zusatzwissen als auch Zugriffsmöglichkeiten auf die gespeicherten Volkszählungsdaten voraus. Durch eine strikte Abschottung der Statistischen Landesämter von der übrigen Verwaltung und über besondere Sicherungsmaßnahmen bei der maschinellen Verarbeitung der VZ-Daten (vgl. 4.4.3.2) muß gewährleistet werden, daß ein solcher nicht zulässiger Zugriff auf die bei der Volkszählung erhobenen Daten unterbleibt, so daß eine notwendige Voraussetzung für eine erfolgreiche Reidentifizierung nicht gegeben ist.

Die Reidentifizierungsproblematik kann nicht mit dem Hinweis abgetan werden, bisher durchgeführte Reidentifizierungsversuche bedienten sich eines Datenbanksystems, und die Volkszählungsdaten würden nicht im Rahmen eines solchen Systems gespeichert. Zum einen ist es ein leichtes, in einer sequentiellen Datei abgelegte Daten in ein Datenbanksystem zu bringen. Genau dies ist sogar in einigen Statistischen Landesämtern — bisher aber nicht in Hamburg — mit den Volkszählungsdaten geplant (vgl. Jahresbericht 1987 des BlnDSB, S. 8). Zum anderen ist es durchaus möglich, durch einen bloßen Abgleich von Merkmalen aus der Volkszählung mit Merkmalen aus einem anderen Datenbestand (z.B. Meldedaten) einen Personenbezug bei einer nicht unbeträchtlichen Zahl der Datensätze herzustellen. Vor diesem Hintergrund ist es notwendig, die Volkszählungsdaten nicht nur in der Phase der maschinellen Erfassung und Vorverarbeitung, sondern auch bei ihrer dauerhaften Speicherung gegen einen unberechtigten Zugriff besonders zu schützen. Dies wird für die Datenschutzbeauftragten ein Grund sein, den Umgang mit Volkszählungsdaten auch längerfristig zu überwachen.

4.4.4 Einzelprobleme bei der Durchführung der Volkszählung

4.4.4.1 Zählerauswahl und -bestellung

Die ehrenamtlichen Zähler waren von der Erhebungsstelle auszuwählen und zu bestellen. Bund, Länder und Gemeinden waren verpflichtet, den Erhebungsstellen auf Anfor-

derung Bedienstete für die Zählertätigkeit zu benennen. Für die Durchführung der Volkszählung wurden allein in Hamburg Zähler für etwa 13.000 Zählbezirke benötigt.

Da eine groß angelegte Aktion zur Werbung freiwilliger Zähler zunächst nicht den gewünschten Erfolg brachte — es meldeten sich nur ca. 2.600 Personen —, wurde die zwangsweise Verpflichtung von Zählern eingeleitet. Auf die dabei aufgetretenen Probleme bin ich auch schon in meinem 5. TB ausführlich eingegangen (vgl. 5. TB, 5.3.1.4, S. 43).

(1) Benennungsverfahren

Nach § 10 Abs. 2 VZG 1987 war zur Übernahme der Zählertätigkeit jeder Deutsche vom vollendeten 18. bis zum vollendeten 65. Lebensjahr verpflichtet. Zu befreien war, wem eine solche Tätigkeit aus gesundheitlichen oder anderen wichtigen Gründen nicht zugemutet werden konnte (§ 10 Abs. 2 Satz 2 VZG 1987). Wie meine Umfrage vom Februar 1987 bei allen Behörden und Ämtern ergab, verfuhren die Behörden sehr unterschiedlich. Während einige Stellen überhaupt keine Bediensteten benannten, wurden von anderen nach nicht einheitlichen Kriterien jeder dritte oder zweite prinzipiell als Zähler in Frage kommende Beschäftigte ausgewählt. Die Ungleichbehandlung der Bediensteten verschiedener Behörden führte dazu, daß mehr Personen ihre Daten für das Zählerbestellungsverfahren offenbaren mußten, als es bei einem gleichförmigen Auswahlverfahren der Fall gewesen wäre. Darüber hinaus wurden mir mehrere Einzelfälle bekannt, in denen Mitarbeiter vor der Benennungsentscheidung von Fachvorgesetzten nach ihrer Einstellung zur Volkszählung befragt wurden.

§ 10 Abs. 5 VZG 1987 verbietet den Einsatz von Personen als Zähler, „wenn aufgrund ihrer beruflichen Tätigkeit oder aus anderen Gründen zu besorgen ist, daß Erkenntnisse aus der Zählertätigkeit zu Lasten der Auskunftspflichtigen genutzt werden". Deswegen wurden keine Bediensteten aus den Bereichen Polizei, Steuerverwaltung, Staatsanwaltschaft, Einwohnerzentralamt und Verfassungsschutz benannt. Darüber hinaus wurden Richter in Rechtsprechungsfunktionen von der Benennung von vornherein ausgenommen. Bedienstete der Bezirksverwaltungen durften nur in Zählbezirken außerhalb ihres örtlichen Zuständigkeitsbereichs eingesetzt werden.

Das Statistische Landesamt verzichtete aufgrund meiner Kritik auf die Benennung von Gerichtsvollziehern und von Mitarbeitern des Arbeitsamtes. Hinsichtlich der Rechtspfleger führten meine Bedenken zu einer Verfügung der Justizbehörde, daß alle inzwischen bereits zu Zählern bestellten Rechtspfleger bei Einlegung eines Widerspruchs wieder befreit wurden.

Entsprechend einem Musterschreiben des Statistischen Landesamtes hatten einige Behörden die zu benennenden Bediensteten in einem Benachrichtigungsschreiben aufgefordert, evtl. Einwände der (eigenen) Beschäftigungsbehörde (Personalabteilung) gegenüber mitzuteilen. Die Einwände offenbarten aber zum Teil sehr persönliche und sensible Informationen, z.B. über Krankheiten, psychische Belastbarkeit, besondere familiäre Inanspruchnahme, außerdienstliches Engagement. Nachdem ich in meinem 5. TB (5. TB, 5.3.1.4, S. 14) auf die Gefahr aufmerksam gemacht hatte, daß durch eine mißbräuchliche Verwendung der angegebenen Einwendungsgründe berufliche Nachteile für die Betroffenen entstehen könnten, erinnerte die Innenbehörde alle Behörden und Ämter daran, „daß bei den Beschäftigungsbehörden entstandene und noch entstehende Vorgänge über den Einsatz von Beschäftigten als ehrenamtliche Zähler nach § 10 des Volkszählungsgesetzes 1987 aufgrund von Abs. 2 Nr. 2 der Anordnung über die Führung und Verwaltung der Personalakten (MittVw 1971, S. 279) nicht zu den Personalakten gehören".

Im zweiten Durchgang des Benennungsverfahrens, der nicht zuletzt wegen des oben geschilderten uneinheitlichen ersten Benennungsverfahrens notwendig war, wurde in der von mir vorgeschlagenen Weise vorgegangen, Beschwerden hiergegen sind mir nicht bekannt geworden.

(2) Bestellungsverfahren

Die vom Statistischen Landesamt unter den Benannten ausgewählten Bediensteten erhielten den Bestellungsbescheid gegen Empfangsbekenntnis über ihre Beschäftigungsdienststelle (§ 5 Verwaltungszustellungsgesetz). Dies führte insbesondere dort zu Beschwerden, wo die Mitarbeiter der Personalstelle oder direkte Fachvorgesetzte die Bescheide aushändigten und damit von der Bestellung — und ggf. auch von der Annahmeverweigerung — erfuhren. Eine Zustellung durch die Poststelle der Behörde wäre das geeignetere Verfahren gewesen.

Durch eine Heraufsetzung der Aufwandsentschädigung für Zähler meldeten sich kurz vor Erhebungsbeginn noch eine Reihe von interessierten Freiwilligen, die nicht öffentlich Bedienstete waren. Um zu gewährleisten, daß diese Personen dem Zuverlässigkeitsgebot des § 10 Abs. 5 VZG 1987 genügen, entwickelte die Bfl einen Fragebogen zur Klärung der Zuverlässigkeit der Betroffenen. Bei der Abstimmung dieses Fragebogens war ich davon ausgegangen, daß nur volljährige Personen zu Zählern bestellt würden. Die Zählerwerbung richtete sich aber auch gezielt an Minderjährige (so wurden entsprechende Angebote an Schulen verteilt). Die Erhebungsstelle bestellte auch sie ohne weiteres, wenn sie mindestens 16 Jahre alt waren und aufgrund ihres Ausbildungsstandes keinen Anlaß zu weiteren Nachfragen boten. Dabei wurde weder eine Einverständniserklärung der Sorgeberechtigten verlangt noch in der Regel ein persönliches Gespräch mit dem interessierten Minderjährigen geführt. Eingaben zeigten, daß minderjährige Zähler z.T. überfordert waren.

4.4.4.2 Durchführung der Erhebung in Einrichtungen und Anstalten

Das BVerfG ist in seinem Urteil zum VZG 1983 auf die besondere Sensibilität der Durchführung der Zählung in Einrichtungen eingegangen, deren Bewohner der Gefahr einer sozialen Abstempelung (etwa als Drogensüchtiger, Vorbestrafter, Geisteskranker, Asozialer) unterliegen (BVerfGE 65, 1. S. 48 f.). Dort muß schon vom Gesetzgeber bei Anordnung der Auskunftspflicht geprüft werden, ob das Ziel der Erhebung nicht auch durch eine anonymisierte Ermittlung erreicht werden kann. Zwar wurde — anders als bei der VZ 1983 geplant — auf die Erhebung des Merkmals „Anstaltsinsasse" verzichtet, durch die Anschrift werden die Bewohner bestimmter Anstalten jedoch ebenfalls eindeutig als Angehörige diskriminierter Gruppen ausgewiesen. Ich hatte aus diesem Grund einen Verzicht auf eine namentliche Erhebung in einer Reihe von Einrichtungen gefordert, die ich dem Statistischen Landesamt benannt habe.

Das Statistische Landesamt ist dem nur zum Teil gefolgt: lediglich in Behinderteneinrichtungen sowie Einrichtungen für psychisch Kranke und Drogenabhängige wurde darauf verzichtet, namentliche Adressenlisten durch die Zähler ausfüllen zu lassen. Auf den VZ-Briefumschlägen war nur der Name der Einrichtung für die Zuordnung beim Rücklauf, nicht jedoch der Name des Auskunftspflichtigen einzutragen. Auch auf das Ausfüllen von Haushaltsmantelbögen wurde hier verzichtet.

Da die Planungen erst sehr spät ansetzten, war es der Erhebungsstelle nicht mehr möglich zu verhindern, daß die in den entsprechenden Einrichtungen lebenden Personen auch in die Begehungslisten aufgenommen wurden. Die Zähler erhielten also eine komplette namentliche Aufstellung der Heiminsassen, bei denen auf eine namentliche Erhebung verzichtet werden sollte. Um so wichtiger wäre es unter diesen Umständen gewesen, den Zählern die klare Anweisung zu geben, daß eine namentliche Erhebung hier auf jeden Fall unterbleiben mußte. Die Zähleranleitung des Statistischen Landesamtes genügte diesem Anspruch leider nicht. Den Zählern wurde lediglich mitgeteilt, sie möchten — falls sie auf eine solche Einrichtung treffen — der Zählungsdienststelle deren Namen und Anschrift mitteilen. Die Erhebung sollte dann durch die Zählungsdienststelle durchgeführt werden. Eine stichprobenartige Überprüfung im Statistischen Landesamt ergab, daß einzelne Zähler die Bewohner derartiger Einrichtungen doch namentlich auf der Begehungsliste markiert hatten. In einigen Fällen wurden die Namen sogar mit dem Hinweis, daß es sich um Behinderte handele, in die Adressenliste übertragen. Zumindest in diesen Fällen handelte es sich um einen eindeutigen

Verstoß gegen die Anonymität der Erhebung, der durch klarere Anweisungen und bessere Zählerschulung zu verhindern gewesen wäre.

Prüfungen in den Alsterdorfer Anstalten und in der JVA Fuhlsbüttel gaben keinen Anlaß zur Kritik. Hier waren die Verantwortlichen verhältnismäßig frühzeitig an mich herangetreten und hatten unter meiner Mitwirkung Konzepte entwickelt, die eine einwandfreie anonymisierte Zählung sicherstellten.

Hingegen war die Durchführung der Zählung in Wohnunterkünften für Asylbewerber und für Obdachlose, deren Bewohner ebenfalls der Gefahr einer sozialen Abstempelung unterliegen, datenschutzrechtlich bedenklich. Ich hatte vorgeschlagen, auf eine namentliche Erhebung auch in diesen Einrichtungen zu verzichten, weil die Bewohner Gefahr laufen, als besonders Bedürftige, Asoziale oder „Scheinasylanten" diskriminiert zu werden. Dem war die Erhebungsstelle nicht gefolgt. Sie führte aus, entscheidend wäre nicht die Frage, welches Sozialprestige eine bestimmte Bevölkerungsgruppe aus der Sicht eines „Durchschnittsbeobachters" habe. Vielmehr komme es darauf an, ob durch die namentliche Erfassung der Erhebungsstelle Tatsachen offenbart werden müßten, die der Öffentlichkeit oder anderen Verwaltungsbehörden nicht bekannt seien. Dies könne für die genannten Einrichtungen nicht bejaht werden. Die Bewohner dieser Einrichtungen seien mit ihrer „abgestempelten" Anschrift oder mit ihrem Status bei anderen Behörden (z.B. Sozialdienststellen, Ausländerbehörde) bekannt. Eine soziale Abstempelung durch die namentliche Erfassung erfolge danach nicht.

Diese Argumentation hat mich nicht überzeugt. Sie läuft darauf hinaus, daß eine namentliche Erfassung dort zulässig war, wo die Bewohner — etwa dadurch, daß sie sich an Sozialdienststellen wenden müssen — bereits abgestempelt sind. Dies widerspricht aber den mit dem „Volkszählungsurteil" verfolgten Zielsetzungen. Im übrigen hatte sich durch eine solche Argumentation auch eine namentliche Erfassung psychisch Kranker rechtfertigen lassen, da auch sie anderen Stellen, etwa dem sozialpsychiatrischen Dienst der Bezirksämter oder den Krankenkassen, als Insassen entsprechender Einrichtungen bekannt sind.

4.4.4.3 Datenübermittlungen von der und an die Meldebehörde

(1) Datenübermittlung für die Durchführung der Gebäudevorerhebung und Arbeitsstättenzählung

Für die Vorbereitung der Gebäudevorerhebung (GVE) ließ sich das Statistische Landesamt Daten aus dem Liegenschaftskataster der Baubehörde übermitteln, obwohl das Liegenschaftskataster nicht zu den von § 11 Abs. 2 VZG 1987 zugelassenen Übermittlungsquellen gehört. Von der Feuerkasse Hamburg wurden mehr Daten übermittelt, als nach § 11 Abs. 2 VZG 1987 zulässig war. Auch die in das Verfahren Gebäudevorerhebung eingeflossenen Einwohnerdaten waren z.T. nicht in dem Merkmalskatalog des § 11 VZG 1987 enthalten. Für die Vorbereitung der Arbeitsstättenzählung (AZ) beschränkte sich das Statistische Landesamt nicht auf die in § 11 Abs. 3 VZG 1987 genannten Quellen (die für die Entgegennahme von Gewerbeanzeigen zuständigen Stellen) und Daten, sondern griff auch auf nicht öffentlich zugängliche Daten der Handwerkskammer zurück. Diese wurden jedoch auf meine Beanstandung hin nicht für die Durchführung der Zählung verwendet.

Der Senat rechtfertigte das Verhalten der beteiligten Behörden damit, daß es zweifelhaft sei, ob § 11 VZG 1987 einen abschließenden Regelungscharakter habe. Der Senat hielt dieRechtsauffassung für vertretbar, daß sich der Zweck des § 11 darauf beschränke, bereits vorhandene Möglichkeiten der Datenübermittlungen in Zweifelsfällen noch einmal klarzustellenbzw. zu erweitern. Im übrigen habe es sich nur um einen formalen Verstoß gehandelt, da nur die in § 11 vorgesehene Daten weiterverarbeitet worden seien. Die vom Senat vertretene Ansicht halte ich — übrigens in Übereinstimmung mit dem Bundesinnenministerium — nicht für richtig. Datenübermittlungen an die Erhebungsstelle sind ebenso wie in umgekehrter Richtung Übermittlungen von Volkszählungsdaten durch das Statistische Landesamt an

andere Stellen im VZG 1987 abschließend geregelt. Mit dem Volkszählungsgesetz hat der Gesetzgeber eine Rechtsgrundlage schaffen wollen, die den vom Bundesverfassungsgericht formulierten Grundsätzen entspricht. Dürften über die im VZG 1987 genannten Stellen hinaus auch beliebige andere Stellen als Datenlieferanten für die Organisation der Zählung herangezogen werden und dürften zusätzliche, nicht im Gesetz aufgeführte Merkmale übermittelt werden, wäre die nach dem Grundgesetz erforderliche Rechtsklarheit nicht hergestellt und die die Volkszählung durchführenden Stellen könnten selbst festlegen, welche Daten sie von wem anfordern und verarbeiten dürften.

Die Erhebungsstelle hat meiner Rechtsauffassung nunmehr insofern Rechnung getragen, als bei der Rücklaufkontrolle der Arbeitsstättenzählung nur Daten Verwendung finden, die entgegen der ursprünglichen Planung öffentlich zugänglichen Quellen entstammt, bzw. von der Handwerkskammer nach Einwilligung der Betroffenen übermittelt wurde.

(2) Rückfragen der Erhebungsstelle beim Einwohnerzentralamt

Einer der wichtigsten Punkte, die zur Verfassungswidrigkeit des Volkszählungsgesetzes 1983 beigetragen hatten, war der seinerzeit geplante „Melderegisterabgleich". Damals sollten die bei der VZ gewonnenen Erkenntnisse auch dazu benutzt werden, das Melderegister zu aktualisieren. Dies hat das Bundesverfassungsgericht untersagt (BVerfGE 65, 1. S. 2 und S. 63ff.). Einen Schwerpunkt meiner Kontrolltätigkeit bildet deshalb auch die Prüfung, ob ein derartiger Abgleich unterbleibt. Ich habe dabei festgestellt, daß ein systematischer Abgleich zwar nicht stattgefunden hat, aber bei der Vollzähligkeitskontrolle der postalisch durchgeführten Gebäudevorerhebung Rückfragen beim Einwohnerzentralamt erfolgten, wenn Unklarheiten über die Anschrift der Auskunftspflichtigen bestanden. Derartige Rückfragen stellten aber unzulässige Übermittlungen der Erhebungsstelle an die Meldebehörde dar, da damit indirekt signalisiert wurde, daß mit der Anschrift der Betroffenen irgendetwas nicht stimmt. Dadurch hätte sich die Meldebehörde veranlaßt sehen können, den Sachverhalt durch eigene Ermittlungen aufzuklären, was auf eine durch die Volkszählung angestoßene Aktualisierung des Melderegisters hinausgelaufen und somit unzulässig gewesen wäre.

Weil in Tausenden von Fällen, in denen Rückfragen erforderlich waren oder keine Erhebungsunterlagen vorlagen, die aktuelle Anschrift mit der im Melderegister zum Erhebungsstichtag gespeicherten Adresse nicht übereinstimmte, hielt ich es für eine zulässige Alternative, wenn die Meldebehörde an die Erhebungsstelle Volkszählung einmalig die neuen Anschriften derjenigen in Hamburg gemeldeten Personen übermittelte, die seit dem Erhebungsstichtag umgezogen waren. Dadurch hätte eine mit der individuellen Melderegisteranfrage verbundene indirekte Datenübermittlung an die Meldebehörde entfallen können. Einem derartigen Verfahren hatte die Behörde für Inneres im Prinzip auch zugestimmt.

Nach meinen Feststellungen hat das Einwohnerzentralamt jeweils monatlich einen kompletten Datenbestand der Umzugsfälle an die Erhebungsstelle übermittelt. Dieser enthält die bisherige Anschrift, die neue Anschrift sowie das Geburtsdatum. Auf die Übermittlung der übrigen in § 11 VZG enthaltenen Merkmale hat die Bfl aufgrund meiner Intervention verzichtet. Dennoch ist dieses Verfahren bedenklich, weil weitaus mehr Daten übermittelt werden, als für den eigentlichen Zweck erforderlich ist; denn auch die Umzugsmeldungen derjenigen Hamburger Bürger sind übermittelt worden, die bereits geantwortet haben.

(3) Übermittlung von gesperrten Daten durch die Meldebehörde

Das Einwohnerzentralamt hatte der Erhebungsstelle Daten, die mit einem Sperrvermerk versehen sind, ohne den Hinweis weitergegeben, daß die Übermittlungssperre bestand. Ich hatte mich mit etlichen Beschwerden von Adoptiv- (Pflege-)eltern zu befassen, die sich dagegen richteten, daß der Geburtsname ihres Kindes in der Namensliste des Volkszählers aufgeführt war und diese Liste vom Zähler im

Haus offen herumgezeigt wurde mit der Frage, welcher Familie dieser Name zuzuordnen wäre. Durch diese Frage wurde Nachbarn die Tatsache der bevorstehenden, in einigen Fällen inzwischen schon rechtskräftigen Adoption bekannt.

Die Übermittlung geschützter Daten ohne Sperrvermerk wurde vom Einwohner-Zentralamt und vom Statistischen Landesamt damit begründet, daß zwar die Übermittlung aller Daten (also auch derjenigen, die mit einem Sperrvermerk versehen waren), durch § 11 Abs. 1 VZG angeordnet war, die Übermittlung des Datums „Übermittlungssperre" aber nicht möglich gewesen sei, weil es sich um ein nach der Struktur der Meldegesetze eigenständiges Datum handele, das in § 11 VZG 1987 nicht genannt sei.

Dieser Rechtsauffassung des Einwohner-Zentralamtes und des Statistischen Landesamtes habe ich widersprochen. Gem. § 1748 BGB dürfen Tatsachen, die dazu geeignet sind, die Adoption zu offenbaren, nicht bekannt gemacht werden.

Diesen Grundsatz schränkt § 31 Hamburgisches Meldegesetz (HmbMG) ein. Danach darf die Meldebehörde Daten auch von Personen, für die eine Übermittlungssperre eingetragen ist (dies ist bei allen in Adoptivpflege befindlichen Kindern der Fall) an andere Behörden und sonstige Stellen übermitteln, wenn dies zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit oder der Zuständigkeit des Empfängers liegenden Aufgaben erforderlich ist.

Die Übermittlung ist allerdings dann verboten, wenn sie schutzwürdige Belange der Betroffenen beeinträchtigen würde (§ 6 HmbMG). Ob dies der Fall ist, ist für jeden Einzelfall zu prüfen. Selbst wenn man sich auf den Standpunkt stellen will, daß eine Beeinträchtigung schutzwürdiger Belange durch die Übermittlung ausgeschlossen werden kann, hat die Meldebehörde nach § 6 HmbMG dem Übermittlungsempfänger zumindest mitzuteilen, daß für die übermittelten Daten eine Übermittlungssperre besteht, damit dieser bei der weiteren Verarbeitung den besonderen Schutz der Daten beachten kann (vgl. Medert, Süßmuth, Schweinoch, Weigert, Erl. z. MRRG, § 18 Rdnr. 20, § 21 Rdnr. 59). Die Prüfung, ob schutzwürdige Belange Betroffener beeinträchtigt werden, entfällt nur dann, wenn die Übermittlung durch Rechtsvorschrift vorgeschrieben ist (§ 6 Satz 3 HmbMG).

Es ist nicht ersichtlich, daß der Gesetzgeber mit § 11 VZG 1987 den durch § 1758 BGB und die Meldegesetze gewährleisteten Schutz der in Adoptivpflege befindlichen Kinder und ihrer künftigen Eltern für die Volkszählung aufheben wollte. Eine solche Absicht des Gesetzgebers hätte auch dem im Volkszählungsurteil des Bundesverfassungsgerichts niedergelegten Grundsatz widersprochen, daß Eingriffe des Staates in das informationelle Selbstbestimmungsrecht des Einzelnen nur dann zulässig sind, wenn das Interessse des Staates das Interesse des Einzelnen an der Geheimhaltung seiner Daten erheblich überwiegt.

In Hamburg befanden sich zum Zeitpunkt der Übermittlung der in Frage stehenden Daten ca. 250 Kinder in Adoptivpflege. Ein Verzicht auf die Übermittlung an die Erhebungsstelle hätte das statistische Gesamtergebnis der Volkszählung nicht beeinträchtigt, so daß das Interesse des Staates an einer möglichst lückenlosen Erhebung hinter dem Recht der Betroffenen auf informationelle Selbstbestimmung hätte zurückstehen müssen. Selbst wenn man der Meinung des Statistischen Landesamtes folgen wollte, daß auf die Übermittlung dieser Daten nach dem Wortlaut des Volkszählungsgesetzes nicht verzichtet werden durfte, konnte jedenfalls eine Übermittlung ohne Sperrvermerk bei sinnvoller Auslegung des Gesetzes aus folgenden Gründen nicht in Betracht kommen:

Nach dem Volkszählungsurteil des Bundesverfassungsgerichts sind bei jeder gesetzlich vorgeschriebenen Beeinträchtigung des informationellen Selbstbestimmungsrechts die organisatorischen und verfahrensrechtlichen Vorkehrungen zu treffen, welche der Gefahr einer unrechtmäßigen Persönlichkeitsverletzung entgegenwirken (BVerfGE 65, S. 1 Leitsatz). Das bedeutet, daß bei mehreren möglichen Wegen der Aufgabenerfüllung die Verwaltung den Weg zu wählen hat, der am

sichersten gewährleistet, daß Persönlichkeitsrechtsverletzungen ausgeschlossen sind. Die Übernahme der Geburtsnamen potentieller Adoptivkinder in die Zählerlisten hat die Geheimhaltung dieser Daten von dem korrekten Verhalten vieler, nur kurz in ihre Aufgabe eingewiesener und kaum überprüfbarer Personen abhängig gemacht.

4.4.4.4 Beschwerden über den Zählereinsatz und das Zählerverhalten

Naturgemäß haben sich die Bürgerbeschwerden auf diejenigen Personen, die als Zähler die Erhebung vor Ort durchzuführen hatten, konzentriert:

(1) Zähler verweigerten die Herausgabe von Volkszählungsbriefumschlägen und setzen damit die Bürger indirekt unter Druck, ihnen die ausgefüllten Fragebögen persönlich zu übergeben. Die dem Bürger durch § 13 Abs. 4 VZG 1987 eingeräumte Wahlmöglichkeit zwischen Übergabe der Fragebögen an die Zähler oder postalischer Rücksendung an die Erhebungsstelle wurde durch dieses Zählerverhalten unterlaufen. Hierzu beigetragen hat sicher die nicht immer ausreichende Ausstattung der Zähler mit VZ-Briefumschlägen. Es mag auch eine Rolle gespielt haben, daß die Zähler für selbst eingesammelte ausgefüllte Fragebögen eine höhere Vergütung bekamen als für Fragebögen mit postalischer Rücksendung.

(2) In einigen Fällen hatten Bürger festgestellt, daß nicht der amtliche Zähler, sondern einer seiner Familienangehörigen vor ihnen stand. Dies könnte darauf zurückzuführen sein, daß das Statistische Landesamt zum Teil sehr große mehrere Zählbezirke umfassende Zählgebiete vergeben hat. Da derartig große Erhebungsgebiete von einem einzelnen Zähler kaum zu bewältigen waren, hatten sich offenbar manche Zähler veranlaßt gesehen, Familienangehörige um Hilfe zu bitten. Dies war natürlich nicht zulässig.

(3) Zähler traten zusammen mit „Begleitpersonen" auf, die nicht selbst Zähler waren und somit auch nicht auf das Statistikgeheimnis verpflichtet waren.

(4) In verschiedenen Fällen hatten versehentlich Zähler bereits von anderen Auskunftspflichtigen ausgefüllte Erhebungsunterlagen anstelle leerer Formulare verteilt, so daß die Daten derjenigen Bürger, die ihre Angaben schon abgegeben hatten, Dritten bekannt wurden.

(5) Häufig versuchten Zähler, Informationen über Auskunftspflichtige bei anderen Hausbewohnern zu erlangen, wenn sie die Betroffenen selbst nicht antrafen. In einigen Fällen hatten Zähler die so erlangten Angaben in die Erhebungsunterlagen eingetragen, ohne daß der Auskunftspflichtige selbst befragt wurde. Besonders gravierend waren einige Fälle, in denen Zähler sich bei Hauseigentümern nach den Wohnverhältnissen von Mietern erkundigten, weil diese den Wohnungsbogen nur unvollständig ausgefüllt hatten. Dadurch hat z.B. ein Hauseigentümer von einem ihm bislang unbekannten Untermietverhältnis erfahren und Maßnahmen gegen die betroffenen Mieter eingeleitet.

(6) Für die Begehung ihres Zählbezirkes wurden den Zählern vom Statistischen Landesamt sog. „Namenslisten" ausgehändigt, die die im Melderegister gespeicherten Namen und Anschriften der Auskunftspflichtigen enthielten. In vielen Fällen hatten Zähler diese Listen offen herumgezeigt und auch gezielt nach nicht gefundenen, aber auf der Liste vermerkten Personen gefragt. Dadurch wurden Dritten unzulässigerweise personenbezogene Daten bekannt, was im Einzelfall, z.B. bei den oben geschilderten Adoptionsfällen, zu einer schwerwiegenden Beeinträchtigung schutzwürdiger Belange von Betroffenen geführt hat (vgl. 4.4.5.6 (3)).

(7) Einige Beschwerden richteten sich dagegen, daß Zähler — entgegen den Bestimmungen von § 10 Abs. 6 VZG 1987 — ohne Erlaubnis der Wohnungsinhaber in Wohnungen eingedrungen wären.

(8) Mir ist bekanntgeworden, daß einige Zähler die Koffer mit den Erhebungsunterlagen nicht oder nicht vollständig bei der Erhebungsstelle abgegeben haben. Es

handelt sich dabei um insgesamt neun Fälle, bei denen bis Jahresende 1987 nicht geklärt ist, wo die Koffer mit den ausgefüllten Erhebungsunterlagen geblieben sind. Ich bin der Auffassung, daß die betroffenen Auskunftspflichtigen mit Aushändigung der Erhebungsunterlagen an den Zähler als dem Beauftragten der Erhebungsstelle ihren Pflichten genügt haben und nicht noch einmal zur Auskunftserteilung herangezogen werden dürfen, wie dies z.T. geschehen ist.

Die geschilderten Sachverhalte — es handelt sich dabei nur um einen kleinen Ausschnitt — lassen mich annehmen, daß die Erhebungsstelle ihrer Verpflichtung zur sorgfältigen Zählerauswahl (§ 10 Abs. 5 VZG 1987) nicht in ausreichendem Maße nachgekommen ist. In den Fällen, in denen ich das Statistische Landesamt auf ein fehlerhaftes Zählerverhalten hingewiesen habe, ist die Erhebungsstelle den Beschwerden zwar nachgegangen, was bei direkten Beschwerden der Bürger beim Statistischen Landesamt selten vorkam; Sanktionen gegen die Zähler sind jedoch in diesen Fällen — obwohl es sich z.T. um schwerwiegende Verstöße gehandelt hat — m.W. unterblieben. Dies geschah in den meisten Fällen mit der Begründung, die betreffenden Zähler hätten ihre Tätigkeit bereits abgeschlossen.

4.4.4.5 Erinnerungs- und Mahnverfahren

Ich bin schon in meinem 5. TB ausführlich auf den ADV-Einsatz in der Erhebungsstelle eingegangen (vgl. 5. TB,5.3.1.2, S. 40). Das Statistische Landesamt Hamburg wickelt die Vollständigkeitskontrolle der Erhebungsbögen, die „Ersatzvornahme" nach § 11 Abs. 1 VZG 1987 und die Vorbereitung von Zwangsmaßnahmen gegen diejenigen, die ihrer Auskunftspflicht nicht nachkommen, über ein On-line-Verfahren ab. Dabei sind in der Erhebungsstelle aufgestellte Terminals mit der Datenverarbeitungszentrale der Hamburger Verwaltung (DVZ) verbunden. Das eingesetzte System ist so konzipiert, daß neben diesen standardmäßigen Sicherungen zusätzliche Maßnahmen ergriffen werden, die einen unzulässigen Zugriff auf die gespeicherten Daten erschweren:

— Zugriff auf die Dateien nur über die in der Erhebungsstelle aufgestellten Terminals,

— differenzierte Benutzerprofile (jeder Benutzer kann nur diejenigen Aktionen ausführen, die in seiner Zuständigkeit liegen),

— lückenlose Protokollierung der Systemaktivitäten (einschließlich aller schreibenden oder ändernden Zugriffe auf Daten).

Das Verfahren wurde nach einem Abnahmetest von der fachlich zuständigen Stelle freigegeben. Meine diesbezüglichen Forderungen wurden hier also berücksichtigt (vgl. Abschnitt 4.4.3.2).

Eine Prüfung vor Ort hat ergeben, daß die gem. § 11 Abs. 1 von der Meldebehörde übermittelten Daten und Bearbeitungsmerkmale gespeichert werden.

Diese Bearbeitungsmerkmale sind weder Erhebungs- noch Hilfsmerkmale. Es handelt sich dabei um Markierungen für diejenigen, die erklärt haben, die Zählungsunterlagen per Post zurückzusenden (Merkmal „P") und diejenigen, die entweder nicht angetroffen wurden oder aus sonstigen Gründen keine Erhebungsbögen erhalten haben (Merkmal „R"). Nach Eingang der ausgefüllten Fragebögen werden die Bearbeitungsmerkmale („Marker") gelöscht. Die Eingabe anderer als der beschriebenen Merkmale ist nicht möglich. Die Datensätze selbst (mit den in § 11 Abs. 1 genannten Merkmalen) bleiben jedoch gespeichert.

Zur Löschung dieser Daten gibt es mittlerweile eine Verfügung der Erhebungsstelle Volkszählung, die eine zählbezirksweise Löschung der Daten erst dann vorsieht, wenn geprüft ist, daß für sämtliche Einwohner eines Zählbezirks entweder

— die ordnungsgemäß ausgefüllten Erhebungsunterlagen vorliegen oder

— unter der angegebenen Adresse keine Auskunftspflicht besteht oder

— die „Ersatzvornahme" gemäß § 11 Absatz 1 VZG 1987 erfolgt ist.

Die Bindung der Löschung daran, daß alle Bewohner eines Zählbezirks entweder ihre Fragebögen ordnungsgemäß ausgefüllt haben bzw. daß geprüft wurde, ob unter der angegebenen Adresse keine Auskunftspflicht besteht oder die Ersatzvornahme erfolgt ist, hat zur Folge, daß die Daten derjenigen Bürger, von denen ausgefüllte Erhebungsunterlagen vorliegen, bis weit in das Jahr 1988 hinein in der Datenbank gespeichert bleiben, ohne daß dies fachlich erforderlich oder technisch unumgänglich wäre. Die weitere Speicherung würde damit rechtswidrig, weil die rechtlichen Voraussetzungen hierfür (Erforderlichkeit für die rechtmäßige Aufgabenwahrnehmung) nicht mehr vorliegen.

Die Verfügung entspricht im übrigen nicht den früheren Zusagen der Behörde für Inneres, wonach eine sukzessive Reduzierung der Datei entsprechend dem Rücklauf der Erhebungsunterlagen erfolgen sollte. Nur unter dieser Voraussetzung hatte ich überhaupt der automatisierten Erfassung von Hilfsmerkmalen zugestimmt, obwohl eine bereichsspezifische Rechtsgrundlage fehlt. Deshalb habe ich die Verfügung beanstandet. Ich habe den Senat darauf hingewiesen, daß Verzögerungen bei der Durchführung der VZ nicht dazu führen dürfen, daß die in dem automatisierten Erinnerungs- und Mahnverfahren erfaßten Identifikationsangaben länger als unbedingt notwendig gespeichert bleiben. Die Löschung muß zum frühest möglichen Zeitpunkt erfolgen.

Diese Beanstandung hat der Senat zurückgewiesen. Er hat ausgeführt, die Löschung der Daten erfolge insofern sukzessiv, als sie unmittelbar nach Abschluß der Prüfungen, ob für alle Auskunftspflichtigen Fragebogen vorliegen (Vollzähligkeitskontrolle) und ob die Fragebogen vollständig ausgefüllt sind (Vollständigkeitskontrolle), für jeden Zählbezirk vorgenommen werde. Diese Prüfungen fänden in zwei Arbeitsgängen statt: Zunächst werde für alle im Zählbezirk Auskunftspflichtigen die Vollzähligkeitskontrolle durchgeführt und sodann in einem zweiten Durchgang die Vollständigkeitskontrolle.

Meine Bedenken sind damit nicht ausgeräumt. Sie richten sich vor allem dagegen, daß die Löschung bis zum Abschluß der Vollständigkeitskontrolle hinausgezögert wird. Es ist überhaupt nicht ersichtlich, wie die für das Erinnerungs- und Mahnverfahren gespeicherten Daten bei der Vollständigkeitskontrolle verwendet werden sollen:

— Die Beschränkung der „Marker", d.h. der gespeicherten Bearbeitungsmerkmale auf die Merkmale „P" (Postrücksender) und „R" (die Auskunftspflichtigen, denen noch keine Unterlagen zugestellt werden konnten) lassen einen Einsatz des automatisierten Verfahrens bei unvollständiger Auskunftserteilung nicht zu.

— Eine automatisierte Ersatzvornahme ist nach Auskünften der Bfl nicht vorgesehen. Sie ist bei lediglich unvollständigen Angaben, d. h. wenn zwar Erhebungsunterlagen vorliegen, diese aber nicht gänzlich ausgefüllt sind, auch gar nicht sinnvoll.

Gem. § 15 Abs.3 HmbDSG sind Daten zu löschen, wenn ihre Kenntnis für die speichernde Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist. Ich sehe in dem vorgesehenen und vom Senat bestätigten Löschungsverfahren einen Verstoß gegen diese Vorschrift.

4.4.4.6 Wiederholungsbefragung

Gem. § 1 Abs. 4 VZG 1987 sind Wiederholungsbefragungen zur Prüfung der Zuverlässigkeit der Ergebnisse der Volkszählung mit einem Auswahlsatz bis zu 0,2 v.H. der Befragten zulässig. Dabei dürfen die Erhebungsmerkmale nach § 5 Nr. 1, 3 und 5 bei den Betroffenen erfragt werden. Es handelt sich dabei um die Merkmale

— Gemeinde,

— Nutzung der Wohnung als alleinige Wohnung,

— Wohnung als Ausgangspunkt des Arbeits-, bzw. Ausbildungsweges,

— Zahl der Personen im Haushalt,

— Gesamtzahl der Personen und Haushalte in Gemeinschafts- und Anstaltsunterkünften,

— Wohnungs- und Haushaltszugehörigkeit,

— Geschlecht,

— Geburtsjahr,

— Geburtstag im Zeitraum 1. 1. bis 24. 5. oder 25. 5. bis 31. 12.,

— Familienstand,

— Staatsangehörigkeit,

— Beteiligung am Erwerbsleben.

Ich hatte im Juli 1987 der Behörde für Inneres mitgeteilt, daß es sich nach meiner Rechtsauffassung bei den in § 1 Abs.4 VZG 1987 genannten Merkmalen um eine abschließende Aufzählung handelt und weitere Daten nicht erhoben werden dürften.

Ich hatte weiter ausgeführt, daß sich eine Zusammenführung der individuellen Erhebungsunterlagen aus der Haupt- und aus der Wiederholungsbefragung verbiete, da sich der Zweck der Befragung auf die Prüfung der Zuverlässigkeit der Ergebnisse zu beschränken habe und die Hilfsmerkmale gem. § 8 VZG 1987 nicht in dem abschließenden Katalog des § 1 Abs. 4 VZG 1987 enthalten sind.

Ohne auf meine Bedenken einzugehen oder sich überhaupt damit auseinanderzusetzen, hat mir die Bfl nach wiederholten Anmahnungen mit Schreiben vom 28. 10. 1987 eine Anzahl von — offensichtlich zum großen Teil durch das Statistische Bundesamt gefertigten — Unterlagen übersandt, aus denen jedoch nicht hervorgeht, wie die Befragung in Hamburg abgewickelt wird.

Aufgrund telefonischer Auskünfte gehe ich davon aus, daß die Befragung auch in Hamburg so abgewickelt werden soll, wie sich aus einem mir vom Bundesbeauftragten für den Datenschutz übersandten Vermerk aus dem Bundesinnenministerium ergibt.

Ich möchte an dieser Stelle ausdrücklich feststellen, daß die Wiederholungsbefragung nicht mit mir abgestimmt wurde und ich an meinen Bedenken festhalte.

Folgende Punkte halte ich für bedenklich:

— Die Zusammenführung der Einzeldatensätze bei der Erhebungen (Haupt- und Wiederholungsbefragung) ist nicht durch das VZG 1987 gedeckt. Hätte der Gesetzgeber ein solches Verfahren im Auge gehabt, so hätte er dies sicherlich auch im Gesetzestext deutlich gemacht. Das ist jedoch nicht geschehen. Da die Hilfsmerkmale gem. § 8 VZG 1987 nicht zum Erhebungsprogramm der Wiederholungsbefragung gehören, dürfen sie auch nicht erfragt werden.

— Der durch Zusammenführung der Angaben aus der Haupt- und aus der Wiederholungsbefragung gewonnene Datensatz soll neben den in § 1 Abs. 4 VZG 1987 genannten Merkmalen zusätzlich auch die Angaben zu den Fragen 8, 9, 10 und 15 des Personenbogens der Haupterhebung enthalten. Auch dies ist nicht durch das VZG 1987 gedeckt und deshalb unzulässig.

— Auf dem Haushaltsmantelbogen für die Wiederholungsbefragung sind — für jedes Haushaltsmitglied getrennt — Angaben darüber zu machen, ob der Betreffende in dieser Wohnung am 25. 5. 1987
  — gewohnt und auch jetzt noch wohnend,
  — gewohnt, jetzt aber nicht mehr wohnend,
  — nicht gewohnt aber jetzt wohnend ist.

  Es handelt sich dabei um ein zusätzliches Merkmal, das weder in dem abschließenden Katalog des § 5 VZG 1987 (Erhebungsmerkmale) noch des § 8 Abs. 1 VZG 1987 (Hilfsmerkmale) genannt ist. Es darf also nicht erhoben werden.

Ich habe aus den genannten Gründen die Behörde für Inneres aufgefordert, auf die Erhebung der Hilfsmerkmale bei der Wiederholungsbefragung und auf eine Zusam-

menführung von Einzelangaben aus der Haupt- und Wiederholungsbefragung zu verzichten. Bereits ausgefüllte Haushaltsmantelbögen, Adressen und Regionallisten müssen vernichtet werden.

4.5 Archivwesen

In meinem letzten Tätigkeitsbericht (Ziff. 5.4) wies ich auf die Notwendigkeit hin, die Nutzung von Archivalien des Staatsarchivs auf eine landesgesetzliche Rechtsgrundlage zu stellen, die das Grundrecht auf freie Forschung und Wissenschaft mit dem Grundrecht auf informationelle Selbstbestimmung lebender Personen in Einklang bringt.

Das Staatsarchiv hat inzwischen einen ersten Referentenentwurf erarbeitet und beabsichtigt, ihn Anfang 1988 mit den anderen Behörden abzustimmen und dann der Bürgerschaft als Gesetzesinitiative des Senats vorzulegen. Eine Durchsicht des Entwurfs und ein Vergleich mit dem Gesetzesvorhaben des Bundes und des schon verabschiedeten Archivgesetzes von Baden-Württemberg zeigen, auf welche Fragen der Hamburger Gesetzgeber sein Augenmerk noch besonders zu richten hat:

— Müssen dem Staatsarchiv auch solche Unterlagen angeboten werden, die einem besonderen Geheimnisschutz unterliegen bzw. unterlagen (z.B. Steuerakten, Krankenhausakten)? Sollen hierbei besondere Maßnahmen zum Schutz personenbezogener Daten vorgeschrieben werden, etwa eine Anonymisierung vor Ablieferung?

  Das Spannungsverhältnis zwischen dem Forschungsinteresse an einem zu erhaltenden Personenbezug und dem Betroffeneninteresse an einer Geheimhaltung wird im Bundesgesetzentwurf sehr differenziert gelöst, im baden-württembergischen Archivgesetz allgemein durch das Gebot, vor Übergabe der Unterlagen „schutzwürdige Belange des Betroffenen durch geeignete Maßnahmen unter Abwägung aller Umstände des Einzelfalls angemessen" zu berücksichtigen. Der Hamburger Entwurf erstreckt die Anbietungspflicht bisher ganz allgemein auch auf „Unterlagen, die besonderen Geheimhaltungs-, Vernichtungs- und Löschungsvorschriften unterliegen".

— Welche Sperrfristen müssen vor der Nutzung personenbezogenen Archivguts eingehalten werden? Unter welchen Voraussetzungen können diese Fristen verkürzt werden? Als Regel bestimmen der Bundes- und der Hamburger Gesetzentwurf eine Frist von 30 Jahren nach dem Tod des Betroffenen bzw. 100 (Hamburg) 120 Jahre (Bund) nach der Geburt. Baden-Württemberg hält eine Regelfrist von 10 Jahren nach dem Tod bzw. 90 Jahren nach der Geburt für ausreichend. Für die Bedürfnisse zeitgeschichtlicher Forschung ist der Ausschluß einer Nutzung von Archivgut über noch lebende Personen unbefriedigend. Deswegen sehen die Archivgesetz(entwürf)e die Möglichkeit einer Verkürzung der Sperrfristen vor, wenn entweder der Betroffene einwilligt oder wenn die Nutzung zu wissenschaftlichen Zwecken oder zur Wahrnehmung berechtigter persönlicher Belange erfolgt (Bund) bzw. notwendig (Hamburg) oder unerläßlich (Baden-Württemberg) ist und die schutzwürdigen Belange des Betroffenen berücksichtigt werden. Als Mittel nennen Bund und Baden-Württemberg zunächst die Anonymisierung, der Hamburger Entwurf begnügt sich allgemein mit „geeigneten Maßnahmen". Die Vorlage des Hamburger Staatsarchivs sieht weiter vor, daß die Sperrfristen für personenbezogenes Archivgut nicht gelten sollen für „Archivgut, das sich auf die Tätigkeit von Personen bezieht, die in Ausübung öffentlicher Ämter gehandelt haben".

— Welche Rechte hat ein Betroffener, wenn er die Richtigkeit personenbezogenen Archivguts bestreitet? Der Bundesentwurf sieht in diesen Fällen die Anonymisierung der Angaben bzw. auf Verlangen des Archivs eine ergänzende Gegendarstellung des Betroffenen vor. Die Regelungen von Baden-Württemberg und Hamburg verlangen vom Betroffenen eine Glaubhaftmachung des Gegendarstellungsinteresses. Das Auskunftsrecht des Betroffenen aus dem Datenschutzgesetz — Voraussetzung eines Gegendarstellungsbegehrens — erstreckt sich nach allen drei Regelungen auch auf nicht in Dateien (sondern in Akten) gespeicherte Daten.

Da es sich bei dem Archivgesetz-Entwurf der Hamburger Senatskanzlei noch um ein sehr vorläufiges Papier handelt, dessen offizielle Abstimmung in den Behörden noch aussteht, begnüge ich mich an dieser Stelle mit dem Aufzeigen datenschutzrelevanter Regelungspunkte. Eine Bewertung einzelner Formulierungen des Entwurfs und ggf. Änderungsvorschläge behalte ich mir in dem dafür vorgesehenen Verfahren vor.

4.6 Gewerbewesen — Automation des Gewerberegisters

4.6.1 Rechtsgrundlagen und gegenwärtige Praxis

Wer ein Gewerbe beginnt, den Betrieb verlegt, auf andere Gegenstände ausdehnt oder aufgibt, muß dies nach §§ 14 bzw. 55 c Gewerbeordnung „der für den betreffenden Ort zuständigen Behörde" anzeigen. Die Form dieser Anzeige, insbesondere welche Angaben der Gewerbetreibende zu machen hat, schreibt die Gewerbeanzeigenverordnung im einzelnen vor.

In Hamburg nehmen gegenwärtig 22 Wirtschafts- und Ordnungs-Dienststellen (WI-Dienststellen) in den Bezirks- und Ortsämtern jeweils für ihren Bereich die Gewerbeanzeigen entgegen. Nach der Fachlichen Weisung WG Nr. 186 führen die WI-Dienststellen manuell eine Gewerbekartei, die — alphabetisch nach Gewerbetreibenden geordnet — zur Zeit insgesamt etwa 500.000 bis 600.000 Karteikarten umfaßt, oft mehrere für denselben Gewerbetreibenden. Allein die „laufende Kartei", die gegenwärtig ausgeübte Gewerbe betrifft, enthält ca. 174.000 Karteikarten. Jede Gewerbeanzeige wird vom Sachbearbeiter der WI-Dienststelle maschinenschriftlich in ein Formular mit 8 Durchschriften eingetragen. Diese werden entsprechend der Fachlichen Weisung an verschiedene Behörden, Kammern, Berufsgenossenschaften weitergeleitet. Die WI-Dienststellen geben schließlich auch Auskunft an Behörden und Privatpersonen über Name und Adresse des Gewerbetreibenden und über die Gewerbeart. Da es derzeit 22 voneinander unabhängige Gewerbekarteien gibt, erfordert die Beantwortung eines Auskunftsverlangens eine Abfrage bei vielen Stellen, wenn der Standard des Gewerbebetriebes dem Anfragenden nicht bekannt ist.

4.6.2 Konzept einer Automatisierung des Gewerberegisters

Nicht zuletzt, um diesen Aufwand zu verringern, hat sich das Senatsamt für Bezirksangelegenheiten in seinem IuK-Plan (Plan für Vorhaben der Informations- und Kommunikationstechnik) für 1987-1989 das Ziel gesetzt, die Gewerbekarteien zu automatisieren und behördenübergreifend zugriffsfähig zu machen. Seit Februar 1987 entwickelt eine Arbeitsgruppe, der Vertreter der Bezirksämter, der Wirtschaftsbehörde, der Senatsämter für Bezirksangelegenheiten und für den Verwaltungsdienst, der Personalräte sowie des Datenschutzbeauftragten angehören, ein Konzept. Angestrebt wird eine in der Datenverarbeitungszentrale geführte zentrale Datenbank, auf die die Sachbearbeiter der WI-Dienststellen über Bildschirmgeräte sowohl lesend als auch — im eigenen Zuständigkeitsbereich — ändernd direkten Zugriff haben (Dialogverfahren, online-Zugriff). Die automatisierte Gewerbedatei soll insbesondere

- — die Suche nach bestimmten Gewerbetreibenden über ganz Hamburg erleichtern,
- — die Sachbearbeitung durch Datenausdruck und Bearbeitungshinweise vereinfachen,
- — die Auskunftserteilung beschleunigen,
- — (statistische) Auswertungen als Hilfsmittel für Stadtplanung, Wirtschaftsordnung und Umweltplanung ermöglichen,
- — Anforderungen des Datenschutzes (Datensicherheit, Löschungsgebote) erfüllen.

4.6.3 Probleme des Datenschutzes

Schon das bisherige Verfahren genügt den vom Bundesverfassungsgericht aufgestellten Anforderungen an eine bereichsspezifische gesetzliche Grundlage nicht. Die

Gewerbeordnung legitimiert lediglich die von den traditionellen Datenschutzgesetzen ohnehin nicht erfaßte Erhebung von Daten. Die Speicherung in einer Gewerbekartei und erst recht die Übermittlung von Anzeigendurchschriften und Auskünften an andere Behörden und Privatpersonen sind jedoch gesetzlich nicht vorgesehen. Dem Drängen der Datenschutzbeauftragten, hier für eine eindeutige konkrete Gesetzesermächtigung zu sorgen, stellten die Wirtschaftsministerien bisher den Hinweis auf geplante Generalklauseln im Verwaltungsverfahrensgesetz entgegen.

In einem Gespräch mit der Behörde für Wirtschaft, Verkehr und Landwirtschaft habe ich deutlich gemacht, daß die Auffassung der Wirtschaftsministerien den Forderungen des Bundesverfassungsgerichts nicht genügt. Der vom Bundesverfassungsgericht eingeräumte Übergangsbonus kann eine fehlende Gesetzesgrundlage heute auch nicht mehr ersetzen: Nach Erlaß des Volkszählungsurteils wurde anläßlich einer anderen Änderung der Gewerbeordnung auch die Ergänzung um eine Datenübermittlungsklausel diskutiert (vgl. Bundestagsdrucksache 10/1646 vom 20. 6. 84), aber schließlich verworfen. Es sollte erst eine Auswertung des Volkszählungsurteils abgewartet werden.

Die Behörde kündigte daraufhin an, eine eigene Hamburger Gesetzesinitiative für das automatisierte Verfahren zu prüfen. Leider habe ich seit dem Gespräch nichts mehr davon gehört. Soweit es um die organisatorische Seite der Einrichtung einer Hamburger Gewerbedatei geht, hat das Land meines Erachtens auch insofern die Gesetzgebungskompetenz, als Übermittlungen aus dieser Datei betroffen sind. Da die Gewerbeordnung Datenübermittlungsbestimmungen nicht enthält, kann hier ein Bundesland seine (konkurrierende) Gesetzgebungskompetenz nach Art. 74 Ziff. 11 GG wahrnehmen. Da die Einrichtung einer zentralen Datenbank mit neuen dezentralen Zugriffs- und Auswertungsmöglichkeiten der Gewerbedatei eine ganz neue datenschutzrelevante Qualität verleiht, ist dies auch geboten: Die Verwendung von Daten, die für Zwecke der Gewerbeüberwachung erhoben wurden, auch für Zwecke der Stadt- und Umweltplanung etwa bedarf einer gesetzlichen Ermächtigung.

Bei der näheren Ausgestaltung der automatisierten Gewerbedatei stellen sich aber auch Datenschutzprobleme inhaltlicher Art. Ich habe sie in der Arbeitsgruppe bereits angesprochen, sie sind bislang noch nicht gelöst:

— Wie weit geht der online-Zugriff eines Sachbearbeiters auf Daten von Gewerbetreibenden, die nicht in seinem lokalen Zuständigkeitsbereich ihren Sitz haben? Sinnvoll erscheint, daß der Sachbearbeiter schnell feststellen kann, welcher Kollege z.B. für eine Auskunft über den Betrieb zuständig ist. Derzeit sehe ich keine Notwendigkeit für weitere Zugriffs-(Lese-)Möglichkeiten.

— Wer darf welche Auswertungen des gesamten Datenbankbestandes vornehmen? Hier wird möglicherweise die von der Gewerbeordnung eingeräumte „örtliche" (= gemeindliche) Zuständigkeit überschritten, die bislang ausschließlich den Bezirksämtern übertragen war. Eine Differenzierung in zentrale Auswertungen z.B. durch die Wirtschaftsbehörde und dezentrale Sachbearbeitung führt angesichts der Regelung in der Gewerbeordnung zu verfassungsrechtlichen Problemen. Datenschutzrechtlich bestehen gegen Auswertungen dann keine Bedenken, wenn der Personenbezug aufgegeben, d.h. die Daten der Gewerbedatei anonymisiert werden.

— Ist gewährleistet, daß bei Auskunftsverlangen die notwendige Abwägung zwischen Datenschutz und Informationsinteresse im Einzelfall auch wirklich vorgenommen wird? Allein der Druck auf die Taste „Ausdruck Anfrage" genügt nicht. Etwas ähnliches gilt auch für die Weitergabe der Gewerbeanzeige an andere Behörden in besonderen Fällen (z.B. Güterkraftverkehrsgewerbe-Anmeldung an die Wirtschaftsbehörde).

— Wie kann das EDV-Programm die Einhaltung der Prüfungs- und Löschungsgebote des § 15 HmbDSG gewährleisten bzw. erleichtern? Bei der bisherigen manuellen Handhabung der Gewerbedateien wurde diesen Geboten nicht entsprochen.

— Die notwendigen technischen und organisatorischen Maßnahmen zur Datensicherheit (vgl. § 8 HmbDSG) sind noch im einzelnen festzulegen.

— Der Arbeitnehmer- bzw. Personaldatenschutz fordert schließlich, daß die Sicherungs- und Dokumentationsmaßnahmen nicht zu einer Überwachung von Leistung und Verhalten der Sachbearbeiter führen. Auch hier ist ein vernünftiger Kompromiß zu finden. Den betroffenen Personalräten steht nach § 86 Abs. 1 Ziff. 4 HmbPersVG ein Mitbestimmungsrecht zu.

4.7 Einsichtsrecht in Umweltakten

Viele Menschen sind durch den besorgniserregenden Zustand unserer Umwelt und die daraus für den Menschen erwachsenden gesundheitlichen Gefahren alarmiert. Aus der Erfahrung heraus, daß staatliche Organe bisher wenig getan haben, um diese Entwicklung durch entschiedene Maßnahmen zu verändern, haben Bürger aus allen Bevölkerungskreisen begonnen, ihre Angelegenheiten in die eigenen Hände zu nehmen. Sie haben sich zu Bürgerinitiativen, Arbeitskreisen, Komitees zusammengeschlossen und gemeinsam oder als Einzelpersonen mit besonderem Engagement eine bemerkenswerte fachliche Kompetenz erworben. Damit hoffen sie, der mächtigen und einflußreichen Industrielobby ein qualifiziertes Gegengewicht entgegensetzen zu können. Sie wollen erreichen, daß das politische Handeln den vitalen Interessen der Menschen besser gerecht wird als bisher.

Dieses Anliegen der an Umweltfragen interessierten Bürger wird jedoch erheblich behindert durch allerlei Restriktionen, durch die die Beschaffung der nötigen Informationen erschwert wird. Viele der bekanntgewordenen Umweltskandale sind auch deshalb zu Skandalen geworden, weil die Unternehmen — häufig mit Unterstützung der zuständigen Behörden — die Öffentlichkeit und die direkt Betroffenen über Art, Umfang und Auswirkungen von Gefahren und eingetretenen Schäden im Ungewissen gelassen oder zu spät oder auch falsch informiert haben.

Vor diesem Hintergrund sind zwei Gesetzentwürfe zu betrachten, die die Stellung des Bürgers bei der Informationsbeschaffung stärken wollen. Die Freie und Hansestadt Hamburg brachte den Entwurf eines Gesetzes zum Auskunftsrecht über Umweltdaten (Umweltdatenauskunftsgesetz -UAG-, veröffentlicht als BR-Drs. 172/87 v. 24. 4. 87) in den Bundesrat ein. Die GRÜNE/GAL Fraktion in Hamburg legte einen Entwurf eines Gesetzes über das Einsichtsrecht in Umweltakten (Akteneinsichtsrechtsgesetz -AERG-, veröffentlicht als Bürgerschafts-Drs. 11/6958 v. 17. 9. 86) vor, der — abgesehen von solchen Passagen, die in einer bundesgesetzlichen Regelung im Gegensatz zu einer landesgesetzlichen Regelung abweichend formuliert sein müssen — identisch ist mit einem Gesetzentwurf gleicher Bezeichnung, den die Fraktion der GRÜNEN in der letzten Legislaturperiode in den Bundestag (BT-Drs. 10/5884) eingebracht hatte und jetzt erneut vorgelegt hat (BT-Drs. 11/1152 v. 11. 11. 1987).

Beide Gesetzesinitiativen gehen übereinstimmend von der Existenz erheblicher Umweltbelastungen und von einer Betroffenheit aller Bürger aus. Übereinstimmung herrscht auch in der Anerkennung eines Anspruchs jedes Bürgers auf Informationen über die Umweltsituation und die sie beeinflussenden Faktoren wegen dieser allgemeinen Betroffenheit. Unterschiede werden jedoch deutlich bei der Begründung der Notwendigkeit für eine gesetzliche Regelung des Informationsanspruchs und in der Art und Weise, wie diesem Anspruch entsprochen werden soll.

Der Senatsentwurf eines UAG wird damit begründet, daß „die Unsicherheit im Umgang mit umweltrelevanten Daten" beseitigt werden müsse. Der Umstand, daß umweltrelevante Daten meist zugleich auch personenbezogene Daten oder Betriebs- und Geschäftsgeheimnisse darstellten, die von den Behörden nicht unbefugt offenbart werden dürften, hätte in der Vergangenheit zu einer zurückhaltenden, zum Teil sogar restriktiven Informationspraxis der Behörden geführt. Hamburg sehe einen Bedarf für eine bundesweite Regelung auch deswegen, weil Bürger in den einzelnen Bundesländern nicht unterschiedlich über Umweltdaten informiert werden sollten und weil ver-

mieden werden müsse, daß Standortentscheidungen der Unternehmen durch die „Informationspolitik" eines Bundeslandes beeinflußt werden.

Entsprechend dieser Begründung fällt der dem Bürger nach dem UAG zugedachte Auskunftsanspruch eher bescheiden aus, und vor die Auskunft sind auch noch einige Hürden gesetzt. So ist der Antrag auf Auskunft schriftlich bei der jeweils zuständigen Behörde zu stellen, und die Auskunft kann von einer Gebühr abhängig gemacht werden. Antragsberechtigt ist zwar „jedermann", aber Auskunft gewährt wird grundsätzlich nur über anlage- und gebietsbezogene Daten aus dem jeweiligen Bundesland, in dem der Antragsteller wohnt, arbeitet oder ein Gewerbe ausübt. Steht z.B. eine emittierende Anlage in Wedel, so haben die östlich nur wenige Kilometer entfernt in Hamburg-Rissen wohnenden Bürger, die die Emissionen mit dem Westwind erhalten, keinen Auskunftsanspruch über diese anlagebezogenen Daten. Entsprechend haben die Bürger in Schleswig-Holstein und Niedersachsen keinen Anspruch auf Auskunft über Anlagen in Hamburg. Daß die Formulierung („grundsätzlich") es den Behörden ermöglicht, ausnahmsweise auch Bürgern aus angrenzenden Gebieten Daten mitzuteilen, kann nicht darüber hinwegtäuschen, daß der Bürger in einer solchen Situation keinen Anspruch auf eine Auskunft hat.

Schließlich ist die Auskunft „innerhalb einer angemessenen Frist" zu erteilen. Eine derart vage Frist läßt häufige Streitigkeiten erwarten. Schon über die „Angemessenheit" der Beantwortungsfrist können Auskunftsansprüche leerlaufen.

Der Auskunftsanspruch nach dem UAG ist auf „Umweltdaten" gerichtet, die der Gesetzentwurf definiert als „anlagebezogene, gebietsbezogene und stoffbezogene Daten nach Maßgabe des § 2 Absätze 2 bis 4 des UAG". Der Auskunftsanspruch soll dann nicht bestehen, wenn durch die Auskunft personenbezogene Daten oder Betriebs- und Geschäftsgeheimnisse offenbart würden. Damit der Auskunftsanspruch der Bürger, der ja aus einem wegen der Umweltsituation anerkannten berechtigten Interesse resultiert, nicht dadurch weitgehend wieder aufgehoben wird, daß betroffene Personen oder Betriebe ihre Rechte auf Datenschutz oder auf Wahrung ihrer Betriebs- und Geschäftsgeheimnisse geltend machen, sieht der Gesetzentwurf zwei Ausnahmen vor.

(1) Soweit es sich um die Offenbarung von Umweltdaten nach diesem Gesetz(-entwurf) handelt, die nur deshalb auch als personenbezogene Daten zu beurteilen sind, weil sie einer natürlichen Person zugeordnet werden können, soll die Auskunft erteilt werden. Soweit für die Bestimmung, Unterscheidung oder Zuordnung von Umweltdaten erforderlich, dürfen auch der Name und der Beruf sowie Branchen- und Geschäftsbezeichnungen weitergegeben werden.

(2) Anlagebezogene Daten nach § 2 Abs. 2 sollen keine Betriebs- und Geschäftsgeheimnisse darstellen, soweit es sich um die jährliche Menge und die Konzentration von Emissionen einschließlich ionisierender Strahlen handelt. Dies gilt nicht für Forschungs- und Entwicklungsanlagen.

Der Gesetzentwurf des Hamburger Senats ist im Bundesrat gescheitert. Dieser hat am 16. Oktober 1987 beschlossen, den Gesetzentwurf nicht beim Deutschen Bundestag einzubringen, und zwar mit der Begründung, es fehle dem Bund für eine solche Regelung die Gesetzgebungskompetenz. In seinem ablehnenden Beschluß erkennt der Bundesrat zwar ausdrücklich an, daß die Information der breiten Öffentlichkeit über Umweltdaten eine entscheidende Voraussetzung für wirksamen Umweltschutz sei, da sich wirksame Fortschritte im Umweltschutz nicht allein durch Gesetzgeber und Verwaltung erzielen ließen, sondern das Umweltbewußtsein der Bevölkerung und das Engagement der Bürger ebenfalls erforderlich seien. Er hält jedoch — unabhängig von der fehlenden Gesetzgebungskompetenz des Bundes — den Entwurf weder für erforderlich noch für geeignet, weil

— bereits jetzt auf Grund von Rechtsvorschriften vielfältige Informationsrechte für Bürger und Öffentlichkeit existierten, die nötigenfalls spezialgesetzlich zu ergänzen seien;

— der Gesetzentwurf erforderliche Differenzierungen vermissen lasse;

— es nicht zweckmäßig erscheine, angesichts der bestehenden Rechtslage und des ohnehin bestehenden Harmonisierungsbedarfs ein weiteres, mit dem übrigen Umweltrecht nicht abgestimmtes Gesetz zu erlassen, das zudem mit zahlreichen unbestimmten Rechtsbegriffen belastet sei und

— weil zu befürchten stehe, daß die Durchführung eines solchen Gesetzes — also die Auskunfterteilung über Umweltdaten — Verwaltungskapazitäten binden würde, die für einen effektiven Umweltschutz selbst vorrangig und dringend benötigt würden.

Der AERG-Entwurf der GRÜNEN geht von einem anderen Ansatz aus als das UAG. In weiten Kreisen der Bevölkerung habe die Entwicklung der Umweltsituation in der Bundesrepublik den Eindruck entstehen lassen, die staatlichen Organe seien außerstande oder nicht gewillt, einen angemessenen Ausgleich zu schaffen zwischen dem Bestreben der Industrie nach extensiver Nutzung der natürlichen Ressourcen zur Gewinnerzielung sowie dem Wunsch der jeweiligen Arbeitnehmer nach Erhaltung ihres Arbeitsplatzes und dem Wunsch der übrigen Menschen, in einer schadstoffarmen Umwelt möglichst gesund leben zu können. Engagierte und betroffene Bürger wollten daher direkten Einfluß auf politische Entscheidungsabläufe nehmen können und seien, wenn dies qualifiziert geschehen solle, auf bessere Informationsmöglichkeiten angewiesen. Der Ansatzpunkt des AERG ist daher die Herstellung von mehr Chancengleichheit in bezug auf den Zugang zu Daten über Umweltbelastungen und ihre Ursachen bzw. Verursacher.

Entsprechend dieser Intention sieht der Gesetzentwurf statt eines Auskunftsrechts für den Bürger (passiver Informationsgewinnung) ein Akteneinsichtsrecht des Bürgers zur aktiven Informationsgewinnung vor. Die Akteneinsicht kann mündlich beantragt werden, sie ist gebührenfrei (für Ablichtungen aus Akten können kostendeckende Gebühren verlangt werden) und sie ist „unverzüglich" zu gewähren. Bei Hindernissen oder Ablehnung der Einsicht ist innerhalb kurzer Fristen (2 bis 4 Wochen) zu bescheiden, die Verweigerung oder Beschränkung des Einsichtsrechts ist zu begründen.

Die Ausgestaltung des Akteneinsichtsrechts nach dem Gesetzentwurf läßt eine Abwägung erkennen zwischen dem berechtigten Interesse der Allgemeinheit an Umweltdaten und den schutzwürdigen Belangen betroffener Personen und Unternehmen (§ 5 — Schutz personenbezogener Daten, § 6 — Schutz von Betriebs- und Geschäftsgeheimnissen). Der Entwurf regelt darüber hinaus den Schutz der Rechtsdurchsetzung und Strafverfolgung sowie den Schutz des behördlichen Entscheidungsbildungsprozesses.

Die Gesetzesinitiativen der GRÜNEN bzw. der GAL sind mit dem Ende der letzten jeweiligen Legislaturperioden der Diskontinuität anheimgefallen (im Bund und in Hamburg). Bisher ist der Gesetzentwurf nicht erneut in die Bürgerschaft eingebracht worden, wohl aber — wie oben erwähnt — in den Bundestag.

Warum wird nun ausgerechnet ein Akteneinsichtsrecht in Umweltakten bzw. ein Auskunftsrecht über Umweltdaten erörtert? Ist der Bürger nicht an anderen Verwaltungsvorgängen und -akten ebenso interessiert? Muß nicht — wie in anderen Staaten schon seit langem — ein generelles Informationsrecht des Bürgers eingeführt werden? Darüber wird heftig gestritten. Ich habe mich in meinem 4. TB (S. 154, 155) schon einmal zu einem allgemeinen Akteneinsichtsrecht geäußert und angeregt, diesem Problem im Zusammenhang mit der Novellierung des HmbDSG nachzugehen. Dabei hatte ich auf die beiden konkurrierenden Aspekte des Datenschutzes, den Transparenzgedanken und den Schutz der Persönlichkeitssphäre, hingewiesen.

In meinen Stellungnahmen zu den Gesetzentwürfen habe ich folgenden Standpunkt vertreten: Ich stehe den Bemühungen um bessere Informationsmöglichkeiten über Umweltdaten für den Bürger positiv gegenüber. Ich bin nicht der Ansicht, aus Gründen des Datenschutzes könne es ein allgemeines Informationsrecht des Bürgers nicht geben. Wie ich in früheren Tätigkeitsberichten mehrfach betont habe, stellen die Datenschutzgesetze das Ergebnis eines Abwägungsprozesses zwischen dem Recht

des einzelnen, über seine Daten selbst zu bestimmen, und dem Recht der Allgemeinheit auf Information dar. Das informationelle Selbstbestimmungsrecht ist nicht absolut, wie das Bundesverfassungsgericht in seinem Volkszählungsurteil vom 15. 12. 1983 ausgeführt hat. Folgerichtiger Datenschutz kann daher nur Teil einer umfassenden Informationsregelung sein, die auch das Recht des einzelnen und der Allgemeinheit auf Information umfaßt. In der Diskussion über die Einführung eines Bürgerrechts auf Akteneinsicht kann es meiner Ansicht nach nicht mehr darum gehen, ob eine solche Regelung geboten ist, sondern nur noch darum, wie sie auszugestalten ist.

Für den mit den Gesetzentwürfen beschrittenen Weg, zunächst einen begrenzten Teilbereich zu regeln, sprechen folgende Argumente:

(1) Die Aussichten, in der Bundesrepublik einen politischen Konsens über ein generelles Informationsrecht herstellen zu können, sind zur Zeit gleich null.

(2) Die mit dem Datenschutz gewonnenen Erfahrungen zeigen deutlich, daß überzeugende und wirksame Regelungen nur gelingen, wenn man sich auf einen konkreten und begrenzten Problemkomplex konzentriert. Der Umweltschutz ist nun gerade ein Problembereich, der in der Bevölkerung mit großem Interesse verfolgt wird, so daß es naheliegt, diesen Bereich für ein „Pilotgesetz" zu wählen.

Es gibt, wie die Begründung zu den Gesetzentwürfen, die Stellungnahmen und der Beschluß des Bundesrates gezeigt haben, Übereinstimmung über die Notwendigkeit und Berechtigung einer besseren Information des Bürgers über Umweltdaten. Es bestehen zum Teil aber ersichtlich Hemmungen, diesem Grundkonsens entsprechend den Informationsanspruch des Bürgers in einem Gesetz zu regeln. Ich halte es in diesem Zusammenhang für bemerkenswert, wenn in einer Stellungnahme der Verwaltung zu dem Gesetzentwurf der GRÜNEN die Befürchtung geäußert wird, Unternehmen könnten sich durch ein auf Hamburg beschränktes Informationsrecht des Bürgers zu einer an Hamburg vorbeigehenden Standortentscheidung veranlaßt sehen und Hamburg würde mit einem entsprechenden Gesetz eine „negative Sonderstellung" einnehmen.

Deshalb verdient der Vorstoß Hamburgs mit seinem Entwurf eines Umweltdatenauskunftsgesetzes durchaus Anerkennung. Er war ein ernsthafter Versuch, durch bessere Information über Umweltdaten den Bürgern die Möglichkeit zu kritischer Beobachtung des Verwaltungshandelns und zu mehr Einflußnahme auf die Nutzung der Umwelt zu verschaffen. In Kenntnis der z.Z. noch herrschenden Widerstände gegen ein gesetzlich garantiertes Informationsrecht in weiten Kreisen der Verwaltung und der Wirtschaft haben die Initiatoren einen Versuch unternommen, der nicht von vornherein zum Scheitern verurteilt war.

Die Aussicht, daß das von den GRÜNEN in den Bundestag eingebrachte AERG angenommen wird, scheint mir dagegen — jedenfalls in absehbarer Zeit — nicht gegeben. Die Widerstände gegen eine vermeintliche Beeinträchtigung der Belange von Wirtschaft und Verwaltung durch Bürger und Bürgerinitiativen scheinen mir nach wie vor zu stark zu sein.

Ich bin der Meinung, daß das Informationsbedürfnis des Bürgers durch Einsichtnahme besser zu gewährleisten ist als durch Auskunfterteilung. Auskünfte können unscharf, unvollständig, mißverständlich und irreführend sein. Auskünfte können auch so erteilt werden, daß die Fragen zwar den Buchstaben nach beantwortet werden, die erkennbare Idee einer Frage aber übergangen wird. Auch ist das Erfragen von Vorgängen und Zusammenhängen äußerst mühsam, sodaß häufig Nachfragen erforderlich werden. Bei Einsichtnahme entfällt ein erheblicher Teil des Arbeitsaufwandes, der für Auskunfterteilung aufzuwenden ist, und die Bürger haben es selbst in der Hand, richtige und vollständige Informationen zu gewinnen. Aus den Akten selbst entnommene Informationen, die der Bürger vielleicht mangels Fachkunde nicht versteht, können immerhin gezielt hinterfragt und nutzbar gemacht werden.

Ich meine auch, daß durch den AERG-Entwurf der Schutz personenbezogener Daten, dem mein besonderes Augenmerk zu gelten hat, mit den Regelungen im § 5 trotz

der sehr weitgehenden Ausgestaltung des Informationsanspruchs nicht unverhältnismäßig eingeschränkt worden ist: personenbezogene Daten dürfen im Zusammenhang mit Umweltdaten nur in ganz beschränktem Umfang offenbart werden. Die wenigen personenbezogenen Daten, deren Offenbarung in diesem Zusammengang zugelassen ist, sind auch ihrer Art nach nicht als besonders kritisch anzusehen (Name, Titel, Beruf, innerbetriebliche Funktion halte ich für unbedenklich, über Geburtsdatum, Anschrift und Rufnummer müßte noch genauer nachgedacht werden). Die Möglichkeit zur Offenbarung personenbezogener Daten hält sich damit nach meiner Auffassung in den Grenzen, die aus überwiegendem Allgemeininteresse gerechtfertigt sind.

4.8 Bauwesen

In meinem 5. TB (Seiten 50, 51) habe ich über die Hamburgische Bauordnung (HBauO) berichtet und der Bewertung Ausdruck gegeben, der Senat werde im Laufe des Jahres 1987 eine Rechtsverordnung zu § 81 Abs. 2 Nr. 4 HBauO erlassen, in der die Datenverarbeitung im Rahmen bauaufsichtlicher Aufgaben klar und abschließend geregelt wird. Diese Erwartung ist mit der Bauvorlagenverordnung (BauVorlVO) vom 1. 12. 1987 (HmbGVBl. I S. 211) erfüllt worden. Die Verordnung ist am 1. 1. 1988 in Kraft getreten.

Teil 5 der BauVorlVO (§§ 14 — 16) ist dem Datenschutz gewidmet. § 14 regelt die Übermittlung von Daten, die der Betroffene der Bauaufsichtsbehörde zur Erlangung eines baurechtlichen Bescheides zur Verfügung gestellt hat, an andere Stellen, soweit die Übermittlung notwendig ist, um die Vereinbarkeit des Vorhabens mit öffentlich-rechtlichen Vorschriften zu prüfen. Es geht hierbei um die Beteiligung von Stellen mit spezieller Sachkunde zum Zwecke der Erteilung eines baurechtlichen Bescheids. Es wurde eine Regelung angestrebt, in der — dem Gebot der Normenklarheit entsprechend — sämtliche zugelassenen Datenempfänger, der jeweilige Verwendungszweck (das ist hier im wesentlichen die Einhaltung der speziellen öffentlich-rechtlichen Vorschriften, für die die zu beteiligende andere Stelle zuständig und besonders sachkundig ist) und die zu übermittelnden Daten abschließend genannt werden. Die explizite Aufzählung von sechsundzwanzig (!) möglichen Empfängern unterstreicht m. E., wie berechtigt die Forderung nach einer Regelung der Datenverarbeitung im Rahmen des bauaufsichtlichen Verfahrens war. Welcher Bürger ahnt wohl, wenn er einen Bauantrag bei der Bauprüfabteilung abgibt, wie viele andere Stellen seine mit dem Antrag preisgegebenen Daten zur Kenntnis erhalten? Zwar wird nicht bezweifelt, daß die genannten Stellen aufgrund ihrer Zuständigkeiten über die besondere Sachkunde verfügen, auf die die Bauprüfabteilung sich von Fall zu Fall bei einer Entscheidung stützen muß und daß eine Übermittlung von Daten aus einem baurechtlichen Verfahren an diese Stellen notwendig ist; aber dies darf nicht geschehen, ohne daß es dem Bürger mitgeteilt wird. Das Verwaltungshandeln muß für ihn transparent sein. Außerdem ist es für die als Sachverständige zu beteiligenden dritten Stellen zur Beurteilung der Frage, ob ein Bauvorhaben mit öffentlich-rechtlichen Vorschriften in Einklang steht, nicht in jedem Fall erforderlich, den Namen und die Anschrift des Bauherrn, des Entwurfsverfassers oder des Bauvorlageberechtigten zu kennen. In § 14 Abs. 3 wird daher die Möglichkeit eröffnet, bei der Übermittlung solche Unterlagen zu verwenden, die diese personenbezogenen Daten nicht enthalten. Der Bauherr kann entsprechende Unterlagen einreichen, wenn er diese Möglichkeit nutzen will.

Obwohl mit sechsundzwanzig explizit aufgeführten möglichen Datenempfängern alle denkbaren erforderlichen Übermittlungen geregelt sein dürften, konnte ich die Aussage der Fachleute der Bauaufsichtsbehörde, es können in seltenen Fällen weitere Übermittlungen zur Erteilung eines baurechtlichen Bescheides erforderlich werden, nicht widerlegen. Ich konnte aber durchsetzen, daß die Übermittlung an weitere Stellen nur mit Einwilligung des Betroffenen erfolgen darf (§ 14 Abs. 2 Satz 2).

§ 15 regelt die Übermittlung von Daten aus dem bauaufsichtlichen Verfahren zu anderen Zwecken als zur Erteilung eines baurechtlichen Bescheids. Die anderen Zwecke liegen — entsprechend dem gesetzlichen Erfordernis (§ 81 Abs. 2 Nr. 4 zweite Alt. HBauO) — im Rahmen der Erfüllung öffentlicher Aufgaben. Wegen der völlig unter

schiedlichen Zwecke, die mit dem eigentlichen bauaufsichtlichen Verfahren nicht zusammenhängen, mußten die Empfänger der Daten, der Zweck der Verwendung sowie Art und Umfang der jeweils zu übermittelnden Daten im einzelnen genannt werden. An Stellen, die in § 15 nicht explizit aufgeführt sind, dürfen Daten aus dem bauaufsichtlichen Verfahren nur mit Einwilligung des Betroffenen übermittelt werden (§ 15 Abs. 3).

Mit den §§ 14, 15 BauVorlVO liegt nun eine Regelung vor, die dem Bürger weitgehend Kenntnis darüber verschafft, wer alles von seinem Bauvorhaben erfährt. So umfassend die Aufzählung der Übermittlungsempfänger in der BauVorlVO auch ist, ist sie gleichwohl nicht abschließend: Befugnisse zur Datenübermittlung aus dem bauaufsichtlichen Verfahren an Stellen, die nicht in der BauVorlVO genannt sind, finden sich z.B. auch noch im Bezirksverwaltungsgesetz und dem Gesetz über Verwaltungsbehörden (Beteiligung der Bauausschüsse und der Baudeputationen). § 16 verpflichtet nichtöffentliche Stellen, die ihnen übermittelten Daten aus dem bauaufsichtlichen Verfahren spätestens vier Wochen nach Zweckerfüllung zu löschen. Für öffentliche Stellen wird keine besondere Löschungsfrist festgelegt, sondern es wird auf die allgemeinen Vorschriften verwiesen.

4.9 Steuerwesen

4.9.1 Steuerdaten-Abrufverordnung

Im Berichtszeitraum sind weitere Entwürfe einer Steuerdaten-Abrufverordnung (Verordnung zu § 30 Abs. 6 Satz 2 AO, s. 5. TB S. 57) vorgelegt worden. In der Diskussion über die Entwürfe spielen vor allem zwei Aspekte eine Rolle: Die Festlegung der Zugriffsberechtigten und der Umfang der Protokollierung zur Kontrolle der Zugriffe.

Es dürfen nur solche Abrufberechtigungen geschaffen werden, die zur Aufgabenerfüllung erforderlich sind. Erforderlich sind Abrufmöglichkeiten für die Sachbearbeitung in den Finanzämtern. Mit der Finanzbehörde (und mit dem Bayerischen Staatsministerium der Finanzen) bin ich der Auffassung, daß für Amtsträger bei Oberbehörden, die in Steuerverfahren im Rahmen von Dienst- und Fachaufsicht tätig werden, ein unmittelbarer Zugriff auf die in den automatisierten Dateien aller ihrer Finanzämter gespeicherten Daten der Steuerpflichtigen zur Aufgabenerfüllung nicht erforderlich ist. Durch eine direkte Abrufmöglichkeit ist keine Effizienzsteigerung zu erwarten, da bei der Bearbeitung von Einzelfällen ohnehin die Heranziehung der Akten unerläßlich ist. Außerdem sind im Rahmen der Dienst- und Fachaufsicht Entscheidungen nicht zeitkritisch. Falls in Einzelfällen doch einmal eine schnelle Datenübermittlung notwendig wird, stehen andere Möglichkeiten (Telefon, Telefax, Fernschreiber, Eilbrief) zur Verfügung.

Die Regelung in dem Entwurf (Stand: 3. 9. 1987), mit der eine Datenabrufmöglichkeit für Amtsträger von Oberbehörden für Zwecke der Dienst- und Fachaufsicht geschaffen wird, sollte wieder gestrichen werden. Im ersten Entwurf war diese Regelung auch nicht enthalten.

Um beim Betrieb von Datenabrufverfahren Nichtzugriffsberechtigte auszuschließen und Zugriffsberechtigte daran zu hindern, ihre Kompetenzen zu überschreiten, sind technische und organisatorische Maßnahmen zu treffen. Der Entwurf schreibt hierfür Mindestanforderungen vor. Eine der vorgesehenen Maßnahmen, nämlich die automatische Protokollierung ausgewählter Datenabrufe als Grundlage für eine nachträgliche Kontrolle, ob bestimmte Datenabrufe erforderlich waren, entspricht z.Z. noch nicht den Vorstellungen der Datenschutzbeauftragten von einer dem Schutzzweck angemessenen Maßnahme. In dem Entwurf ist vorgesehen, daß nur mindestens 5 % der Datenabrufe durch Zugriffsberechtigte anderer Behörden als der speichernden Stelle automatisch aufgezeichnet werden sollen. Dies ist unzureichend. Der Bundesbeauftragte für den Datenschutz hat die Protokollierung aller Abrufe durch Zugriffsberechtigte anderer Behörden als der speichernden Stelle gefordert. Er verweist darauf, daß solche Datenabrufe zahlenmäßig gering sind und hält deshalb den mit der Protokollierung aller dieser Datenabrufe verbundenen Aufwand für verhältnismäßig im Hinblick auf den angestrebten Schutzzweck.

Auch ich bezweifle, daß bei einer Protokollierung von nur 5 % der Abrufe nicht zuständiger Stellen der Zweck dieser Maßnahme, nämlich Zugriffsberechtigte davon abzuhalten, ihre Zugriffsberechtigung zu mißbrauchen, erfüllt werden kann. Ob eine 100 %ige Protokollierung jedoch geboten ist, wage ich ebenfalls zu bezweifeln. Um zu einer angemessenen Lösung zu gelangen, müßte statistisches Material über die Zugriffshäufigkeit ausgewertet werden. Möglicherweise kommt man auch über eine probeweise, zeitlich begrenzte Protokollierung aller Abrufe zu einer „vernünftigen" Lösung.

4.9.2 Kontrollmitteilungsverordnung

Die Kontrollmitteilungsverordnung soll Einzelheiten des Mitteilungsverfahrens nach § 93 a AO regeln. Mit § 93 a AO war, wie ich berichtet hatte (zuletzt: 5. TB S. 56), der Auffassung der Datenschutzbeauftragten Rechnung getragen worden, daß der Austausch von Kontrollmitteilungen über steuerlich relevante Sachverhalte zwischen anderen Behörden und den Finanzämtern nicht ohne gesetzliche Grundlage erfolgen dürfe. § 93 a AO nennt abschließend die Fälle, in denen der Austausch von Kontrollmitteilungen angeordnet werden kann. In der Kontrollmitteilungsverordnung wird festgelegt, in welchen Fällen tatsächlich Kontrollmitteilungen angeordnet werden. Außerdem wird in der Verordnung das Mitteilungsverfahren geregelt.

Bei dem Verordnungsentwurf gilt es darauf zu achten, daß in der Verordnung nur solche Kontrollmitteilungen angeordnet werden, die nach § 93 a AO zugelassen sind. Bei der Anordnung von Kontrollmitteilungen ist auch der Grundsatz der Verhältnismäßigkeit zu wahren, so z. B. bei der Festlegung von Bagatellfällen, in denen eine Kontrollmitteilung unterbleiben kann, und bei der Festlegung der in den Kontrollmitteilungen mitzuteilenden Daten. Z. B. sollte die Steuernummer der Betroffenen nicht verlangt werden, weil es sonst nicht ausbleiben kann, daß die mitteilungspflichtigen Stellen diese Angabe vom Betroffenen auch dann erheben, wenn sie sie für die eigene Aufgabenerfüllung gar nicht benötigen.

Die nach Bekanntwerden des ersten Entwurfs aufgekommene Unsicherheit darüber, ob auch Sozialleistungsträger zu Kontrollmitteilungen verpflichtet werden können (s. 5 TB, S. 57, 58), ist inzwischen beseitigt: Der neue Entwurf stellt ausdrücklich fest, daß Sozialleistungen und personenbezogene Daten, die den Leistungsträgern im Zusammenhang mit der Erfüllung ihrer Aufgaben nach dem Sozialgesetzbuch bekannt sind, nicht aufgrund der Verordnung mitzuteilen sind.

4.9.3 Verwaltungsvorschriften zur Landeshaushaltsordnung

Durch die Bekanntmachung der Neufassung von Verwaltungsvorschriften zur Landeshaushaltsordnung (LHO) im Amtlichen Anzeiger (Hmb. GVBl Teil II 1985 S. 2381 ff.) wurde ich auf eine Kontrollmitteilung aufmerksam, die ich für unzulässig hielt. In Nr. 5.2 der Anlagen 1 bis 3 der Verwaltungsvorschriften zu §§ 23 und 44 LHO wurde bestimmt, daß Empfänger von Zuwendungsmitteln ihrem Finanzamt die Zahlungen mitzuteilen haben, die sie aufgrund von Verträgen an Dritte leisten. Diese Mitteilungen haben den Charakter von Kontrollmitteilungen. Eine gesetzliche Grundlage für diese Kontrollmitteilungen habe ich nicht feststellen können, insbesondere enthält die LHO keine entsprechende Rechtsgrundlage.

Ausgehend von der der Einführung des § 93 a AO zugrundeliegenden Rechtsauffassung, daß Kontrollmitteilungen ohne Rechtsgrundlage nicht zulässig sind, habe ich der Finanzbehörde gegenüber meine Bedenken gegen diese Kontrollmitteilungen geäußert. Ich habe darauf hingewiesen, daß die fraglichen Kontrollmitteilungen auch nicht auf eine — als Klausel in den Vertrag zwischen Zuwendungsempfänger und dem Dritten aufgenommene — Einwilligung des Dritten gestützt werden können. Im übrigen habe ich die Ansicht vertreten, der Bundesgesetzgeber habe mit § 93 a AO eine abschließende gesetzliche Regelung für Kontrollmitteilungen zur Sicherung der Besteuerung schaffen wollen, und § 93 a AO lasse eine Verpflichtung von Zuwendungsempfängern, die keine Behörden, sondern private Personen, Vereine, Firmen usw. sind, überhaupt nicht zu.

Die Finanzbehörde teilt meine Bedenken und hat zugesagt, die Regelung in Nr. 5.2 der Anlagen 1 bis 3 zur Verwaltungsvorschrift zu §§ 23 und 44 LHO bei ohnehin anstehenden Änderungen ersatzlos zu streichen.

4.10 Einwohnerwesen

4.10.1 Paß- und Personalausweiswesen

4.10.1.1 Hamburgisches Personalausweisgesetz

Die notwendige landesrechtliche Umsetzung des Bundespersonalausweisgesetzes, die ich in meinem 5. TB (5.7.4.2, S. 64) bereits angemahnt hatte, wurde im Dezember 1987 endlich vom Senat eingeleitet.

Mit dem Bundespersonalausweisgesetz hat der Bundesgesetzgeber die rechtlichen Voraussetzungen für die Einführung eines neuen Ausweissystems geschaffen. Seit dem 1. 4. 1987 werden auch in Hamburg die neuen maschinenlesbaren Personalausweise ausgegeben. Die Ergänzung des Bundesgesetzes durch landesrechtliche Bestimmungen ist inzwischen — außer in Niedersachsen, Hessen und Hamburg — in allen Bundesländern durch die Verabschiedung von Landespersonalausweisgesetzen erfolgt. Der nunmehr in Hamburg vorgelegte Entwurf orientiert sich im wesentlichen an den Gesetzen der anderen Länder, die wiederum auf einem zwischen dem Bundesminister des Innern und den Innenministern/-senatoren der Länder abgestimmten Formulierungsvorschlag aufbauen.

Ich habe zu dem Gesetzesentwurf ausführlich Stellung genommen und mich dabei insbesondere mit der beabsichtigten Durchführung von erkennungsdienstlichen (ed) Maßnahmen im Zusammenhang mit der Ausstellung von Personalausweisen auseinandergesetzt. Der Gesetzesentwurf sieht nämlich vor, daß die Ausweisbehörde in Zweifelsfällen Maßnahmen zur Personenfeststellung durchführen darf, d.h. sie ist nicht nur befugt, Auskünfte von anderen Stellen einzuholen und Gegenüberstellungen mit anderen Personen durchzuführen. Wenn die Person des Ausweisbewerbers mit diesen Maßnahmen nicht oder nur unter erheblichen Schwierigkeiten festgestellt werden kann, darf die Ausweisbehörde auch die Aufnahme von Lichtbildern und Fingerabdrücken sowie die Durchführung von Messungen und ähnlichen Maßnahmen (ed-Maßnahmen) anordnen. Eine solche ed-Behandlung soll — im Wege der Amtshilfe — durch die Polizei erfolgen und dabei soll ein Abgleich mit polizeilichen Datenbeständen zugelassen werden.

Ed-Maßnahmen sind besonders schwerwiegende Eingriffe in das Recht auf informationelle Selbstbestimmung. Sie sind unter Zwangsanwendung ansonsten nur zulässig bei Tatverdächtigen oder Beschuldigten zur Strafverfolgung oder bei Personen, die sich aus Gründen der Gefahrenabwehr einer Identitätsfeststellung zu unterziehen haben. In der Bevölkerung wird die ed-Behandlung zu Recht als diskriminierend empfunden, so daß sich die Frage stellt, ob sie im Rahmen der Ausstellung von Personalausweisen wirklich unerläßlich ist. Immerhin bestimmt § 163 b Abs. 2 StPO, daß ed-Maßnahmen bei Nichttatverdächtigen nicht gegen deren Willen getroffen werden dürfen.

Ich verkenne nicht, daß die ed-Behandlung im Personenfeststellungsverfahren als ultima ratio prinzipiell in Betracht kommen kann. Gleichwohl habe ich die Behörde für Inneres gebeten, sehr sorgfältig zu prüfen, ob bereits einige theoretisch denkbare Fälle es rechtfertigen, die Befugnis zur ed-Behandlung und damit unnötigerweise auch die Gefahr einer unverhältnismäßigen und mißbräuchlichen Anwendung dieses Zwangsmittels zu begründen. Aus meiner Sicht ist bislang nicht erkennbar, daß für einen derart schwerwiegenden Eingriff in das Persönlichkeitsrecht ein überwiegendes öffentliches Interesse — wie es das Bundesverfassungsgericht verlangt — besteht. Im Gegenteil:

Die Behörde für Inneres hat eingeräumt, daß ed-Maßnahmen gegenwärtig nur in sehr wenigen Fällen zur Anwendung kommen und die Trefferquote offenbar außerordentlich gering ist. Auch der Hinweis, es könne nicht ausgeschlossen werden, daß ein größe-

res praktisches Bedürfnis für die ed-Behandlung unter veränderten gesellschaftlichen Verhältnissen wieder zu Tage treten könne, vermag die Notwendigkeit entsprechender Befugnisse zum heutigen Zeitpunkt nicht zu begründen. Sofern tatsächlich einmal durch gegenwärtig nicht vorhersehbare Entwicklungen das Bedürfnis für ed-Behandlungen bei der Ausstellung von Personalausweisen deutlicher werden sollte, könnte der Gesetzgeber immer noch rechtzeitig die erforderlichen Rechtsgrundlagen schaffen.

4.10.1.2 Erste Erfahrungen mit dem maschinenlesbaren Personalausweis

Seit dem 1. 4. 1987 werden bundesweit die maschinenlesbaren Personalausweise ausgegeben — trotz der schwerwiegenden verfassungsrechtlichen Bedenken, die auch ich in meinen bisherigen Tätigkeitsberichten erhoben hatte. Eine Reihe von Bürgern waren, nachdem sie die Plastikkarte in Händen hielten, verunsichert und ließen sich über die Bedeutung insbesondere der beiden Zeilen am unteren Rand der Vorderseite, die automatisch gelesen werden können, unterrichten. Auch die sichtbaren Echtheitsmerkmale, die keinerlei Bezug zu den Inhabern der Ausweise haben, führten zu Anfragen.

Im November 1987 wurde zunächst in Hessen bekannt, daß dort über 175 Personalausweise mit identischer Seriennummer von den Personalausweisbehörden ausgegeben worden sind. Ich habe daraufhin auch in Hamburg in etwa 80 Fällen derartige Pannen feststellen müssen, die im wesentlichen darauf beruhten, daß die örtlichen Ausweisbehörden (= Meldedienststellen in den Bezirks- und Ortsämtern) bei der Vergabe der Nummern nicht in jedem Einzelfall mit der gebotenen Sorgfalt gearbeitet haben.

Da es aus Gründen des Datenschutzes, insbesondere wegen der Folgen, die etwa eine Verwechslung mit einer polizeilich gesuchten Person für den Betroffenen haben könnten, oder auch im Interesse der öffentlichen Sicherheit und Ordnung erforderlich ist, daß jeder Ausweis mit einer einmaligen Seriennummer versehen wird, muß die Kontrolle der Seriennummern durch die Bundesdruckerei in Berlin, in der sämtliche Ausweise hergestellt werden, verbessert werden. Die Seriennummer sollte — statt durch die örtliche Ausweisbehörde — direkt bei der Herstellung des Ausweises durch die Bundesdruckerei zentral vergeben werden. Aus der Sicht des Datenschutzes bestehen dagegen keine Bedenken, weil nach dem Gesetz über Personalausweise ohnehin alle vergebenen Seriennummern — ohne sonstige Ausweisdaten — bei der Bundesdruckerei dauerhaft gespeichert werden. Mit einem zentralen Verfahren hatte sich der Bundesbeauftragte für den Datenschutz schon 1979 ausdrücklich einverstanden erklärt und außerdem in den vergangenen Jahren wiederholt beim Bundesinnenminister geeignete Vorkehrungen gegen eine Mehrfachvergabe der Seriennummer gefordert. Erreicht werden konnte aber leider nur, daß solche Fehler wenigstens nachträglich bald entdeckt werden.

Solange die von mir unterstützte Änderung des Verfahrens nicht realisiert wird, bleibt mir nur der Appell an die örtlichen Ausweisbehörden, durch verstärkte Anstrengungen eine Mehrfachvergabe gleicher Seriennummern zu verhindern.

4.10.2 Meldewesen

4.10.2.1 Maschineller Abgleich des kirchlichen und staatlichen Meldebestandes

Erst durch zahlreiche Eingaben und Presseveröffentlichungen habe ich davon erfahren, daß die Meldebehörde den öffentlich-rechtlichen Religionsgesellschaften über die Einwohner, die im Melderegister als Mitglieder der jeweiligen Religionsgesellschaft eingetragen waren, die in § 33 Hamburgisches Meldegesetz (HmbMG) genannten Daten stichtagsbezogen übermittelt hat. Sinn und Zweck dieses Verfahrens war es, eine Übereinstimmung zwischen den bisher offensichtlich unterschiedlichen Datenbeständen von Kirche und Staat herzustellen. Der Abgleich der Datenbestände ist in zwei Arbeitsschritten durchgeführt worden:

— Im ersten Schritt wurde ein Magnetband, in dem alle im Melderegister als Kirchenangehörige verzeichneten Personen enthalten waren, mit dem kirchlichen Datenbe-

stand verglichen. Als Ergebnis dieses Abgleichs wurde ein Band mit allen Fällen erstellt, die im kirchlichen Datenbestand enthalten sind, für die im Melderegister aber keine Religionszugehörigkeit verzeichnet ist.

— In einem zweiten Arbeitsschritt wurde mit Hilfe dieses Bandes ein weiteres Band erstellt, das für alle dort verzeichneten Fälle die aktuelle Anschrift ausweist, soweit diese Personen noch in Hamburg gemeldet sind.

Dieser Datenbestand bildete die Grundlage für eine Briefaktion der Religionsgesellschaften. Alle in Hamburg gemeldeten Personen, bei denen hinsichtlich ihrer Kirchenmitgliedschaft im staatlichen und kirchlichen Meldebestand keine Übereinstimmung festgestellt werden konnte, wurden um eine schriftliche Stellungnahme gebeten. Falls keine Rückäußerung erfolgte gingen die Kirchen davon aus, daß eine Kirchenmitgliedschaft besteht. Gegen diese Praxis gab es zahlreiche Proteste, die dazu führten, daß das Verfahren zur Bereinigung der Datenbestände zunächst unterbrochen wurde.

Ich habe in einer ersten Stellungnahme gegenüber der Behörde für Inneres bezweifelt, ob die Übermittlung des melderechtlichen Datenbestandes sämtlicher Kirchenmitglieder zu einem bestimmten Stichtag nach dem Hamburgischen Meldegesetz zulässig ist. Auf meine Anregung wird demnächst ein Gespräch mit der Behörde für Inneres und den Kirchen stattfinden.

4.11 Polizei

Eines der dringendsten datenschutzrechtlichen Anliegen ist die Schaffung bereichsspezifischer Grundlagen für die Datenverarbeitung der Polizei. Schon in meinem ersten Tätigkeitsbericht habe ich darauf hingewiesen. Spätestens seit dem „Volkszählungsurteil" des Bundesverfassungsgerichts (BVerfGE Bd. 65 S. 1 ff.) vom 15. 12. 1983 ist das gesetzliche Regelungsdefizit für jedermann offenbar. So hat u.a. auch der Bayerische Verfassungsgerichtshof in seiner Entscheidung vom 9. 7. 1985 (Amtl. Sammlung 1985 S. 74 ff.) bezogen auf die polizeiliche Datenverarbeitung hervorgehoben, daß diese Materie, die bisher Gegenstand nur von (Verwaltungs-) „Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen (KpS)" ist, durch den Gesetzgeber geregelt werden müsse.

Dringend ist das Anliegen deshalb, weil mit der Erhebung, Speicherung und Weitergabe personenbezogener Daten durch die Polizei sowohl bei der Strafverfolgung als auch bei der Gefahrenabwehr permanent in die Grundrechte der Betroffenen eingegriffen wird, ohne daß dafür die verfassungsrechtlich gebotenen gesetzlichen Grundlagen auch nur ansatzweise vorhanden sind, so daß bei einer streng formalen Betrachtungsweise die polizeiliche Datenverarbeitung als verfassungswidrig bezeichnet werden kann (so auch Verwaltungsgericht Frankfurt, Urteil vom 18. 2. 1987; in: Recht der Datenverarbeitung 1987 S. 88 ff.). Gleichwohl kommen die gesetzgeberischen Initiativen zur Behebung dieses Zustandes nur äußerst schleppend voran. Auch aus Hamburg kann ich nicht berichten, daß die Novellierung des SOG entscheidende Fortschritte gemacht hätte.

Andererseits wird die Datenverarbeitung bei der Polizei ständig ausgebaut. Im Berichtszeitraum sind mir wieder eine Reihe von Errichtungsanordnungen für neue Dateien zugeleitet worden; es hat den Anschein, der Polizei sei gar nicht bewußt, daß sie ohne gesetzliche Grundlage ihre Informationsverarbeitung einschränken muß und nicht ausweiten darf.

4.11.1 Übergangslösungen

In meinem letzten Tätigkeitsbericht (5.8.1 S. 67 ff.) habe ich ausführlich dargestellt, daß polizeiliche Informationsverarbeitung derzeit nur mit den Beschränkungen möglich ist, die das Bundesverfassungsgericht für Grundrechtseingriffe ohne hinreichende gesetzliche Grundlage für eine Übergangszeit der Exekutive auferlegt (BVerfGE Bd. 41 S. 251/266 ff; Bd. 51 S. 268/287 ff.).

Gegen einige Stimmen in Literatur (vgl. Alberts, „Übergangszeit im bereichsspezifischen Datenschutz?" in: ZRP 1987 S. 193 ff.) und Rechtsprechung (VG Frankfurt, a.a.O.; zweifelnd VG Hannover, Urt. v. 1. 12. 1986 — 10 VGA 126/85) bin ich auch weiterhin der Auffassung, daß die Datenverarbeitung der Polizei für eine Übergangszeit verfassungsrechtlich hingenommen werden muß. Aber gerade deshalb muß ich darauf bestehen, daß die verfassungsrechtlichen Vorgaben auch eingehalten werden, d.h. daß die Befugnisse der Polizei während dieser Zeit auf das Unerläßliche beschränkt werden. So halte ich es für unzulässig und mit den vom Bundesverfassungsgericht festgelegten reduzierten Befugnissen für unvereinbar, während der Übergangsfrist bereits bestehende Datenverarbeitungsabläufe noch auszuweiten durch den Aufbau neuer Datenbanken sowie der Ausschöpfung neuer technischer Möglichkeiten wie

— Einrichtung von Direktanschlüssen an Datenbanken Dritter,

— Einführung flexibler Abfragesprachen,

— elektronische Bildspeicherungs- und -erkennungssysteme

— Sprachidentifizierungstechniken u.ä.

Generell ist bei neuer oder bisher nicht verwendeter Technik die Frage zu stellen, ob durch ihren Einsatz nicht intensiver in Grundrechte eingegriffen wird als zuvor mit Hilfe konventioneller Datenverarbeitung.

Aber auch die bestehende Praxis der polizeilichen Informationsverarbeitung ist daraufhin zu überprüfen, welche Maßnahmen für die Aufrechterhaltung der Funktionsfähigkeit der Polizei unerläßlich und welche Einschränkungen bis zur Schaffung bereichsspezifischer Grundlagen unvermeidlich sind.

Die Polizei hat sich dort besondere Zurückhaltung aufzuerlegen, wo durch Eingriffe nicht nur das informationelle Selbstbestimmungsrecht, sondern noch weitere Grundrechte, wie etwa das Versammlungsrecht und das Recht auf Unverletzlichkeit der Wohnung, betroffen sind. Das bedeutet:

— Personenfeststellungen, damit verbundene Datenabgleiche sowie Film- und Videoaufnahmen sind anläßlich von öffentlichen Versammlungen während der Übergangszeit jedenfalls dann als unzulässig anzusehen, wenn sie nicht einen unmittelbaren Bezug zu konkreten Straftaten haben.

— Die Nutzung technischer Hilfsmittel zur verdeckten Datenerhebung durch Lauschangriffe in Wohnungen muß grundsätzlich ausgeschlossen sein.

Im Prinzip einig bin ich mit der Behörde für Inneres ferner darüber, daß für die Funktionsfähigkeit der Polizei jedenfalls nicht mehr Befugnisse unerläßlich sein können, als sie in dem Ende 1985 vorgelegten Entwurf zur Novellierung des hamburgischen SOG vorgesehen waren. Wenigstens diesen Rahmen dürfen Informationseingriffe während der Übergangszeit keinesfalls sprengen. Schon Anfang 1986 habe ich der Behörde für Inneres einen Katalog mit den aus meiner Sicht gebotenen zusätzlichen Beschränkungen übersandt, dessen wichtigste Forderungen wie folgt aussehen:

— Bei der Erhebung von Informationen
  - Der Einsatz von verdeckten Ermittlern, V-Leuten und langfristigen Observationen
    darf nur für bestimmte Straftaten zugelassen werden. Darüber hinaus muß festgelegt werden, wer diese Maßnahmen anordnen darf, wie die anfallenden Erkenntnisse verwertet werden dürfen und wann die Betroffenen zu unterrichten sind.
  - Daten sog. „Begleitpersonen", die im Rahmen der polizeilichen Beobachtung anfallen, dürfen grundsätzlich nicht verwendet werden, es sei denn in eng begrenzten Fällen vorher festgelegter Schwerstkriminalität.

— Bei der Speicherung von Informationen
  - Keine Speicherung personenbezogener Hinweise auf Geistesschwäche, Entmündigung, Prostitution, internationale Rechtsbrecher, häufig wechselnden Aufenthalt, Freitodgefahr, Land- und Stadtstreicher in polizeilichen Informationssystemen.

- Speicherung (ehemals) verdächtiger Personen in Kriminalakten und/oder Straftäterdateien einschließlich der Aufbewahrung der zu ihnen gefertigten erkennungsdienstlichen Unterlagen nur dann, wenn eine verantwortbare prognostische Einschätzung den Schluß zuläßt, daß die Gefahr besteht, der Betroffene könnte wieder Straftaten von erheblichem Gewicht begehen.
- Keine Speicherung von Daten über Personen, für deren strafrechtlich zu bewertendes Verhalten eine Anklageerhebung mangels öffentlichen Interesses abgelehnt oder das Ermittlungsverfahren wegen geringer Schuld eingestellt wurde.
- Grundsätzlich keine Speicherung von Störern nach Beseitigung der Gefahr/Störung zu anderen als Dokumentationszwecken.
- Keine Speicherung von Daten, die für unterschiedliche Zwecke benötigt werden (Gefahrenabwehr, vorbeugende Bekämpfung von Straftaten, Aktenverwaltung, Dokumentation) in einem Datenbanksystem, das einen Grunddatenbestand für sämtliche Nutzungen zur Verfügung stellt.

— Bei der Weitergabe von Daten

- Keine — routinemäßige — Weitergabe von Daten, insbesondere an Verfassungsschutz, Ausländerbehörde, Jugendämter u.a., ohne daß konkrete Anhaltspunkte dafür vorliegen, daß die jeweilige Information für die Aufgabenerfüllung der Empfängerbehörde erforderlich ist.
- Keine Weitergabe von Daten, die die Polizei mit ihren speziellen Befugnissen erhoben hat; insbesondere keine Partizipation der Verfassungsschutzbehörden an polizeilichen Vorfeldermittlungen.
- Keine Weitergabe von Daten ohne vorherige Überprüfung auf Akteninhalte und Aktualität.
- Grundsätzlich keine Weitergabe von „Zufallsfunden".

Bisher war eine Verständigung mit der Behörde für Inneres auf einen konkreten Maßnahmenkatalog nicht zu erreichen. Sie war nicht einmal dazu bereit, das Zugeständnis, sich auf die im SOG-Entwurf vorgesehenen Befugnisse beschränken zu wollen, in konkrete schriftliche Anweisungen an die Polizei umzusetzen. Damit sind selbst diese bescheidenen Ansätze gescheitert, denn es liegt auf der Hand, daß Einschränkungen nicht greifen können, die der Polizei gar nicht bekannt sind und die nicht in die Dienstvorschriften Eingang finden. Eine solche Anweisung wäre vordringlich zu erstellen. Auf sie kann nicht verzichtet werden, weil irgendwann eine SOG-Novelle verabschiedet wird, was möglicherweise eine erneute Änderung der Dienstvorschriften erforderlich macht. Entgegen der Auffassung des Senats zu meinem 5. Tätigkeitsbericht (Bürgerschafts-Drs. 12/572, 8.1, S. 8) sehe ich diese Forderungen nicht als überholt an. Die ebenfalls in der Stellungnahme erwähnten, von der Behörde für Inneres aufgegebenen Informationseingriffe haben zu diesen Forderungen keinen für mich erkennbaren Bezug.

Abschließend möchte ich auch an dieser Stelle noch einmal darauf aufmerksam machen, daß Übergangsfristen ihrer Natur nach nicht unbegrenzt in Anspruch genommen werden können. Das Bundesverfassungsgericht hat ausdrücklich darauf hingewiesen, daß sie dann nicht mehr anerkannt werden können, wenn der Gesetzgeber eine Neuregelung ungebührlich verzögert. Es hat aber vermieden, die Dauer allgemein festzulegen, sondern sie im Einzelfall von verschiedenen zu berücksichtigenden Faktoren abhängig gemacht. So haben schon

— die Komplexität der zu erlassenden Regelungen,

— der Zusammenhang mit anderen Rechtsmaterien,

— die Divergenz der — auch in der Öffentlichkeit — vertretenen Auffassungen (Bd. 51 S. 291), oder

— die Belastung des Gesetzgebers (Bd. 25 S. 186)

bei der Bemessung der Frist eine Rolle gespielt.

Vor diesem Hintergrund scheint es mir vertretbar zu sein, trotz der schon einige Jahre dauernden Diskussion noch nicht vom Ablauf der Übergangszeit auszugehen. Die zu regelnde Materie ist sehr komplex und auf vielfältige Weise mit anderen Rechtsgebieten, u.a. mit dem Strafprozeßrecht, dem Verkehrs- und dem Melderecht, verzahnt. Deshalb meine ich, daß der Spielraum des Gesetzgebers noch bis zum Ablauf der laufenden Legislaturperiode reicht.

Diese Auffassung wird von einigen Gerichten allerdings nicht geteilt. Das Verwaltungsgericht Hannover (a.a.O.) war schon vor einem Jahr davon ausgegangen, eine Übergangszeit sei — wenn man sie überhaupt einräumen wollte — drei Jahre nach dem Volkszählungsurteil inzwischen abgelaufen. Auch das Verwaltungsgericht München (Bericht der Süddeutschen Zeitung vom 9. 12. 87, S. 15) nimmt den Ablauf der Übergangszeit an, nachdem der Bayerische Gesetzgeber es trotz des Urteils des Bayerischen Verfassungsgerichtshofes (a.a.O.) mehr als zwei Jahre unterlassen habe, unverzüglich gesetzliche Grundlagen für die Führung kriminalpolizeilicher Sammlungen zu schaffen.

Diese Urteile scheinen mir erste Anzeichen dafür zu sein, daß die Rechtsprechung nicht bereit ist, einen allzu großzügigen Umgang mit der Übergangszeit weiter zu dulden. Gleichgültig, ob sie von den Obergerichten bestätigt werden, sollten sie doch auch den hamburgischen Gesetzgeber ermutigen, die notwendigen Arbeiten unverzüglich in Angriff zu nehmen.

4.11.2 Einsatz von Personalcomputern

Die automatisierte Datenverarbeitung bei der Polizei hat sich bisher auf Großrechenanlagen vollzogen. Da die vorhandenen Kapazitäten z.Z offensichtlich weitgehend erschöpft sind, will die Polizei in Zukunft auch Personalcomputer für ihre Zwecke nutzen. Erstmalig wurde ich deshalb mit der Überlegung konfrontiert, daß polizeiliche Dateien, die gezielt für die Verbrechensbekämpfung verwendet werden, auf Personalcomputer abgewickelt werden sollen. Dies wirft aus meiner Sicht verschiedene Probleme auf.

Auf die besonderen Risiken, die bei der Verarbeitung personenbezogener Daten auf PC's entstehen, habe ich schon hingewiesen (vgl. 3.5.1). Es dürfte unstreitig sein, daß beim gegenwärtigen Stand der Technik die Datenverarbeitung über Personalcomputer auch bei allergrößtem Bemühen nicht den Sicherheitsstandard erreichen kann, wie er bei Großrechenanlagen erreicht ist. Dies bedeutet, daß die für polizeiliche Zwecke gesammelten — in der Regel sehr sensiblen — Daten der Betroffenen erhöhten Gefährdungen ausgesetzt sind, die sogar in Gefahren für die Betroffenen selbst umschlagen können, wenn bestimmte Informationen in die falschen Hände geraten. Darüber hinaus kann die geringere Sicherheit auch den Erfolg der polizeilichen Arbeit gefährden. Ermittlungsergebnisse, die bisher in z.T. sehr umfangreichen Akten und zusätzlich auf besonders gesicherten Magnetbändern der Großrechner dokumentiert waren, werden nunmehr auf Disketten gespeichert, die in der Hosentasche von ihrem bestimmungsmäßigen Platz entfernt werden können. Dies zeigt deutlich eine Schwachstelle der Datenverarbeitung auf Personalcomputern, die auch interessierten kriminellen Kreisen nicht verborgen bleiben wird.

Vor diesem Hintergrund habe ich gefordert, daß die Risiken durch zusätzliche technische und organisatorische Maßnahmen auf ein Mindestmaß reduziert werden. So halte ich es für erforderlich, daß durch eine Rahmenrichtlinie festgelegt wird, daß nur Programme, die nach einer Abnahmekontrolle von der fachlich zuständigen Abteilung der Landespolizeiverwaltung freigegeben wurden, verwendet werden. Dies muß durch zusätzliche technische Sicherungen gewährleistet werden. Darüber hinaus sind die einzelnen Arbeiten an den Geräten durch automatische mitlaufende Protokolle aufzuzeichnen, um in- und externe Kontrollen zu ermöglichen. Schließlich ist zu bestimmen, wie bewegliche Datenträger zu sichern sind. Letztlich ist nach meiner Auffassung für den Einsatz jedes einzelnen Verfahrens festzulegen, wer für die Einhaltung der technischen und organisatorischen Sicherheitsvorkehrungen verantwortlich ist.

Die Behörde für Inneres und die Polizei haben meine Bedenken und Anregungen konstruktiv aufgegriffen und zugesagt, ein entsprechendes Sicherungskonzept in Abstimmung mit mir in die Praxis umzusetzen. Dies halte ich für ein Beispiel, wie durch frühzeitige Beteiligung des Datenschutzbeauftragten ein angemessener Interessenausgleich geschaffen werden kann.

4.11.3 Datenverarbeitung beim polizeilichen Staatsschutz

4.11.3.1 Datenschutzrechtliche Prüfung bei der Fachdirektion 7

In der Zeit von Mai bis September 1987 habe ich die vom polizeilichen Staatsschutz geführten Dateien überprüft. Die Prüfung diente dem Ziel, einen Überblick über die Datenverarbeitung in diesem Bereich zu gewinnen und festzustellen, ob sie datenschutzrechtlichen Anforderungen genügt.

Im Hinblick auf die Massendatenverarbeitung durch die Polizei mußte sich die Prüfung von vornherein auf Stichproben und einzelne Aspekte der Datenverarbeitung beschränken. Gegenstand der Prüfung waren zwei manuell geführte Dateien sowie die Datenstruktur und einzelne Datensätze der automatisierten Datei „APIS", die bundesweit geführt wird. Dazu ist folgendes zu bemerken. Die Fachdirektion 7 der hamburgischen Polizei nimmt die Aufgaben des polizeilichen Staatsschutzes wahr. Im Rahmen dieser Aufgabe arbeitet sie eng mit dem BKA und den polizeilichen Staatsschutzdienststellen der anderen Bundesländer zusammen. Diesem Zweck dient die — auf der Grundlage des BKA-Gesetzes und der „Richtlinien für den Kriminalpolizeilichen Meldedienst in Staatsschutzsachen (KPMD-S)" geschaffene — Verbunddatei „PIOS-Innere Sicherheit (APIS)". Die APIS ist seit 2. 1. 1986 in Betrieb.

Obwohl die Beratungen mit der Behörde für Inneres über meinen Prüfbericht noch nicht abgeschlossen sind, kann schon jetzt festgestellt werden, daß die Prüfung erhebliche Mängel zutage gefördert hat.

Bei einer der manuell geführten Dateien war festzustellen, daß ohne inhaltliche Vorgaben sämtliche Personen erfaßt werden, die mit der FD 7 in Berührung kommen; sei es als Anzeigenerstatter, Zeuge, andere Person oder Verdächtiger. Dieser Mangel wird noch verstärkt durch die Tatsache, daß weder Aussonderungs- noch Überprüfungsfristen festgesetzt sind. Dies kann nicht ersetzt werden durch eine tatsächlich wohl stattfindende Überprüfung, bei der völlig unklar bleibt, nach welchen Kriterien überprüft wird. Daneben wird über sämtliche Vorgänge der FD 7 schon seit vielen Jahren eine Vorgangskartei geführt. In ihr werden zwar Aussonderungs- und Prüffristen notiert, allerdings habe ich festgestellt, daß diese Fristen für die vergangenen zwei Jahre nicht mehr überprüft wurden. Aussonderungsfristen können jedoch ihren Zweck nicht erfüllen, wenn sie nicht überwacht werden. Dies ist völlig unakzeptabel, zumal diese Datei nicht nur für sämtliche Zwecke der Vorgangsverwaltung, sondern auch zur Erteilung von Auskünften genutzt wird.

Schließlich war festzustellen, daß beide manuellen Dateien nicht aufeinander abgestimmt sind. Zunächst einmal kann beim gegenwärtigen Kenntnisstand nicht ausgeschlossen werden, daß unzulässige Mehrfacherfassungen erfolgen. Zum anderen ist durch weitere organisatorische Maßnahmen sicherzustellen, daß ausgesonderte Daten in beiden Dateien gelöscht werden.

Die APIS soll nach ihrer Errichtungsanordnung ermöglichen, in Staatsschutzssachen

— relevante Personen, Institutionen, Objekte, Sachen und Ereignisse sowie Zusammenhänge zwischen diesen zu erkennen,

— Erkenntnisse für polizei- und ermittlungstaktisches Vorgehen zu gewinnen und

— unbedeutende Informationen und Erkenntnisse auszuscheiden.

Die Datei soll Erkenntnisse über Straftaten aufnehmen, die u.a. gegen die freiheitlich demokratische Grundordnung, den Bestand und die Sicherheit des Bundes oder der

Länder und gegen die Amtsführung von Mitgliedern verfassungsmäßiger Organe des Bundes oder eines Landes gerichtet sind (sog. „klassische" Staatsschutzdelikte). Daneben sollen jedoch auch Erkenntnisse über sämtliche anderen Straftaten (von der Beleidigung über die Sachbeschädigung, den Diebstahl bis hin zur Gewaltkriminalität) gespeichert werden, wenn über die einzelne Straftat hinaus Erkenntnisse vorliegen, daß der Täter allein oder in Verbindung mit einer Organisation Ziele von Staatsschutzdelikten verfolgt oder das Objekt der Straftat solchen Verdacht begründet.

Schon während der Diskussion über die Errichtungsanordnung für APIS haben die Datenschutzbeauftragten die Befürchtung geäußert, daß unter diese Formulierung auch alle jene Straftaten und Sachverhalte subsumiert werden können, die nur ganz allgemein einen Zusammenhang mit politischen Themen haben könnten und deren Sachbearbeitung deshalb auch von den Staatsschutzdienststellen wahrgenommen wird. Aus meiner Sicht war von Anfang an zweifelhaft, ob die Regelung dem Sachbearbeiter vor Ort klare Hinweise zur Fallbehandlung an die Hand geben kann.

Diese Zweifel haben sich durch die Prüfung verstärkt. Deshalb erscheint es mir wichtig, auch an dieser Stelle ausdrücklich darauf hinzuweisen, daß weder die Richtlinien für den kriminalpolizeilichen Meldedienst in Staatsschutzsachen (KPMD-S) noch die Errichtungsanordnung für APIS die Weitergabe und Speicherung über jede (vermutete) Straftat erlauben, die im weitesten Sinne einen „politischen" Hintergrund (etwa der Protest gegen die Diskriminierung von Frauen und Kindern in der Gesellschaft) hat. APIS soll dem Erkunden und der Verfolgung staatsschutzrelevanter Sachverhalte, nicht aber der Registrierung politischer Aktivitäten dienen. Letzteres wäre mit der demokratischen Grundordnung nicht vereinbar. Deshalb ist nach meiner Auffassung bei der Speicherung von Erkenntnissen über andere Straftaten (Ziff. 2.1.10 der Errichtungsanordnung) besondere Sorgfalt geboten. Dies gilt auch wegen der zusätzlichen Stigmatisierungsgefahren, die von einer Speicherung personenbezogener Daten in das System APIS ausgehen. Letztlich muß es — unabhängig von datenschutzrechtlichen Gesichtspunkten — auch im Interesse effektiver Polizeiarbeit liegen, in der APIS, mit der ganz spezifische Ziele verfolgt werden, nur Daten mit Staatsschutzrelevanz zu speichern, da sonst sehr bald die Gefahr besteht, daß mit dieser Datei die angestrebten Ziele nicht mehr erreicht werden können.

Vor diesem Hintergrund habe ich bei der Überprüfung des Datenbestandes von APIS, bei dem Hamburg Besitz oder Mitbesitz hat, mein Augenmerk vor allem auf die „anderen Straftaten" (s.o.) gerichtet, und zwar sowohl bei der Datenstruktur wie bei den einzelnen Datensätzen.

— Datenstruktur

Im Bereich der „klassischen Staatsschutzdelikte" (Ziff. 2.1.1 bis 2.1.9 der Errichtungsanordnung) hat Hamburg im APIS-Bestand bis Ende Juli 1987 273 Notierungen gespeichert. Dagegen finden sich bei den anderen Straftaten (Ziff. 2.1.10 der Errichtungsanordnung) 1.301 Notierungen: Das sind 82,6 % des gesamten Bestandes.

Dieser hohe Anteil der „anderen Straftaten" scheint dafür zu sprechen, daß der eng begrenzte Einsatzbereich der Datei nicht voll erkannt wurde. Datenschutzrechtlich heißt das, daß offensichtlich mehr Betroffene mit dem Etikett des „Staatsfeindes" bedacht werden, als selbst nach der Errichtungsanordnung zulässig ist. Darüber hinaus besteht die Gefahr, daß ein auf diese Weise „aufgeblähter" Datenbestand in APIS rechtspolitisch als Rechtfertigung für die Einengung von Freiheitsrechten herangezogen wird. Ich habe deshalb Anlaß, dringend zu empfehlen, Erfassungs- und Speicherpraxis bei der FD 7 einer kritischen Kontrolle zu unterziehen.

— Einzelfälle

Um eine systematische Querschnittsuntersuchung zu gewährleisten, habe ich sämtliche in der Zeit vom 19. — 31. Januar 1987 von Hamburg in APIS eingestellte Datensätze anhand der vorliegenden polizeilichen Erkenntnisse überprüft. Daneben waren Gegenstand der Überprüfung Datensätze, die sich auf Erkenntnisse im

Zusammenhang mit öffentlichen Versammlungen bezogen und solche, die über Erkenntnisse für die Tage 8./9. 6. 1986 angelegt wurden (am 8. 6. 1986 fand der Polizeieinsatz auf dem Heiligengeistfeld — sog. „Hamburger Kessel" — statt). Die Ergebnisse dieser Prüfung bestätigen die zuvor schon beschriebene Tendenz.

Dabei soll noch einmal hervorgehoben werden, daß in vielen Fällen nicht etwa die polizeilichen Ermittlungen selbst Gegenstand der vorzubringenden Kritik sind, sondern die Speicherung der Erkenntnisse in der Datei APIS. So dürfte es gerechtfertigt sein, polizeiliche Ermittlungen aufzunehmen, wenn Demonstranten waffenähnliche Gegenstände mit sich führen. In den meisten Fällen ist es jedoch nicht gerechtfertigt, hierin einen staatsschutzrelevanten Sachverhalt zu sehen. Bei anderen Sachverhalten scheint die polizeiliche Bewertung, die zur Speicherung führte, völlig außer Kontrolle geraten zu sein.

So beschädigte im Oktober 1986 ein 17jähriger Schüler im Vorbeigehen mit dem Fuß ein Wahlplakat der SPD, bei der er sich später dafür entschuldigte. Ein Strafantrag wurde nicht gestellt. Obwohl der Vorgang auch nach den polizeilichen Erkenntnissen als „Dumme-Jungen-Tat" gewertet werden muß, ist der junge Mann in APIS gleichwohl als potentieller Staatsfeind gespeichert. Ich habe die unverzüglich Löschung verlangt.

Die Prüfung einzelner Datensätze betraf großenteils solche Vorgänge, die im Zusammenhang mit öffentlichen Versammlungen standen. Dabei hat sich ergeben, daß tatsächliche oder vermutete Straftaten im Vorfeld, am Rande oder innerhalb von öffentlichen Versammlungen auch dann als Staatsschutzdelikte behandelt und entsprechend gespeichert werden, wenn ein sonstiger Bezug zu Staatsschutzdelikten nicht erkennbar ist. Ich halte eine solche Praxis für bedenklich. Das Bundesverfassungsgericht hat in seinem Brokdorf-Beschluß vom 14. Mai 1985 (BVerfGE Bd. 69 S. 315 ff.) hervorgehoben, daß das Recht des Bürgers, durch Ausübung der Versammlungsfreiheit aktiv am politischen Meinungs- und Willensbildungsprozeß teilzunehmen, zu den unentbehrlichen Funktionselementen eines demokratischen Gemeinwesens gehört. Schon im Urteil zur Parteienfinanzierung (BVerfGE Bd. 20 S. 56 ff.) hatte das Gericht betont, daß sich die Einflußnahme des Bürgers auf den ständigen Prozeß der politischen Meinungsbildung in einem demokratischen Staat frei, offen, unreglementiert und grundsätzlich „staatsfrei" vollziehen müsse; um daran anknüpfend im Volkszählungsurteil (BVerfGE Bd. 65 S. 1 ff) auszuführen, daß es mit der Rechtsordnung unvereinbar wäre, den staatsfreien unreglementierten Charakter von Demonstrationen durch exessive Observationen und Registrierungen zu verändern.

Diese unzweideutige Rechtsprechung verbietet es nach meiner Auffassung, Demonstrationen und in ihrem Zusammenhang begangene Straftaten und Ordnungswidrigkeiten per se als Staatsschutzangelegenheit zu behandeln.

Damit sollen selbstverständlich nicht Straftaten anläßlich von Versammlungen heruntergespielt werden. Sie müssen — wie alle Straftaten — mit Nachdruck von der Polizei aufgeklärt werden. Aber eine Sachbeschädigung oder Beleidigung wird nicht dadurch zum Staatsschutzdelikt, daß sie im Rahmen einer Demonstration begangen wurde. Das schließt nicht aus, daß auch bei Demonstrationen Straftaten begangen werden, deren Aufklärung dem polizeilichen Staatsschutz obliegt und in APIS zu speichern sind. Die Polizistenmorde an der „Startbahn West" in Frankfurt sind ein Beispiel dafür. Aber auch unterhalb dieser Schwelle finden sich in diesem Sinne gerechtfertigte Eintragungen in APIS. Die Mehrzahl der gespeicherten Datensätze erscheint mir jedoch nicht für eine Speicherung in APIS geeignet.

Wenn man akzeptiert, daß die Polizei während der „Übergangszeit" (s. 4.11.1) auch ohne gesetzliche Grundlage personenbezogene Daten verarbeiten darf, so ist jedoch darauf hinzuweisen, daß die Rechtsprechung auch jetzt schon einen Rahmen abgesteckt hat, innerhalb dessen dies möglich ist. So ist u. a. für die Speicherung von Verdächtigen und Beschuldigten Voraussetzung, daß die Schwere der Tat oder die Täterpersönlichkeit nicht ausschließen, daß von dem Betroffenen auch in Zukunft Straftaten von erheblichem Gewicht begangen werden. Für die APIS muß hinzugefügt werden, daß eine Prognose sich auf staatsschutzrelevante Straftaten beziehen muß.

Dies bedeutet: Vorgänge, die schon von Anfang an als unbedeutend einzustufen waren, sind auch in der Datenverarbeitungspraxis anders zu behandeln als schwerwiegende Straftaten. Ermittlungsverfahren, die von der Staatsanwaltschaft oder vom Gericht mangels einer Straftat oder wegen Geringfügigkeit eingestellt wurden, müssen deshalb Konsequenzen für die gespeicherten Daten nach sich ziehen. Deshalb ordnet die Errichtungsanordnung für APIS für all diese Fallvarianten Maßnahmen zur Bestandspflege an, sei es, daß Vorgänge zu löschen sind, sei es, daß kurze Löschungsfristen zu notieren sind. Aber selbst dies ist nach den Ergebnissen meiner Prüfung in allen Fällen nicht geschehen. Einige besonders gravierende Fälle seien hier bezeichnet.

So verteilte ein Gewerkschaftssekretär im März 1986 zusammen mit Mitarbeitern anläßlich von Tarifverhandlungen Handzettel mit DAG-Aufdruck an Kunden der Deutschen Bank in der Nähe des Rathausmarktes. Ihm wurde der Vorwurf einer nicht angemeldeten Demonstration und ein Verstoß gegen das Bannmeilengesetz gemacht. Es sind schon äußerste Zweifel angebracht, ob bei der Aktion von einer Versammlung ausgegangen werden konnte, so daß der strafrechtliche Vorwurf (§ 26 VersG) konstruiert wirkt. Die Staatsanwaltschaft hat das Verfahren nach Auskunft der Behörde für Inneres wegen Geringfügigkeit eingestellt. Nach meiner Einschätzung hätte in diesem Fall eine Speicherung zu Zwecken der vorbeugenden Straftatenbekämpfung von vornherein nicht erfolgen dürfen; zumindest war eine Staatsschutzrelevanz nicht erkennbar. Auf jeden Fall hätte die staatsanwaltschaftliche Entscheidung berücksichtigt werden müssen.

In einem anderen Fall hatte der Betroffene als Versammlungsleiter eine Versammlung „Atomstopp jetzt" in der Nähe des Generalkonsulats der Vereinigten Staaten um etwa 200 m vom genehmigten Versammlungsort verlegt. Das Verfahren wurde von der Staatsanwaltschaft mangels Vorliegen einer Straftat eingestellt. Abgesehen von den von Anfang an bestehenden Zweifeln, ob der Betroffene überhaupt als Verdächtiger hätte gespeichert werden dürfen, abgesehen von der offensichtlich fehlenden Staatsschutzrelevanz, hätte der Sachverhalt nach der Errichtungsanordnung im Anschluß an die Entscheidung der Staatsanwaltschaft unverzüglich gelöscht werden müssen.

In einem dritten Fall demonstrierte eine ehemalige Bürgerschaftsabgeordnete im Mai 1986 zusammen mit 9 weiteren Personen gegen 22.45 Uhr auf einem Bahnsteig des U-Bahnhofs Jungfernstieg gegen die „Gewalt gegen Frauen". Nach einem Bericht der Polizei kam es nicht zu einer Behinderung des U-Bahnverkehrs bzw. zu irgendwelchen anderen Störungen. Eine Einordnung dieses Sachverhalts als Staatsschutzdelikt war offensichtlich nur möglich, weil der Betroffenen Verbindungen zu einer ausländischen (extremen) politischen Organisation unterstellt wurden. Dafür gibt es jedoch nicht die geringsten Anhaltspunkte.

Ein anderer Betroffener zerstörte anläßlich einer Demonstration gegen das „Atomprogramm" und gegen den „Hamburger Kessel" mit einer brennenden Zigarette drei aufgeblasene Luftballons an einem Informationsstand der CDU. Hier drängt sich die Frage auf, wer alles damit rechnen muß, als gefährlicher „Staatsfeind" qualifiziert zu werden, wenn selbst dieser läppische Sachverhalt geeignet ist, in die hochspezialisierte Staatsschutzdatei aufgenommen zu werden.

Dies gilt auch für Fälle, bei denen im Rahmen der Durchsuchung von jungen Frauen aus dem „Hamburger Kessel" Reizgasflaschen gefunden wurden, die von der Polizei eben diesem Personenkreis zum Schutz vor Gewalttaten empfohlen, bei Demonstrationen aber plötzlich zu verbotenen Waffen werden. Die Speicherung in APIS belegt, daß die Polizei auch hier davon ausgeht, der Staat könnte von diesen Frauen besonders gefährdet sein.

Besonders verärgert bin ich über einen Fall, in dem sich die Mutter der Betroffenen auch an mich gewandt hatte. Aufgrund der Eingabe wurde von der Landespolizeidirektion die Vernichtung der erkennungsdienstlichen Unterlagen und die Löschung der

POLAS-Eingaben verfügt und dies der Betroffenen mitgeteilt. Gleichwohl wurde die gravierendere Speicherung in APIS, von der weder die Betroffene noch ich etwas ahnen konnten, aufrechterhalten.

In allen von mir beschriebenen Einzelfällen habe ich die Löschung der entsprechenden Datensätze gefordert. Darüber hinaus ist durch weitere organisatorische Maßnahmen sicherzustellen, daß Fehlspeicherungen auf ein Mindestmaß reduziert und die Aktualisierung und Bereinigung des Datenbestandes gewährleistet werden.

4.11.3.2 Speicherung von Volkszählungsgegnern

Die von mir beschriebene teilweise recht undifferenzierte Speicherungspraxis durch die FD 7 scheint sich auch bei der Erfassung und Speicherung von Volkszählungsgegnern fortgesetzt zu haben. Während mir noch am Anfang der datenschutzrechtlichen Prüfung mündlich versichert worden war, daß Aktivitäten von Volkszählungsgegnern, die nicht in Gewalttaten einmünden, nicht in APIS gespeichert würden, mußte die Behörde für Inneres im Juli 1987 einräumen, daß bis Ende Juni 1987 schon Daten über 53 Personen gespeichert waren. Daraufhin habe ich im August um die Übersendung eines Ausdrucks sämtlicher Datensätze gebeten. Dies ist bis zum Redaktionsschluß für diesen Bericht nicht geschehen. Erst am 23. Dezember ist mir eine — schon um 5 Notierungen bereinigte — Liste sämtlicher erfaßter Personen (insgesamt 105) übersandt worden, die nur eine begrenzte Aussagekraft hat. Aufgrund telefonischer Erläuterungen zu dieser Liste steht jedoch fest, daß in APIS auch solche Personen erfaßt wurden, die lediglich die auf den Volkszählungsbogen vermerkten Kennziffern herausgeschnitten hatten, und sogar solche, die dazu aufgerufen hatten. Ich halte diese Speicherungen für unzulässig, da die Voraussetzungen für die weitere Nutzung von Strafermittlungsdaten (s. 4.11.3.1) nicht vorliegen. Schon gar nicht können in solchen Handlungen Angriffe auf die freiheitlich demokratische Grundordnung oder verfassungsmäßige Einrichtungen gesehen werden. Sie entsprechen deshalb auch nicht der Errichtungsanordnung für APIS. Inzwischen hat der Polizeipräsident angeordnet, daß die Datensätze über Personen, denen nur Sachbeschädigung vorgeworfen wird und „ähnliche Fälle" zu löschen sind. Dies hat nach meinen Feststellungen zur Löschung von 51 Datensätzen geführt. Die restlichen 54 Datensätze werde ich einzeln auf ihre Vereinbarkeit mit der Errichtungsanordnung für APIS überprüfen.

4.11.3.3 Übermittlung polizeilicher Erkenntnisse an den Verfassungsschutz

— Sicherheitsüberprüfungen

Gemäß § 3 Abs. 2 Nr. 1 u. 2 des Gesetzes über den Verfassungsschutz in Hamburg wirkt das Landesamt für Verfassungsschutz (LfV) mit an Überprüfungen von Personen, denen geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse anvertraut werden, oder die an sicherheitsempfindlichen Stellen von lebens- und verteidigungswichtigen Einrichtungen beschäftigt sind oder werden sollen. Dabei fordert es die FD 7 mit einem Vordruck auf, dort bekannte relevante Sachverhalte mitzuteilen. Von mir vorgenommene Überprüfungen einzelner Mitteilungen haben keine Sachverhalte erbracht, die zu beanstanden wären. Allerdings werden Durchschriften sämtlicher Mitteilungen an das LfV mit konkreten Erkenntnissen der Polizei bei der FD 7 unbegrenzt verwahrt. Vernichtungsfristen bestehen nicht. Dies müßte geändert werden. Zumindest ist sicherzustellen, daß die Durchschriften dann zu vernichten sind, wenn die den Mitteilungen zugrunde liegenden polizeilichen Erkenntnisse auszusondern, zu vernichten und zu löschen sind.

— Informationsberichte der FD 7

Seit 1968 verteilt die Staatsschutzabteilung der Polizei mehrfach wöchentlich sogenannte Informationsberichte (IB) über laufende Ermittlungsverfahren an diverse in- und ausländische Dienststellen, u.a. an das LfV. Mit den IB werden auch personenbezogene Daten übermittelt. Über diese Praxis und die dagegen von mir vorgebrachten Bedenken habe ich ausführlich in meinem 3. TB (3.8.4, S. 74 ff.) berichtet. Konsequenzen sind daraus nicht gezogen worden. Sowohl die Praxis wie die Bedenken bestehen fort.

— Übermittlungen im Einzelfall

Darüber hinaus unterrichtet die FD 7 das LfV gezielt über Erkenntnisse aus einzelnen Ermittlungsverfahren, wenn sie der Auffassung ist, daß Aufgaben des Verfassungsschutzes berührt sind.

Für sämtliche Übermittlungen der Polizei an das LfV stehen hinreichende gesetzliche Grundlagen, die diese Informationsbeziehungen normenklar regeln, nicht zur Verfügung. Neben einer unzureichenden Amtshilfevorschrift in § 5 des Gesetzes über den Verfassungsschutz in der Freien und Hansestadt Hamburg kann nur auf die Richtlinien für die Zusammenarbeit der Verfassungsschutzbehörden, des Bundesnachrichtendienstes (BND), des Militärischen Abschirmdienstes (MAD), der Polizei und der Strafverfolgungsbehörden in Staatsschutzangelegenheiten (Zusammenarbeitsrichtlinien) vom 18. September 1970 in der Fassung vom 23. 7. 1973 zurückgegriffen werden. Nach deren §§ 8 und 11 i.V.m. § 4 hat die Polizei das LfV (und andere Verfassungsschutzbehörden) über alle Erkenntnisse stets dann zu unterrichten, wenn die Zuständigkeit des LfV berührt sein könnte. Die Unterrichtungspflicht gilt auch in allen Zweifelsfällen. Unabhängig davon, daß Richtlinien nicht als Grundlage für Grundrechtseingriffe herangezogen werden können, habe ich schon mehrfach darauf hingewiesen, daß eine derart unpräzise und konturenlose weite Richtlinie völlig ungeeignet ist, die heiklen Informationsbeziehungen zwischen Polizei und Verfassungsschutz zu regeln. Da eine Präzisierung der Richtlinien auf Bundesebene kurzfristig nicht zu erreichen ist, müssen jedenfalls für die Beziehungen der hamburgischen Behörden untereinander eindeutige Regelungen geschaffen werden. Da auch mit einer alsbaldigen Novellierung des Hamburgischen SOG und des Hamburgischen Verfassungsschutzgesetzes nicht gerechnet werden kann, sollte die Behörde für Inneres für die Übergangszeit wenigstens in Form von Verwaltungsvorschriften präzisere Regelungen schaffen.

— Übermittlungen des APIS-Bestandes vom Bundeskriminalamt (BKA) an das Bundesamt für Verfassungsschutz (BfV)

Der Kreis der fast lückenlosen Informationsübermittlungen von Staatsschutzerkenntnissen an den Verfassungsschutz schließt sich, wenn eine Praxis berücksichtigt wird, über die der Bundesbeauftragte für den Datenschutz in seinem 9. TB berichtet hat und die inzwischen in der Stellungnahme der Bundesregierung zu diesem Bericht bestätigt wurde. Danach werden vom Bundeskriminalamt sämtliche Personalien von Beschuldigten und Verdächtigen, die in APIS — bzw. bei nachrichtendienstlichen Hintergrund in der Arbeitsdatei „PIOS — Landesverrat (APLV)" — erfaßt werden, mit der jeweiligen Aktenfundstelle, auch in das Informationssystem der Verfassungsschutzämter NADIS (vgl. dazu 1. TB, 6.7.3, S. 43 f.) eingestellt. Auf diesem Umweg werden auch dem hamburgischen Landesamt für Verfassungsschutz Informationen zur Verfügung gestellt, die ihm direkt nicht übermittelt werden und auch nicht übermittelt werden dürfen. Diese Praxis, die ich für verfassungswidrig halte, führt die gesamte bisherige Diskussion zum Trennungsgebot ad absurdum.

Nicht einmal der heftig kritisierte Entwurf eines Zusammenarbeitsgesetzes (ZAG) hätte eine so weitgehende Übermittlung von polizeilichen Erkenntnissen an die Verfassungsschutzbehörden zugelassen. Diesem „Mangel" will die Bundesregierung nunmehr offensichtlich abhelfen. Während der ZAG-Entwurf noch darauf abstellte, daß Übermittlungen nur dann zulässig sein sollten, wenn sie zur Terrorismus- und Spionagebekämpfung erforderlich sind, sollen mit dem als Nachfolger für das ZAG gedachten Verfassungsschutzmitteilungsgesetz — VerfSchMiG — (Stand: 16. Oktober 1987) sämtliche Informationsschranken zwischen Polizei und Geheimdiensten niedergerissen werden. Damit wird sich meine schon gegen den ZAG-Entwurf vorgebrachte Kritik (vgl. 4. TB, 4.10.6, S. 82 ff.) noch verstärken müssen, die darin bestanden hat, daß die Konturen des Trennungsgebotes verwischt würden und eine nachvollziehbare Unterscheidung von Aufgaben und Befugnissen der verschiedenen Sicherheitsbehörden faktisch nicht mehr erkennen ließen.

Obwohl sich der von mir beschriebene, jetzt schon praktizierte Informationsaustausch auf Bundesebene vollzieht, bin ich der Auffassung, daß die FD 7 diesen Hintergrund auch bei der eigenen Speicherpraxis zu berücksichtigen hat, weil sie auf diesem Umweg sämtliche Daten über Beschuldigte und Verdächtige ohne Einzelfallprüfung auch dem LfV übermittelt. Die Daten einer jungen Frau mit Gassprühflasche haben schon nichts in einem polizeilichen Informationssystem, erst recht aber nichts in NADIS zu suchen.

4.11.4 Erfassung von Angehörigen arabischer Staaten

Im August 1987 wurde ich von dritter Seite auf die massenhafte Erfassung von Angehörigen arabischer Staaten, an der auch Hamburg beteiligt war, aufmerksam gemacht. Nachdem ich mir über die Beteiligung hamburgischer Dienststellen Klarheit verschafft hatte, informierte ich den Bundesbeauftragten für den Datenschutz (BfD), da die Aktion offensichtlich vom Bundeskriminalamt koordiniert wurde. Die anschließenden Beratungen im Innenausschuß des Deutschen Bundestages, eine Prüfung des BfD und meine Feststellungen haben folgenden Sachverhalt geklärt.

Seit Mai 1986 wurden in der Datei „Grenzpolizeiliche Ein-/Ausreisekontrolle — GEAK" personenbezogene Daten von Angehörigen verschiedener arabischer Staaten bei der Ein- und Ausreise sowie bei der Zurückweisung gespeichert. Während zwischenzeitlich bis zu 20 arabische Staaten betroffen waren, wurden zuletzt noch Staatsangehörige aus Libyen, Libanon, Syrien, Tunesien und Marokko erfaßt. Begründet wurde die Erfassung mit der in den Jahren 1985/86 zunehmenden terroristischen Bedrohung aus den arabischen Staaten, die aus verschiedenen Anschlägen im In- und Ausland gefolgert wurde. Der Bundesinnenminister erhoffte sich durch die Datei in Fällen drohender oder erfolgter Anschläge die Unterstützung präventiver oder repressiver Maßnahmen. Erst Ende August 1987 — also etwa 15 Monate nach Einrichtung der Datei — wurde eine nach den Dateirichtlinien erforderliche Errichtungsanordnung erlassen. Da die Datei beim BKA geführt wurde, dem BKA aber dafür keine Kompetenzen zustanden, wurde mit der Errichtungsanordnung der Versuch unternommen, eine Auftragsdatenverarbeitung durch das BKA für die Grenzschutzdirektion zu konstruieren. In Übereinstimmung mit dem BfD halte ich diese Konstruktion für unhaltbar. Der BfD hat bei der Prüfung darüber hinaus festgestellt, daß das BKA die Datei nicht nur wie eine eigene behandelt und genutzt hat, sondern darüber hinaus sogar der Grenzschutzdirektion als angeblichen Auftraggeber einen direkten Zugriff auf diese Datei verwehrt hat. Der BfD hat die Führung und Nutzung von GEAK beanstandet; der Bundesinnenminister hat im Oktober 1987 mitgeteilt, daß er es für vertretbar halte, die Fortführung der Datei auszusetzen und deshalb ihre Einstellung angeordnet habe. Bis zu ihrer Einstellung konnte mit der Datei nicht ein einziger polizeilicher Erfolg erzielt werden.

Neben GEAK bestand beim BKA eine Spuren- und Hinweisdokumentationsdatei FAMAL, mit deren Hilfe zwei Morde an libyschen Staatsangehörigen aufgeklärt werden sollten. In dieser Datei wurden gesondert Sichtvermerksanträge sowie Ein- und Ausreisen libyscher Staatsangehöriger erfaßt. Auch hier wurde versucht, das BKA als Auftragnehmer — diesmal für das Bundesverwaltungsamt als Dienststelle, die das Ausländerzentralregister unterhält — darzustellen. Dieser Versuch des BKA, sich Befugnisse anzueignen, ist ebenso fragwürdig wie die „Auftragslösung" bei der GEAK. Nachdem der BfD auch diese Datei beanstandet hat, hat der Bundesinnenminister mitgeteilt, daß nach der inzwischen abgeschlossenen Auswertung ein Großteil der Daten in FAMAL gelöscht seien.

An der Auffüllung des Datenbestandes der Datei GEAK war auch die Wasserschutzpolizei Hamburg beteiligt. Zwar wurden in der Innenbehörde zunächst sowohl rechtliche als auch polizeitaktische Einwände gegen die Erfassung des betroffenen Personenkreises erörtert, seit November 1986 war aber auch Hamburg bereit, daran mitzuwirken. Nachdem ich dies etwa 9 Monate später von dritter Seite (!) erfahren hatte, habe ich die Mitwirkung Hamburgs noch im August 1987 gegenüber der Behörde für Inneres als rechtswidrig bemängelt und sie dringend gebeten, die Beteiligung der Wasser-

schutzpolizei Hamburg noch einmal zu überprüfen. Bis auf eine kurze Zwischennachricht habe ich auf mein Schreiben bis Ende 1987 keine Antwort erhalten. Ich habe u. a. darauf hingewiesen, daß eine konkrete Gefahr, wie sie Voraussetzung für die Speicherung von Daten aller ein- und ausreisenden Araber oder auch der Angehörigen bestimmter arabischer Staaten wäre, auch nicht andeutungsweise erkennbar war. Darüber hinaus konnte ich — auch nach den Erfahrungen, die in der Zwischenzeit gesammelt worden waren — nicht nachvollziehen, daß das zur Gefahrenabwehr eingesetzte Mittel geeignet, erforderlich oder gar verhältnismäßig war. Ich bemängelte, daß hier ein Datenlager gigantischen Ausmaßes entstanden sei, für das es unter keinem polizeilichen Gesichtspunkt eine Rechtfertigung gebe.

Auch wenn inzwischen die rechtswidrigen Maßnahmen eingestellt wurden, ist aus meiner — und aus hamburgischer — Sicht auf folgende nachwirkende Problematik aufmerksam zu machen. Dabei geht es um die Einbindung der hamburgischen Wasserschutzpolizei in grenzpolizeiliche Aufgaben. Diese obliegen nach § 1 Bundesgrenzschutzgesetz — BGSG — im Regelfall dem Bundesgrenzschutz. Nach § 1 Nr. 1 BGSG kann auch ein Bundesland mit eigenen Kräften im Einvernehmen mit dem Bund Aufgaben des grenzpolizeilichen Einzeldienstes wahrnehmen. Das Einvernehmen ist gem. § 63 Abs. 1 BGSG in einer schriftlichen Vereinbarung zwischen dem Bundesminister des Innern und dem beteiligten Land herzustellen, die im Bundesanzeiger bekanntzugeben ist. Eine solche Vereinbarung wurde für Hamburg mit dem „Verwaltungsabkommen über die Wahrnehmung der polizeilichen Kontrolle des grenzüberschreitenden Verkehrs im Hamburger Hafen" vom 22. Januar 1974 (BAnz Nr. 18 vom 26.1.1974) geschlossen, in dem die der Hamburger Wasserschutzpolizei übertragenen Aufgaben beschrieben sind. Die dem Bundesgrenzschutz zur Erfüllung grenzpolizeilicher Aufgaben durch Gesetz übertragenen Befugnisse sind der hamburgischen Polizei durch das Abkommen indessen nicht übertragen worden. Sie durften auf diese Weise auch nicht übertragen werden, denn kraft ausdrücklicher gesetzlicher Bestimmung (§ 63 Abs. 4 BDSG) richten sich die Befugnisse bei Wahrnehmung der übertragenen Aufgaben ausschließlich nach Landesrecht. Das hamburgische Landesrecht aber stellt hinreichende Befugnisse, die beispielsweise die Mitwirkung beim Aufbau von GEAK erlaubt hätten, nicht zur Verfügung. Insbesondere fehlt es an Befugnissen, die dem Anhalterecht des BGS nach § 17 BGSG entsprechen. Auf diese Problematik habe ich die Behörde für Inneres schon 1984 aufmerksam gemacht. Dies hat zum Entwurf eines § 16 m für das HmbSOG (Stand: 20. 8. 85) bzw. § 16 n (Stand: 2. 12. 85) geführt, mit dem dieses Defizit beseitigt werden sollte. Unabhängig von der Frage, ob die damals vorgesehene Lösung als gelungen bezeichnet werden kann, bleibt festzuhalten, daß auch sie — wäre sie im letzten Jahr in Kraft gewesen — die Beteiligung der hamburgischen Wasserschutzpolizei an der GEAK nicht erlaubt hätte.

Im übrigen hat auch dieser Fall wieder gezeigt, daß ich über wichtige Vorhaben mit datenschutzrechtlicher Relevanz von der Behörde für Inneres oft unzureichend, zu spät oder gar nicht informiert werde. Dafür habe ich in diesem, aber auch in früheren Berichten viele Beispiele benannt. Da die Beteiligung des Datenschutzbeauftragten in solchen Fällen nicht konkret geregelt, sondern als allgemeine Unterstützungsaufgabe nur abstrakt umrissen ist (§ 20 Abs. 4 S. 1 HmbDSG) und auch meine bisherigen Tätigkeitsberichte nichts an dem Zustand haben ändern können, bleibt mir nur ein erneuter Appell an den Innensenator, durch rechtzeitige Information eine vertrauensvolle Zusammenarbeit zu unterstützen und so auch schutzwürdigen Belangen der Betroffenen gerecht zu werden.

4.11.5 Personenfeststellungsverfahren

Im Rahmen strafrechtlicher Ermittlungen (§§ 81 b 1. Alt., 163 b StPO) oder für Zwecke des Erkennungsdienstes (§ 81 b 2. Alt. StPO) ist die Polizei befugt, die Identität von Betroffenen festzustellen. Das geschieht in der Regel durch Vorlage eines gültigen Ausweispapiers. Wenn Zweifel an der Identität einer Person bestehen, wird ein Personenfeststellungsverfahren durchgeführt. Zweifel an der Identität einer Person können bestehen bei

— Verdacht falscher Personalienangaben

— Personalienverweigerung

— Zweifeln an der Richtigkeit der Ausweispapiere oder

— Ausweislosigkeit.

Das Personenfeststellungsverfahren besteht u.a. aus der Vorlage von Fotografien der Betroffenen bei Angehörigen und anderen Auskunftspersonen, die die Person kennen.

Es liegt auf der Hand, daß dieses Verfahren als besonders intensiver Eingriff in das informationelle Selbstbestimmungsrecht zu werten ist, da auf diesem Wege ggf. Freunde, Verwandte, Nachbarn und Arbeitgeber des Betroffenen von polizeilichen Ermittlungen zu seinem Nachteil erfahren. Ich bin deshalb der Auffassung, daß das Personenfeststellungsverfahren aus Gründen der Verhältnismäßigkeit nur dann durchgeführt werden darf, wenn auf andere Art und Weise berechtigte Zweifel an der Identität der Betroffenen nicht ausgeräumt werden können. Insbesondere ist diesen Personen zuvor selbst Gelegenheit zu geben, an ihrer Identitätsfeststellung mitzuwirken, die zunächst nur daran gescheitert sein mochte, daß ein Ausweispapier zum Zeitpunkt der Identitätsprüfung nicht zur Verfügung stand.

Auf meine Intervention hatte die Behörde für Inneres schon Ende 1986 zugesichert, das Personenfeststellungsverfahren zu ändern. Gleichwohl hat eine im März des Berichtsjahres von mir durchgeführte Prüfung immer noch erhebliche Mängel bei der Durchführung dieses Verfahrens ergeben. Von einer förmlichen Beanstandung habe ich jedoch abgesehen, da mir die Polizei versicherte, daß das Verfahren nunmehr durch schriftliche Fachanweisung geändert werde, und mir gleichzeitig den Entwurf für die Anweisung übergab.

Nach dem neuen Verfahren wird dem Betroffenen grundsätzlich die Möglichkeit eingeräumt, selbst zur Identifizierung beizutragen, ohne daß ein Lichtbild bei anderen Personen vorgelegt wird.

Das soll insbesondere dann geschehen, wenn der Betroffene zwar kein gültiges Ausweispapier, jedoch andere Papiere wie Führerschein, Betriebsausweis, HHA-Zeitkarte o.ä. vorzeigt, oder seine Angaben zur Person in anderer Weise, etwa durch Anfrage beim Einwohnerzentralamt glaubhaft gemacht werden können. In diesen Fällen kann der Betroffene ein gültiges Ausweispapier innerhalb einer angemessenen Frist (etwa 8 Tage) bei der Polizei vorlegen. Wenn der Betroffene seine Wohnung in der Nähe der Dienststelle hat, die die erkennungsdienstliche Behandlung anordnet, kann er die erforderlichen Ausweispapiere auch sofort dort vorlegen.

Die Vorlage von Lichtbildern bei anderen Personen ohne ausdrückliche Einwilligung des Betroffenen ist nun auch nach Auffassung der Polizei nach dem Grundsatz der Verhältnismäßigkeit als letztes Mittel anzusehen, wenn eine Identifizierung sonst nicht möglich ist.

Gegen dieses Verfahren sind aus datenschutzrechtlicher Sicht durchgreifende Bedenken nicht mehr zu erheben. Von seiner Einhaltung werde ich mich jedoch durch eine erneute Prüfung überzeugen.

4.11.6 Aufarbeitung des „Hamburger Kessels" durch die Gerichte

In meinem letzten Tätigkeitsbericht (5.8.2, S. 68 ff.) habe ich umfassend über die datenschutzrechtlichen Probleme berichtet, die durch den Polizeieinsatz auf dem Heiligengeistfeld vom 8. 6. 1986 aufgeworfen wurden. Inzwischen haben die hamburgischen Gerichte rechtskräftig meine Auffassung bestätigt, daß auf dem Heiligengeistfeld eine Versammlung i.S.d. Versammlungsrechts stattgefunden hatte und daß deshalb die Anwendung des allgemeinen Polizeirechts ausgeschlossen (Verwaltungsgericht Hamburg, Urt. v. 30. 10. 86 — 12 VG 244286 — in: NVwZ 1987 S. 829 ff; Landgericht Hamburg, Urt. v. 6. 3. 87 — 3 O 22986 — in: NVwZ 1987 S. 833 f.) und die Feststellung der Identität der Betroffenen unzulässig war (Landgericht Hamburg, a.a.O.). Da das Land-

gericht Hamburg die Einschließung und Ingewahrsamnahme der Teilnehmer darüber hinaus als schuldhafte Amtspflichtverletzung angesehen hat, hat es den jeweiligen Klägern für die erlittenen Rechtsbeeinträchtigungen ein Schmerzensgeld in Höhe von DM 200,-- zugesprochen.

4.11.7 Löschung von Daten über Suizidversuche

Bekanntlich hatte der Senat im Januar 1986 beschlossen, auf die Speicherung von Suizidversuchen in Zukunft zu verzichten und die zur Zeit noch gespeicherten Hinweise zu löschen. Da diese Daten in den polizeilichen Auskunftssystemen nicht gesondert abrufbar sind, kann die Löschung nur bei Gelegenheit eines Zugriffs aus anderem Grund auf einen entsprechenden Datensatz erfolgen. So wird seit Mai 1986 verfahren. Eine Überprüfung im Februar des Berichtsjahres hat ergeben, daß bis zum 25. 2. 1987 der personengebundene Hinweis „Freitodgefahr" in 7.008 (!) Fällen in POLAS-Datensätzen und den dazugehörenden Kriminalakten bei Gelegenheit des Zugriffs gelöscht wurden. Ich werde die Löschungen weiter überwachen.

4.11.8 Polizei in der Zentralambulanz für Betrunkene (ZAB)

In meinem letzten Tätigkeitsbericht (5. TB, 5.8.8, S. 74) hatte ich bemängelt, daß von allen Patienten, die in die ZAB eingeliefert werden, Identifizierungsdaten erhoben und diese mit polizeilichen Auskunftsystemen abgeglichen werden.

Nach weiteren Gesprächen im Laufe des Berichtsjahres hat die Gesundheitsbehörde zugesichert, in Zukunft darauf zu achten, daß das regelhafte Abgleichen von Patientendaten durch den Polizeiposten nicht mehr möglich ist. Die Behörde für Inneres hält den Polizeiposten unter diesen Bedingungen nicht mehr für erforderlich und strebt seine Auflösung an. Die Entwicklung werde ich weiter beobachten.

4.11.9 Personengebundene Hinweise (PHW)

Über die Problematik der personengebundenen Hinweise habe ich schon früher berichtet (3. TB, 3.8.1.1, S. 66 f.). Sie ist bei der Diskussion über die Speicherung von HIV-Hinweisen in polizeilichen Informationssystemen (vgl. 4.15.1) jetzt wieder deutlich geworden. Im einzelnen geht es um folgendes.

Im INPOL-Verbund sind vier Dateien bundesweit zusammengefaßt: Personenfahndung, Kriminalaktennachweis, Haftdatei sowie die Datei Erkennungsdienst (zum Inhalt der Dateien vgl. 3. TB, 3.8.1.2 — 3.8.1.5, S. 67 ff.). Bei den genannten Anwendungen handelt es sich zwar um logisch voneinander getrennte Dateien; diese werden jedoch in einer gemeinsamen Datenbank und verfahrenstechnisch mit einer einheitlichen Datensatz-Struktur geführt: Die Personen- (Identifikations-) Daten („rechtmäßige Personalien") werden nur einmal in das Datenbanksystem eingestellt und die zusätzlichen Informationen (Fahndung, Haft, ED etc.) werden als Datengruppe angehängt. Die Datengruppe „rechtmäßige Personalien" enthält im Datenfeld PHW auch sog. personengebundene Hinweise. Bis Juni 1987 waren Hinweise auf folgende Umstände vorgesehen:

— bewaffnet,

— gewalttätig,

— Ausbrecher,

— Betäubungsmittel-Konsument,

— Freitodgefahr,

— Ansteckungsgefahr,

— geisteskrank,

— geistesschwach,

— entmündigt,

— Prostitution,

— internationaler Rechtsbrecher,

— Land- oder Stadtstreicher,

— häufig wechselnder Aufenthaltsort.

Diese Hinweise sind von mir und den anderen Datenschutzbeauftragten immer kritisch hinterfragt worden. So hat z.B. der Senat nach jahrelanger Diskussion zwischen mir und der Innenbehörde im Januar 1986 beschlossen, auf die Speicherung des PHW's „Freitodgefahr" in Zukunft zu verzichten. Von den anderen Bundesländern wird er immer noch eingestellt. Nach Meinung der Polizei sind die personengebundenen Hinweise erforderlich zur

— Eigensicherung des einschreitenden Beamten,

— Einleitung gezielter Fahndungsmaßnahmen,

— Unterstützung der polizeilichen Ermittlungen und

— zum Schutz des Betroffenen bei polizeilichen Maßnahmen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einem Beschluß vom 15. 11. 1985 auf die Gefahr hingewiesen, daß diese Hinweise zu einer sozialen Abstempelung der betroffenen Personen führen kann und daß polizeiliche Maßnahmen nur aufgrund des Dateiinhalts ergriffen werden. Sie war der Ansicht, daß polizeiliche Entscheidungen und insbesondere polizeiliches Einschreiten nur ausnahmsweise auf den Inhalt von Nachweisdateien gestützt werden dürfen, in der Regel jedoch Auskunft aus der Akte eingeholt werden muß. Die PHW sind keine geeignete Entscheidungsgrundlage, weil sie nur bruchstückhafte Informationen darstellen und ihre ständige Aktualisierung nicht gewährleistet ist.

Die Datenschutzbeauftragten halten die Speicherung derartiger Hinweise allenfalls dann für zulässig, wenn dies zur Erreichung des mit der betreffenen Datei verfolgten Zwecks im jeweiligen Einzelfall unabdingbar ist. Danach dürfen personengebundene Hinweise also nur in solchen Dateien niedergelegt werden, die als alleinige Grundlage für ein polizeiliches Einschreiten in Betracht kommen (z.B. die Personenfahndungsdatei). Bei einer Abwägung der erkennbaren Interessen der Polizei an schnell verfügbaren Informationen mit der Gefahr unangemessener Stigmatisierungen der Betroffenen sahen die Datenschutzbeauftragten insbesondere die folgenden PHW nicht als erforderlich an:

— geistesschwach,

— entmündigt,

— Prostitution,

— internationaler Rechtsbrecher,

— häufig wechselnder Aufenthalt,

— Land- und Stadtstreicher.

Nunmehr kann ich berichten, daß auch die Innenverwaltungen in eine Überprüfung der Erforderlichkeit von personengebundenen Hinweisen eingetreten sind. Im Juni 1987 wurden die Hinweise „geistesschwach", „entmündigt" und „internationaler Rechtsbrecher" gestrichen. Eine von der Innenministerkonferenz eingesetzte Arbeitsgruppe hat darüber hinaus vorgeschlagen, in Zukunft auf die PHW „häufig wechselnder Aufenthalt" und „Land- und Stadtstreicher" zu verzichten. Auch soll sichergestellt werden, daß die für die Vergabe des PHW verantwortliche Dienststelle erkennbar und dort die Zulässigkeit des Hinweises überprüfbar bleibt. Weiter sollen für die einzelnen Hinweise differenzierte Löschungsfristen vergeben werden. Abschließend war die Arbeitsgruppe mehrheitlich der Auffassung, daß die Hinweise bei der Haftdatei und der Datei Erkennungsdienst keine Bedeutung haben und sie in Zukunft nur noch in den Kriminalaktennachweis und in die Personenfahndungsdatei eingestellt werden sollen.

Diese Vorschläge sind zu begrüßen. Sie tragen vielen Bedenken der Datenschutzbeauftragten Rechnung. Es bleibt abzuwarten, ob und wann sie von der Innenministerkonferenz beschlossen und in die Praxis umgesetzt werden, zumal sie auch weitreichende Änderungen in der Technik des INPOL-Verbundes erfordern. Es wäre zu begrüßen, wenn sich die Innenministerkonferenz entschließen könnte, auch auf die Hinweise „Prostitution" und „Freitodgefahr" zu verzichten. Auch die Aufnahme der PHW in den Kriminalaktennachweis ist aus meiner Sicht nicht erforderlich.

4.12 Verfassungsschutz

4.12.1 Auskunftsrechte der Bürger

Ein Dauerthema datenschutzrechtlicher Bemühungen (vgl. zuletzt 5. TB, 5.9, S 76 ff) ist das Bestreben, die Auskunftsrechte der Bürger gegenüber den Verfassungsschutzbehörden den verfassungsungsrechtlichen Erfordernissen anzupassen. Im letzten Tätigkeitsbericht (s. o.) hatte ich darauf hingewiesen, daß zu dieser Frage ein Verfahren beim Bundesverfassungsgericht anhängig ist, in dem auch ich mich geäußert habe. Eine Entscheidung ist bisher nicht ergangen.

In meiner Auffassung, die ich gegenüber dem Bundesverfassungsgericht geäußert habe, bin ich weitgehend bestätigt worden durch ein Urteil des Oberverwaltungsgerichtes Bremen vom 24. 2. 1987 (NJW 1987, S. 2393 ff), mit dem das Gericht seine bisherige Rechtsprechung fortentwickelte. Darin wird in erfreulicher Klarheit nochmal darauf hingewiesen, daß der datenschutzrechtliche Auskunftsanspruch eine wesentliche verfahrensrechtliche Vorkehrung zum Schutze des Rechts auf informationelle Selbstbestimmung und eines effektiven Rechtsschutzes ist und die Verfassungsschutzbehörden deshalb verpflichtet sind, den Konflikt zwischen den Datenschutzrechten der Betroffenen einerseits und den Geheimhaltungsinteressen des Verfassungsschutzes andererseits unter Beachtung des Verhältnismäßigkeitsprinzips zu einem möglichst schonenden Ausgleich zu bringen. Das bedeutet nach Auffassung des OVG Bremen, daß z.B. bei einem auf einen bestimmten Tatbestand bezogenen Auskunftsbegehren — namentlich wenn der Anfragende weiß oder vermutet, daß Informationen über ihn gespeichert sind — die Auskunft nur verweigert werden darf, wenn dafür triftige Gründe bestehen und einleuchtend dargelegt werden. Auch gesteigerte Auskunftsinteressen der Antragsteller, die auf besonderen Umständen (z.B. erschwerte Arbeitsplatzsuche, drohender Arbeitsplatzverlust, gesundheitliche Beeinträchtigung, Herabsetzungen in der Öffentlichkeit) haben danach die Verfassungsschutzbehörden zu veranlassen, besonders sorgfältig abzuwägen, ob ein bestehendes Geheimhaltungsinteresse die mit einer Auskunftsverweigerung verbundenen persönlichen Belastungen der betroffenen Bürger rechtfertigen kann. Lediglich bei Informationen über Bestrebungen, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen verfolgt werden, oder über geheimdienstliche Tätigkeiten mochte das Gericht ein in der Regel striktes Geheimhaltungsbedürfnis anerkennen.

Den Verfassungsschutzbehörden fällt es jedoch schwer, ihre Auskunftspraxis diesen rechtstaatlichen Vorgaben anzupassen. So mußte ich im Falle eines Petenten auf der Freigabe einer Auskunft bestehen, obwohl diesem sogar ein Datenauszug des Verfassungsschutzes von anderer Seite zugespielt worden und dies dem Landesamt für Verfassungsschutz (LfV) bekannt war. Da auch das LfV einsehen mußte, daß in solchen Fällen die Gefahr der Ausforschung der Tätigkeit des Verfassungsschutzes nicht besteht, hat es schließlich einer eingeschränkten Auskunft an den Betroffenen zugestimmt.

In einem weiteren Fall hatte zwar das hamburgische LfV nichts gegen eine Auskunftserteilung einzuwenden; es bedurfte jedoch einer Intervention durch den von mir eingeschalteten Bundesbeauftragten für den Datenschutz beim Bundesamt für Verfassungsschutz, bevor eine Petentin informiert werden durfte, daß über sie keine Informationen gespeichert sind. Sie war irrtümlich in den Verdacht extremistischer Bestrebungen geraten und mußte deshalb die Überwachung ihres Post- und Fernmeldeverkehrs

erdulden. Sie hatte Sorge, aufgrund dieser Tatsache nicht mehr in den öffentlichen Dienst eingestellt zu werden.

Es bleibt zu hoffen, daß die Verfassungsschutzbehörden in Zukunft in vermehrtem Maße bereit sein werden, die Rechte der Betroffenen zu berücksichtigen. Noch wichtiger wäre es aber, wenn die Gesetzgeber in Bund und Ländern nicht nur die Arbeit dieser Behörden auf eine verfassungsrechtlich nicht zu beanstandende Grundlage stellen, sondern die Auskunftsrechte der Betroffenen im vorbeschriebenen Sinne eindeutig modifizieren würden. Leider sieht auch der jüngste Entwurf zur Änderung des Bundesdatenschutzgesetzes, den das Bundesinnenministerium vor einigen Wochen zur Diskussion gestellt hat, sogar eine Verschlechterung der Rechtsposition von auskunftssuchenden Bürgern vor. Es soll nicht nur dabei bleiben, daß — neben anderen — auch die Verfassungsschutzbehörden generell die Auskunft verweigern dürfen, sondern sie brauchen ihre Entscheidung auch in keinem Fall mehr zu begründen. Der mir unmittelbar vor Redaktionsschluß für diesen Bericht übersandte Entwurf für die Neufassung des Hamburgischen Datenschutzgesetzes scheint dagegen eine Lösung anzustreben, die den verfassungsrechtlichen Vorgaben entspricht. Dies ist eine erfreuliche Entwicklung, wie ich ausdrücklich hervorheben möchte.

Über die dringend gebotene Novellierung des hamburgischen Verfassungsschutzgesetzes kann ich leider Vergleichbares nicht sagen. Noch immer gibt es keine Anzeichen, daß die hierfür erforderlichen Arbeiten vorangetrieben werden.

4.12.2 Speicherung von Volkszählungsgegnern

Aufgrund verschiedentlich geäußerter Befürchtungen, personenbezogene Daten von Volkszählungsgegnern würden pauschal und in großer Anzahl vom LfV gespeichert, habe ich mich zur Klärung mit dem Amt in Verbindung gesetzt. Dabei wurde mir versichert, daß die Tatsache der Gegnerschaft zur Volkszählung allein keine Aktivitäten des LfV auslösen würde. Lediglich wenn sich links- oder rechtsextremistische Organisationen, die schon bisher Beobachtungsobjekte des Verfassungsschutzes waren, auch an Aktivitäten gegen die Volkszählung beteiligen, wurden in diesem Zusammenhang auch personenbezogene Informationen verarbeitet. Dagegen habe ich keine Bedenken erhoben.

4.13 **Justiz**

In immer stärkerem Maße werden jetzt auch in der Justiz Überlegungen angestellt, wie durch den Einsatz automatisierter Verfahren bestehende oder zukünftige Arbeitsabläufe unterstützt und erleichtert werden können. Eine einheitliche Konzeption, die für eine kontinuierliche Entwicklung wünschenswert wäre und die aufeinander abgestimmte Hard- und Software-Entscheidungen ermöglichen würde, ist zur Zeit noch nicht erkennbar. Dagegen wurden von einzelnen Mitarbeitern Teilproblemlösungen auf privaten Personalcomputern erarbeitet und in einem — für mich noch nicht überschaubaren — Umfang für dienstliche Aufgaben eingesetzt. Dies wirft eine Reihe von Problemen auf, um deren Lösung sich die Justizbehörde in naher Zukunft wird bemühen müssen. So können durch einen unkoordinierten Einsatz der verschiedensten Produkte „Datenverarbeitungs-Inseln" entstehen, die später nicht mehr zu einem Ganzen zusammengeführt werden können. Schwerwiegender aus meiner Sicht sind jedoch die datenschutzrechtlichen Fragestellungen. So wird insbesondere zu klären und festzulegen sein, ob und ggf. in welchem Umfang personenbezogene Daten aus Strafermittlungs- oder Gerichtsverfahren, die in der Regel als sensibel anzusehen sind, auf privaten Personalcomputern verarbeitet werden dürfen. Wollte man dies — etwa aus Gründen, die mit der richterlichen Unabhängigkeit zusammenhängen — zulassen, würden faktisch unüberwindbare Hindernisse für die Datensicherung entstehen. Darüber hinaus sind strafbewehrte Verschwiegenheitspflichten und mit ihnen die dem Dienstherrn obliegende Fürsorgepflicht berührt. Diese von mir nur angerissenen Probleme zeigen schon den dringenden Handlungsbedarf in diesem Bereich. Zunächst scheint mir eine Bestandsaufnahme erforderlich zu sein, die ich für dieses Jahr anstrebe.

Nicht auf der exekutivischen, sondern auf der Gesetzgebungsebene sind weitere Arbeiten erforderlich, um die erforderlichen gesetzlichen Grundlagen für die justizspezifische Datenverarbeitung zu schaffen. Neben der Strafprozeßordnung erscheinen mir in erster Linie die übrigen Prozeßordnungen (ZPO, VwGO, FGG, SGG und ArbGG) ergänzungsbedürftig.

4.13.1 Justizmitteilungsgesetz

Aus staatsanwaltschaftlichen und gerichtlichen Verfahren werden in vielfältiger Weise personenbezogene Daten an die verschiedensten Stellen übermittelt. Diese Übermittlungen erfolgen bisher auf der Grundlage bundeseinheitlicher Verwaltungsvorschriften, deren bekanntesten die „Anordnung über Mitteilungen in Strafsachen (MiStra)" und die „Anordnung über Mitteilungen in Zivilsachen (MiZi)" sind. Die Problematik solcher Mitteilungen habe ich in meinen Tätigkeitsberichten häufiger dargestellt (vgl. 1. TB 6.8.1 und 6.8.2, S. 46; zuletzt 4. TB 4.11.2 und 4.11.3, S. 90 f.). Insbesondere habe ich darauf hingewiesen, daß auch dafür gesetzliche Grundlagen erforderlich sind. Mit dem mir Ende 1986 zur Stellungnahme übersandten Entwurf für ein „Gesetz über Mitteilungen der Justiz von Amts wegen in Zivil- und Strafsachen (Justizmitteilungsgesetz)" wird nun der Versuch unternommen, solche gesetzlichen Grundlagen zu schaffen.

Auf die vorgesehenen gesetzlichen Bestimmungen im einzelnen einzugehen, würde den Rahmen dieses Berichts sprengen. Eine entsprechende Stellungnahme habe ich der Justizbehörde nach Abstimmung mit den anderen Datenschutzbeauftragten übersandt. Auch meine bisherigen Stellungnahmen zur inhaltlichen Ausgestaltung von MiStra und MiZi halte ich ausdrücklich aufrecht. Auf einige grundsätzliche Probleme möchte ich jedoch aufmerksam machen.

Der Entwurf verfolgt die Konzeption, die Mitteilungspflichten nur mit generalklauselartigen Bestimmungen zu umschreiben und die konkrete Mitteilung in Verwaltungsanordnungen auf der Grundlage der bisherigen MiStra und MiZi zu regeln. Dieser Konzeption haben sich die Datenschutzbeauftragten, aber z. B. auch der Deutsche Richterbund (vgl. Deutsche Richterzeitung 1987 S. 105), widersetzt. Sie entspricht nicht dem vom Bundesverfassungsgericht im Zusammenhang mit dem informationellen Selbstbestimmungsrecht besonders hervorgehobenen Grundsatz der Normenklarheit. Es ist deshalb zu fordern, daß die Betroffenen und die Normadressaten schon aus dem Gesetz entnehmen können, durch wen welche Informationen bei welcher Gelegenheit an welche Stelle übermittelt werden. Wo dies nicht konsequent durchgeführt werden kann, darf die Auffüllung des gesetzlichen Rahmens keinesfalls durch bloße Verwaltungsvorschriften, sondern muß zumindest durch Rechtsverordnungen erfolgen.

Darüber hinaus bin ich der Auffassung, daß die Betroffenen von den Mitteilungen umfassender als bisher vorgesehen informiert werden müßten. Ausnahmen sollten nur dann zugelassen werden, wenn schwerwiegende Bedenken in der Person der Betroffenen entgegenstehen oder der Zweck des zugrundeliegenden Verfahrens gefährdet würde.

Schließlich muß der Entwurf noch mit dem geltenden Recht harmonisiert werden. So dürfen beispielsweise durch neue Bestimmungen keinesfalls Schutzvorschriften des Bundeszentralregistergesetzes unterlaufen werden. Aber auch die Besonderheiten und die erzieherische Zielsetzung von Strafverfahren gegen Jugendliche und Heranwachsende müssen durch die Begrenzung von Mitteilungspflichten noch angemessener berücksichtigt werden.

4.13.2 Novellierung der Strafprozeßordnung

In meinem letzten Tätigkeitsbericht (5.10.1 — 5.10.1.11, S. 80 ff) habe ich ausführlich zur geplanten Novellierung der Strafprozeßordnung Stellung genommen. Nunmehr hat der Bundesjustizminister den vorliegenden Arbeitsentwurf ergänzt durch „Allgemeine Bestimmungen über die Speicherung, Verwendung und Übermittlung personenbezo-

gener Daten durch die Strafverfolgungsbehörden". Die Datenschutzbeauftragten des Bundes und der Länder sowie die Datenschutzkommission des Landes Rheinland-Pfalz beabsichtigen, auch diese „Allgemeinen Bestimmungen" gemeinsam zu beraten, um möglichst zu einer abgestimmten Stellungnahme zu gelangen. Dies ist bis zum Redaktionsschluß für den vorliegenden Bericht noch nicht geschehen. Ich gehe jedoch davon aus, daß ich Anfang 1988 meine Stellungnahme gegenüber der Justizbehörde abgeben kann.

4.13.3 Neues Informationssystem der Staatsanwaltschaften

Die Vorbereitungen für die Einführung eines bundesweiten staatsanwaltlichen Informationssystems — SISY — (4. TB, 5.10.3, S. 88) sind in diesem Jahr weiter vorangetrieben worden. In der 58. Konferenz der Justizminister und -senatoren vom 2.-4. Juni 1987 wurde beschlossen, den Bundesminister der Justiz zu bitten, alsbald einen Entwurf für eine bundesgesetzliche Regelung eines solchen Systems vorzulegen, die auch den Belangen des Datenschutzes Rechnung trägt.

Die Überlegungen darüber, welche Daten in ein solches System aufgenommen werden sollen und in welchem Umfang es genutzt werden soll, sind noch nicht abgeschlossen. Dabei ist nach meiner Auffassung zu berücksichtigen, daß ein Teil der Justizdaten schon in anderen Dateien und Systemen vorhanden sind. Einerseits sind Daten, die der Strafverfolgung dienen, in diversen polizeilichen Dateien vorhanden, ungeachtet der Tatsache, daß nach der geltenden Rechtsordnung die Staatsanwaltschaft „Herrin" des Strafermittlungsverfahrens und die Polizei deshalb verpflichtet ist, die Ergebnisse polizeilicher Ermittlungen unverzüglich der Staatsanwaltschaft zu übergeben (§ 163 Abs. 2 StPO). Andererseits sind im Bundeszentralregister u. a. sämtliche rechtskräftige strafgerichtliche Verurteilungen, aber auch Vermerke über Entmündigungen und die Schuldfähigkeit von Personen gespeichert.

Es ist deshalb aus meiner Sicht unabdingbar, daß ein neues System — wie immer es aussehen wird — in die vorhandenen Datenbestände eingepaßt und mit ihnen abgestimmt wird. Mehrfachspeicherungen derselben Sachverhalte sind weder mit dem datenschutzrechtlichen Grundsatz der Erforderlichkeit noch mit dem verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit zu vereinbaren. So wird der Gesetzgeber insbesondere klarzustellen haben, welche Daten wie lange für repressive Zwecke gespeichert werden dürfen und in welchen Verantwortungsbereich diese Datensammlungen fallen. Darüber hinaus sollte darauf geachtet werden, daß die mit dem Bundeszentralregistergesetz schon jetzt erreichten Standards bezüglich der Speicherungsdauer und der Auskunftserteilung durch das geplante System nicht unterlaufen werden.

4.13.4 Einsicht in Gerichtsakten zu Forschungszwecken

Justizdaten bieten Ansatzpunkte für die verschiedensten Forschungsbereiche. So ist an ihnen nicht nur die Kriminologie, sondern beispielsweise auch die Sozialforschung zur Untersuchung der Auswirkungen einzelner Familienrechtsbestimmungen (Unterhalt, Sorgerecht) interessiert. Diese Forschung ist zum Teil unentbehrlich; sie wird aus öffentlichen Haushalten gefördert und bietet dem Gesetzgeber wichtige Hinweise für seine Arbeit. Aus datenschutzrechtlicher Sicht ist sie gleichwohl als problematisch einzustufen, da weder das materielle Recht noch die verschiedensten Verfahrensordnungen Befugnisnormen enthalten, die es erlauben, die für Justizzwecke erhobenen Daten ohne Zustimmung der Betroffenen für Forschungszwecke zu benutzen. Solche Befugnisnormen sind nach dem Volkszählungsurteil des Bundesverfassungsgerichts jedoch erforderlich und müssen daher dringend geschaffen werden. Um bis dahin gleichwohl wissenschaftliche Forschung zu ermöglichen, habe ich mit der Justizbehörde vereinbart, daß die Einsicht in Gerichtsakten zu Forschungszwecken für die Übergangszeit durch eine Allgemeine Verfügung der Justizbehörde geregelt wird, in der die schutzwürdigen Belange der Betroffenen mit den Forschungsinteressen zu einem Ausgleich gebracht werden sollen und in der folgende unverzichtbaren Datenschutzforderungen festgehalten werden sollen:

— Personenbezogene Angaben dürfen für ein Forschungsvorhaben nur offenbart werden, wenn dieses nicht auf andere Weise durchgeführt werden kann.

— Eine Einsichtnahme in Akten bzw. eine Weitergabe personenbezogener Daten — ohne Einwilligung der Betroffenen — kommt nur in Betracht, wenn die Einholung von Einwilligungen unmöglich oder nur unter unverhältnismäßigem Aufwand möglich ist und das Allgemeininteresse an der Durchführung eines bestimmten Forschungsvorhabens das Geheimhaltungsinteresse der Betroffenen erheblich überwiegt. Die Entscheidung dieser Frage ist dem zuständigen Gerichtspräsidenten bzw. dem Leiter der Staatsanwaltschaft vorzubehalten; die Genehmigung kann mit Auflagen versehen werden.

— Die erlangten personenbezogenen Informationen sind von dem Forscher sobald wie möglich zu anonymisieren und dürfen nur zum Zweck eines bestimmten Forschungsvorhabens verwendet werden. Auswertungsergebnisse dürfen nur in anonymisierter Form weitergegeben und veröffentlicht werden.

— Eine Einsichtnahme bzw. Übermittlung ist auf Informationen aus rechtskräftig abgeschlossenen Verfahren zu beschränken.

— Die Einsichtnahme in Akten sollte möglichst nur in den Räumen der aktenführenden Dienststelle erfolgen.

— In die entsprechenden Vereinbarungen sind die notwendigen technischen und organisatorischen Datensicherungsmaßnahmen aufzunehmen.

— Eine effektive Kontrolle durch den Datenschutzbeauftragten ist zu gewährleisten.

Bis zum Redaktionsschluß für diesen Bericht lag mir ein Entwurf für die geplante Verfügung noch nicht vor. In Anbetracht der auch in diesem Jahr wieder zahlreich angemeldeten Forschungsvorhaben sollte mit der Regelung dieses Problems nicht mehr gewartet werden.

4.13.5 Gerichtsakten zu Prüfungszwecken

Rechtsreferendare und Studenten der einstufigen Juristenausbildung haben in der Regel im Rahmen ihrer Abschlußprüfung häusliche Arbeiten aufgrund von Aktenstücken anzufertigen (§ 7 Abs. 1 der Übereinkunft der Länder Freie Hansestadt Bremen, Freie und Hansestadt Hamburg und Schleswig-Holstein über ein gemeinsames Prüfungsamt und die Prüfungsordnung für die Große Juristische Staatsprüfung; § 51 Abs. 3 Nr. 2 Juristenausbildungsordnung — JAO —). Traditionell werden dafür gerichtliche und behördliche Originalakten aus meist abgeschlossenen Verfahren verwendet. Dies hat sich insbesondere im Hinblick auf die in Ausbildung und Prüfung angestrebte Praxisnähe bewährt und wäre prinzipiell auch aus datenschutzrechtlicher Sicht nicht zu beanstanden, da die Prüflinge besonderen Verschwiegenheitspflichten unterliegen. Gleichwohl muß auch in diesem Zusammenhang darauf hingewiesen werden, daß durch die Übermittlung von personenbezogenen Daten — insbesondere von Sozial-, Arzt- und Betriebsgeheimnissen — an die Prüfungsämter eine Zweckänderung erfolgt, für die eine gesetzliche Grundlage derzeit nicht besteht. Aus diesem Grunde verweigern vereinzelt Verwaltungsbehörden die Übersendung ihrer Sachakten zu Prüfungszwecken. Von einem Prüfungsamt darauf angesprochen, habe ich empfohlen, für eine Übergangszeit die Prüfungskandidaten durch ein besonderes Merkblatt auf ihre Verschwiegenheitspflicht und die aus der Verletzung dieser Pflicht möglicherweise folgenden zivil- und strafrechtlichen Konsequenzen hinzuweisen. So wird derzeit verfahren. Es wäre allerdings wünschenswert, wenn die — bewährte — Praxis in naher Zukunft gesetzlich abgesichert würde.

4.13.6 Öffentliche Bekanntmachungen von Entmündigungen

Nach einer Pressemitteilung des Bundesjustizministers strebt die Bundesregierung eine Revision des gesamten Entmündigungsrechts an. Es bleibt zu hoffen, daß dabei auch das Problem der Bekanntmachungen von Entmündigungsentscheidungen befrie-

digend gelöst wird, zu dem ich mich im Rahmen eines Verfahrens vor dem Bundesverfassungsgericht geäußert habe.

Nach § 687 Zivilprozeßordnung (ZPO) sind Entmündigungen von Personen wegen Verschwendung oder wegen Trunksucht (nach herrschender Auffassung auch wegen Rauschgiftsucht) vom Amtsgericht öffentlich bekanntzumachen. Diese Vorschrift ist nach meiner Auffassung mit geltendem Verfassungsrecht nicht in Einklang zu bringen.

Gegen den Willen der Betroffenen erfolgende Veröffentlichungen von Entmündigungsentscheidungen stellen Eingriffe in das informationelle Selbstbestimmungsrecht dar, die nur im überwiegenden Allgemeininteresse zulässig sind.

Die gesetzliche Anordnung der Veröffentlichung soll nach herrschender Auffassung dem Schutz des Rechtsverkehrs dienen. Schon die Erreichung dieses Zwecks ist zweifelhaft. Zum einen machen die auf Trunk-, Rauschgift- und Verschwendungssucht zurückzuführenden Entmündigungen nur einen sehr kleinen Teil der insgesamt ausgesprochenen Entmündigungen aus. Der weitaus größte Anteil von Entmündigungen betrifft die Geisteskrankheiten und -schwächen. Für diese Fälle ist die öffentliche Bekanntmachung jedoch nicht angeordnet (vgl. §§ 660, 674 ZPO). Es kann deshalb nicht davon ausgegangen werden, daß der Rechtsverkehr durch die Bekanntgabe eines sehr kleinen Teils von Entmündigungsentscheidungen wirksam geschützt werden kann. Zum anderen werden die Entscheidungen durch einen Aushang im Gericht oder in Amtsblättern veröffentlicht; Kommunikationsformen mithin, die nach der Lebenserfahrung von Beteiligten am „Rechtsverkehr" praktisch nicht wahrgenommen werden.

Dagegen stellt die öffentliche Bekanntmachung für den Betroffenen einen besonders tiefen Eingriff in seine Persönlichkeitsrechte dar. Allein die Möglichkeit, daß jeder Beliebige Kenntnis von der als entwürdigend empfundenen Gerichtsentscheidung Kenntnis erlangen kann, birgt die Gefahr in sich, daß die Betroffenen sich zurückziehen und in die gesellschaftliche Isolation geraten, in der die Überwindung der Sucht noch ungleich schwerer gelingen kann.

Soweit die Veröffentlichung aus erzieherischen Gründen für erforderlich gehalten wird, wird damit faktisch einem öffentlichen Pranger das Wort geredet, der den Betroffenen zu gesellschaftskonformen Verhalten anhalten soll. Dies wäre mit heutigem Verfassungsverständnis, insbesondere mit der von aller staatlichen Gewalt zu achtenden und zu schützenden Würde des Menschen unvereinbar. Darüber hinaus dürfte eine derartige gesetzgeberische Motivation einem inzwischen überholten Verständnis von Suchtursachen und -auswirkungen entsprungen sein. Es ist inzwischen anerkannt, daß Suchtkranke und Suchtgefährdete im Rahmen der Gesundheitsfürsorge, die ihren verfassungsrechtlichen Anknüpfungspunkt im Sozialstaatsprinzip findet, betreut werden müssen. Sie bedürfen der Entziehungs- und Entwöhnungsbehandlung und anschließender Betreuung, die zur sozialen Wiedereingliederung führt. Gerade diesem Ziel dürfte aber die öffentliche Bekanntmachung nach § 687 ZPO im Wege stehen.

4.13.7 Grundbuchämter

Mehrfach haben sich Betroffene wegen der Auskunftspraxis bei den Grundbuchämtern an mich gewandt. Insbesondere wurde bemängelt, daß die Bekanntmachungen nach § 55 Grundbuchordnung (GBO) oft mehr personenbezogene Daten enthalten, als das Gesetz zuläßt. Nach § 55 GBO soll jede Eintragung dem Antragsteller, dem eingetragenen Eigentümer sowie den Personen bekanntgemacht werden, zu deren Gunsten die Eintragung erfolgt ist, oder deren Recht durch sie betroffen wird.

Diesen Beschwerden wird gelegentlich entgegengehalten, daß jedenfalls dann, wenn die Unterrichteten auch ein Grundbucheinsichtsrecht haben (§ 12 GBO), datenschutzrechtliche Belange nicht verletzt sein können.

Dazu habe ich gegenüber der Justizverwaltung die Auffassung vertreten, daß § 55 GBO als gesetzliche Einschränkung des informationellen Selbstbestimmungsrechts

verfassungskonform ausgelegt werden muß. Das müsse dazu führen, daß Personen, die nach dieser Vorschrift zu informieren sind, nur solche Informationen erhalten dürfen, durch die ihre Rechte tangiert werden. Die Übersendung vollständiger Grundbuchauszüge, die sämtliche Eintragungen des Grundbuchs enthalten, sind danach nicht zulässig. Auch ein mögliches Einsichtsrecht der Unterrichteten kann nach meiner Auffassung daran nichts ändern, denn dieses Recht ist kraft Gesetzes an die Darlegung eines berechtigten Interesses gebunden, das in jedem Einzelfall zu prüfen ist. Das Grundbuchamt ist nicht berechtigt, die Einsichtsbegehrenden von ihrer Darlegungspflicht zu befreien, indem es die Bekanntmachung nach § 55 GBO auch auf solche Eintragungen erweitert, die nicht unmittelbar die Rechte der Empfänger betreffen.

Inzwischen hat der Präsident des Amtsgerichts Hamburg mitgeteilt, daß er meine Rechtsauffassung teile und die betroffenen Mitarbeiter bei den Grundbuchämtern entsprechend unterrichtet habe. Gleichwohl habe ich die Justizbehörde gebeten, sich zusammen mit anderen Justizverwaltungen für eine Novellierung von § 55 GBO einzusetzen, die den Grundbuchämtern normenklar die erforderlichen Beschränkungen auferlegt.

4.13.8 Schuldnerverzeichnis

Die Bemühungen, die Vorschriften über Auskünfte aus dem Schuldnerverzeichnis unter Beachtung der Rechtsprechung des Bundesverfassungsgerichts zum informationellen Selbstbestimmungsrecht neu zu regeln (vgl. zuletzt 5. TB, 5.10.5, S. 88 f.), sind erfreulicherweise vom Bundesjustizministerium wieder aufgenommen worden. Neu gefaßte Entwürfe eines Gesetzes zur Änderung von Vorschriften über das Schuldnerverzeichnis und einer Verordnung über die Erteilung von Abdrucken und Listen aus den Schuldnerverzeichnissen (Stand: 28. 8. 1987) befinden sich jetzt im Stadium der Abstimmung mit den beteiligten Behörden, u.a. auch den Datenschutz-Aufsichtsbehörden für den nicht-öffentlichen Bereich und den Landes- und dem Bundesdatenschutzbeauftragten.

Ich habe zu den neuen Entwürfen wie folgt Stellung genommen:

Positiv sind einige Elemente der Entwürfe zu beurteilen, die einen besseren Persönlichkeitsschutz der Betroffenen bewirken sollen, wie etwa

— die automatische Löschung nach drei Jahren ohne Antrag des Betroffenen;

— der Wegfall des Einsichtsrechts in das Schuldnerverzeichnis;

— die Verpflichtung für Bezieher von Abdrucken aus dem Schuldnerverzeichnis, diese unverzüglich in einer Datei zu verarbeiten und die Abdrucke danach zu vernichten;

— die Aufsicht der zuständigen Datenschutz-Aufsichtsbehörde über Bezieher von Abschriften aus dem Schuldnerverzeichnis ohne das Erfordernis des Vorliegens einer Beschwerde.

Allerdings ist der BMJ meinen früher vorgetragenen Anregungen (vgl. 4. TB, 4.11.4.1, S. 91 ff.) weitgehend nicht gefolgt. Insbesondere meine Forderung, die listenmäßige Verteilung der Angaben aus dem Schuldnerverzeichnis auf Kammern und Stellen wie die SCHUFA zu beschränken, die dann nur noch im Einzelfall Auskunft geben dürften, ist bedauerlicherweise nicht berücksichtigt worden.

Es ist zwar zu begrüßen, daß in die jetzt vorliegenden Entwürfe verschiedene Zweckbindungsregelungen aufgenommen worden sind. Als Beispiel zitiere ich § 915 d Abs. 3 des Entwurfs: „Abdrucke und Dateien sind vertraulich zu behandeln und dürfen Dritten nicht zugänglich gemacht werden. Personenbezogene Informationen aus Abdrucken und Dateien dürfen nur verwendet werden, um wirtschaftliche Nachteile abzuwenden, die daraus entstehen können, daß der Schuldner seinen Zahlungsverpflichtungen nicht nachkommt." Leider sind diese Regelungen jedoch nicht mit Maßnahmen und Vorkehrungen verknüpft worden, die ihre Beachtung in der Praxis sicherstellen. Die Kontrolle durch die Datenschutz-Aufsichtsbehörden wird immer punktuell sein und kann eine breite Beachtung der Zweckbindungsvorschriften nicht lückenlos sicherstellen.

Ich muß deswegen an meiner Forderung festhalten, daß die Empfänger der Abschriften aus dem Schuldnerverzeichnis diese nicht selbst vervielfältigen oder durch andere Stellen vervielfältigen lassen dürfen und sie auch nicht Dritten in anderer Form listenmäßig zur Verfügung stellen oder zur Verfügung stellen lassen dürfen.

Im übrigen verweise ich auf meine früher vorgetragenen Forderungen, die ich aufrechterhalte.

4.14 Strafvollzug

4.14.1 Bereichsspezifische Rechtsgrundlagen

Die Erhebung und Verarbeitung zum Teil sehr sensibler personenbezogener Daten von Strafgefangenen und Untersuchungshäftlingen erfordert dringend die Schaffung bereichsspezifischer gesetzlicher Datenverarbeitungsgrundlagen. Darauf habe ich schon mehrfach hingewiesen.

4.14.1.1 Strafvollzugsgesetz

Nach einer im September 1985 vorgelegten „Entwurfsskizze" für datenschutzrechtliche Ergänzungen des Strafvollzugsgesetzes war die Arbeit zunächst ins Stocken geraten. Nunmehr hat der Bundesminister der Justiz einen Arbeitsentwurf für eine entsprechende Novellierung des Strafvollzugsgesetzes (Stand: 31. 3. 1987) vorgelegt, der von mir und anderen Datenschutzbeauftragten trotz einiger Verbesserungsmöglichkeiten insgesamt positiv aufgenommen worden ist. Von einer umfassenden Darstellung der vorgeschlagenen Regelungen und meiner Auffassung dazu sehe ich jedoch ab, da nach einer Diskussion des Bundesjustizministeriums mit den Landesjustizverwaltungen im Juli 1987 der Entwurf als überholt angesehen werden muß. Das Bundesjustizministerium hat den Auftrag erhalten, einen stark überarbeiteten neuen Entwurf vorzulegen, der nun erst einmal abzuwarten ist. Über den Fortgang der Gesetzgebungsarbeit werde ich berichten.

4.14.1.2 Jugendstrafvollzugsgesetz

Leider nicht einmal so weit gediehen ist die Arbeit an einem Jugendstrafvollzugsgesetz. Über einen Arbeitsentwurf aus dem Jahre 1984 hinaus, der die Rechtsprechung des Bundesverfassungsgerichts zum Persönlichkeitsrecht im allgemeinen und zum informationellen Selbstbestimmungsrecht im besonderen noch weitgehend unberücksichtigt läßt, sind Arbeitsfortschritte nicht ersichtlich. Auch der Justizbehörde lagen im Juli des Berichtsjahres keine neuen Erkenntnisse vor.

4.14.1.3 Untersuchungshaft

Auch das Recht der Untersuchungshaft ist durch gesetzliche Bestimmungen zu ergänzen, die normenklar regeln, welche Informationseingriffe die Untersuchungsgefangenen im überwiegenden Allgemeininteresse hinzunehmen haben. Dafür liegen Vorschläge noch gar nicht vor. Zwar hat die Bundestagsfraktion der SPD einen „Entwurf eines Gesetzes zur Änderung des Rechts der Untersuchungshaft" eingebracht (BTDrs. 11/688 vom 11. 8. 1987), dieser verfolgt jedoch andere wichtige justizpolitische Ziele wie die Reduzierung der Zahl der Untersuchungshaftfälle und die Einschränkung der Dauer der Untersuchungshaft. Ich hoffe jedoch, daß dieser Entwurf für den Gesetzgeber Anlaß sein wird, die notwendigen Datenverarbeitungsregelungen in die Novellierungsüberlegungen mit einzubeziehen.

4.14.2 Eingaben

Auch im letzten Jahr habe ich wieder zahlreiche Eingaben von Strafgefangenen erhalten. In einigen Fällen mußte ich feststellen, daß beim Umgang mit personenbezogenen Daten von Gefangenen nicht immer die notwendige Sorgfalt aufgewendet wird. So wurde einem Gefangenen ein medizinischer Untersuchungsbefund zugestellt, der ein-

fach zusammengefaltet und mit einer Heftklammer „gesichert" war. Auf dem Wege dorthin hatte er mehrere Hände durchlaufen. Der Leiter der Haftanstalt hat nunmehr angeordnet, daß medizinische Befunde zukünftig entweder in verschlossenen Umschlägen versandt oder persönlich ausgehändigt werden; an sich eine Selbstverständlichkeit, die schon vorher hätte beachtet werden können.

In einem anderen Fall hatte sich eine Insassenvertretung an mich gewandt, weil die Strafanstalt dem Arbeitsamt auf einem nur für die interne Verwendung entwickelten Formular personenbezogene Vollzugsdaten übermittelte, die für die Entscheidung des Arbeitsamtes (berufliche Fortbildung, Umschulung der Betroffenen) ohne Bedeutung waren. Auf meine Intervention hin hat der Anstaltsleiter das bisherige Verfahren untersagt; die Justizbehörde hat sich eine Überprüfung im Wege der Dienstaufsicht vorbehalten.

4.15 AIDS

Die Ausbreitung des AIDS (HI-) Virus stellt eine der größten gesellschaftspolitischen Herausforderungen der letzten Jahre dar. Da ein Impfstoff wohl noch für lange Zeit nicht zur Verfügung stehen wird und der bedeutendste Infektionsweg (Sexualverkehr) direkter staatlicher Einflußnahme faktisch nicht zugänglich ist, wird nach meiner Auffassung zu Recht versucht, die Ausbreitung des Virus durch Aufklärung, mit der eine Änderung des Sexualverhaltens bewirkt werden soll, einzudämmen. Allerdings verläuft die Krankheit, wenn sie nach einer Infektion ausbricht, mit hoher Wahrscheinlichkeit tödlich. Diese Tatsache weckt Ängste und andere Emotionen, die den Boden auch für Forderungen nach staatlichen Repressionsmaßnahmen bieten. So soll nicht nur das Instrumentarium des Bundesseuchengesetzes ausgeschöpft werden (vgl. dazu Ministerialamtsblatt Nr. 10/1987 der Bayrischen Inneren Verwaltung vom 25. Mai 1987), sondern es wird vereinzelt sogar die gesetzliche Einführung einer allgemeinen Meldepflicht für sämtliche HIV-Infizierte gefordert. Mit solchen Forderungen haben sich auch die Datenschutzbeauftragten auseinanderzusetzen, denn auch der Gesetzgeber darf nach der Rechtsprechung des Bundesverfassungsgerichts (BVerfGE Bd. 65 S.1 ff) die zwangsweise Erhebung und Weitergabe dieser personenbezogenen Daten nur im überwiegenden Allgemeininteresse zulassen. Ich gehe gegenwärtig allerdings davon aus, daß die Einführung einer allgemeinen Meldepflicht nicht ernsthaft erwogen wird, da ihr von den meisten Gesundheitspolitikern und Sachverständigen bezüglich der Ausweitung des Virus eine kontraproduktive Wirkung zugeschrieben wird, weil in diesem Fall die Bereitschaft, an Tests und anderen Präventionsmaßnahmen teilzunehmen, voraussichtlich drastisch sinken wird. Gleichwohl darf nicht verkannt werden, daß auch heute schon in verschiedenen Bereichen der öffentlichen Verwaltung rechtmäßig personenbezogene Infektionsdaten erhoben und aufbewahrt werden. In diesen Fällen richtet sich mein Augenmerk darauf, daß die Daten hinreichend vor unbefugter oder fahrlässiger Offenbarung an Dritte geschützt werden und daß keine mehr oder weniger vollständige „AIDS-Dateien" entstehen. Insbesondere dem Schutz der vorhandenen und noch anfallenden Daten kommt gegenwärtig eine besondere Bedeutung zu, da die gesellschaftlichen Folgen, die den Betroffenen drohen, wenn ihre Infektion unbefugt Dritten bekannt wird, sehr einschneidend sein können. So kann nicht nur der Verlust des Arbeitplatzes sondern die totale gesellschaftliche Isolierung, bis hinein in den Familienverband, drohen. Diese Folgen wurden meiner Meinung nach zutreffend mit dem Stichwort vom „sozialen Tod" beschrieben. „AIDS-Dateien" dagegen können ebenso wie die allgemeine Meldepflicht zur gesundheitspolitischen Konzeption kontraproduktiv wirken und darüber hinaus die Gefahr begründen, daß sie irgendwann einmal zu Lasten der Betroffenen für andere Zwecke genutzt werden.

4.15.1 AIDS-Daten im polizeilichen Informationssystemen

Die Bekämpfung der weiteren Ausbreitung von HIV-Infektionen und der damit verbundenen Erkrankung ist in erster Linie Aufgabe der Gesundheitspolitik. Polizeiliche Aufgaben, die eine Speicherung von HIV-Hinweisen rechtfertigen könnten, sind nicht

erkennbar. Entsprechende Speicherungen werden für erforderlich gehalten, um Polizeibeamte und evtl. auch solche Personen, die sich in Polizeigewahrsam befinden, zu schützen. Daß Polizeibeamte vor den spezifischen Gefahren, denen sie sich bei der Berufsausübung ausgesetzt sehen, optimal zu schützen sind, ergibt sich aus den allgemeinen beamtenrechtlichen Fürsorgepflichten. Dies wird auch von mir ohne Einschränkung anerkannt.

Allerdings lassen die bekannten Infektionswege den Schluß zu, daß Polizeibeamte bei den üblichen sozialen Kontakten mit anderen Personen während des Dienstes nicht gefährdet sind. Allenfalls dann, wenn in Ausübung des Dienstes ein direkter Blut-zu-Blut-Kontakt oder eine Verletzung mit kontaminierten Injektionskanülen zu befürchten sind, können Infektionsgefahren entstehen. Davor müssen sich Polizeibeamte durch geeignete Eigensicherungsmaßnahmen schützen. Sie dürfen erwarten, daß sie von den für die Einhaltung der Fürsorgepflichten Verantwortlichen aufgeklärt werden und Sicherungsmittel zur Verfügung gestellt bekommen.

Darüber hinaus habe ich eine Speicherung von HIV-Hinweisen für zulässig gehalten, wenn Polizeibeamte voraussehbar in Situationen geraten, in denen es mit hoher Wahrscheinlichkeit zu gewaltsamen Auseinandersetzungen mit infizierten Personen kommt, etwa bei der beabsichtigten Festnahme infizierter Gewalttäter. Diese Auffassung wird auch von der Behörde für Inneres geteilt. Sie hat deshalb schon 1985 nach Abstimmung mit mir die Absicht geäußert, auf allgemeine HIV-Hinweise in polizeilichen Dateien zu verzichten (vergl. 5. TB, 5.8.7,S.73 f). Lediglich bei Fahndungsausschreibung soll ein Hinweis auf Ansteckungsgefahren und die Warnung vor Blutkontakt erfolgen, wenn

— die gesuchte Person aufgrund eines Hinweises von amtlicher Stelle als Träger des AIDS-Erregers gilt oder

— die gesuchte Person gegenüber amtlichen Stellen glaubhaft erklärt hatte, Träger dieser Erregers oder daran erkrankt zu sein und

— die gesuchte Person nach amtlichen Erkenntnissen zur Gewalttätigkeit neigt.

Nach dieser Regelung wird in Hamburg seit 10. März 1987 verfahren. Soweit mir bekannt ist, hat dies noch zu keiner einzigen Speicherung eines HIV-Hinweises geführt. Wenn es zu Speicherungen kommt, werden diese automatisch gelöscht, wenn nach Erledigung der Fahndung die Fahndungsnotierung selbst gelöscht wird.

Anfang Juli 1987 wurde die Öffentlichkeit durch eine Fernsehsendung auf das Problem der Speicherung von HIV-Hinweisen in polizeilichen Informationssystemen aufmerksam gemacht. Weitere Recherchen ergaben, daß nach dem Stand vom 1. 7. 87 im bundesweiten INPOL-System insgesamt 343 Hinweise auf infizierte Personen vorhanden waren, und zwar in der Datengruppe „rechtmäßige Personalien" im Datenfeld PHW (personengebundene Hinweise). Diese Speicherung hat den Nachteil, daß der Personendatensatz, der im INPOL-Datenbanksystem nur einmal für alle über INPOL abgewickelten — ansonsten logisch getrennten — Polizeidateien eingestellt ist, bei sämtlichen INPOL-Abfragen erscheint, so daß der personengebundene Hinweis auf AIDS auch dann mitgeteilt wird, wenn polizeiliches Einschreiten gar nicht geplant ist. Ich halte sie deshalb für unzulässig. Darüber hinaus ist darauf hinzuweisen, daß in Anbetracht der bestehenden Auswertungsmöglichkeiten für die INPOL-Dateien die Speicherung von AIDS-Informationen im Bereich der derzeitigen personengebundenen Hinweise zwangsläufig zu einer — wenn auch eingeschränkten — „AIDS-Datei" führen wird.

Schon im Juni 1987 hatten sich Vertreter der Innenministerkonferenz an die Datenschutzbeauftragten des Bundes und Länder mit der Bitte gewandt, die Speicherungspraxis der Polizei zu erörtern. In zwei gemeinsamen Sitzungen der jeweils gebildeten Arbeitsgruppen hat dies inzwischen stattgefunden. Nach eingehender Beratung der Ergebnisse dieser Gespräche hat die Konferenz der Datenschutzbeauftragten bei Gegenstimme des Bayerischen Landesbeauftragten für den Datenschutz zur polizeilichen Speicherung von HIV-Hinweisen einen Beschluß gefaßt, in dem es heißt:

Die Speicherung von HIV-Hinweisen soll die Eigensicherung von Polizeibeamten und evtl. auch den Schutz von solchen Personen in Polizeigewahrsam gewährleisten, die mit HIV-Infizierten in Kontakt kommen. Die Datenschutzbeauftragten verkennen nicht, daß Polizeibeamte bei der Berufsausübung spezifischen Gefahren ausgesetzt sind und die notwendigen Maßnahmen ergriffen werden müssen. Insbesondere ein direkter Blutkontakt oder eine Verletzung mit infizierten Injektionskanülen bei Kontakten mit Drogenabhängigen stellen eine solche spezifische Gefährdung dar. Dem Anspruch der Polizeibeamten auf einen weitestgehenden Schutz vor einer Infektion, die zu einer tödlichen Erkrankung führen kann, steht der Anspruch der Betroffenen gegenüber, daß Datenspeicherungen nur dann vorgenommen werden, wenn diese geeignet sind, die Gefährdung wirksam zu verringern, und sie dadurch nicht unverhältnismäßig belastet werden. Hierbei ist auch zu berücksichtigen, daß eine automatisierte Speicherung von medizinischen Daten eine schwerwiegende Beeinträchtigung für die Betroffenen darstellt. Ebenso sind auch die gravierenden sozialen Folgen für diesen Personenkreis zu bedenken, wenn die gespeicherten Daten an Dritte gelangen.

Sowohl medizinische Experten als auch Fachleute aus dem Sicherheitsbereich und dem Gesundheitswesen haben wiederholt Zweifel daran geäußert, daß durch die Speicherung von Informationen über HIV-Infizierte in polizeilichen Informationssystemen die Gefährdung von Polizeibeamten abgewendet werden kann. Hierfür werden folgende Gründe vorgebracht:

In vielen Situationen, wie z.B. bei der Hilfeleistung für verletzte Unfallopfer, der Festnahme unbekannter Personen oder auch der plötzlichen Konfrontation mit Straftätern oder Störern sei eine vorherige Überprüfung vorhandener Dateibestände ohnehin nicht möglich. Hinzu komme, daß der Polizei immer nur ein sehr geringer Teil der Infizierten bekannt sein werde, so daß die Polizei in jedem Fall und auch ohne besondere Hinweise Schutzmaßnahmen treffen müsse.

Angesichts dieser Zweifel, die von den Datenschutzbeauftragten geteilt werden, kann die Speicherung — wenn überhaupt — nur unter sehr eingeschränkten Voraussetzungen hingenommen werden. Möglich erscheint dies allenfalls für Situationen, in denen es mit hoher Wahrscheinlichkeit zu gewaltsamen Auseinandersetzungen mit infizierten Personen kommt. Keinesfalls darf eine „AIDS-Datei" entstehen. Im übrigen wäre dabei mindestens folgendes zu beachten:

1. Die Speicherung von HIV-Hinweisen im Datenfeld der „personengebundenen Hinweise" im bundesweiten Inpol-System und in vergleichbaren Landessystemen muß eingestellt werden, da diese Hinweise bei sämtlichen Abfragen erscheinen.

2. HIV-Hinweise dürfen allenfalls in solche Dateien aufgenommen werden, in denen sie als Grundlage für die Eigensicherung bei polizeilichem Einschreiten tatsächlich in Betracht kommen.

3. Die Speicherung von HIV-Infektionen aufgrund von Verdächtigungen und ungeprüften Informationen verbietet sich in jedem Fall. Kommt der Hinweis vom Betroffenen selbst, muß dieser über die Tatsache und die Bedeutung der Speicherung aufgeklärt werden. Im übrigen kommt nur die Speicherung von ärztlich gesicherten Informationen in Betracht, die die Polizei rechtmäßig erlangt hat.

4. Auf die gespeicherten Daten darf nur ein besonders dazu befugter Benutzerkreis zugreifen, und dies nur zu Zwecken der Eigensicherung. Die Weitergabe an andere Stellen ist nur in besonders festzulegenden Fällen zulässig.

5. Es müßte in jedem Fall erkennbar sein, wer wann den HIV-Hinweis in das System eingespeichert hat und hierfür verantwortlich ist, da nur so die Speicherungspraxis überprüft werden kann und notwendige Berichtigungen ermöglicht werden.

Durch diesen Beschluß sehe ich mich in meiner Auffassung bestätigt, daß die Speicherung von HIV-Hinweisen — wenn überhaupt — nur in dem Umfang erforderlich und zulässig sein kann, wie er in Hamburg festgelegt ist.

4.15.2 AIDS im Strafvollzug

Über den Umgang mit Daten von HIV-infizierten Gefangenen habe ich Anfang 1986 auf der Grundlage des damaligen Kenntnisstandes mit dem Strafvollzugsamt beraten. Trotz einiger Zweifel und Bedenken habe ich mich u. a. mit einer Unterrichtung aller Bediensteten, die sich dienstlichen Kontakten mit den infizierten Gefangenen nicht entziehen können, einverstanden erklärt (vgl. 5. TB, 5.11.4, S. 92 f). Dies beruhte insbesondere auf der Annahme, daß die medizinischen Erkenntnismöglichkeiten über die Infektionsgefahren möglicherweise noch nicht abgeschlossen waren. In der Zwischenzeit scheint mir zu dieser Frage mehr Klarheit zu bestehen, so daß ich den Zeitpunkt für gekommen halte, die bisherige Praxis einer kritischen Prüfung zu unterziehen. Ich habe deshalb mit dem Strafvollzugsamt verabredet, Anfang 1988 das Problem erneut zu erörtern.

4.15.3 Dateien der Blutspendedienste

Personenbezogene Daten von Blutspendern werden bei den Blutspendediensten der Gesundheitsbehörde auf Personalcomputern verarbeitet. Wenn ein Spendewilliger vom Blutspenden wegen einer Krankheit ausgeschlossen ist, wird nur dies im Datensatz vermerkt. Ein konkreter Hinweis, um welche Krankheit es sich im Einzelfall handelt, findet sich nach Auskunft der Gesundheitsbehörde lediglich in der Blutspendeakte, die wie eine Krankenakte angesehen und entsprechend gesichert wird. Ich werde Anfang des neuen Jahres das Verfahren und die Datensicherung überprüfen.

Eine früher einmal geäußerte Absicht, einen Datenverbund zwischen den verschiedenen Blutspendediensten herzustellen, um mehrfache Bluttests zu vermeiden, hat die Gesundheitsbehörde nach eigenem Bekunden wieder aufgegeben, so daß davon auszugehen ist, daß in jeder Datei nur die jeweils eigenen Daten verarbeitet werden und Datenübermittlungen nicht stattfinden. Auch dies werde ich in meine Prüfung mit einbeziehen.

4.15.4 AIDS-Tests bei Bewerbern für den öffentlichen Dienst

Die allgemeine AIDS-Diskussion berührt auch die Frage, ob Bewerber für den öffentlichen Dienst vom Personalarzt auf eine HIV-Infektion untersucht werden sollten oder gar müßten. Ich habe das Senatsamt für den Verwaltungsdienst — Personalamt — nach der Hamburger Praxis befragt: Bewerber für den Hamburger Staatsdienst — so die Antwort vom Mai 1987 — werden nur bei Anhaltspunkten für eine AIDS-Infizierung und nur mit seinem/ihrem Einverständnis gezielt untersucht. Ich gehe davon aus, daß es sich hier ausschließlich um medizinische und nicht etwa um soziologische (z.B. Homosexualität) Anhaltspunkte handeln muß. Die Untersuchung erfolgt in anonymer Form durch das Hygienische Institut. Das Testergebnis wird der einstellenden Behörde nicht mitgeteilt, nur das Ergebnis der gesamten personalärztlichen Untersuchung (Eignung/Nichteignung). Dabei führt eine AIDS-Infizierung nicht unbedingt zum Urteil „Nichteignung". Bisher scheiterte in Hamburg keine Bewerbung an einem positiven HIV-Testergebnis. Zwei Infizierte wurden eingestellt. Auch eine Berufung in das Beamtenverhältnis ist grundsätzlich nicht ausgeschlossen. Stimmt ein Bewerber trotz bestehender Anhaltspunkte einem AIDS-Test nicht zu, muß er es sich zurechnen lassen, wenn seine gesundheitliche Eignung nicht festgestellt werden kann.

Ich halte dies vom Personalamt geschilderte Verfahren für einwandfrei. Dabei gehe ich davon aus, daß ein positives Testergebnis in jedem Falle geheimgehalten, d.h. auch bei Rechtsmittelverfahren, Entscheidungsproblemen der Einstellungsbehörde und Feststellungen einer Erwerbsfähigkeitsminderung nur mit Zustimmung des Betroffenen offenbart wird. Bei anderen Krankheiten bzw. Behinderungen wurden der Einstellungsbehörde in der Praxis verschiedentlich durchaus Befunde bzw. Diagnosen mitgeteilt; hiergegen habe ich in anderem Zusammenhang Bedenken geltend gemacht.

4.15.5 Gesundheitsämter als AIDS-Beratungsstellen

Die Entscheidung des Senats, die AIDS-Beratung auch den Bezirksgesundheitsämtern zu übertragen, hat zusätzlich datenschutzrechtliche Problemstellungen aufgeworfen.

Diese ergeben sich aus der Mehrfunktionalität der Gesundheitsämter. Neben der ihnen nunmehr übertragenen Aufgabe der AIDS-Beratung betreiben die Gesundheitsämter/Amtsärzte — quasi als Serviceleistung für andere hamburgische Behörden — einen Gutachterdienst, bei dem neben anderen medizinischen Daten auch Informationen über HIV-Infektionen in den Bereich der Gesundheitsämter gelangen. Die besondere Problematik ergibt sich nun daraus, daß die Gesundheitsämter auch die zuständigen Behörden zur Durchführung des Bundesseuchengesetzes sind, so daß die Gefahr entstehen kann, daß Offenbarungen, die die Betroffenen zum Zwecke der Beratung oder Begutachtung machen, in Maßnahmen nach dem Bundesseuchengesetz einmünden. Das wäre mit dem datenschutzrechtlich anerkannten Zweckbindungsgebot nicht vereinbar. Darüber hinaus können einer Übermittlung von einem Funktionsbereich in den anderen auch das Sozialgeheimnis und die ärztliche Schweigepflicht entgegenstehen. Da solche Schutzvorschriften nicht mehr greifen können, wenn sich die verschiedenen Funktionen der Gesundheitsämter in einer Person vereinigen, sind nach meiner Auffassung die Rechte der Betroffenen durch organisatorische Maßnahmen und inhaltliche Ausgestaltung des Beratungsdienstes abzusichern. Ich habe deshalb folgendes gefordert:

— Der Beratungsdienst sollte in völliger Anonymität der Betroffenen durchgeführt werden. Eine listen- oder karteikartenmäßige Erfassung sollte ausgeschlossen werden. Als Vorbild könnte die von mir schon geprüfte AIDS-Beratungsstelle der Gesundheitsbehörde dienen.

— Die verschiedenen Funktionsbereiche der Gesundheitsämter sollten, soweit personenbezogene Daten verarbeitet (auch in Akten) und genutzt werden, vollständig voneinander abgeschottet werden. Datenflüsse darf es ohne ausdrückliche gesetzliche Grundlage nicht geben.

— Diese Abschottung muß auch in der Aufgabenzuweisung (Organisationsplan) an einzelne Mitarbeiter ihren Ausdruck finden. Gegenseitige Vertretungen von Mitarbeitern verschiedener Funktionsbereiche müssen ebenso ausgeschlossen werden wie Loyalitätskonflikte gegenüber Vorgesetzten.

— Auch im Bereich des Gutachterwesens sollte eine listen- oder karteimäßige Erfassung der Begutachteten, die Aufschluß über die festgestellten oder begutachteten Erkrankungen oder Behinderungen zuläßt, untersagt werden. Die Gutachten selbst müssen in besonders gesicherten Behältnissen (z.B. Stahlblechschränke mit Sicherheitsschloß), die nur von Berechtigten geöffnet werden dürfen, verwahrt werden.

Die Gesundheitsbehörde hat mir zugesichert, daß meine Forderungen, soweit sie nicht schon erfüllt sind, weitgehend erfüllt werden. In der von mir als zentral angesehenen Forderung nach dem Ausschluß gegenseitiger Vertretungen innerhalb eines Gesundheitsamtes hat sie allerdings mitgeteilt, daß dies wegen der knappen Personaldecke leider nicht möglich sein wird. Ich meine, der Senat sollte prüfen, ob statt dessen eine Vertretung der AIDS-Berater der verschiedenen Gesundheitsämter in Betracht zu ziehen ist. Die Amtsärzte selbst haben in einer Presseerklärung ausdrücklich betont, daß sie die Anonymität der Betroffenen und das Sozialgeheimnis strikt wahren werden und daß es eine Zweckentfremdung von personenbezogenen Daten zur Anwendung des Bundesseuchengesetzes nicht geben wird.

4.15.6 Prävalenz — Studie über HIV-Infektionen bei Schwangeren

Das Bundesgesundheitsamt führt eine bundesweite Studie zur Ermittlung der Infektionsquote bei Schwangeren durch. Dazu soll nach eingehender Information und Beratung der Schwangeren auf freiwilliger Basis ein HIV-Antikörpertest durchgeführt und im Falle der Bestätigung eines positiven Ergebnisses durch einen Kontrolltest die Risikoanamnese an das Bundesgesundheitsamt übermittelt werden. Die Kennzeichnung des Falls sollte durch Angabe des jeweils dritten Buchstabens des Vor- und Familiennamens, der Anzahl der Buchstaben der Namen und des Alters in Jahren erfolgen.

Der mir zur Stellungnahme vorgelegte Berichtsbogen sah keine Einwilligungserklärung der Betroffenen vor. Diese ist jedoch als Grundlage für die Erhebung und Übermittlung der Daten zu Forschungszwecken unabdingbar, zumal es sich um außerordentlich sensible, der ärztlichen Schweigepflicht unterfallende Informationen handelt, die nicht von vornherein und auch nicht vollständig anonymisiert werden. Zusammen mit der Gesundheitsbehörde habe ich deshalb eine den datensschutzrechtlichen Anforderungen genügende Einwilligungserklärung mit Informationstext erarbeitet, die den zur Teilnahme an der Studie bereiten Schwangeren zur Unterschrift vorzulegen ist.

4.16 Gesundheitswesen

4.16.1 Krankenhaus

4.16.1.1 Entwurf eines hamburgischen Krankenhausgesetzes

Die Gesundheitsbehörde hat Ende August des Berichtsjahres den schon lange erwarteten Referentenentwurf eines Hamburgischen Krankenhausgesetzes vorgelegt, der in einem Abschnitt über „Patient und Krankenhaus" in drei Paragraphen die Verarbeitung von Patientendaten regelt.

Ich begrüße es, daß damit meiner schon vor Jahren erhobenen Forderung nach einer bereichsspezifischen gesetzlichen Regelung für die Informationsverarbeitung im Krankenhaus Rechnung getragen wird. Der Vorentwurf hatte überhaupt noch keine datenschutzrechtlichen Vorschriften enthalten. Zu meinem Bedauern sind allerdings die Vorschläge, die ich der Behörde Ende 1985 für die Regelung des Patientendatenschutzes unterbreitet hatte, nicht in den Entwurf eingeflossen. Da mir insbesondere die zentrale Vorschrift, die den krankenhausinternen Umgang mit Patientendaten und deren Übermittlung an externe Stellen regelt, überarbeitungsbedürftig erschien und ich auch die Regelungen für die Forschung mit Patientendaten und für klinische Krankheitsregister in der vorgeschlagenen Fassung nicht akzeptieren kann, habe ich mit meiner Stellungnahme noch einmal einen ausformulierten Entwurf für die datenschutzrechtlichen Vorschriften vorgelegt, der im wesentlichen auf meinen früheren Vorschlägen beruht, aber auch Anregungen aus gesetzlichen Regelungen bzw. Entwürfen anderer Bundesländer aufgreift.

Dabei habe ich, der besseren Übersicht wegen, gesonderte Vorschriften für die interne Datenverarbeitung und die Datenübermittlung vorgesehen. Inhaltlich bemühen sie sich, die heute im Krankenhausbetrieb praktizierten Datenverarbeitungsvorgänge gesetzlich abzusichern, die bislang aufgrund unterstellter oder pauschal erteilter Einwilligungserklärungen als vereinbar mit der ärztlichen Schweigepflicht angesehen wurden. Die gesetzliche Regelung bietet den Vorteil größerer Rechtssicherheit, da die Wirksamkeit der Einwilligung in vielen Fällen — sei es mangels ausreichender Information des Patienten oder wegen fehlenden Erklärungsbewußtseins — angezweifelt werden konnte.

Auch die von mir vorgeschlagene Regelung für die Forschung mit Patientendaten soll den Ärzten größere Rechtssicherheit geben und die betroffenen Patienten besser über die Verwendung ihrer Daten aufklären. Das Hamburgische Datenschutzgesetz enthält in seiner geltenden Fassung noch keine Forschungsklausel. Abgesehen vom Krebsregistergesetz mit seinen Spezialregelungen fehlt es bisher an einer Rechtsgrundlage und an Abwägungskriterien für die Forschung mit personenbezogenen Daten ohne Einwilligung des Patienten. Dadurch werden unbestreitbar wichtige und sinnvolle Forschungsvorhaben mit großer Unsicherheit belastet. Das gilt vor allem für die Auswertung bereits vorhandener Daten, für deren Verwendung zu Forschungszwecken keine Einwilligung vorliegt. Nach meinem Vorschlag soll den Patienten für die klinik- oder abteilungsinterne Forschung ein Widerspruchsrecht gegen die Nutzung ihrer Daten eingeräumt werden. In engen Grenzen dürfen die Daten auch ohne Beteiligung des Patienten verwertet werden, wenn nämlich schutzwürdige Belange nicht beeinträchtigt werden und die Möglichkeit zum Widerspruch nicht oder nur mit unverhältnismäßigem Aufwand eingeräumt werden kann.

Die Übermittlung von Daten für bestimmte Forschungsvorhaben an Stellen außerhalb der Klinik bzw. Abteilung sollte grundsätzlich nur mit Einwilligung des Patienten zugelassen werden. Für die ausnahmsweise Übermittlung ohne seine Einwilligung sind strenge Anforderungen zu stellen und besondere Sicherungsmaßnahmen vorzuschreiben.

Für die Klinischen Krankheitsregister weicht mein Regelungsvorschlag deutlich von dem der Gesundheitsbehörde ab. Ich halte es für notwendig, zwischen den Registern, die ausschließlich Forschungszwecken zu dienen bestimmt sind, und solchen, die primär für Behandlungszwecke eingerichtet werden, zu differenzieren. Erstere bedürfen meiner Meinung nach einer spezialgesetzlichen Grundlage, wie sie etwa für das Hamburgische Krebsregister geschaffen worden ist. Die Forschung mit Patientendaten aus einem der Behandlung dienenden Register ist kein Sonderfall, der eine privilegierende Regelung rechtfertigt. Sie hat vielmehr die gleichen Voraussetzungen und Abwägungskriterien zu beachten wie jede andere Forschung im Geltungsbereich des Krankenhausgesetzes.

Schließlich will mein Alternativentwurf die Stellung des — bisher auf freiwilliger Grundlage eingesetzten — Datenschutzbeauftragten im Krankenhaus dadurch stärken, daß er in die gesetzliche Regelung mit einbezogen wird.

Die Gesundheitsbehörde hat zu meinen Vorschlägen bis zum Ende des Berichtsjahres noch nicht Stellung nehmen können.

4.16.1.2 Dienstanweisung über die Führung und Herausgabe von Krankenakten und Röntgenbildern

Im 5. TB (5.12.2, S. 94) habe ich über den Entwurf einer Dienstanweisung berichtet. Sie ist am 6. 1. 1987 in Kraft getreten. Meine Anregungen und Änderungswünsche sind im wesentlichen berücksichtigt worden. Lediglich für die Informationsweitergabe an vor- und nachbehandelnde Ärzte habe ich anstelle der zunächst geforderten Einwilligung eine Widerspruchslösung akzeptiert, wie sie auch im Entwurf des Hmb. Krankenhausgesetzes für diese Fälle vorgesehen ist.

4.16.1.3 Auskunft an der Krankenhauspforte

Bereits wenn sich Besucher an der Pforte oder bei der Verwaltung des Krankenhauses erkundigen, ob sich eine bestimmte Person dort zur Behandlung aufhält, sind Fragen der ärztlichen Schweigepflicht berührt. Im Regelfall ist allerdings davon auszugehen, daß der Patient die Kontaktaufnahme von Angehörigen und Bekannten wünscht und eine Auskunftserteilung von Verwaltungsstellen geradezu erwartet. Deshalb erscheint es mir ausreichend, wenn in geeigneter Form über die Möglichkeit informiert wird, in besonderen Fällen eine Auskunftssperre zu erwirken. Eine generelle Einwilligungserklärung für die Auskunftserteilung an der Pforte halte ich weder für erforderlich noch für praktikabel.

Besondere Brisanz hat die Auskunftserteilung für Patienten einer psychiatrischen Klinik. Ihnen wird man nicht ohne weiteres die Bereitschaft zur Offenbarung ihres Patientenstatus gegenüber jedem Anfragenden unterstellen können. Es bedarf vielmehr der Prüfung im Einzelfall, ob eine Kontaktaufnahme erwünscht ist. Ich habe angeregt, nähere Einzelheiten im Kreis der Datenschutzbeauftragten der Krankenhäuser mit dem Ziel zu diskutieren, eine differenzierende Regelung zu erarbeiten.

Mit einem Sonderfall der Auskunftserteilung durch die Krankenhausverwaltung habe ich mich auf Anfrage der Gesundheitsbehörde befaßt: Es ging um die Auskunftserteilung an Gerichtsvollzieher bei Zustellungsversuchen und bei beabsichtigten Zwangsvollstreckungshandlungen im psychiatrischen Krankenhaus. Probleme treten hier zum einen auf, wenn der Gerichtsvollzieher nicht erkennen kann, ob es sich bei dem Adressaten um eine auf dem Krankenhausgelände wohnende Pflegeperson oder um einen Patienten handelt und er mit dieser Fragestellung an die Verwaltung herantritt. Zum anderen kommt es vor, daß der Gerichtsvollzieher nach mißlungenen Zustellungs-

oder Zwangsvollstreckungsversuchen aufgrund mehr oder weniger vager Hinweise in der psychiatrischen Klinik nachfragt, ob sich der Gesuchte dort befindet.

Ich halte in beiden Fällen die Auskunftserteilung über die Patienteneigenschaft des Gesuchten für einen Verstoß gegen die ärtzliche Schweigepflicht. Das Krankenhauspersonal ist weder verpflichtet noch berechtigt, dem Gerichtsvollzieher die gewünschte Auskunft zu erteilen.

Es ist Aufgabe des Gläubigers, den in seinem Auftrag tätigen Gerichtsvollzieher über die exakte Anschrift des Schuldners zu informieren. Da das auf dem Krankenhausgelände wohnende Personal mit Haus- und Zimmernummer bei der Meldebehörde erfaßt wird, können die erforderlichen Angaben bezüglich dieser Personengruppe von der zuständigen Behörde eingeholt werden. Patienten, die sich zwar vorübergehend im psychiatrischen Krankenhaus aufhalten, aber ansonsten einen festen Wohnsitz unterhalten, können, wie jeder andere Schuldner auch, über diese Anschrift erreicht werden, notfalls im Wege der Ersatzzustellung. Lediglich für die kleine Gruppe der Patienten ohne gemeldeten Wohnsitz außerhalb des Krankenhauses müßte eine Zustellungsmöglichkeit, evtl. durch einen Zustellungsbevollmächtigten geschaffen werden. Sie sind unter der Adresse des Krankenhauses ohne näheren Zusatz bei der Meldebehörde registriert. Sofern dem Gerichtsvollzieher ihr Aufenthaltsort, z.B. aufgrund einer Auskunft aus dem Melderegister bekannt ist, wird auch die ärztliche Schweigepflicht nicht berührt.

4.16.1.4 *Ergebnisse aus der Prüfung des AK Altona*

Über die Mängel und Probleme bei der Verarbeitung von Patientendaten, die anläßlich der Prüfung der Abrechnungsabteilung des AK Altona offensichtlich wurden, habe ich in meinem 4. TB berichtet. Insbesondere hatte ich gerügt, daß bei der Aufnahme von Patienten eine Reihe von Daten routinemäßig erhoben werden, die zur Abwicklung des Behandlungsvertrages nicht erforderlich sind.

Aufgrund meines Prüfungsberichts hat der Landesbetrieb Krankenhäuser die Patientenerfassungsbelege für die Allgemeinen Krankenhäuser geändert und meine Vorschläge weitgehend berücksichtigt. So wird bei der Datenerhebung über die Religionszugehörigkeit und über Name und Anschrift von Angehörigen auf die Freiwilligkeit der Angaben hingewiesen. Der Geburtsort, die Ausweis- bzw. Paßnummer und der Beruf werden nicht mehr erfragt. Die Erhebung von Angaben über den Arbeitgeber und den einweisenden Arzt hält der Landesbetrieb weiterhin für erforderlich, um in Zweifelsfällen den Kostenträger ermitteln zu können. Die Erhebung des Geburtsnamens sei im Hinblick auf die Einwohnermeldeamtsanfrage unverzichtbar.

Zunächst nicht berücksichtigt wurde meine Forderung, auf die routinemäßige Erhebung des Familienstandes zu verzichten. Der zur Begründung gegebene Hinweis auf § 9 Abs. 3 Hmb. Gebührengesetz, der die Zahlungspflicht des Ehegatten regelt, rechtfertigt indessen nicht die differenzierende Erhebung der Merkmale „geschieden", „verwitwet" oder gar „getrennt lebend", sondern läßt allenfalls die Frage zu, ob der Patient verheiratet ist oder nicht. Der Landesbetrieb hat eine entsprechende Änderung des Erfassungsbelegs zugesagt.

Noch eine Konsequenz aus dem Prüfungsbericht hat der Landesbetrieb gezogen. Nunmehr sind Mitarbeiter der Rechnungsabteilung und der Aufnahme auf das Datengeheimnis verpflichtet worden.

4.16.1.5 Übermittlung von Patientendaten von den Krankenhäusern an Krankenkassen

Bei der Prüfung eines Vertragsentwurfs, in dem gem. § 372 RVO zwischen der Hamburgischen Krankenhausgesellschaft und dem Landesverband der Krankenkassen Art und Umfang der Krankenhauspflege vereinbart werden sollen, hatte ich mich mit der Frage zu befassen, welche Daten von Krankenhäusern an Krankenkassen übermittelt werden dürfen. Gegenstand der vertraglichen Regelung sind auch Auskunftspflichten der Krankenhäuser über Patientendaten, die die Krankenkassen zur Erfüllung ihrer

gesetzlichen Pflichten, insbesondere zu Abrechnungszwecken und zur Prüfung ihrer Leistungspflicht benötigen. Dabei setzt der Vertragsentwurf stillschweigend voraus, daß § 372 RVO eine Befugnis des Krankenhauses zur Offenbarung von Patientendaten an die Kostenträger beinhaltet.

Diese Ansicht wird zwar insbesondere vom 6. Senat des Bundessozialgerichts, zuletzt im Urteil vom 19. 11. 1985 (NJW 1986, 1574) vertreten, die Argumentation des Bundessozialgerichts ist jedoch umstritten und für mich wenig überzeugend.

Aus der Systematik der RVO-Vorschriften ergibt sich, daß § 372 lediglich das Verhältnis zwischen Kostenträger und Krankenhaus regelt, dagegen die Rechtsbeziehungen zwischen Patient und Krankenhaus unberührt läßt. Das Bundessozialgericht hingegen schließt von den gesetzlich geregelten Mitwirkungspflichten des Leistungserbringers im Verhältnis zum Kostenträger ohne weiteres auf die Offenbarungsbefugnis im Arzt-Patientenverhältnis. Die Begründung, daß die Mitteilungspflicht typischerweise die Offenbarung von Patientengeheimnissen mit sich bringe und das komplexe Leistungssystem der Reichsversicherungsordnung ohne Übermittlung von bestimmten Patientendaten funktionsunfähig werde, läßt die Forderung des BVerfG nach normenklaren bereichsspezifischen Regelungen und Transparenz für den Betroffenen außer Betracht.

Eine Befugnis des Krankenhauses zur Offenbarung von Patientendaten muß aus anderen Erlaubnistatbeständen hergeleitet werden. In Betracht kommt mangels gesetzlicher Befugnisnorm die Einwilligung des Patienten. Für den für Abrechnungszwecke bzw. zur Prüfung der Leistungspflicht unverzichtbaren Datenfluß wird man eine stillschweigende Einwilligung durch Inanspruchnahme der Leistung unterstellen können. Für die darüber hinausgehenden Übermittlungen ist zu fordern, daß eine Befugnisnorm in der RVO geschaffen wird. Unbefriedigend erschiene mir allerdings die bloße Einfügung einer formal einwandfreien, die derzeitige Übermittlungspraxis absichernden Rechtsgrundlage. Erforderlich ist vielmehr die Erarbeitung und Festlegung inhaltlicher Kriterien für die Beurteilung der erforderlichen Informationsflüsse, die bei der anstehenden Novellierung der RVO im Rahmen ihrer Einarbeitung in das Sozialgesetzbuch eingebracht werden könnten. Für eine Übergangszeit muß der zur Aufrechterhaltung des Systems der Krankenhausversorgung unabdingbar erforderliche Informationsaustausch hingenommen werden, weitergehende Übermittlungen sind aus Sicht des Datenschutzes nicht akzeptabel.

4.16.2 Gesundheitsämter

In den vorangegangenen Tätigkeitsberichten habe ich bereits mehrfach über datenschutzrechtliche Probleme in den Gesundheitsämtern berichtet, auf die ich bei der Prüfung eines Bezirksgesundheitsamtes gestoßen bin. Zur Aufarbeitung der kritischen Anmerkungen in meinem Prüfungsbericht war ein Arbeitskreis „Datenschutz im Gesundheits- und Umweltamt" gebildet worden, in dem Vertreter der Gesundheitsbehörde und der Gesundheitsämter in sechs Arbeitsgruppen die Bereiche „Zentralkartei", „Gutachterwesen", „Medizinalkartei", „Überwachung des BTM-Verkehrs", „Geburts- und Todesbescheinigungen" und „Sozial- und Jugendpsychiatrischer Dienst" behandelten.

Die Arbeitsgruppen tagten zunächst ohne Beteiligung des Datenschutzbeauftragten. Erst zu Anfang des Berichtsjahres legten sie mir ihre Arbeitsergebnisse zur Stellungnahme vor, diese wurde dann wieder intern von den einzelnen Arbeitsgruppen diskutiert und in der Folgezeit — bislang von drei Arbeitsgruppen — mit mir beraten. Die Beratungen mit zwei Arbeitsgruppen stehen noch aus, der Bereich „Überwachung des BTM-Verkehrs" wurde schriftlich erörtert.

Nach wie vor halte ich die von den Arbeitsgruppen gewählte Verfahrensweise, bei der der Rat des Datenschutzbeauftragten erst in einem späten Stadium gehört wird, für wenig sachdienlich. Aufgabe der Arbeitsgruppen ist weniger die Rechtfertigung der bisherigen, von mir bemängelten Praxis als vielmehr eine Neuorientierung der Informationsverarbeitung in den Gesundheits- und Umweltämtern unter Berücksichtigung

des Grundrechts auf informationelle Selbstbestimmung. Dies hätte m.E. die frühzeitige Einbeziehung datenschutzrechtlichen Sachverstandes bei der Suche nach sowohl praxisgerechten als auch datenschutzkonformen Lösungswegen erfordert und nicht eine Reduzierung der Informations- und Diskussionsbasis auf Arbeitsgruppenergebnisse.

Einen abschließenden Bericht über die Konsequenzen aus der Prüfung des Bezirksgesundheitsamtes kann ich zwar noch nicht abgeben, in einzelnen Arbeitsgruppen zeichnen sich jedoch bereits Teilergebnisse ab.

4.16.2.1 Zentralkartei

Die Arbeitsgruppe hat bei der Vorstellung ihrer ersten Arbeitsergebnisse betont, daß die Zentralkartei, über die Vorgänge aus den Abteilungen Gutachterwesen, Körperbehindertenfürsorge, Sozialpsychiatrische Dienste und zum Teil Seuchenbekämpfung erschlossen werden können, für eine rationelle Verwaltungstätigkeit unverzichtbar sei. Allenfalls die Vorgänge aus der Abt. Seuchenbekämpfung könnten ausgegliedert werden. Die Zentralkartei diene vor allem der Postverteilung, in Ausnahmefällen würden auch telefonische Auskünfte über bestehende Vorgänge erteilt.

In meiner Stellungnahme habe ich klargestellt, unter welchen Voraussetzungen die Zentralkartei als interne Suchdatei weiter benutzt werden kann: Neben geeigneten technischen und organisatorischen Maßnahmen zur Verhinderung der unbefugten Einsichtnahme in die Kartei oder Wegnahme von Karteikarten ist eine eindeutige Festlegung der Zugangsberechtigung erforderlich. Aus der Datei dürfen Auskünfte an Dritte, sei es an andere Dienststellen oder sonstige Anfrager, nicht erteilt werden. Nach Ablauf der Aufbewahrungsfrist für einen Vorgang ist die entsprechende Karteikarte zu vernichten bzw. der Hinweis auf den Altvorgang zu löschen, wenn die Karteikarte mehrere Vorgänge erschließt.

Vor allem aber muß die Trennung der verschiedenen Funktionsbereiche des Gesundheitsamtes auch in der Zentralkartei beachtet werden: Der hoheitliche Funktionsbereich ist strikt vom nicht-hoheitlichen zu trennen. Die Zentralkartei darf nicht dazu genutzt werden, Erkenntnisse z.B. aus der Beratungstätigkeit auf freiwilliger Grundlage für den hoheitlichen Funktionsbereich nutzbar zu machen.

Abschließende Beratungen mit der Arbeitsgruppe Zentralkartei werden voraussichtlich im nächsten Monat stattfinden.

4.16.2.2 Gutachterwesen

Die Abteilung Gutachterwesen des Gesundheitsamtes fertigt aus verschiedenen Anlässen Gutachten über den Gesundheitszustand von Bürgern an, die i.d.R. anderen Behörden als Entscheidungsgrundlage für den Nachweis der Anspruchsberechtigung auf einen begünstigenden Verwaltungsakt oder für einen Eingriff in Rechtspositionen dienen.

Sowohl bei der bisher üblichen Beiziehung von bereits im Gesundheitsamt vorhandenen Vorgängen als auch bei der Übermittlung des Untersuchungsergebnisses an die anfordernde Stelle sind Fragen des Datenschutzes und der ärztlichen Schweigepflicht berührt, die mit der Arbeitsgruppe Gutachterwesen mit folgendem Ergebnis beraten wurden:

Auch für die Abteilung Gutachterwesen gilt der Grundsatz der informationellen Abschottung der einzelnen Funktionsbereiche des Gesundheitsamtes. Grundsätzlich muß eine strikte Trennung zwischen den Beratungsdiensten auf freiwilliger Grundlage und der amtsärztlichen Tätigkeit sichergestellt werden. Auf keinen Fall darf die Zentralkartei dazu genutzt werden, Vorgänge über den zu Begutachtenden aus anderen Funktionsbereichen aufzuspüren und ohne seine Einwilligung beizuziehen. Das gilt auch für bereits im Gesundheitsamt vorliegende Gutachten, die aus anderem Anlaß erstellt worden sind.

Grundlage für ein amtsärztliches Gesundheitszeugnis sind die Ergebnisse einer aktuellen ärztlichen Untersuchung und die Angaben des Untersuchten, die er im

Hinblick auf eine bestimmte Fragestellung entweder freiwillig oder aus einer gesetzlichen Verpflichtung heraus macht. Diese Datenerhebung ist zweckgebunden und kann später nicht beliebig für andere Gutachten verwertet werden. Eine Beiziehung bereits vorhandener Vorgänge ist von der Einwilligung des Betroffenen abhängig. Soweit deren Erteilung für die Erstellung des Gutachtens unverzichtbar erscheint und den Betroffenen eine Mitwirkungspflicht trifft, ist er auf die möglichen Folgen einer fehlenden Mitwirkung hinzuweisen. Im übrigen muß in Kauf genommen werden, daß bei einer Verweigerung der Einwilligung Qualität und Aussagekraft eines Gutachtens leiden können, weil die mangelnde Kenntnis der Altvorgänge nicht immer durch die ärztliche Kunst, die Vorgeschichte gesprächsweise und untersuchungstechnisch vollständig zu erfassen, ausgeglichen werden kann.

Die Weitergabe des Gutachtens an die anfordernde Stelle ist i.d.R. bei einem für den Untersuchten positiven Ergebnis unproblematisch. In diesen Fällen kann man eine Einwilligung in die Weitergabe des Ergebnisses der Untersuchung unterstellen, nicht dagegen in die Offenbarung von Befunden, Diagnosen oder einzelnen Gesundheitsdaten. Übermittelt werden darf nur das für die konkrete Fragestellung relevante Ergebnis.

Kommt das Gutachten zu einem für den Betroffenen nachteiligen Ergebnis und sind für die Begründung des ablehnenden Bescheids Diagnosen und Befunde erforderlich, bedarf die Übermittlung dieser Daten an die anfordernde Stelle der Einwilligung des Untersuchten in die Durchbrechung der ärztlichen Schweigepflicht. Eine wirksame Einwilligung setzt voraus, daß der Betroffene über Inhalt und Umfang der Gesundheitsdaten, die der anfordernden Stelle mitgeteilt werden sollen, informiert wird. Dies kann in aller Regel nicht generell und vorab geschehen, sondern erst dann, wenn das Untersuchungsergebnis vorliegt und die zu übermittelnden Daten bekannt sind.

Im Falle einer nicht duldungspflichtigen Begutachtung wird dem Betroffenen freigestellt, die Weitergabe eines für ihn nachteiligen Gesundheitszeugnisses zu untersagen mit der Folge, daß er auf den beantragten begünstigenden Verwaltungsakt verzichten muß. Das Verfahren der Gutachtenübermittlung wird durch eine mit mir abzustimmende Fachliche Weisung festgelegt.

4.16.2.3 Medizinalkartei

Zur Überprüfung der Berechtigungsnachweise von Medizinalpersonen, zur Überwachung ihrer Betätigung in den Grenzen ihres Befähigungszeugnisses sowie zur Überwachung der Ausübung des Heilgewerbes durch staatlich nicht anerkannte Heilpraktiker führt jedes Gesundheitsamt eine Medizinalkartei über die in seinem Bezirk tätigen Medizinal- und Heilhilfspersonen.

Über die Aufnahme der Tätigkeit von Ärzten, Zahnärzten und Apothekern erhält das Gesundheitsamt Kenntnis durch Meldung der jeweiligen Kammern. Rechtsgrundlagen für die Datenübermittlung gibt es im Ärzte-, Zahnärzte- und Apothekergesetz. Letzteres nimmt allerdings Bezug auf die „zuständige Behörde" und das ist in Hamburg nach der Zuständigkeitsanordnung die Gesundheitsbehörde. Die Datenübermittlung an die Gesundheitsämter ist daher mangels Aufgabenzuweisung unzulässig, soweit die Apotheker betroffen sind.

Die sonstigen vom Gesundheitsamt erfaßten und überwachten Medizinalpersonen unterliegen mit Ausnahme der Hebammen keiner gesetzlichen Meldepflicht. Die Registrierung erfolgt nur lückenhaft bei Selbstmeldung oder — beim Krankenpflegepersonal — aufgrund von Erkenntnissen aus Betriebsbesichtigungen.

Hier stellt sich die Frage, ob eine in dieser Form praktizierte Überwachung noch sinnvoll und zeitgemäß ist, zumal es jedenfalls bei abhängig Beschäftigten in erster Linie Aufgabe des Arbeitgebers ist, eine Betätigung im Rahmen der vorhandenen Qualifikation sicherzustellen.

Grundsätzlich dürfen von allen registrierten Medizinalpersonen nur die Daten erfaßt und gespeichert werden, die zur Erfüllung der Überwachungsaufgaben des Gesund-

heitsamtes erforderlich sind. Unzulässig ist z.B. die Erfragung von Angaben zu wirtschaftlichen Verhältnissen, Familienstand, Religionszugehörigkeit. Auch die Auswertung der Mitteilungen in Strafsachen für die Medizinalkartei erscheint nicht zur Aufgabenerfüllung erforderlich, da Maßnahmen aufgrund dieser Mitteilungen von der Gesundheitsbehörde eingeleitet werden. Es wäre für die Überwachung der Grenzen der Betätigung der Medizinalpersonen ausreichend, wenn die Gesundheitsbehörde den Gesundheitsämtern berufsbeschränkende Maßnahmen (z.B. Ruhen der Approbation) melden würde. Die Speicherung von Bestrafungen ist auch insofern problematisch, als die Beachtung der Verwertungsverbote des Bundeszentralregistergesetzes nicht sichergestellt ist.

Unter diesen Gesichtspunkten ist der Datenbestand der Gesundheitsämter zu überprüfen und ggf. zu bereinigen. Eine Berechtigung zur kartei- oder listenmäßigen Erfassung besteht nur hinsichtlich der Medizinalpersonen, die im Zuständigkeitsbereich des Gesundheitsamtes tätig sind. Die Führung einer „toten Kartei" ist unzulässig. Sie ist daher zu vernichten. Scheidet eine Medizinalperson aus dem Berufsleben aus, darf das Gesundheitsamt von ihr keine Daten mehr speichern. Verläßt sie den Bezirk, bestehen keine Bedenken, mit der von der Arbeitsgruppe vorgeschlagenen Einverständniserklärung eine Grundlage für die Datenübermittlung an das zuständige Gesundheitsamt zu schaffen.

Die abschließenden Beratungen mit der Arbeitsgruppe stehen noch aus.

4.16.2.4 Überwachung des BTM-Verkehrs, Suchterkennung

Die Gesundheits- und Umweltämter sind für die Überwachung des BTM-Verkehrs außerhalb von Apotheken und tierärztlichen Hausapotheken zuständig. Unter Berufung auf diese Aufgabe forderten sie in der Vergangenheit Kopien von allen BTM-Rezepten von den Apotheken an. Schon die Arbeitsgruppe war zu der Erkenntnis gekommen, daß dieses Verfahren mangels Rechtsgrundlage unzulässig war. Unter Mitwirkung meiner Dienststelle ist ein Verfahren entwickelt worden, wonach Ärzte stichprobenartig aufgefordert werden, über Anzahl und Kennzeichnung der bei ihnen vorhandenen und der verbrauchten BTM-Rezepte Auskunft zu geben und dem Gesundheitsamt die bei ihnen verbliebenen BTM-Rezeptdurchschriften zur Überprüfung einzureichen. Gegen dieses Verfahren, das in § 22 BtMG seine Rechtsgrundlage hat, bestehen keine datenschutzrechtlichen Bedenken.

4.16.2.5 Geburts- und Todesbescheinigungen

Die Gesundheitsämter benutzen die ihnen von Standesbeamten zur Aufbewahrung zugeleiteten Geburtsbescheinigungen als Informationsquelle für die Erfüllung ihrer Aufgaben. Dabei haben sie bisher auch auf Daten zurückgegriffen, die ohne Rechtsgrundlage oder nur für statistische Zwecke erhoben worden sind. Dies soll nach dem Ergebnis der Beratungen mit der Arbeitsgruppe für die Zukunft durch eine Neugestaltung des Formulars der Geburtsbescheinigung verhindert werden.

Unzulässig war insbesondere die Auswertung der Geburtsbescheinigungen hinsichtlich des Merkmals der „sichtbaren körperlichen Fehler", das aufgrund des „Gesetzes über die Statistik der Bevölkerungsbewegung und die Fortschreibung des Bevölkerungsstandes" erhoben wird, und die Erhebung von Risikofaktoren bei der Geburt. Die Gesundheitsämter nutzten diese Informationen gezielt zu Hausbesuchen, was von einigen Betroffenen als unerwünschte Einmischung und Kontrolle aufgefaßt wurde und auch zu einer Eingabe beim Datenschutzbeauftragten geführt hat.

In der Arbeitsgruppe konnte Einvernehmen darüber hergestellt werden, daß eine gezielte Datenerhebung über behinderte oder durch eine Risikoentbindung belastete Kinder nur aufgrund einer spezialgesetzlichen Regelung zulässig wäre, in der Zweck und Umfang der Datenerhebung und -nutzung präzise bestimmt sind.

Nachdem mein Vorschlag, mit Hilfe der Entbindungsstationen über Angebote der Mütterberatung zu informieren, als nicht durchführbar zurückgewiesen wurde, habe ich

es für akzeptabel erklärt, künftig Namen und Anschrift der Eltern eines Neugeborenen der Geburtsbescheinigung zu entnehmen, da diese — weniger sensiblen — Daten auch von der Meldebehörde zur Aufgabenerfüllung abgefordert werden dürften.

Im übrigen ist die Geburtsbescheinigung so umzugestalten, daß keine Daten über Risikofaktoren bei der Geburt mehr erhoben werden und die zu statistischen Zwecken erhobenen Daten nicht mehr personenbezogen ausgewertet werden können.

Hinsichtlich der Todesbescheinigungen bestehen nach geltendem Recht keine ausreichenden Grundlagen für die Übermittlung von Daten an Dritte, z.B. an Angehörige oder Versicherungen. Der Entwurf eines Hamburgischen Bestattungsgesetzes, der z.Z. das Behördenabstimmungsverfahren durchläuft, enthält jedoch eine entsprechende, aus datenschutzrechtlicher Sicht akzeptable Regelung.

4.16.2.6 Sozial- und Jugendpsychiatrischer Dienst

Die Sozial- und Jugendpsychiatrischen Dienste der Gesundheits- und Umweltämter bieten aufgrund des Hmb. Gesetzes über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten (PsychKG) Hilfe und Beratung für psychisch Kranke an, treffen aber auch Maßnahmen zur Abwendung einer Selbstgefährdung oder einer Gefährdung der öffentlichen Sicherheit und Ordnung bis hin zur zwangsweisen Unterbringung in einer geschlossenen Anstalt.

Aus der Sicht des Betroffenen kann er die Hilfs- und Beratungsangebote freiwillig annehmen oder ablehnen, während Maßnahmen zur Gefahrenabwehr einschließlich der Unterbringung gegen seinen Willen gegen ihn durchgesetzt werden können.

Datenschutzrechtliche Probleme treten auf, wenn ein Erkrankter zunächst freiwillig die Hilfs- und Beratungsangebote annimmt und hierüber ein Vorgang mit sensiblen, der ärztlichen Schweigepflicht unterliegenden Daten angelegt wird, der bei einer späteren, krisenhaften Zuspitzung der Erkrankung für Zwangsmaßnahmen beigezogen wird. In meiner Stellungnahme zum Bericht der Arbeitsgruppe „Sozial- und Jugendpsychiatrischer Dienst" habe ich daher gefordert, daß für den betroffenen Bürger jederzeit klar erkennbar sein müsse, in welcher Rechtsbeziehung er sich zur psychiatrischen Dienststelle befindet. Für die Beiziehung von Vorgängen aus einer früheren, freiwillig angenommenen Beratung sowie für die Weitergabe derartiger Vorgänge vom Jugend- an den Sozialpsychiatrischen Dienst oder an die entsprechenden Dienste anderer Bezirksämter im Falle eines Umzugs des Betroffenen sei die Einwilligung des Hilfsbedürftigen einzuholen, sofern sein Zustand dies zulasse.

In den Beratungen der Arbeitsgruppe ist diese Forderung als nicht praxisgerecht abgelehnt worden. Nach Auffassung der Praktiker werden die Psychiatrischen Dienste stets hoheitlich tätig, da sie zur Gewährung der Hilfen verpflichtet seien. Außerdem sei im Falle von Zwangsmaßnahmen die Einwilligung in die unbedingt erforderlich Beiziehung von früheren Vorgängen kaum zu erlangen, häufig gehöre die Verleugnung der Erkrankung zum Krankheitsbild.

Auch wenn ich die Probleme der Dienste mit der Einholung von Einwilligungserklärungen nachvollziehen kann, halte ich es für unzulässig, das Grundrecht auf informationelle Selbstbestimmung für psychisch Kranke faktisch pauschal außer Kraft zu setzen. Für die Datenerhebung und -verarbeitung im Rahmen der für den Betroffenen freiwilligen Beratungs- und Betreuungsangebote gibt es nach geltendem Recht keine bereichsspezifische gesetzliche Grundlage. Allerdings ist im Entwurf eines Hamburgischen Maßregelvollzugsgesetzes die Ergänzung des PsychKG um Vorschriften über Erhebung, Nutzung und Übermittlung von Daten psychisch Kranker geplant.

Im Hinblick darauf, daß mit einem alsbaldigen Inkrafttreten der neuen Regelung gerechnet werden kann und auch ich die Probleme mit der Einwilligung zur Beiziehung von früheren Vorgängen nicht in Abrede stelle, habe ich meine datenschutzrechtlichen Anforderungen modifiziert: Für unverzichtbar halte ich eine Aufklärung des Hilfe- und Beratungsuchenden über die Freiwilligkeit seiner Angaben, über den Zweck der

Datenerhebung und die Möglichkeit einer künftigen Datenübermittlung. Das ergibt sich schon aus geltendem Recht: § 9 Abs. 2 HmbDSG bestimmt, daß der Betroffene, sofern Daten aufgrund einer Rechtsvorschrift bei ihm erhoben werden, auf sie, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen ist. Diese Aufklärungspflicht wird durch den Referentenentwurf der Justizbehörde zur Novellierung des HmbDSG (§ 12 Abs. 3), der insoweit Neuregelungen des Hessischen und des Bremer Datenschutzgesetzes aufgreift, in mehrfacher Hinsicht erweitert: Werden Daten beim Betroffenen erhoben, ist er über den Verwendungszweck aufzuklären. Werden sie aufgrund einer durch Rechtsvorschrift festgelegten Auskunftspflicht erhoben, dann ist er in verständlicher Form auf sie, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Werden vom Betroffenen freiwillige Angben erbeten, so ist er über mögliche Folgen einer Nichtbeantwortung aufzuklären.

Wenn der Betroffene in geeigneter Form darauf hingewiesen wird, daß die vertraulichen Informationen aktenmäßig erfaßt werden und später übermittelt werden können, und wird ihm das Recht eingeräumt, die Speicherung von Angaben, die er nicht aktenkundig machen möchte, zu untersagen, scheint mir eine spätere Einwilligung in die Beiziehung von bereits vorhandenen Vorgängen entbehrlich.

Ein weiteres Problem, das von der Arbeitsgruppe erörtert wurde, betrifft die Meldung über Suizidversuche von der Polizei an die Gesundheits- und Umweltämter. Ich halte die Rechtsgrundlage aus § 3 SOG, auf die die Polizei die Datenübermittlung stützt, für fragwürdig. Bei Personen, die nach einem Suizidversuch ins Krankenhaus eingeliefert werden, erfolgt die Abwehr der unmittelbaren Gefährdung durch die dortige ärztliche Behandlung, eine Meldung an das Gesundheitsamt ist nicht erforderlich.

In der Arbeitsgruppe bestand im Prinzip Übereinstimmung, daß die polizeiliche Meldung über Suizidversuche baldmöglichst abgestellt werden soll. Anzustreben ist, daß der Patient vom behandelnden Arzt auf nachsorgende Hilfsangebote der Bezirksämter und anderer Stellen hingewiesen und gebeten wird, in die Weitergabe von Informationen über den Suizidversuch an das Gesundheitsamt einzuwilligen.

4.16.3 Entwurf eines hamburgischen Maßregelvollzugsgesetzes

Am Ende des vorigen Berichtsjahres war mir der Entwuf eines Hamburgischen Maßregelvollzugsgesetzes zur Prüfung und Stellungnahme zugeleitet worden. Gegenüber dem Vorentwurf sind einige Fortschritte vor allem in Richtung auf die erforderliche Normenklarheit zu begrüßen. Dies gilt insbesondere für den neu gefaßten § 36 des Entwurfs, der die Voraussetzungen für die Verarbeitung von personenbezogenen Patientendaten regelt, und für die in § 40 vorgesehene Änderung des Hmb. Gesetzes über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten, in das eine mit dem § 36 im wesentlichen inhaltsgleiche Vorschrift eingefügt werden soll.

Gegen einzelne Erhebungstatbestände und die entsprechenden Regelungen für die Speicherung und Übermittlung habe ich in meiner Stellungnahme Bedenken geäußert, die von der Gesundheitsbehörde nur zum Teil berücksichtigt worden sind. Erhebliche Meinungsverschiedenheiten bestehen noch in zwei Punkten:

Die Durchführung wissenschaftlicher Forschungsvorhaben knüpft der Entwurf lediglich an zwei Voraussetzungen: Die Daten müssen dem forschenden Wissenschaftler in näher bezeichneter Weise bei der Durchführung des Vollzuges oder damit zusammenhängenden Tätigkeiten bekannt geworden sein und schutzwürdige Belange der Betroffenen dürfen nicht beeinträchtigt werden. Eine Unterrichtung oder gar die Einwilligung des Betroffenen ist nicht vorgesehen. Demgegenüber bin ich der Ansicht, daß auch und gerade für zwangsweise Untergebrachte der Grundsatz gelten muß: Kein Patient darf ohne sein Wissen und sein Einverständnis zum Objekt der Forschung mit Daten gemacht werden, die zu seiner Behandlung erhoben werden. Deshalb habe ich gefordert, entweder klarzustellen, daß auch die interne Verwendung von Daten Untergebrachter zu Forschungszwecken nur in anonymisierter Form zulässig ist, oder für den Fall, daß der Forschungszweck nur durch die Verarbeitung personenbezogener

Daten zu erreichen ist, den Betroffenen über die Verwendung seiner Daten zu Forschungszwecken zu informieren und ihm zumindest ein Widerspruchsrecht einzuräumen.

Datenschutzrechtliche Bedenken bestehen auch gegen die in §§ 36 Abs. 3 S. 3 und § 40 Abs. 1 Ziff. 4 des Entwurfs vorgesehene Regelung, wonach nicht benötigte personenbezogene Daten übermittelt werden dürfen, wenn sie von den benötigten nur mit unverhältnismäßigem Aufwand getrennt werden können. Ein rechtswidriger Eingriff in Grundrechte des Betroffenen wird nicht dadurch rechtmäßig, daß ein rechtmäßiger Eingriff zu viel Aufwand erfordern würde. Vielmehr sind organisatorische Vorkehrungen zu treffen, um sicherzustellen, daß bei den typischen Übermittlungsvorgängen derartige Konflikte gar nicht erst auftreten. Ich hoffe, daß meine Vorschläge bei der bevorstehenden Beschlußfassung des Senats oder in den Beratungen der Bürgerschaft aufgegriffen werden.

4.16.4 Schweigepflichtentbindung im Verfahren nach dem Schwerbehindertengesetz

Anläßlich einer Eingabe, in der es um die Schweigepflichtentbindung eines in der Psychoanalyse bzw. -therapie tätigen Arztes in einem Verfahren des Versorgungsamtes nach dem Schwerbehindertengesetz ging, hatte ich dem Versorgungsamt mitgeteilt, daß aus datenschutzrechtlicher Sicht die Schweigepflichtentbindungsklausel geändert werden müsse. Erforderlich sei eine Konkretisierung der Formulierung für die Beiziehung von Untersuchungsunterlagen, um zum Ausdruck zu bringen, daß nur die für die Aufgabenerfüllung des Versorgungsamtes wirklich benötigten Informationen angefordert werden dürfen, ferner ein Hinweis auf die Mitwirkungspflicht des Antragstellers und auf die für die Erklärung maßgeblichen Rechtsgrundlagen. Auch das Schreiben, mit dem Informationen bei den Ärzten angefordert werden, erschien mir problematisch.

Die Verhandlungen mit dem Versorgungsamt haben zu dem Ergebnis geführt, daß die Antragsvordrucke für den Erstantrag und den Neufeststellungsantrag nach dem Schwerbehindertengesetz überarbeitet werden. In den „Allgemeinen Hinweisen" wird auf die Mitwirkungspflicht nach §§ 60 ff. SGB I verwiesen und auf die Verarbeitung der Daten mittels EDV aufmerksam gemacht.

Für die Schweigepflichtentbindungserklärung wurde folgende Fassung festgelegt:

„Einwilligungserklärung (§§ 67, 100 des Sozialgesetzbuches — Verwaltungsverfahren)

Ich erkläre mich damit einverstanden, daß das Versorgungsamt

— die für die Feststellung erforderlichen Auskünfte einholt und

— die über mich bei Ärzten, Krankenanstalten, Behörden, Sozialleistungsträgern und gleichgestellten Stellen geführten medizinischen Unterlagen, insbesondere Entlassungsberichte/Zwischenberichte, Befundberichte, Röntgenbilder, in dem Umfang zur Einsicht bezieht, wie diese Aufschluß über die bei mir vorliegenden Behinderungen geben können."

Diese Erklärung erstreckt sich auch auf Unterlagen über psychiatrische, psychoanalytische und psychotherapeutische Untersuchungen/Behandlungen.

Die Einwilligungserklärung gilt für das mit diesem Antrag eingeleitete Verwaltungsverfahren und für ein evtl. anschließendes Widerspruchsverfahren. Sie bezieht sich auch auf die während des Verfahrens eintretenden Sachverhalte und angefertigten Unterlagen.

Ich genehmige die Verwertung dieser Unterlagen im Feststellungsverfahren und entbinde die beteiligten Ärzte insoweit von ihrer Schweigepflicht."

Auch das Anschreiben, mit dem das Versorgungsamt Unterlagen bei Ärzten, Krankenhäusern und sonstigen Einrichtungen unter Hinweis auf die vorliegende Schweigepflichtentbindungserklärung anfordert, wird eine neue Form erhalten. Es wird von der

EDV-Anlage ausgedruckt. Einer namentlichen Benennung bzw. sonstigen Kennzeichnung des Sachbearbeiters hat der Personalrat widersprochen, da so die tätigkeitsbezogene Kontrolle der Mitarbeiter ermöglicht würde. Angestrebt wird die Benennung der jeweils zwei Mitarbeiter eines Sachgebiets, die für ein bestimmtes Kontingent von Vorgängen, das nach dem Alphabet zugeteilt wird, gemeinsam zuständig sind. Als Veranlasser werden dann beide Mitarbeiter im Anforderungsschreiben genannt.

Diese Lösung wäre eine Verbesserung gegenüber dem derzeitigen unpersönlichen Schreiben, das als Absender lediglich das Versorgungsamt unter Zusatz einer Telefonnummer aufweist. Die namentliche Benennung erleichtert dem Empfänger des Anforderungsschreibens bei Rückfragen die Kontaktaufnahme mit dem zuständigen Sachbearbeiter, der das Vorliegen der Schweigepflichtentbindungserklärung versichert hat, und ermöglicht ihm, die angeforderten sensiblen Unterlagen diesem direkt zuzusenden.

Auf der Rückseite des Anforderungsschreibens, das an Krankenhausärzte versandt wird, soll zukünftig der Text der neuen Schweigepflichtentbindungsklausel abgedruckt werden, damit der Arzt prüfen kann, ob die Übersendung der von ihm geforderten Unterlagen mit der Entbindungserklärung vereinbar ist.

Das Anforderungsschreiben für niedergelassene Ärzte ist bereits auf beiden Seiten eng bedruckt. Ein eigenes Blatt für den sich stets wiederholenden Text hält das Versorgungsamt sowohl aus Kostengründen als auch wegen der zusätzlichen Papierflut beim Empfänger für unzweckmäßig. Der neue Text soll aber an geeigneter Stelle (Vorschlag: Ärzteblatt) veröffentlicht und im Anforderungsschreiben auf die Fundstelle hingewiesen werden, so daß auch dem niedergelassenen Arzt die eigene Prüfung des Umfangs der Schweigepflichtentbindungserklärung ermöglicht wird. Unter diesen Voraussetzungen wird die Zusicherung des zuständigen Sachbearbeiters des Versorgungsamtes, die Entbindungserklärung liege für diesen konkreten Fall vor, als ausreichend akzeptiert. Auf die Einholung und Übersendung einer auf jeden Arzt bezogenen Einzelfallerklärung kann dann verzichtet werden.

Das Versorgungsamt hat zugesichert, auf der Grundlage der geführten Verhandlungen die Schweigepflichtentbindungserklärungen in den anderen vom Versorgungsamt verwendeten Antragsformularen zu überarbeiten.

4.17 Wissenschaft und Forschung

4.17.1 UKE-Studien über gesundheitliche Folgeschäden durch Holzschutzmittel

Unter der Federführung des Instituts für Medizinsoziologie führt das Universitäts-Krankenhaus Eppendorf zwei Studien über mögliche gesundheitliche Folgeschäden bei Kindern und bei Beschäftigten durch, die sich in holzschutzmittelbelasteten Kindergärten aufgehalten haben. Für beide Studien läßt das Institut neben den belasteten Personen auch unbelastete Vergleichsgruppen untersuchen. Von allen Teilnehmern wird eine Fülle von zum Teil sehr sensiblen Daten über den Gesundheitszustand, über Vorerkrankungen, über das soziale Umfeld und über mögliche Belastungen mit Schadstoffen erhoben. Sowohl für die Betroffenen als auch für die Vergleichspersonen ist die Teilnahme an der Studie freiwillig.

Für die Kindergartenstudie, die die Belastung der Kinder untersucht, ist als Rechtsgrundlage für die Datenerhebung und -verarbeitung eine schriftliche Einwilligungserklärung vorgesehen, die ebenso wie der dazugehörige Informationsteil des Formblatts mit meiner Dienststelle abgestimmt wurde. Nach Abschluß der Untersuchungen und Auswertung der Daten werden die Erhebungsunterlagen an die Eltern der untersuchten Kinder herausgegeben.

Die Holzschutzmittelstudie II, die der Erforschung gesundheitlicher Folgeschäden bei den Beschäftigten der belasteten Kindergärten dient, befindet sich noch in der Vorbereitungsphase. Voraussetzung für die Teilnahme als Betroffener und nicht bloß als „Vergleichsperson" ist eine Berufskrankheitenmeldung. Nach der epidemiologischen Aus-

wertung durch das UKE ist vorgesehen, die erhobenen Daten an die Berufsgenossenschaft für Gesundheitsdienst und Wohlfahrtspflege, die für die Beschäftigten der privaten Kindergartenträger zuständig ist, bzw. an die Landesunfallkasse, soweit Beschäftigte städtischer Einrichtungen betroffen sind, zur individuellen Bewertung weiterzugeben. Die von der Vergleichsgruppe erhobenen Befunde und Labordaten werden nach Anonymisierung und Auswertung für die Studie an die Untersuchten herausgegeben.

Die Information über die geplante Datenverarbeitung und die Einwilligungserklärung, die für die Datenerhebung, -auswertung und personenbezogene Übermittlung erforderlich ist, werden sich an den Grundsätzen, die für die Kindergartenstudie festgelegt worden sind, orientieren.

Im Laufe der Durchführung der Kindergartenstudie war auch die Frage zu behandeln, ob Belastungsdaten der einzelnen Einrichtungen an das UKE weitergegeben werden dürfen, oder ob der Gesichtspunkt des Betriebs- und Geschäftsgeheimnisses einer Übermittlung entgegensteht. Nachdem die Bezirksämter zunächst unter Berufung auf Datenschutzbestimmungen die Herausgabe der Belastungsdaten abgelehnt hatten, ist mit der Behörde für Arbeit, Jugend und Soziales, der als Fachbehörde die Aufsicht über die Kindergärten obliegt, eine Regelung für die Übermittlung der erforderlichen Daten getroffen worden:

Anstelle der pauschalen Anfrage an die Gesundheitsämter nach allen dort vorhandenen Daten über die Belastung von Kindergärten wird sich das UKE unter genauer Angabe der benötigten Daten an die Behörde für Arbeit, Jugend und Soziales wenden und dort eine Forschungsgenehmigung gem. § 75 Abs. 2 SGB X erhalten, aufgrund derer die für das Forschungsvorhaben relevanten Daten offenbart werden dürfen. Auch in der Zukunft werde ich die Studien, insbesondere zu Fragen der Datensicherung, beratend begleiten.

4.18 Schulwesen

4.18.1 Bereichsspezifische Datenschutzbestimmungen im Schulgesetz

In meinem 3. TB (3.5.1) und 4. TB (4.7.1) hatte ich darüber berichtet, daß mit der Behörde für Schule und Berufsbildung (BSB) Einvernehmen darüber besteht, daß eine bereichsspezifische Regelung für die Datenverarbeitung im Schulbereich erforderlich ist. Meine Vorstellungen von einer Regelung, die den verfassungsrechtlichen Anforderungen genügt, habe ich der BSB seit 1984 mehrfach ausführlich erläutert. Ich habe außerdem zu mehreren Entwurfsfassungen, die mir die BSB zugesandt hatte, Stellung genommen, zuletzt im Jahre 1986.

Die umfangreiche Datenverarbeitung im Schulbereich ist — auch im Hinblick auf das immer stärkere Vordringen der Informationstechnologie und die damit verbundenen Gefahren für die Betroffenen — ohne gesetzliche Grundlage nicht mehr akzeptabel. Mehrere Bundesländer haben inzwischen die nötigen gesetzlichen Regelungen geschaffen. Ich meine, daß der Hamburger Gesetzgeber ihrem Beispiel folgen sollte. Ich gehe deshalb davon aus, daß der Prüfungsauftrag, den die Koalitionsvereinbarung enthält, bald ausgeführt ist und bereichsspezifische Datenschutzbestimmungen im Schulgesetz nunmehr zügig in Angriff genommen werden.

4.19 Verkehrswesen

4.19.1 ZEVIS — Fahrzeugregisterverordnung

Das Gesetz zur Änderung des Straßenverkehrsgesetzes vom 28. 1. 1987 verlangt eine bereichsspezifische Regelung für die Führung und Nutzung der Fahrzeugregister; das sind die örtlichen Register bei den Kfz-Zulassungsstellen und das zentrale Register beim Kraftfahrt-Bundesamt. Eine solche Regelung ist insbesondere auch von Bedeutung für das Zentrale Verkehrs-Informationssystem (ZEVIS) beim Kraftfahrt-Bundesamt, zu dessen Einführung ich mich in den letzten Jahren wiederholt geäußert habe (vgl. zuletzt 5. TB, 5.8.9, S. 74).

Der Bundesminister für Verkehr hat am 20. 10. 1987 die Fahrzeugregisterverordnung erlassen, die Regelungen enthält über

— die Erhebung und Speicherung der Daten, wobei insbesondere die Fahrzeugdaten näher bestimmt werden,

— die regelmäßige Übermittlung der Fahrzeug- und Halterdaten, die Bestimmung der Daten und ihrer Empfänger, die Maßnahmen zur Sicherung gegen Mißbrauch und die Protokollierung bei Abrufen im automatisierten Verfahren (on-line),

— die Übermittlungssperren und die Löschung der Daten.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich mit der Fahrzeugregisterverordnung ausführlich auseinandergesetzt und gegen die nunmehr verabschiedete Fassung — bis auf eine Ausnahme — keine Einwendungen erhoben. Doch gerade dieser Ausnahme kommt aus datenschutzrechtlicher Sicht eine besondere Bedeutung zu: In den ersten Entwürfen, die von der Bundesregierung vorgelegt worden sind, war vorgesehen, daß eine Auswahlprotokollierung von 5 % der Abrufe aus ZEVIS erfolgen sollte, um hiermit die Voraussetzung für eine Datenschutzkontrolle zu schaffen. Die Datenschutzbeauftragten hatten zunächst eine Protokollierung von 10 % der Abrufe gefordert und eine Reduzierung auf 5 % als einen wenig befriedigenden Kompromiß hingenommen. Gleichwohl wurde auf Initiative des Bundesrats in der Fahrzeugregisterverordnung nunmehr geregelt, daß die Protokollierung der Abrufe auf 2 % der Fälle zu beschränken ist. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat durch Beschluß vom 4./5. Mai 1987 gegen diese Beschränkung protestiert, weil damit eine systematische Überprüfung des Abfrageverhaltens der abrufberechtigten Dienststellen kaum mehr möglich ist. Die vorgenommene Einschränkung ist außerdem mit Sinn und Zweck der im Straßenverkehrsgesetz vorgeschriebenen Auswahlprotokollierung, mit der Mißbrauch und falsche Rechtsanwendung durch eine Kontrolle der Abrufe seitens der Fachaufsicht und der Datenschutzbeauftragten vermieden oder unterbunden werden sollen, nicht vereinbar. Damit wird auch die vom Bundesverfassungsgericht zum Volkszählungsurteil aufgestellte Forderung nach einer effektiven Datenschutzkontrolle durch unabhängige Datenschutzbeauftragte mißachtet. In der Praxis heißt dies, daß nach dem erwarteten Umfang der ZEVIS-Nutzung und der vorgesehenen Zahl der abrufberechtigten Dienststellen durchschnittlich alle zwei Monate nur eine Protokollierung pro Dienststelle erfolgen wird. Bei einer solchen Protokollierungspraxis braucht eine abrufende Person mit der Protokollierung gerade ihres Abrufes ernstlich nicht mehr zu rechnen.

4.19.2 Automation des Kraftfahrzeug-Zulassungswesens

Die Arbeiten an dem Projekt „Automation des Kraftfahrzeug-Zulassungswesens", über das ich mich in meinem letzten Tätigkeitsbericht (5.8.11, S. 76) kurz geäußert habe, wurden fortgesetzt.

Bei den drei hamburgischen Kfz-Zulassungsstellen (Ausschläger Weg, Harburg und Bergedorf) stehen dem Bürger nur begrenzte Öffnungszeiten zur Verfügung, da ein hoher Zeitbedarf für nachbereitende und verwaltende Tätigkeiten sowie für die Postbearbeitung benötigt wird. Die Auskunftsbearbeitung ist im gegenwärtigen konventionellen Verfahren (Karteikarten) nur innerhalb des Zuständigkeitsbereiches des einzelnen Sachbearbeiters möglich, da nur dort die benötigten Unterlagen und Daten zur Verfügung stehen. Telefonische Auskunftserteilungen innerhalb der Öffnungszeiten unterbrechen zwangsläufig die Sachbearbeitung in Anwesenheit des Bürgers.

Das bisherige Verfahren führte auch zu ungleichen Arbeitsbelastungen für die Mitarbeiter, wobei Über- und Unterbelastungen einzelner Arbeitsbereiche nicht effizient auszugleichen waren. Ursachen waren schwer prognostizierbare, kurzfristig und plötzlich auftretende Warteschlangen des Publikums vor einzelnen Sachbearbeitungsschaltern sowie eine Vielzahl von Sonderschaltern mit spezialisierten Mitarbeitern und die dadurch begrenzte Flexibilität in der Möglichkeit zu vorübergehender, ausgleichender Personalumsetzung.

Das angestrebte automatisierte Verfahren soll diese Probleme lösen. Die Forderung nach Reduzierung der Sonderschalter, einer technisch gesteuerten Zuweisung der Bürger zu den Sachbearbeitern, einer weitgehend einheitlichen Ausbildung der Sachbearbeiter soll dazu führen, daß nahezu jeder Zulassungsvorgang von jedem Sachbearbeiterplatz zu bearbeiten und ggf. auch zu vervollständigen ist. Hierfür soll ein Bildschirm-Dialogverfahren eingeführt werden, das

— die Erfassung und Fortschreibung eines Datenbestandes ermöglicht, der die bundeseinheitlichen Anforderungen berücksichtigt und sich in ein einheitliches Datenmanagement der Behörde für Inneres einpaßt,

— die Aufgabenerfüllung der Zulassungsstellen technisch zuverlässig, insbesondere in bezug auf

- Korrektheit der Ergebnisse,
- Robustheit des Systems,
- hohe Ausfallsicherheit,

und effizient im Sinne eines angemessenen Antwortzeitverhaltens unterstützt,

— die Ausbaufähigkeit und damit Zukunftssicherheit im Hinblick auf künftig evtl. entstehende zusätzliche Anforderungen durch ein hohes Maß an Flexibilität offenhält,

— die ablauforganisatorischen und insbesondere ergonomischen Anforderungen der Anwender berücksichtigt,

— den Service für die Bürger verbessert,

— den Datenschutz und die Datensicherheit gewährleistet und

— die Wirtschaftlichkeit der Aufgabenerfüllung erhöht.

Die angestrebte Konzeption soll die Sachbearbeitung in Anwesenheit des Bürgers auf einen Bildschirm-Dialog beschränken, der notwendige Aufgabenteile sofort verarbeitet und nachbereitende und verwaltende Tätigkeiten dabei steuert und koordiniert, um sie im Hintergrund (Batch-Verfahren) gesammelt automatisiert ablaufen zu lassen.

Insbesondere standardisierter Schriftverkehr, Fristensetzung und -überwachung, Erstellen von Statistik sowie Dateireorganisationen sollen durch die Automation zur erheblichen Entlastung der Sachbearbeiter führen.

Aus datenschutzrechtlicher Sicht kommt es darauf an, daß die eingesetzte Hard- und Software die Beachtung von Vorgaben, wie z.B.

— der Fahrzeugregisterverordnung (Art und Umfang zu erfassender Daten sowie Speicherungsfristen) und

— der Datenschutzgesetze (Datensicherung, Zugriffsberechtigungen)

sicherstellt. Zu Beginn der Projektberatungen habe ich die Behörde für Inneres gebeten, sie möge auch prüfen, ob die Zulassungsstellen funktionell und organisatorisch aus dem Verantwortungsbereich der Polizei gelöst werden können. Ich habe die Behörde für Inneres an die Forderung des Bundesverfassungsgerichts erinnert, „mehr als früher auch organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken (BVerfGE Bd. 65 S. 144)." Solche Gefahren sind aber unvermeidlich, wenn die Herrschaft über Halterdaten und die Entscheidung über polizeiliche Maßnahmen spätestens bei der Leitung der Polizei zusammengefaßt sind. Daran kann auch eine materiell-rechtliche Trennung nichts ändern.

Ich möchte betonen, daß ich keinen Anlaß habe anzunehmen, die Polizei würde sich nicht an gesetzliche Vorgaben halten. Es geht mir vielmehr darum, den Möglichkeiten von Mißbrauch (durch einzelne), vor allem aber von Interessenkonflikten entgegenzuwirken. Solche Konflikte sind für die Leitung der Polizei aber unvermeidlich, wenn innerhalb der Polizei zwischen dem Recht auf informationelle Selbstbestimmung von

Kraftfahrzeughaltern einerseits und der Berücksichtigung von Sicherheitsbelangen abzuwägen ist; insbesondere dann, wenn zwischen den beteiligten Dienststellen der Abwägungsvorgang kontrovers diskutiert wird. Dabei darf auch nicht übersehen werden, daß die Polizei aufgrund der Erwartungshaltung der Öffentlichkeit und ihrer gesetzlichen Aufgaben nach dem SOG und der Strafprozeßordnung unvermeidlich dazu tendieren muß, diesen Konflikt zugunsten der Sicherheitsinteressen zu lösen.

Die Prüfung durch die Behörde für Inneres ist noch nicht abgeschlossen.

5. Einzelne Probleme des Datenschutzes im nicht-öffentlichen Bereich

5.1 Versandhandel

5.1.1 Interne Bonitätsprüfung

Im 5. TB hatte ich von einem Versandhandelsunternehmen berichtet, das seine frühere Praxis, bei Erstbestellungen von Hausfrauen regelmäßig die SCHUFA über den Ehegatten zu befragen, aufgegeben hatte. Dafür war Voraussetzung, daß das interne Bonitätsprüfungsverfahren vorher verbessert wurde. Das ist so gut gelungen, daß nicht nur auf die SCHUFA-Anfrage bei Ehegatten, sondern ganz generell darauf verzichtet werden konnte.

Ein Risiko sieht das Versandhaus bei der Eröffnung eines als normal angebotenen Versandhauskontos, das das Zahlen auf Rechnung und in Raten bis zu einem Betrag von DM 3.000,- erlaubt. Die Tatsache, daß die Bonität geprüft wird, ist nicht zu beanstanden.

Ich erhielt jedoch ein paar besorgte Anfragen von solchen Erstbestellern, denen die Kontoeröffnung abgelehnt worden war und die die Vermutung äußerten, das Versandhaus hätte hinter ihrem Rücken doch Informationen von dritter Seite erhalten. Meine Überprüfung dieses Verdachts führte zu dem Ergebnis, daß für die interne Bonitätsprüfung tatsächlich keine anderen Daten verwendet werden als die, die der Erstbesteller selbst angibt.

Das System der Bonitätsprüfung basiert auf einer wissenschaftlichen Untersuchung und ist das Ergebnis jahrelang beobachteter Erfahrungen im Umgang mit den Erstbestellern. Dabei war die Grundidee die, daß Erfahrungen der Vergangenheit Vorhersagen über ein zukünftiges Verhalten ermöglichen. Die Untersuchung der Erfahrungen bezog sich auf alle Angaben im Erstbestellschein, die bei einer Bonitätsprüfung von Bedeutung sein könnten; dazu zählen u.a. das Alter, der Familienstand, der Umfang und der Wert der Bestellung. Diese Erfahrungen sind eingeflossen in eine Wahrscheinlichkeitsrechnung, deren Ergebnisse zum Aufbau einer Bewertungstabelle verwendet wurden. Dieses Bewertungssystem ist inzwischen so weit ausgereift, daß das Versandhaus deutlich weniger Forderungsausfälle zu beklagen hat als in der Vergangenheit.

Wenn nun eine Erstbestellung eingeht, werden die angegebenen Daten per Computerprogramm in Beziehung gesetzt zu den Erfahrungswerten. Wird eine intern festgesetzte Grenze unterschritten, wird das Konto automatisch nicht eröffnet. Der Kunde erhält einen Computerbrief, in dem er gebeten wird, per Nachnahme zu bestellen.

Da diese Bonitätsprüfung nicht auf den konkreten Einzelfall abstellt, sondern auf die Summe der gesammelten Erfahrungen, kann es vorkommen, daß einem Besteller das Konto abgelehnt wird, obwohl ein Kreditrisiko tatsächlich nicht besteht. Die Ablehnung gibt jedoch keinen Hinweis auf die Gründe, und man kann ohne nähere Kenntnisse durchaus den Eindruck gewinnen, es würden zusätzliche Informationen ausgewertet. Man darf aber davon ausgehen, daß Fremddaten — etwa von der SCHUFA oder einer Auskunftei erst dann herangezogen werden, wenn ein Besteller gegen die Ablehnung protestiert. Eine genauere Prüfung der tatsächlichen Verhältnisse kann dann dazu führen, daß es bei der Kontoablehnung bleibt. Oft ist auch eine Kontoeröffnung mit einem etwas herabgesetzten Limit möglich. Stellt sich aber heraus, daß die hypothetische Bewertung zu einem falschen Ergebnis geführt hat, wird das Konto zu normalen Bedingungen eröffnet.

Meine datenschutzrechtliche Bewertung dieses Verfahrens ist noch nicht abgeschlossen.

5.1.2 Gespräch mit dem Bundesverband des Deutschen Versandhandels

Die Arbeitsgruppe „Datenschutz beim Versandhandel" des Düsseldorfer Kreises hat im Mai 1987 ein Gespräch mit Vertretern des Bundesverbandes des Deutschen Versandhandels e.V. über verschiedene Datenschutzprobleme geführt, die es nach Auffassung der Datenschutz-Aufsichtsbehörden beim Versandhandel gibt. Das Gespräch verlief ohne Einigung zwischen beiden Seiten. Der Versandhandel war bedauerlicherweise nicht bereit, die Anliegen und Forderungen der Datenschutz-Aufsichtsbehörden aufzugreifen.

Im einzelnen sind folgende Themen strittig:

5.1.2.1 Werbeaktionen des Versandhandels

Die Datenschutz-Aufsichtsbehörden halten an ihrer Forderung nach mehr Transparenz für den Betroffenen fest. Gleichzeitig haben sie noch einmal klargestellt, daß sie nicht beabsichtigten, für den Umworbenen über das BDSG hinausgehende Rechte zu begründen. Die Gewährleistung der Rechte des Betroffenen setze jedoch bereits nach der geltenden Rechtslage ein Höchstmaß an Transparenz voraus; auch die Entwicklung der Rechtsprechung und die geplante BDSG-Novelle zielten in diese Richtung.

Zahlreiche Eingaben zeigten, daß bei den Betroffenen z.T. großes Unbehagen herrsche, weil sie nicht nachvollziehen könnten, auf welchem Wege ein werbendes Unternehmen in den Besitz ihrer Adressen gelangt sei. Die Geltendmachung ihrer Rechte, insbesondere die Löschung von Anschriften, stoße in der Praxis auf erhebliche Schwierigkeiten. Die Datenschutz-Aufsichtsbehörden schlagen deshalb vor, die mit den Vertretern des Zentralausschusses der Werbewirtschaft und des Deutschen Direktmarketing-Verbandes einvernehmlich erzielten Lösungsvorschläge auch beim Versandhandel als Grundlage für Werbemaßnahmen zu übernehmen.

Der Bundesverband des Deutschen Versandhandels (BVH) hat mit Nachdruck darauf hingewiesen, daß die dort erzielten Lösungsmöglichkeiten vom Versandhandel nicht akzeptiert werden könnten. Zum einen bestehe keine umfassende Deckungsgleichheit der Interessenlage der Verbände, zum anderen hätten die Mitglieder des BVH die Vorschläge bereits zurückgewiesen, weil es sich um Forderungen handele, die im BDSG nicht vorgesehen seien. Man habe zwar Verständnis für die Haltung der Aufsichtsbehörden, sei aber nicht bereit, Zugeständnisse zu machen, die über das Gesetz hinausgingen, um nicht weitere, neue Forderungen zu präjudizieren. Der Bundesverband sehe keine Notwendigkeit für das von den Datenschutz-Aufsichtsbehörden vorgeschlagene Verfahren. Im übrigen habe er auch keine Möglichkeit, seinen Mitgliedern eine bestimmte Verfahrensweise vorzuschreiben, sondern sei auf deren freiwillige Mitwirkung angewiesen.

Der BVH hat weiter mitgeteilt, eine Umfrage unter seinen Mitgliedern habe ergeben, daß Anfragen nach der Adressenherkunft nur in verschwindend geringem Umfang gestellt würden. Dies zeige, daß die Umworbenen an weiterer Aufklärung nicht interessiert seien. Die wenigen Auskunftssuchenden würden in der Regel ausführliche Informationen durch das werbende Unternehmen selbst oder den eingeschalteten Adressen-Broker erhalten. Im übrigen sei die Herkunft einer Anschrift in vielen Fällen schon deshalb nicht mehr feststellbar, weil zumeist mehrere Adressenbestände zusammengeführt würden und eine Zuordnung einzelner Adressen anschließend nicht mehr möglich sei. Außerdem bereite es in diesen Fällen technische Schwierigkeiten, dem Betroffenen die Selektionskriterien mitzuteilen. Um die von den Datenschutz-Aufsichtsbehörden geforderte Bekanntgabe der Selektionskriterien erfüllen zu können, müßten in die Werbeschreiben unterschiedliche, auf die jeweils genutzten Adreßbestände bezogene Hinweise aufgenommen werden. Eine solche Verfahrensweise sei aber völlig unverhältnismäßig. Jede zusätzliche Information, sei es durch einen gesonderten Hin-

weis im Werbeschreiben, sei es durch einen besonderen Beipackzettel, würde erhebliche Zusatzkosten verursachen und sei damit für den Versandhandel nicht mehr zumutbar, zumal — wie die Erfahrungen gezeigt hätten — von den Umworbenen kein Bedürfnis für eine solche Aufklärung gesehen werde. So habe auch ein Probelauf mit entsprechenden Hinweisen bei einem mittleren Versandunternehmen nicht zu einem erhöhten Auskunftsverlangen der Kunden geführt.

Der Vorschlag der Datenschutz-Aufsichtsbehörden, auf den Bestellscheinen durch ein entsprechendes Ankreuzfeld dem Betroffenen die Möglichkeit zu eröffnen, der Weitergabe seiner Anschrift zu Werbezwecken an Dritte zu widersprechen, ist vom Versandhandel mit dem Hinweis zurückgewiesen worden, daß dies bei der geringen Zahl von Widersprüchen gegen die Adressenweitergabe nicht gerechtfertigt sei und jede zusätzliche Information den Kunden verunsichere.

Diese uneinsichtige Haltung des Versandhandels veranlaßt mich, an die Vorschläge zu erinnern, die ich in meinem 4. TB (Nr. 6.2.2.9) dem Gesetzgeber gemacht habe, um die mit der Direktwerbung verbundenen Probleme zu lösen. Ich hoffe, daß meine Forderungen bei den im nächsten Jahr erneut anstehenden Beratungen zur Novellierung des BDSG aufgegriffen werden.

5.1.2.2 Verhältnis des Versandhandels zur Schufa

Der Bundesverband des Deutschen Versandhandels hat deutlich gemacht, daß die Forderung der Datenschutz-Aufsichtsbehörden, dem Betroffenen das Verfahren bei Anfragen des Versandhandels an die SCHUFA transparenter zu machen, von seinen Mitgliedsunternehmen unter Hinweis auf die sehr geringe Zahl von Anfragen ebenfalls grundsätzlich abgelehnt werde. Allerdings erklärte er sich bereit, mit seinen Mitgliedsunternehmen die Frage zu erörtern, ob der für den normalen Kunden häufig mißverständliche Zusatz „Bonität vorausgesetzt" durch eine andere Formulierung ersetzt werden könne, die für Neukunden oder bei Einrichtung eines Kreditkontos dem Kunden deutlich mache, daß eine SCHUFA-Anfrage erfolge. Auch soll mit den Mitgliedsunternehmen diskutiert werden, wie ein Betroffener von einer Negativmeldung an die SCHUFA unterrichtet werden kann. Über das Ergebnis der verbandsinternen Meinungsbildung sind die Aufsichtsbehörden bislang noch nicht unterrichtet.

Ich bedaure, daß auf der Seite des Versandhandels so wenig Bereitschaft zur Kooperation mit den Datenschutz-Aufsichtsbehörden besteht.

Die SCHUFA ist aufgerufen, ihr Verhältnis zu den B-Vertragspartnern wie etwa dem Versandhandel zu klären und ihrerseits darauf hinzuwirken, daß auch hier — wie bei der Kreditwirtschaft — die Position der Kunden verbessert wird. Bei der jetzt anstehenden Novellierung des BDSG muß sichergestellt werden, daß die Forderungen der Datenschutz-Aufsichtsbehörden (insbesondere nach einer besseren Information der Betroffenen) in das Gesetz einfließen. Anders scheint mir eine Verbesserung des Datenschutzes im Bereich des Versandhandels jetzt nicht mehr erreichbar zu sein.

5.2 Kreditwirtschaft/SCHUFA

5.2.1 Neues SCHUFA-Verfahren: Kartellrechtliche Entwicklung

Das im Gefolge des SCHUFA-Urteils des Bundesgerichtshofes vom 19. 9. 1985 zwischen Kreditwirtschaft, SCHUFA und Datenschutz-Aufsichtsbehörden verabredete neue SCHUFA-Verfahren hatte — wie in meinem letztjährigen Tätigkeitsbericht bereits ausführlich dargestellt (6.4.2, S. 111 ff.) — zu kartellrechtlichen Problemen geführt. Einige der bisherigen SCHUFA-Vertragspartner, die aufgrund der Vereinbarungen über das neue Verfahren ihren SCHUFA-Anschluß verloren, weil sie keine Risiken aufgrund von Geld- und Warenkrediten an Endverbraucher (Konsumenten) eingehen, hatten sich

beschwerdeführend an das Bundeskartellamt gewandt. Einige der Beschwerden veranlaßten das Amt zu der Einleitung einer Untersuchung, ob durch diese Kündigungen das Diskriminierungsverbot des § 26 GWB verletzt worden sein könnte. Die Frage war, ob die SCHUFA die gekündigten Vertragspartner diskriminierte, indem sie nur diese von ihren Informationen ausschloß, während die anderen Vertragspartner nach wie vor daran partizipieren können.

Die Problematik wurde verschiedentlich zwischen Datenschutz-Aufsichtsbehörden, Bundeskartellamt, Kreditwirtschaft, SCHUFA und Vertretern der gekündigten Wirtschaftszweige erörtert. Der Sachstand ist folgender:

— Für den Bereich der Wohnungsbaufinanzierung (vgl. 5. TB, 6.4.2, S. 112) wurde eine Lösung gefunden, die den Besonderheiten dieser Branche Rechnung trägt. Danach ist jetzt für grundpfandrechtlich gesicherte Kredite ein Anschluß bei der SCHUFA wahlweise auf Grundlage des A- oder B-Vertrages möglich. Es ist zu erwarten, daß Hypothekenbanken, Bausparkassen und Versicherungen entsprechend ihren früheren Erklärungen überwiegend einen B-Vertrag wählen werden. Bei beiden Vertragsformen sind Anfragen bei der SCHUFA unabhängig von der Höhe der vorgesehenen Kredite und der Art der vorhandenen Sicherheiten möglich. Der SCHUFA zu melden sind beim B-Vertrag alle anfallenden Negativmerkmale, nicht nur solche aus Krediten, bei denen zuvor eine SCHUFA-Anfrage erfolgt ist. Beim A-Vertrag muß, beim B-Vertrag kann außerdem die Tatsache gemeldet werden, daß ein grundpfandrechtlich gesichertes Darlehen gewährt wurde, nicht aber Betrag und Laufzeit des Kredits. Bei beiden Vertragsformen kann die SCHUFA Nachmeldungen erteilen. Wird ein A-Anschlußvertrag gewählt, muß auch eine „große" SCHUFA-Klausel entsprechend der Klausel für Konsumentenkredite verwendet werden. Bei B-Verträgen ist die „kleine" Klausel maßgeblich, die zwar keine Einwilligung des Betroffenen in die Datenübermittlung enthält, wohl aber auf die möglichen Datenflüsse hinweist und damit für die notwendige Aufklärung sorgt. Die Einbeziehung grundpfandrechtlich gesicherter Kredite in das SCHUFA-System ist von der ab 1. 7. 1986 verwendeten SCHUFA-Klausel gedeckt. Erforderlich ist allerdings eine Anpassung des Kundenmerkblattes.

— Die Datenschutz-Aufsichtsbehörden hatten von Anfang an die Auffassung vertreten, daß die Kündigungen der Autovermieter bestehen bleiben müßten, weil diese eindeutig keine Kreditrisiken eingehen und deswegen vom Geschäftszweck der SCHUFA nicht erfaßt werden (vgl. 5. TB, 6.4.2, S. 113). Nach längerer Diskussion ist jetzt geklärt, daß die Autovermieter von der SCHUFA ausgeschlossen bleiben.

  Das Bundeskartellamt hatte ihnen auf ihre Diskriminierungsbeschwerde hin Gelegenheit gegeben, ihre angebliche unbillige Behinderung zu belegen. Sie sollten für das Jahr 1985 diejenigen Ausfälle aufgrund von Unterschlagungen, nicht gezahlten Mieten und Zerstörungen/Schäden vorlegen, bei denen aus unterschiedlichen Gründen die Kfz-Vermietung ohne vorherige Einholung einer SCHUFA-Auskunft erfolgte. Für diese Ausfälle sollten dann in einem zweiten Schritt nachträglich SCHUFA-Auskünfte eingeholt werden, um festzustellen, in welchen Fällen Vermietungen aufgrund negativer Auskünfte unterblieben wären. Die Umfrage unter etwa 850 Autovermietungsunternehmen erbrachte jedoch nur 19 verwertbare Beantwortungen. Das Bundeskartellamt sah diesen Rücklauf von kaum mehr als 2 % für eine beweisfähige Aussage hinsichtlich einer unbilligen Behinderung der gesamten Gruppe der Autovermieter als unzureichend an. Auch lag der mit dieser — ohnehin also nicht aussagefähigen — Umfrage ermittelte Ausfallsatz von durchschnittlich nicht einmal 3 % des Vermietungsumsatzes nach Ansicht des Bundeskartellamtes weit unterhalb einer wie auch immer definierten Nachweisschwelle. Eine unbillige Behinderung könne durch diesen Ausfallsatz keinesfalls nachgewiesen werden.

  Aufgrund dieses Befragungsergebnisses hat das Bundeskartellamt das Diskriminierungsverfahren eingestellt.

— Offen ist noch die Frage, ob Inkassobüros und Kreditversicherer, die z. T. das Inkasso der bei ihnen versicherten Forderungen betreiben, SCHUFA-Vertragspartner sein

dürfen, um die SCHUFA-Daten zur Suche nach verschwundenen Schuldnern benutzen zu können. Das Interesse der Inkassounternehmen besteht im wesentlichen darin, bei Schuldnern mit titulierten Forderungen nach erfolglosen Vollstreckungsversuchen die aktuelle Anschrift des Schuldners zu erfahren (Suchdienst) und/oder über Veränderungen im Schuldnerverzeichnis — Haftbefehl, eidesstattliche Versicherung — sowie über fruchtlose Pfändungen wegen sonstiger, der Höhe nach anzugebender, titulierter Forderungen informiert zu werden (Beobachtungsdienst). Als Gegenleistung erwartet die SCHUFA die Einmeldung offener titulierter Forderungen, fruchtloser Pfändungen sowie ggf. der Erledigung der Forderung. Wegen dieser Gegenleistung hat die SCHUFA selbst großes Interesse bekundet, für Inkassounternehmen weiterhin den Suchdienst durchzuführen.

Die Datenschutz-Aufsichtsbehörden haben hier zunächst die Auffassung vertreten, daß das System nicht generell für Suchaufträge geöffnet werden darf, daß Suchanträge vielmehr nur zur Durchsetzung eigener Forderungen — nicht also verkaufter Forderungen — möglich sein sollten. Nach ihrer Meinung sollten Suchaufträge nur im Zusammenhang mit Kreditvergaben von SCHUFA-Vertragspartnern erteilt werden. Die Möglichkeit, Suchaufträge zu erteilen, sollte infolgedessen auf Vertragspartner der SCHUFA für eigene Forderungen beschränkt werden. Inkassobüros sollten nicht selbständige Vertragspartner der SCHUFA sein. Wird ein Inkassobüro mit dem Einzug von Forderungen eines SCHUFA-Anschlußpartners beauftragt, obliegt es dem Anschlußpartner, den Suchauftrag zu erteilen. In den verschiedenen Besprechungen über diesen Problembereich ist dann die Frage erörtert worden, ob nicht ein Sonderdienst der SCHUFA für Suchaufträge eingerichtet werden kann. Damit wäre der Nachteil verbunden, daß dann auch andere als kreditorische Risiken in das SCHUFA-System hineinkommen würden, denn die Inkassobüros treiben auch andere als Kreditforderungen ein.

Doch wie immer ein derartiger spezieller Suchdienst beurteilt wird — er könnte nicht ohne eine Änderung der von den Kreditinstituten verwendeten SCHUFA-Klausel eingerichtet werden. Die mit der Klausel vom Bank- oder Sparkassenkunden erteilte Einwilligung in die Übermittlung seiner Daten wäre nur wirksam, wenn er auch wüßte, daß die Daten u.a. auch an Inkassobüros gegeben werden können. Anderenfalls würde die Einwilligung leerlaufen. Es ist bisher nicht abschließend geklärt, ob für die Kreditwirtschaft eine Änderung der erst vor kurzer Zeit neu gefaßten SCHUFA-Klausel in Betracht kommt. Damit steht noch nicht fest, ob die Datenschutz-Aufsichtsbehörden einer Öffnung der SCHUFA für Inkassobüros und Kreditversicherer zustimmen können. Über diesen Problemkomplex müssen noch weitere Gespräche auch mit dem Bundeskartellamt stattfinden.

— Ungeklärt war zunächst noch die Frage, ob Möbelspediteure Anschlußpartner der SCHUFA sein können, wenn sie ihren Kunden zur Finanzierung der Umzugskosten Ratenkredite geben. Die Datenschutz-Aufsichtsbehörden vertreten hier die Ansicht, daß die Möbelspediteure keinesfalls generell einen SCHUFA-Anschluß erhalten dürfen, nur weil vereinzelte Spediteure auch Kredite an ihre Kunden geben, die wie Konsumentenkredite zu betrachten sind. Denkbar wäre allenfalls ein Zugang zur SCHUFA für solche Möbelspediteure, die nachgewiesen haben, daß sie im Rahmen ihres Speditionsgeschäftes in nennenswertem Umfang Kredite vergeben. In diesem Fall läge dann ein Kreditrisiko vor, das einen SCHUFA-Anschluß rechtfertigt.

Angesichts der auch für die SCHUFA ungewöhnlichen Konstellation sind alle Beteiligten einschließlich des Bundeskartellamtes übereingekommen, daß für die Anfangszeit das berechtigte Interesse der anfragenden Möbelspedition in jedem Einzelfall nachträglich überprüft werden soll. Zu diesem Zweck soll die Möbelspedition der SCHUFA zunächst alle Verträge zusenden, soweit für sie angefragt worden ist. Soweit zur Abgabe von Angeboten bei der SCHUFA angefragt worden ist, sollen die von den Betroffenen zu unterschreibenden Einwilligungsklauseln übersandt werden. Wenn die so möglichen Überprüfungen nicht zu Beanstandungen führen, soll das berechtigte Interesse nach einiger Zeit nur noch mit Stichproben überprüft

werden. Wenn allerdings mißbräuchliche Anfragen festgestellt werden, wird über den Anschluß dieser Möbelspediteure an die SCHUFA noch einmal diskutiert werden müssen.

5.2.2 Neues SCHUFA-Merkmal bei Rückständen nach Kündigung eines Kredits

Die SCHUFA ist mit dem Wunsch an die Datenschutz-Aufsichtsbehörden herangetreten, ein neues SCHUFA-Merkmal „SD" einzuführen. Der Hintergrund ist folgender:

Viele Kreditinstitute gehen gerade in jüngster Zeit dazu über, gekündigte Kredite nicht mehr mit Hilfe gerichtlicher Maßnahmen zu realisieren. Vielmehr wird unter Verzicht auf Mahnbescheid, Vollstreckungsbescheid und weitere Zwangsmaßnahmen eine einvernehmliche Regelung mit dem Schuldner angestrebt — ggf. unter teilweisem oder ganzem Verzicht auf Verzugszinsen —, den Saldo in Raten zurückzuführen. Diese Raten werden allein nach den wirtschaftlichen Möglichkeiten des Schuldners festgelegt. Im SCHUFA-Datenbestand erscheint im Zusammenhang mit derartigen Vorgängen lediglich das Merkmal „KU" (Kündigung wegen Verzugs mit einem Betrag, der mindestens zwei vollen Raten entspricht oder bei Kreditverhältnissen ohne Ratenvereinbarung nach zwei vorausgegangenen fruchtlosen schriftlichen Zahlungsaufforderungen). Weitere Merkmale können dann nicht mehr gemeldet werden.

Es ergibt sich die Konsequenz, daß zu dem Schuldner nach Fristablauf, d.h. drei volle Kalenderjahre nach Einmeldung des Merkmals „KU", keinerlei Daten im SCHUFA-Datenbestand enthalten sind. Gleichwohl besteht gerade in derartigen Fällen nach wie vor eine — evtl. sogar erhebliche — Verschuldung. Vielfach handelt es sich um Kunden, bei denen selbst Kosten des Mahnverfahrens nicht riskiert werden sollen. Andererseits werden die Beträge auch nicht ausgebucht, da eine Änderung der wirtschaftlichen Situation in Zukunft noch möglich erscheint. Auf der Basis der jeweiligen wirtschaftlichen Situation werden — zumindest teilweise — etwaige Nachlässe auf die Schuld sowie die Höhe der monatlichen Raten so festgelegt, daß eine Entschuldung in einigermaßen überschaubarer Zeit möglich erscheint. Diese Zeit ist jedoch jedenfalls länger als die dreijährige Frist bis zur Löschung.

Der SCHUFA-Datenbestand ist insoweit also unvollständig. Dieser Mangel kann auch nicht etwa dadurch ausgeräumt werden, daß entsprechende Forderungen als ordentliche Kredite gemeldet werden. Denn eine derartige Meldung würde ein völlig falsches Bild der Kreditwürdigkeit bieten. Nach wie vor handelt es sich bei dem gekündigten Kredit gerade nicht um eine ordnungsgemäße Darlehensschuld, sondern vielmehr um eine sofort fällige Forderung in Verbindung mit einem — möglicherweise reduzierten — Anspruch auf Ersatz des Verzugsschadens. Diese rechtliche Einordnung wird in keiner Weise berührt durch das in den geschilderten Fällen vorliegende einseitige Nachlassen der unverzüglichen Schuldtilgung bzw. durch den ebenfalls einseitigen Verzicht auf Wahrnehmung gerichtlicher Maßnahmen.

Die SCHUFA und die Kreditwirtschaft möchten zur Schließung dieser Lücke im SCHUFA-Datenbestand das folgende neue Negativmerkmal einführen:

> „SD — unbestrittener Saldo nach Kündigung wegen Verzugs mit einem Betrag, der mindestens zwei vollen Raten entspricht, oder bei Kreditverhältnissen ohne Ratenvereinbarung nach zwei vorausgegangenen fruchtlosen schriftlichen Zahlungsaufforderungen."

Die Datenschutz-Aufsichtsbehörden sehen, daß die aufgezeigte Lücke geschlossen werden muß, und haben das von der SCHUFA vorgeschlagene neue Merkmal akzeptiert.

Das neue Merkmal „SD" sollte nicht nur in der TA (Technische Abwicklung) der SCHUFA, sondern auch im SCHUFA-Merkblatt aus Transparenzgründen erwähnt und bei der nächsten Auflage berücksichtigt werden.

5.2.3 Probleme der Selbstauskunft (Auskunft an den Betroffenen)

Den Datenschutz-Aufsichtsbehörden sind Fälle bekanntgeworden, in denen von der SCHUFA gekündigte Unternehmen ihre Geschäftspartner auffordern, eine Selbstaus-

kunft beizubringen. Dagegen bestehen erhebliche Bedenken, denn auf diese Weise würde zum einen die Kündigung umgangen und ein früherer Vertragspartner nicht nur die Informationen von der SCHUFA erhalten, von denen er gerade abgeschnitten werden sollte, er würde künftig sogar noch mehr erfahren. In einem derartigen Vorgehen könnte zudem ein Verstoß gegen Treu und Glauben liegen, denn es wäre praktisch dem „Erzwingen" einer Unterzeichnung der SCHUFA-Klausel gleichzusetzen. Darüber hinaus ist es zumindest zweifelhaft, ob es mit § 9 des Gesetzes zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen vereinbar ist, wenn die Aufforderung zur Vorlage der Selbstauskunft formularmäßig erfolgen würde. Ein solches Verlangen wäre als unangemessene Benachteiligung anzusehen, weil es von wesentlichen Grundgedanken des BDSG abweichen würde.

Ein anderes Problem hat sich daraus ergeben, daß nach den Vereinbarungen mit den Datenschutz-Aufsichtsbehörden aus der dem Betroffenen bei der SCHUFA ausgehändigten Selbstauskunft jetzt auch ersichtlich ist, wer in letzter Zeit über ihn angefragt hat. Diese Verbesserung für die Betroffenen hat sich in einzelnen Fällen als Nachteil erwiesen, nämlich dann, wenn diese Selbstauskünfte anderen vorgelegt werden sollten, die aber nach dem Wunsch der Betroffenen nichts darüber erfahren sollten, wer über sie bei der SCHUFA angefragt hat.

Zwischen den Datenschutz-Aufsichtsbehörden, der Kreditwirtschaft und der SCHUFA besteht Einigkeit, daß die Selbstauskunft grundsätzlich vollständig sein sollte. Auf der anderen Seite muß der Betroffene aber auch eine Selbstauskunft erhalten können, die nicht erkennen läßt, wer über ihn angefragt hat, denn diejenigen, denen er die Selbstauskunft vorlegen will, haben oft kein berechtigtes Interesse an der Kenntnis, wer sich in letzter Zeit eine SCHUFA-Auskunft über den Betroffenen hat geben lassen. Eine auf Wunsch des Betroffenen eingeschränkte Selbstauskunft ist datenschutzrechtlich auch nicht unzulässig. Die SCHUFA Hamburg ist in derartigen Fällen bereit, die Aufzeichnungen über die Anfragen in ihrem Bestand zu löschen und dem Betroffenen dann eine insoweit „bereinigte" Selbstauskunft zu geben.

5.2.4 Verbreitungsverbot für SCHUFA-Daten bei nicht feststehender Identität

In einem Rechtsstreit zwischen einem Bürger und der SCHUFA hat das Hanseatische Oberlandesgericht in Hamburg durch Beschluß vom 23. 1. 1987 (NJW 1987, S. 659) entschieden, daß auch dann, wenn bei der SCHUFA gespeicherte belastende Daten den Zusatz „Identität nicht feststellbar" tragen und diese Daten im Zusammenhang mit einer konkreten Anfrage weitergegeben werden, der Betroffene die Weitergabe der Daten verbieten lassen kann. Der Bürger hatte in diesem Verfahren von der SCHUFA verlangt, die bei einer Auskunft über ihn zusätzlich übermittelten Angaben über zwei Haftbefehle zur Erzwingung der eidesstattlichen Versicherung nicht im Zusammenhang mit seiner Person an andere weiterzugeben. Er hatte bestritten, mit der in den Haftbefehlen bezeichneten Person identisch zu sein. Die bei der SCHUFA gespeicherten Angaben waren jeweils mit dem Zusatz „Identität nicht feststellbar" versehen.

Das OLG hat dem Betroffenen einen Anspruch auf Unterlassung gem. § 35 Abs. 2 Satz 1 BDSG zugesprochen, die betreffenden Daten im Zusammenhang mit Auskünften über seine Person an Dritte weiterzugeben. Es hat ausgeführt, diese Daten hätten zwar nicht positiv zum Inhalt, daß es der Betroffene sei, gegen den in zwei Fällen ein Haftbefehl nach § 901 ZPO ergangen sei; vielmehr hätten die Daten den Zusatz „Identität nicht feststellbar" getragen. Wenn sie aber nach Anfragen über den Betroffenen mitgeteilt würden, so enthalte die Mitteilung auch die Aussage, daß die Identität mit dem Betroffenen nicht ausgeschlossen, möglicherweise also gegeben sei. Der Rechtsgedanke des § 35 Abs. 2 Satz 1 BDSG sei aber, daß Daten, die nur möglicherweise auf eine bestimmte Person zutreffen, möglicherweise aber auf diese Person bezogen unrichtig sind, nicht verarbeitet und verwendet werden dürfen. Diese Rechtsfolge dürfe nicht dadurch umgangen werden, daß die Daten nach Auftreten von Richtigkeitszweifeln etwa mit einem einschränkenden Zusatz, ihre Richtigkeit stehe nicht fest, nun doch weiterverwendet werden. Sie unterliegen vielmehr schlechthin der Sperrung.

Dies gelte aber nicht nur, wenn sich nachträgliche Bedenken gegen die Richtigkeit von Daten ergeben, sondern notwendigerweise auch, wenn sich die Daten von vornherein mit einem Vorbehalt, ob sie sich auf eine bestimmte betroffene Person beziehen, versehen sind, dann aber von dem Betroffenen bestritten wird, daß diese Möglichkeit in Betracht komme. Nur so lasse sich vermeiden, daß eine datenverarbeitende Stelle die gesetzliche Folge in § 35 Abs. 2 Satz 1 BDSG durch Anfügung von Vorbehalten an bestimmte Daten leerlaufen läßt.

Die SCHUFA bemüht sich in Fällen, in denen die Richtigkeit der Angaben bestritten wird, um Aufklärung und Richtigstellung. Sie hat mitgeteilt, daß sie in der Praxis auf der Basis des Beschlusses des OLG Hamburg vom 23. 1. 1987 arbeite. Wenn der Betroffene konkret im Einzelfall die Zuordnung zu seiner Person bestritten habe und sich hieraus Bedenken gegen die Richtigkeit der Zuordnung ergeben, würden die Daten nicht mehr weitergegeben.

Die SCHUFA hat weiter darauf hingewiesen, daß es sich nicht um ein Problem der SCHUFA handele, sondern vielmehr um ein Problem des Schuldnerverzeichnisses, das eine klare Identifizierung wegen des fehlenden Geburtsdatums nicht zulasse.

5.2.5 SCHUFA-Klausel bei Guthaben-Konten

Ich hatte in meinem letzten Tätigkeitsbericht ausführlich dargestellt, daß bei der Führung eines Girokontos auf Guthabenbasis die Unterschrift unter die SCHUFA-Klausel nicht verlangt werden kann, da das Kreditinstitut in diesen Fällen kein berechtigtes Interesse im Sinne des § 32 Abs. 2 Satz 1 BDSG am Erhalt von SCHUFA-Nachmeldungen hat, die es aufgrund seiner Meldung des Girokontos automatisch von der SCHUFA erhält (vgl. 5. TB, 6.4.3, S. 114 f.). Die Erörterungen dieses Problems mit den Verbänden der Kreditwirtschaft haben dazu geführt, daß jetzt Einigkeit mit diesen über die rechtliche Beurteilung dieses Sachverhalts besteht. Die Verbände der Kreditwirtschaft sind wie die Datenschutz-Aufsichtsbehörden der Auffassung, daß bei einer Kontoführung auf Guthabenbasis und bei einem Verzicht auf die Ausgabe von Scheckvordrucken mit Scheckkarte die Meldung dieses Kontos an die SCHUFA juristisch nicht zu rechtfertigen ist und daß deswegen in diesen Fällen auch nicht die Unterschrift unter der SCHUFA-Klausel verlangt werden kann. Wie mir der Zentrale Kreditausschuß mitgeteilt hat, hat sich ein großer Teil der angeschlossenen Kreditinstitute bereit erklärt, solche Konten ohne die SCHUFA-Beobachtung zu führen.

Aus geschäftspolitischen und teils auch aus organisatorischen Erwägungen bestehen einige Kreditinstitute gleichwohl auf der Unterzeichnung der SCHUFA-Klausel und der Meldung an die SCHUFA, auch wenn ein Kunde sein Girokonto ausdrücklich nur auf Guthabenbasis führen will oder wenn das Kreditinstitut von sich aus wegen „beschränkter Bonität" des Kunden nur zu einer Kontoführung auf Guthabenbasis bereit ist. Ich bedaure dies sehr, da diese Kreditinstitute in solchen Fällen die SCHUFA in voller Kenntnis der juristischen Problematik zu rechtswidrigen Nachmeldungen veranlassen.

Zu meiner Überraschung hat die SCHUFA mir jetzt mitgeteilt, daß sie meine Auffassung nicht teile und daß sie auch bei Guthabenkonten von einem kreditorischen Risiko ausgehe, welches als Grundlage für obige Auskünfte ausreiche.

5.3 Automatisierung des Zahlungsverkehrs

Es kann davon ausgegangen werden, daß der Bürger nicht in der Lage ist, die Sicherheit von automatisierten Verfahren zu beurteilen. Das gilt besonders für so komplexe Systeme, wie sie zur Automatisierung des Zahlungsverkehrs eingesetzt werden. Seine Unsicherheit hinsichtlich der mit dem Einsatz möglicherweise für ihn verbundenen Gefahren ist daher entsprechend groß. Systeme des automatisierten Zahlungsverkehrs kommen jedoch — weltweit — zunehmend zum Einsatz, so daß bald jeder Bürger mit diesem Problem konfrontiert wird.

Eine Arbeitsgruppe aus Mitarbeitern der Datenschutzbeauftragten von Berlin, Bremen, Hamburg und Nordrhein-Westfalen hat im Berichtszeitraum die organisatorisch-tech-

nischen Bedingungen der z.Z. wichtigsten automatisierten Zahlungssysteme untersucht und mit ausführlichen Gutachten die Grundlage für eine juristische und datenschutzpolitische Aufarbeitung der diesen Systemen innewohnenden Probleme geschaffen. Untersucht wurden die technischen Bedingungen für:

— POS — Point of Sale,

— Home-Banking mit Btx,

— maschinelle Authentifizierung im Zahlungsverkehr,

— Datenfernverarbeitung zwischen Kreditinstituten,

— Bankdienste wie Geldausgabeautomaten, Selbstbedienungskontenführung u.a.

Aufgrund der vorliegenden Untersuchungen zeichnen sich einige grundsätzliche Probleme ab, die nachfolgend in groben Zügen beschrieben werden sollen.

(1) Fehlen einer Nachweismöglichkeit für den Bürger bei maschinell authentifizierter Transaktion

Ein Bürger, der eine Buchung im Rahmen einer Transaktion, die maschinell authentifiziert wurde, mit der Begründung reklamiert, er habe diese Transaktion nicht getätigt, setzt sich möglicherweise dem schwerwiegenden Vorwurf aus, er bestreite seine Urheberschaft wahrheitswidrig, um sich einen Vermögensvorteil zu verschaffen. Diesen Vorwurf kann der Betroffene immer dann nicht selbst widerlegen, wenn der reklamierten Transaktion kein von ihm unterschriebener Beleg zugrundeliegt. Ein besonderes Risiko für den Bürger besteht also dann, wenn Transaktionen ausschließlich auf der Basis maschineller Authentifizierung erfolgen. In einem solchen Fall existiert kein zu archivierender Beleg, der auf seine Echtheit, d.h. vor allem auf die Echtheit der Unterschrift von einer neutralen Stelle überprüft werden könnte. Es wird günstigstenfalls gespeichert, welche Daten der Datenverarbeitungsanlage zur Authentifizierung zur Verfügung standen, nämlich Daten aus dem Bestand und Daten, die von dem — tatsächlich oder vorgeblich — Berechtigten in das System eingegeben wurden. Der Bürger hat im Streitfall — jedenfalls beim derzeitigen Stand der Entwicklung — keine Möglichkeit, seine Aussage, er habe etwas nicht getan, durch Unterlagen zu stützen. Selbst wenn der Betroffene nachweisen können sollte, daß er die Transaktion nicht ausgelöst haben konnte, weil er sich an einem entfernten Ort aufhielt, wird ihm die Transaktion angelastet mit der Begründung, der Täter könne die Identifikationsmerkmale (Magnetkarte und PIN) nur von ihm, dem Betroffenen, erhalten haben. Dabei spiele es für die Haftung keine Rolle, ob der Täter in den Besitz der Merkmale gekommen sei, weil der Betroffene es an der nötigen Sorgfalt habe fehlen lassen oder weil der Betroffene in betrügerischer Absicht seine Merkmale preisgegeben habe. Beides falle in den Verantwortungsbereich des Betroffenen. Diese Argumentation, die auf der Behauptung beruht, nur vom Betroffenen kann der Dritte die Merkmale erhalten haben, mag in den meisten Fällen richtig sein. Im Einzelfall kann sie allerdings auch falsch sein, wie wir aus Versuchen von TV-Redakteuren und aus aufgeklärten Straftaten wissen.

Zwar haben die Banken in den bisher bekannt gewordenen Fällen, in denen Dritte sich durch Tricks und Manipulationen an Karten und Geldautomaten die Identifikationsmerkmale verschaffen konnten, ohne daß die Betroffenen dafür verantwortlich zu machen wären, den Schaden selbst getragen, wenn auch nur „aus Kulanz" und nicht wegen einer gefestigten Rechtsposition des Betroffenen. Aber wenn es den Dritten etwa gelingen sollte, die Spuren ihres Tuns rechtzeitig wieder zu beseitigen (also — um bei dem bekannten Fall zu bleiben — das „Zusatzgerät" am Geldautomaten und die Staubschicht auf der Tastatur vor der Entdeckung durch Bank oder Polizei wieder zu entfernen), dann hat der „normale" Bürger kaum eine Chance selbst aufzuklären, worin der Fehler gelegen haben könnte bzw. wie ein Mißbrauch abgelaufen sein könnte.

Dies scheint nun auch von den Banken nicht mehr völlig ausgeschlossen zu werden. Uns liegt eine Information darüber vor, daß in Zukunft in solchen Fällen der

Kunde nur noch für 10% des Schadens in Anspruch genommen werden soll, während die Bank 90% des Schadens trägt. Die Vertragsbedingungen sollen entsprechend geändert werden. Damit tragen die Banken dem Umstand Rechnung, daß sie für das technische Konzept eines Bankdienstes verantwortlich sind. Die Banken sind im übrigen dabei, da, wo es ihnen beim derzeitigen Stand der Technik möglich ist, Verfahren zu entwickeln, in denen auch dem Kunden authentische Nachweise über seine Aktivitäten im System zur Verfügung gestellt werden, so z.B. ein Verfahren für die Datenfernübertragung von Zahlungsverkehrsdaten vom Kunden-PC zum Bankrechner. Wesentliches Merkmal dieses Verfahren ist — über die sichere und zuverlässige Übertragung im Sinne eines vollständigen, nachvollziehbaren und fehlerfreien Datentransfers hinaus — der Schutz vor unautorisierter Übertragung sowie vor Eingriffen und Manipulationen Dritter während der Übertragung. Dieser Schutz wird u.a. durch verschlüsselte Datenübertragung und durch korrespondierende Protokollierungen im Bank- und Kundenrechner realisiert. Entsprechende Lösungen für Karten-Systeme und Geldautomaten sind mit Magnetkarten nicht realisierbar. Ob ähnliche Lösungen mit Chipkarten möglich sind, bleibt abzuwarten, denn bei diesen Systemen korrespondiert der Kunde mit seiner Karte nicht nur mit einem einzigen genau definierten „Bankrechner", sondern er will — möglichst europaweit — mit vielen „Bankrechnern" (Geldautomaten, POS-Kassen, Kundenterminals) korrespondieren.

(2) Durchsetzbarkeit von Datenschutzrechten

Das Geflecht der diversen an einem automatisierten Zahlungsvorgang, z.B. einer Zahlung an einer POS-Kasse, beteiligten Stellen birgt die Gefahr in sich, daß der Kunde nicht mehr nachvollziehen kann, welche Stelle aus welchem Grund welche Daten über ihn erhält, verarbeitet, speichert. Er weiß dann wahrscheinlich auch nicht, an wen er sich zu wenden hat, wenn er seine Datenschutzrechte (Auskunft, Löschung, Berichtigung) geltend machen will. Bei POS z.B. tritt an die Stelle eines anonymen Kaufs (mündliche Einigung, Übergabe des Kaufgegenstandes, Barzahlung) ein Vorgang, bei dem Daten des Kunden erfaßt, übermittelt, verarbeitet und gespeichert werden.

Die datenschutzrechtliche Einordnung solcher Stellen wie Autorisierungszentralen (POS-Systeme) oder Clearingstellen (ec-Karten-System, Geldausgabeautomaten) ist bisher nicht eindeutig. Es bleibt unklar, wie das Beziehungsgeflecht Kunde, Handelsunternehmen, Kreditinstitut, Clearingstelle, Autorisierungszentrale den datenschutzrechtlichen Termini „speichernde Stelle", „Auftragsdatenverarbeitung", „Auftragnehmer", „Auftraggeber" zugeordnet werden kann. Wenn der Kunde gar nicht weiß, welche Institutionen an einem Zahlungsvorgang überhaupt beteiligt sind, weiß er auch nicht, wer Adressat seiner datenschutzrechtlichen Ansprüche gem. § 4 BDSG ist.

(3) Preisgabe differenzierter Negativmeldungen an Personal von Handelsunternehmen bei POS-Nutzung

Für den POS-Zahlungsvorgang sind differenzierte Meldungen an den Händler bzw. den Kassierer nicht erforderlich, da für diesen lediglich wichtig ist, ob diese Zahlungsweise in einem bestimmten Fall gewählt werden kann. In dem Berliner POS-System erfolgt im Falle einer Negativmeldung eine gewisse Differenzierung im Antwortcode. Diese läßt Rückschlüsse darauf zu, ob vom Kunden nicht zu vertretende technische Probleme an ec-Karte, ec-Kasse, Datenfernverkehr oder Rechner der Autorisierungszentrale vorliegen, ob die Karte ungültig ist oder ob das Kreditinstitut des Kunden diesen um Rücksprache bitten läßt. Diese differenzierte Meldung geht heute bei bestimmten POS-Kassen-Systemen an den Kassierer, bei anderen ausschließlich an den Kunden. Die Angabe differenzierter Ablehnungsgründe geschieht angeblich im Interesse des Kunden, der nähere Auskunft darüber wünscht, warum sein Zahlungsversuch zurückgewiesen wird. Die Angabe dieser Gründe gegenüber dem Kassierer kann aber u.U. gegen das Interesse des Kunden verstoßen.

(4) Gefahren für die Vertraulichkeit des Dialogs

Bei automatisierten Bankdiensten hat der Kunde keine Möglichkeit zu überprüfen, ob nicht Manipulationen an den Endgeräten (wie es z.B. an Geldautomaten schon tatsächlich geschehen ist, indem ein Gerät vor den Karteneinzugsschlitz montiert und die Zifferntasten präpariert wurden) oder an den Datenfernübertragungsschnittstellen vorgenommen worden sind, die zur Ausforschung der PIN oder für den Kunden bestimmter Nachrichten genutzt werden können. Die Vertraulichkeit der Eingabe der PIN durch den Kunden sowie eventueller Rückmeldungen des Systems an den Kunden hängt auch bei intakten Endgeräten im wesentlichen von der Gestaltung der Endgeräte und den baulichen und organisatorischen Gegebenheiten am Aufstellungsort der Geräte ab, auf die der Kunde keinen Einfluß hat. Eigene Beobachtungen haben gezeigt, daß in manchen Fällen die verwendeten Tastaturen und/oder das Display so angebracht sind, daß eine unbefugte und unbemerkte Beobachtung der Eingabe durch Dritte (z. B. nachfolgende Kunden, die zu nah aufrücken) nicht ausgeschlossen werden kann.

Bei Btx-Kontenführung darf davon ausgegangen werden, daß der Bürger, der die Einrichtung eines solchen Kontos erwägt, nicht abschätzen kann, ob das Sicherungssystem seiner Bank für diesen Dienst ausreicht, um eine richtige Verarbeitung seiner per Btx erteilten Aufträge zu gewährleisten und jeden unbefugten Zugriff auf sein Konto abzuwehren. Die Kreditinstitute rechnen Verfügungen, die durch ihre Programme für die Btx-Kontenführung akzeptiert und ausgeführt werden, aber in jedem Falle dem Kontoinhaber zu. Aus der Sicht von Fachleuten, die mit der Technik vertraut sind, muß die vorgebliche absolute Sicherheit jedoch in Frage gestellt werden.

5.4 Versicherungswirtschaft

5.4.1 Zentrale Dateien der Versicherungsverbände

Die Erörterungen der datenschutzrechtlichen Problematik der Datenübermittlungen zwischen Versicherungsunternehmen und einigen Versicherungsverbänden (vgl. zuletzt 5. TB, 6.5.1, S. 118 ff.) haben dazu geführt, daß in einem Fall (Sonderwagnisdatei der Lebensversicherer) ein datenschutzgerechtes Ergebnis erzielt werden konnte und daß in einem zweiten Fall (Zentrale Registrierstelle Rechtsschutz) Versuche zur Einführung eines datenschutzrechtlich unproblematischen Meldeverfahrens laufen. In einem dritten Fall (Meldeverfahren der Kraftfahrzeughaftpflichtversicherer) befinde ich mich noch in der Prüfung des Meldeverfahrens. In einem vierten Fall (Meldeverfahren der Unfallversicherer) sehe ich datenschutzrechtliche Probleme, die ich derzeit mit dem HUK-Verband erörtere. In einem fünften Fall (Sachschadendatei) sind die Datenschutz-Aufsichtsbehörden dankenswerterweise vor Einführung des Meldeverfahrens beteiligt worden und bringen derzeit in Gesprächen mit der Versicherungswirtschaft ihre Position dazu zur Geltung. Der Sachstand ist im einzelnen folgender:

5.4.1.1 Sonderwagnisdatei der Lebensversicherer

Ich hatte bereits in meinem letzten Tätigkeitsbericht (5. TB, 6.5.1.1, S. 118) ausgeführt, daß der Verband der Lebensversicherungs-Unternehmen ein Match-Code-Verfahren erfolgreich erprobt hat, mit dem die datenschutzrechtlichen Probleme der Meldungen an und durch die Sonderwagnisdatei der Lebensversicherer beseitigt werden konnten. Nachdem die Datenschutz-Aufsichtsbehörden ihre Zustimmung zu diesem neuen Meldeverfahren erklärt haben, sind im Verband der Lebensversicherungs-Unternehmen die technischen Voraussetzungen hierfür geschaffen worden. Die Unternehmen sind nunmehr damit befaßt, das Match-Code-Verfahren in die Praxis einzuführen. Ich bin froh, daß hier ein Weg gefunden werden konnte, der die datenschutzrechtlichen Bedenken gegenüber dem früheren Verfahren weitgehend ausräumt und der gleichzeitig für die Versicherungswirtschaft zumutbar ist.

5.4.1.2 Zentrale Registrierstelle Rechtsschutz

Der HUK-Verband testet seit dem vorigen Jahr ein dem Verfahren bei der Sonderwagnisdatei der Lebensversicherer entsprechendes Match-Code-Verfahren für die Zentrale Registrierstelle Rechtsschutz (vgl. 5. TB, 6.5.1.2, S. 119). Damit soll auch dieses Meldeverfahren so geändert werden, daß kein Anlaß zu datenschutzrechtlicher Kritik mehr verbleibt. Ich hatte in meinem vorigen Tätigkeitsbericht an Einzelheiten des jetzt in der Erprobung befindlichen Verfahrens Kritik geübt.

Der HUK-Verband hat mir im Frühjahr mitgeteilt, daß die bisherigen Erfahrungen, die seine Mitgliedsunternehmen mit dem Match-Code-Verfahren gemacht haben, zeigen, daß die Trefferquote bei Identitätsprüfungen zu gering sei und deshalb zu viele vergebliche Anfragen bei Versicherern verursacht würden.

Von einem Mitgliedsunternehmen über einen längeren Zeitraum durchgeführte Sondererhebungen hätten folgendes ergeben: Bei monatlich etwa 400 Neuanträgen sei durchschnittlich in 16 Fällen Paarigkeit mit den in der Datei enthaltenen Match-Codes festgestellt worden. Die Trefferquote nach Rückfrage beim Vorversicherer hätte jedoch nur bei 0,3 % gelegen, so daß alle übrigen Anfragen vergeblich gewesen seien.

Da der HUK-Verband dieses Ergebnis nicht nur unter Kostengesichtspunkten, sondern auch aus datenschutzrechtlicher Sicht für unerwünscht halte, habe er sich entschlossen, den Match-Code um die Postleitzahl zu erweitern, die er sich in der Vergangenheit bereits mit hatte aufgeben lassen, ohne sie jedoch bisher in den Match-Code einzubeziehen.

Die von mir angeregte Ergänzung des Match-Code um das Geburtsdatum des Betroffenen wäre auch nach Ansicht des HUK-Verbandes sicherlich die wirkungsvollste Maßnahme, lasse sich jedoch leider für den Bereich der Rechtsschutzversicherung nicht verwirklichen, da das Geburtsdatum bei der Antragsaufnahme bisher nicht erfaßt werde. Sollte sich hieran in der Zukunft etwas ändern, werde der HUK-Verband den Match-Code umstellen.

Nachdem die Erprobung bereits fast eineinhalb Jahre andauert, erwarte ich eine endgültige Klärung, ob und mit welchen Modifizierungen das Match-Code-Verfahren für die Zentrale Registrierstelle Rechtsschutz eingeführt wird, im Laufe des Jahres 1988.

5.4.1.3 Meldeverfahren der Kraftfahrzeug-Versicherer

Auch für die Sparte der Kfz-Versicherer besteht beim HUK-Verband in Hamburg ein Auskunftsdienst, dessen Aufgabe es ist, dem Versicherungsbetrug zu begegnen. In der Zentralen Registrierstelle des Verbandes werden zu diesem Zweck die sog. Dateien A, B, C, D und E geführt, zu denen die angeschlossenen Mitgliedsunternehmen ihre Angaben melden und aus denen sie im Bedarfsfalle Auskünfte erhalten können. Diese Informationen ermöglichen es einem Autoversicherer, sich mit einem anderen in Verbindung zu setzen, wenn in Schadensfällen Ähnlichkeiten oder Zusammenhänge erkennbar werden.

Datei A

Zur Datei A werden solche Personen gemeldet, die im Verdacht stehen, einen Versicherungsbetrug begangen zu haben. Gespeichert werden folgende Angaben:

Kennung der meldenden Versicherungsgesellschaft

Schaden-Nr.

Art der Deckung (Kfz-Haftpfl., Vollkasko oder Teilkasko)

Art des Schadens (Totalschaden, Totaldiebstahl, fiktive Reparaturkosten, sonstiges)

Schadentag

Schadenort (PLZ und Name)

Nachname

Vorname

Geburtstag

. PLZ des Wohnortes, bei Ausländern: Nationalitäten-Kennzeichen

Art der Beteiligung (Versicherungsnehmer, Anspruchsteller, Zeuge, Werkstatt, Mietwagenverleih, Abschleppunternehmen, Sachverständiger, Fahrer, sonstige)

amtliches Kennzeichen

Suchbegriffe für die Bearbeitung der Datei und den Auskunftsverkehr sind der Nachname in Verbindung mit dem Vornamen und/oder der Postleitzahl des Wohnortes. Als Verknüpfungsmerkmal zu der Datei B dienen dieselben Angaben.

Die Meldungen und Anfragen erhält der Verband von besonders dazu benannten „Berechtigten Stellen" der angeschlossenen Versicherungsgesellschaften. Nach Eingang der Meldung wird beim Verband geprüft, ob zu dieser Person bereits ein Datensatz besteht, und — soweit dies der Fall ist — der anfragenden Stelle dieser Datensatz in einem Computerbrief bekanntgegeben. Mit dieser Kenntnis kann sich die anfragende Stelle an die Gesellschaft wenden, bei der der frühere Schadensfall aufgetreten war, um zunächst einmal die Identität des Betroffenen zu prüfen und dann ggfs. die Verdachtsmomente zu erhärten. Ein gemeldeter Datensatz bleibt maximal 4 Jahre gespeichert, es sei denn, die meldende Stelle beantragt die vorzeitige Löschung.

Datei B

Zur Datei B werden solche Personen gemeldet, gegen die wegen des Verdachts des Versicherungsbetruges ein Strafantrag gestellt wurde oder die bereits wegen dieser Straftat verurteilt worden sind. Suchbegriff ist der Nachname. Wird bei Meldungen oder Anfragen ein bereits vorhandener Datensatz gefunden, wird wie bei der Datei A ein Computerbrief geschrieben. Die Dauer der Speicherung beträgt 10 Jahre. Es werden die nachstehenden Angaben gespeichert:

Nachname, Vorname, Geburtsdatum

Anschrift (PLZ, Wohnort, Straße u. Haus-Nr.)

Kennung der meldenden Versicherungsgesellschaft

Schaden-Nr.

Art der Beteiligung (verschlüsselt wie bei Datei A)

Schadendatum

Schadenort (PLZ und Name)

Fahrzeug, Hersteller, Identifizierungsnummer

amtliches Kennzeichen

Sind mehrere Personen beteiligt, werden jeweils eigene Datensätze erstellt; dieses gilt auch bei verschiedenen Wohnorten.

Datei C

Außerdem wird eine Datei C geführt, bei der die Fahrgestell-Nrn. von solchen Fahrzeugen als Suchmerkmal verwendet werden, die in einen Schadensfall verwickelt sind. Gespeichert werden:

Kennung des Versicherungsunternehmens

Schaden-Nr.

Art der Deckung

Art des Schadens (wie bei Dateien A und B)

Schaden-Tag

Schadenort

Fahrgestell-Nummer

Fahrzeugart (PKW, LKW, Wohnwagen, Krad, sonstige)

Datum der Erstzulassung

Hersteller

Verkaufsbezeichnung (Typ)

amtliches Kennzeichen

Datei D

Die Datei D ist lediglich eine Hilfsdatei; sie dient ausschließlich dazu, die Verbindung zwischen den Datensätzen der Dateien A und C anhand des amtlichen Kennzeichens herzustellen.

Datei E

Diese Datei ist eine interne Hilfsdatei zur Datei B, hier werden lediglich Schadennummern gespeichert.

Der HUK-Verband hält die Speicherung aller in den vorgenannten Dateien enthaltenen Angaben für nötig, weil es wesentliche Aufgabe der angeschlossenen Mitgliedersunternehmen sei, unbegründete Ansprüche abzuwehren. Dies habe zwangsläufig Auswirkungen auf alle anderen Versicherungsnehmer, nämlich bei der Prämiengestaltung in der Autoversicherung. Schadensmanipulationen gingen zwangsläufig zu Lasten aller Versicherungskunden.

Zum Komplex der Dateien A bis E ergeben sich eine Reihe von Fragen, die ich in der nächsten Zeit mit dem HUK-Verband erörtern werde:

allgemein

Welche generellen Regeln hat der Verband seinen Mitgliedern für den Umgang mit diesen Dateien gegeben?

In welchen Beziehungen stehen die Dateien zueinander?

Datei A

Wie klar ist der Personenkreis definiert, der zur Datei A gemeldet wird?

Sind alle gemeldeten Daten und ihr Speichern zum Erreichen des erstrebten Zieles erforderlich?

Nach welchen Kriterien erfolgt die vorzeitige Löschung?

Datei B

Sind alle gespeicherten Daten zum Erreichen des Zieles erforderlich?

Ist die Speicherung auf die Dauer von 10 Jahren zulässig?

Welche Fortschreibungsregeln bestehen?

Dateien C, D, E

Ist das Speichern personenbezogener Daten im derzeitigen Umfang und zum Erreichen des Zwecks erforderlich?

Welche Löschungs- und Fortschreibungsregeln bestehen?

5.4.1.4 Meldeverfahren der Unfallversicherer

Die Unfallversicherer betreiben über den HUK-Verband ein Meldeverfahren, mit dem sie sich vor Verlusten durch Betrugshandlungen einzelner Versicherungsnehmer schützen wollen.

Diese Betrugshandlungen laufen in der Regel nach folgendem Muster ab: Die Täter schließen — nacheinander oder gleichzeitig — bei mehreren Versicherern Unfallversicherungsverträge mit möglichst hohen Versicherungssummen ab. In den Anträgen werden dabei die bereits anderweitig bestehenden oder beantragten Unfallversicherungsverträge wahrheitswidrig verschwiegen. Anschließend werden angebliche Versicherungsfälle gemeldet, bei denen zwei Hauptgruppen unterschieden werden können:

— Die Täter führen — meist an einem weniger wichtigen Körperteil, z.B. dem Daumen der linken Hand — eine Selbstverstümmelung herbei.

— Die Täter lassen sich mit ärztlich schwer nachprüfbaren angeblichen Unfallbeschwerden für längere Zeit krankschreiben, um in den Genuß von Tagegeld-Leistungen zu gelangen. Es sind auch Fälle bekannt geworden, in denen Ärzte im Ausland in kollusiver Absprache mit Reisenden bewußt unwahre Atteste ausstellten.

Wenn sich bei einem Versicherungsunternehmen bei der Antrags- oder Leistungsbearbeitung ein Verdacht auf verschwiegene anderweitige Versicherungen oder sonst anzeigepflichtige Umstände ergibt, hat das Unternehmen durch das Meldeverfahren die Möglichkeit, über den HUK-Verband Anfragen an die übrigen an den Verband angeschlossenen Unfallversicherungsunternehmen zu richten. Dies geschieht mit einem Vordruck, der den Unternehmen vom Verband zur Verfügung gestellt wurde.

Die wöchentlich versandten Ermittlungsrundschreiben haben im Schnitt einen Umfang von 25 Anfragen. Der HUK-Verband fungiert lediglich als „Poststelle" und leitet die Anfragen an seine Mitgliedsunternehmen weiter. Eine Aufbereitung der Versicherungsnehmerdaten in Form einer Karteikartensammlung oder EDV-Speicherung erfolgt beim Verband nicht. Die einzelnen Versicherungsunternehmen haben diese Daten — soweit ich feststellen konnte — ebenfalls nicht elektronisch gespeichert, planen dies aber z. T. in naher Zukunft zu tun. Zum größten Teil werden die Daten heute in Karteikartensammlungen geführt.

Ich habe Bedenken gegen dieses Meldeverfahren, das dem ähnelt, welches der Deutsche Transportversicherer-Verband (DTV) für Reisegepäckversicherer praktizierte, bevor die Datenschutz-Aufsichtsbehörden Änderungen erwirkt haben (vgl. 2. TB, 4.3.1.3, S. 116; 5. TB, 6.5.1.3, S. 119 f.). Ich halte es für geboten, das Verfahren dem anzupassen, das der DTV heute anwendet. Das geänderte Verfahren müßte demnach wie folgt ausgestaltet werden:

Der HUK-Verband empfängt — wie bisher — die Meldungen/Anfragen der Gesellschaften und gibt sie per Rundschreiben allen anderen Gesellschaften bekannt. Die einzelnen Gesellschaften verpflichten sich, die Verbandsrundschreiben nur für einen Zeitraum aufzubewahren, wie er üblicherweise ausreicht, um im Regelfall einen Schaden zu regulieren.

Für beide oben beschriebenen Fallgruppen ist das Interesse des Versicherers nur auf die jeweils aktuellen Mehrfach-Versicherungen ausgerichtet; eine längerfristige Aufbewahrung erscheint überflüssig.

Wenn bei den Versicherungsunternehmen die Notwendigkeit gesehen werden sollte, die Informationen aus den Meldungen über längere Zeit verfügbar zu haben, um bei jedem neuen auffälligen Schaden oder bei neuen Versicherungsanträgen darauf zurückgreifen zu können, darf dies aus meiner Sicht nicht in der Weise geschehen, daß die einzelnen Unternehmen die Meldungen speichern. Die einzelnen Meldungen müßten vielmehr beim HUK-Verband gespeichert oder anders gesammelt werden und den Unternehmen für Einzelanfragen zur Verfügung stehen. Diese hätten auf diese Weise Gelegenheit, bei jedem neuen auffälligen Schaden und bei jedem neuen Versiche-

rungsantrag eine Rückfrage an den Verband zu richten, wenn sie keine Umfrage nach dem üblichen Verfahren durchführen wollen.

Für die zentrale Datei wären die Vorschriften des 4. Abschnittes des BDSG anzuwenden, weil personenbezogene Daten zum Nutzen Dritter gespeichert und übermittelt werden (§ 31 Abs. 1 Nr. 1 BDSG). Daraus ergeben sich u.a. auch folgende Konsequenzen:

— Die Anfragen interessierter Gesellschaften müssen am Ende des fünften vollen Kalenderjahres nach Speicherung gesperrt werden.

— Die Betroffenen müssen über die Speicherung benachrichtigt oder auf andere Weise in Kenntnis gesetzt werden. Dies könnte in der Datenverarbeitungs-Ermächtigungsklausel geschehen, wenn diese die Speicherung beim HUK-Verband unter Angabe seiner Anschrift deutlich machte. Zu diesem Punkt gilt auch, was die Aufsichtsbehörden allgemein zur Verbesserung der Ermächtigungsklausel fordern.

Ich habe dem HUK-Verband meine Bedenken gegen dieses Meldeverfahren mitgeteilt und werde die Problematik mit ihm in nächster Zeit erörtern.

5.4.1.5 Sachschadendatei

Der Verband der Sachversicherer (VdS) in Köln plant die Errichtung einer Sachschadendatei, die der Aufdeckung von Betrugshandlungen und der Warnung vor Personen dienen soll, die bei der Schadenregulierung aufgefallen sind. Die Datenschutz-Aufsichtsbehörden sind frühzeitig in die Überlegungen zur Ausgestaltung dieser geplanten Meldestelle einbezogen worden, was ich sehr begrüße, weil dadurch die Chance gegeben ist, das Verfahren von vornherein datenschutzgerecht auszugestalten.

Die geplante Sachschadendatei soll nach der Konzeption des VdS Hilfestellung beim Erkennen von Personen und Anschriften leisten, die bei bestimmten Schäden aufgefallen sind. Durch die Speicherung dieser konkreten Einzelfälle bei einer Zentralstelle und durch die regelmäßige Weitergabe von anonymisierten Daten natürlicher Personen und vollen Daten juristischer Personen an alle an den VdS angeschlossenen Versicherungsunternehmen soll es möglich sein, Mehrfachtäter zu ermitteln und unberechtigte Forderungen abzuwehren.

Schäden aus allen Sparten der Sachversicherung sollen meldepflichtig sein zum einem bei einem Schadensaufwand ab DM 10.000,— und der Aufhebung des Vertrages durch das Versicherungsunternehmen, weil Tatbestände strafrechtlicher Art (z.B. Anklageerhebung, Verurteilung), vertragsbezogener Art (z.B. Verschweigen von Vorverträgen, vorläufigen Deckungszusagen oder Vorschäden, Verschweigen von Antragsablehnungen oder Kündigungen durch Vorversicherer) oder schadenbezogener Art (z.B. Gefahrerhöhung, Verletzung von Sicherheitsvorschriften oder Obliegenheiten, Verletzung der Schadensminderungspflicht oder der Schadensaufklärungspflicht, Herbeiführen oder Vortäuschen des Schadens) vorliegen, die der Versicherungsnehmer oder ein beteiligter Dritter zu vertreten haben. Zum zweiten sollen Schäden meldepflichtig sein bei einem Schadensaufwand ab DM 10.000,—, die durch vorsätzliche Brandstiftung (sowohl Eigen- als auch Fremd-Brandstiftung) entstanden sind.

Gemeldet werden sollen Daten des Versicherungsunternehmens und bestimmte Schadendaten sowie Daten zur Identifizierung der aufgefallenen Personen (Versicherungsnehmer und Personen, die in die Schadensabwicklung einbezogen sind).

Die Daten natürlicher Personen sollen vor der Weitergabe an die Meldestelle beim VdS in einen Match-Code umgesetzt werden. Wie dieser im einzelnen aussehen soll, steht noch nicht fest. Es läßt sich somit noch nicht beurteilen, ob er die Daten in genügender Weise anonymisieren wird. Beim VdS sollen die Meldungen gespeichert und monatlich auf Datenträgern an alle an den VdS angeschlossenen Versicherungsunternehmen weitergeleitet werden. Die Daten sollen nach der Vorstellung des VdS nach 10 Jahren gelöscht werden, da die Abwicklung von Groß- und Größtschäden in der Regel mehrere Jahre erfordere.

Die empfangenden Versicherungsunternehmen sollen die vom VdS erhaltenen Daten dann zur Prüfung von Schäden und zur Risikobeurteilung gegen den eigenen Bestand abgleichen. Bei Match-Code-Identität wird schriftlich oder telefonisch bei dem Versicherungsunternehmen angefragt, das den betreffenden Match-Code gemeldet hatte. Bei Identität der Namen natürlicher und/oder juristischer Personen soll sich die Schadenabteilung des empfangenden Versicherungsunternehmens mit der des meldenden Unternehmens in Verbindung setzen, damit dann ein schriftlicher oder telefonischer Informationsaustausch erfolgen kann.

Ich habe mich — auch für die anderen Datenschutz-Aufsichtsbehörden der Länder — über das Konzept für diese geplante Sachschadendatei informieren lassen und ein erstes Gespräch darüber mit der Versicherungswirtschaft geführt. Die Meinungsbildung unter den Datenschutz-Aufsichtsbehörden ist noch nicht abgeschlossen. Die jetzt in der Erprobung befindliche Datei wird noch weiter mit der Versicherungswirtschaft besprochen werden.

Meine vorläufige Beurteilung des jetzt vorliegenden Konzeptes für die Sachschadendatei sieht wie folgt aus:

Das geplante Meldeverfahren soll drei Zwecken dienen:

Die Meldung stellt eine Anfrage bei den anderen Versicherungsunternehmen dar, ob der Betroffene schon einmal einen meldepflichtigen Schaden hatte.

Die Meldungen werden bei allen Versicherungsunternehmen auf Vorrat gespeichert, um spätere Betrugsfälle aufdecken zu können.

Die Meldungen werden bei allen Versicherungsunternehmen auf Vorrat gespeichert, um bei später gestellten Anträgen auf Abschluß von Versicherungsverträgen evtl. verschwiegene Angaben über Vorschäden aufdecken zu können.

Für alle drei Zwecke dürfte das geplante Meldeverfahren datenschutzrechtlich unbedenklich sein. Die Anfrage nach einem Vorschaden entspricht dem beim Deutschen Transportversichererverband (DTV) akzeptierten System. Das gleiche gilt für den zweiten Zweck, wobei ich davon ausgehe, daß die Vorratsspeicherung in anonymisierter Form keine größeren datenschutzrechtlichen Bedenken aufwirft als das Anfragesystem beim DTV. Der dritte Zweck deckt sich mit dem bei der zentralen Datei der Lebensversicherer akzeptierten Verfahren.

Gespeichert werden Daten über die Versicherungsnehmer und über solche Personen, gegen die sich ein Verdacht richtet. Falls die Daten natürlicher Personen (z.B. Geschäftsführer) zwar anonymisiert, aber im Zusammenhang mit den vollen Daten einer juristischen Person gespeichert werden sollten, hielte ich dies für problematisch, soweit dadurch eine Deanonymisierung erleichtert würde.

Ich halte es für notwendig, daß in die Datenverarbeitungs-Ermächtigungsklausel wenigstens eine Unterrichtung über diese zentrale Datei aufgenommen wird, damit die Betroffenen (zumindest soweit sie Versicherungsnehmer sind und die Klausel deswegen bei Antragstellung unterschreiben) über das Meldeverfahren informiert werden. In das Datenschutzmerkblatt könnten weitere erläuternde Hinweise über diese Datei aufgenommen werden.

Der VdS geht davon aus, daß der Betroffene durch die normale Schadensbearbeitung auf andere Weise Kenntnis von der Speicherung erlangt hat und somit gemäß § 26 Abs. 1 BDSG eine separate Benachrichtigung über die Speicherung der Daten nicht mehr notwendig ist. Sie muß nach Auffassung des VdS auch unterbleiben, da sonst der Zweck der Datenbank ins Gegenteil verkehrt würde. Wenn Betroffene keine Kenntnis auf andere Weise haben (z.B. der als Brandstifter verdächtigte Dritte), greife ein Ausnahmetatbestand nach § 26 Abs. 4 Nr. 1 BDSG ein. Durch die Benachrichtigung würde ein potentieller Täter darauf hingewiesen werden, daß er künftig nur den Namen eines anderen verwenden müßte, um Vorverträge und/oder Vorschäden verschweigen und das Risiko der Entdeckung mit allen sich daraus ergebenden vertraglichen Folgen vermeiden zu können.

Die Versicherungswirtschaft legt Wert darauf, daß die Sachschadendatei nicht in den vierten Abschnitt des BDSG fällt, da vermieden werden soll, die Daten jeweils nach fünf Jahren sperren zu müssen (§ 35 Abs. 2 Satz 2 BDSG), denn erfahrungsgemäß können die Schadensregulierungen drei bis fünf Jahre dauern. Ich habe noch nicht im einzelnen geprüft, ob diesem Wunsch unter den Regelungen des BDSG Rechnung getragen werden kann.

Die Konzeption für die Sachschadendatei wird jetzt beim VdS getestet. Die Ergebnisse werden — wie angeführt — zwischen Datenschutz-Aufsichtsbehörden und Versicherungswirtschaft erörtert werden. Dabei wird auch Klarheit hergestellt werden, welche zentralen Dateien der VdS derzeit betreibt und in welchem Verhältnis die neue Sachschadendatei zu den derzeit betriebenen Meldeverfahren stehen soll, was die Datenschutz-Aufsichtsbehörden bisher noch nicht genau feststellen konnten.

5.4.2 Einwilligungsklausel nach dem BDSG

Die Kritik an der von der Versicherungswirtschaft verwendeten Einwilligungsklausel (bisher Datenschutzermächtigungsklausel genannt), die Versicherungsnehmer mit ihrem Antrag auf Abschluß einer Versicherung unterschreiben, habe ich zuletzt im meinem 5. Tätigkeitsbericht dargestellt (6.52, S. 120 ff.). Die Diskussion dieser Problematik zwischen Datenschutz-Aufsichtsbehörden und Versicherungswirtschaft ist im Berichtsjahr weitergeführt worden. Die Standpunkte konnten so weit angenähert werden, daß ich in absehbarer Zeit mit einer Einigung auf eine datenschutzgerechte neue Klausel rechne.

Die Versicherungswirtschaft hat den Entwurf einer neuen Einwilligungsklausel vorgelegt, der die Kritik der Datenschutz-Aufsichtsbehörden an der bisher verwendeten Klausel zum Teil berücksichtigt. Die Versicherungswirtschaft hat dabei Wert auf die Feststellung gelegt, daß die derzeitige Klausel alle Datenübermittlungen abdecke und daher rechtliche Gründe für eine Änderung der Klausel nicht vorhanden seien. Sie hat gleichwohl eine Änderung vorgeschlagen, weil sie der Auffassung ist, daß die derzeitige Klausel in bezug auf einige Datenübermittlungen möglicherweise nicht für jeden Kunden auf den ersten Blick verständlich sei.

Im Hinblick auf die einzelnen problematischen Punkte der Einwilligungsklausel ist der Stand der Diskussion mit der Versicherungswirtschaft folgender: Die Datenschutz-Aufsichtsbehörden bestehen nicht darauf, daß für den Fall des Nichtzustandekommens des Versicherungsvertrages die Datenübermittlung an eine zentrale Datei nur nach einer Abwägung der berechtigten Interessen mit den schutzwürdigen Belangen (§ 24 BDSG) vorgenommen werden kann. Sie vertreten nunmehr den Standpunkt, daß im Falle des Nichtzustandekommens des Vertrages eine Datenübermittlung auch auf der Grundlage einer Einwilligung des Betroffenen erfolgen kann. Dieser muß bei Abgabe seiner Einwilligung allerdings genau wissen, welchen möglichen Datenübermittlungen er zustimmt und daß diese Einwilligung eine Wirkung von mehreren Jahren haben kann.

Eine derartige Einwilligung auch für die Fälle des Nichtzustandekommens des Vertrages ist nach Auffassung der Datenschutz-Aufsichtsbehörden auch im Hinblick darauf wünschenswert, daß für Fälle Klarheit geschaffen werden sollte, in denen die Frage auftritt, ob § 203 StGB verletzt worden ist.

Die neue Klausel soll — wie z. T. bisher schon — so aufgebaut sein, daß sie aus verschiedenen Bausteinen besteht, von denen nur jeweils diejenigen für konkrete Antragsformulare verwendet werden sollen, die jeweils notwendig sind. Eine Einwilligung für Fälle des Nichtzustandekommens des Vertrages ist nur für Lebensversicherungen notwendig, da nur hier eine Meldung an die zentrale Datei erfolgt, (auch) wenn der beantragte Vertrag nicht geschlossen worden ist. Ein entsprechender Baustein muß deswegen auch nur in die Klauseln aufgenommen werden, die in Anträgen auf Abschluß von Lebensversicherungsverträgen Verwendung finden.

Die Datenschutz-Aufsichtsbehörden halten eine bessere Unterrichtung der Adressaten für notwendig. Es sollten nach ihrer Auffassung mindestens die typischen Tatbestände

möglicher Übermittlungen und ihr Zweck offengelegt werden, die zentralen Dateien sollten ausdrücklich erwähnt werden und es sollte darauf hingewiesen werden, unter welchen Umständen Datenübermittlungen von den zentralen Dateien an andere Versicherer vorgenommen werden können.

Die Versicherungswirtschaft hat dazu erklärt, daß die typischen Übermittlungstatbestände bereits jetzt in der Klausel enthalten seien (an Rückversicherer, an den ...-Verband, an andere Versicherer), und daß dabei auch der Zweck erläutert werde (zur Beurteilung des Risikos und der Ansprüche). Eine weitere Konkretisierung — entsprechend der SCHUFA-Klausel — sei kaum realisierbar, da eine abschließende Aufzählung nicht möglich sei. Im übrigen seien die einzelnen Übermittlungen in der „Information zur Datenübermittlung", die jeder auf Wunsch erhalte, näher erläutert; diese Erläuterungen könnten gegebenenfalls auch noch etwas konkreter gefaßt werden.

Nachdem ich in der Vergangenheit deutlich gemacht hatte, daß der in der Klausel enthaltene Zweck „zur Beurteilung des Risikos und der Ansprüche" eindeutig nur Übermittlungen im Rahmen des beantragten Vertrages abdeckt, nicht aber Übermittlungen zur Beurteilung des Risikos bei später zu beantragenden Verträgen, hat die Versicherungswirtschaft in ihrem Entwurf für eine neue Klausel vorgeschlagen, die Datenübermittlung bei künftigen Anträgen ausdrücklich in die Klausel aufzunehmen, um klarzustellen, daß auch dieser Fall von ihr erfaßt wird. Die Versicherungswirtschaft hat im übrigen darauf hingewiesen, daß nur die Lebensversicherer bei Nichtzustandekommen des Vertrages eine Meldung an eine zentrale Datei vornehmen, und zwar dann, wenn die Gründe für das Nichtzustandekommen im Risikobereich des Kunden liegen (Ablehnung durch das Versicherungsunternehmen wegen verweigerter Nachuntersuchung oder aus versicherungsmedizinischen Gründen, Ablehnung durch den Versicherungsnehmer wegen einer Erschwerung). Nicht gemeldet werden dagegen die Fälle, die deswegen nicht zum Vertragsabschluß führen, weil der zu Versichernde sich nicht der ärztlichen Untersuchung unterzieht, der Versicherungsnehmer von seinem Widerrufsrecht Gebrauch macht oder die erste Prämie nicht zahlt.

Die Datenschutz-Aufsichtsbehörden sind der Meinung, daß genau angegeben werden muß, welche Daten an (selbständige) Vertreter weitergegeben werden dürfen. Es wird nicht für zulässig gehalten, daß Gesundheitsdaten an Vertreter weitergegeben werden. Wenn ein Vertreter der Auffassung ist, daß er auch Gesundheitsdaten eines Versicherungsnehmers für seine Tätigkeit benötigt, steht es ihm frei, sich von diesem eine Einzelfallermächtigung zur Übermittlung an ihn geben zu lassen. Im Regelfall ist es ausreichend, wenn Vertreter die allgemeinen Vertragsdaten der Versicherungsnehmer erhalten, und nicht gerechtfertigt, ihnen weitere Daten wie z. B. die Abrechnungs- und Leistungsdaten der Krankenversicherung zukommen zu lassen, aus denen sie sehr detailliert auf die persönlichen Verhältnisse des Versicherungsnehmers schließen könnten.

Die Forderung der Datenschutz-Aufsichtsbehörden, daß Gesundheitsdaten nur dann an Außendienstmitarbeiter gegeben werden dürfen, wenn dies für die Vertragsgestaltung erforderlich ist, ist in dem von der Versicherungswirtschaft vorgelegten Klauselentwurf praktisch berücksichtigt. Die Versicherungswirtschaft hat deutlich gemacht, daß im übrigen allenfalls eine Übermittlung allgemeiner Gesundheitsdaten vom Versicherungsunternehmen an Außendienstmitarbeiter in Frage komme, wenn dem Unternehmen eine Anpassung des Vertrages an eine geänderte Situation sinnvoll und notwendig erscheint. Es ist jedoch im einzelnen noch klärungsbedürftig, wann genau welche Daten unter welchen Voraussetzungen an Außendienstmitarbeiter gegeben werden. Die Versicherungswirtschaft wird sich um eine Klärung des Sachverhaltes bemühen.

Die Datenschutz-Aufsichtsbehörden haben den Vorschlag gemacht, eine Widerspruchsmöglichkeit des Kunden gegen eine Weitergabe an Außendienstmitarbeiter zu erwägen.

In das Merkblatt, das der Kunde sich zur weiteren Information über die einzelnen Datenübermittlungen geben lassen kann, müssen nähere Erläuterungen aufgenom-

men werden, was mit den an Außendienstmitarbeiter gegebenen Daten geschehen kann, insbesondere welche Möglichkeiten der Weiterübermittlung an andere Vertreter (z.B. Nachfolger im Falle des Ausscheidens, Untervertreter) es gibt und welche Vorkehrungen getroffen sind, um dafür zu sorgen, daß der Außendienstmitarbeiter sorgsam mit den anvertrauten sensiblen Daten umgeht.

Nach der Einigung auf den Wortlaut einer neuen Einwilligungsklausel bedarf es auch noch einer Verständigung mit der Versicherungswirtschaft, wie und wo die Klausel in Versicherungsanträgen anzuordnen ist. Die gegenwärtige Gestaltung, bei der die Klausel oft so im „Kleingedruckten" versteckt ist, daß sie mit Sicherheit von fast niemanden gelesen wird, ist aus der Sicht des Datenschutzes nicht akzeptabel und dürfte auch mit § 3 AGB-Gesetz nicht zu vereinbaren sein. Die Versicherungswirtschaft vertritt dagegen die Auffassung, daß die Gestaltung der Klausel sowohl den Anforderungen des § 3 BDSG entspreche als auch denen des § 3 AGBG, da durch einen eindeutigen Hinweis auf die Klausel aufmerksam gemacht werde und außerdem diese drucktechnisch so hervorgehoben sei, daß ihre Kenntnisnahme zu erwarten sei. Im übrigen liege ein Verstoß gegen § 3 AGBG nur dann vor, wenn die Klausel objektiv ungewöhnlich und subjektiv überraschend ist. Davon könne sicherlich ebensowenig gesprochen werden wie davon, daß die Klausel im „Kleingedruckten" versteckt wird.

Diese rechtliche Beurteilung mag für eine Vielzahl von Klauseln zutreffen, wie sie in der Praxis verwendet werden. Nach meinen Erkenntnissen gibt es aber auch Fälle, in denen die vom GdV selbst formulierten Voraussetzungen nicht erfüllt sind.

Die Gespräche mit der Versicherungswirtschaft über diese Problempunkte werden weitergeführt. Ich hoffe, daß eine Einigung in nächster Zeit erreichbar ist.

5.4.3 Schweigepflicht-Entbindungsklausel

Die bereits mehrfach im einzelnen dargestellte Kritik an der derzeit verwendeten Schweigepflicht-Entbindungsklausel (vgl. zuletzt 5. TB, 6.5.3, S. 122 ff.) ist im Berichtsjahr weiter mit der Versicherungswirtschaft erörtert worden. Diese hat inzwischen Entwürfe für Neuformulierungen der Schweigepflicht-Entbindungsklauseln in der Kranken-, Unfall- und Lebensversicherung vorgelegt. Diese haben einige Kritikpunkte der Datenschutz-Aufsichtsbehörden berücksichtigt, einige Problembereiche jedoch bislang noch ungelöst gelassen. Der Stand der Diskussionen ist im einzelnen folgender:

Die Datenschutz-Aufsichtsbehörden halten zwar eine begrenzte und überschaubare Zukunftswirkung der Schweigepflichtentbindung für hinnehmbar, nicht jedoch eine unbegrenzte Zukunftswirkung. Eine Schweigepflichtentbindung für die Überprüfung des Gesundheitszustandes bei Antragstellung in den nächsten zwei oder drei Jahren wird für vertretbar, aber auch für ausreichend gehalten. Im Falle der Lebensversicherungen erscheint der Zeitraum, für den die Schweigepflichtentbindung abgegeben werden soll, überschaubar und die Zukunftswirkung insoweit akzeptabel. Darüber hinaus besteht aber kein berechtigtes Interesse des Versicherungsunternehmens daran, von dem Antragsteller/Versicherungsnehmer bereits bei Vertragsschluß eine unbegrenzte in die Zukunft reichende Schweigepflichtentbindung zu erhalten.

Im Leistungsfall ist es eine Obliegenheit des Versicherungsnehmers, durch Abgabe der Schweigepflicht-Entbindungserklärung bei der Aufklärung der Leistungspflicht mitzuwirken. Die Datenschutz-Aufsichtsbehörden halten es nicht für einen besonderen bürokratischen Aufwand, wenn die Versicherungsunternehmen im Falle einer notwendigen Schweigepflichtentbindung den Versicherungsnehmer schriftlich bitten, diese zusammen mit einer Weitergabe des Schreibens der Versicherung gegenüber seinem Arzt abzugeben, der dem Versicherungsunternehmen dann direkt Auskunft geben kann. Solange die Auskunft des Arztes nicht vorliegt, kann die Versicherung ihre Leistung verweigern. Etwaige Verzögerungen würden zu Lasten des Versicherungsnehmers gehen.

Die Schweigepflichtentbindung für den Fall des Todes, so wie sie jetzt in den Vorschlägen der Versicherungswirtschaft formuliert ist, halten die Aufsichtsbehörden für hinreichend genau und deswegen akzeptabel. Für die Fälle lang andauernder Bewußt-

losigkeit kann demgegenüber auf die Abgabe einer Schweigepflicht-Entbindungserklärung im voraus verzichtet werden, da die Rechtsordnung hierfür genügend Instrumente bereithält (mutmaßliche Einwilligung, Vertretung, Pflegschaft).

Die Versicherungswirtschaft hat dazu erklärt, es müßten zwei Fälle unterschieden werden: Zunächst einmal erfolge eine Schweigepflichtentbindung zur Beurteilung des Risikos, d.h. die Erklärung sei begrenzt auf den Zeitpunkt des Vertragsabschlusses. Zur Beurteilung der Leistungspflicht sei eine Schweigepflichtentbindung mit Zukunftswirkung erforderlich. Diese Ermächtigung sei zum einen begrenzt auf die erforderlichen Auskünfte und zum anderen gelte sie nur für die Ärzte und Personen, die der Versicherungsnehmer im Leistungsfall dem Versicherungsunternehmen nenne. Insofern konkretisiere der Versicherungsnehmer im Leistungsfall seine Schweigepflichtentbindung auf einen ganz bestimmten Arzt. Ohne diese Konkretisierung habe die Schweigepflichtentbindung keinerlei praktische Wirkung, so daß auch nur von einer sehr begrenzten Zukunftswirkung gesprochen werden könne.

Der Vorschlag der Datenschutz-Aufsichtsbehörden, Schweigepflicht-Entbindungserklärungen im Einzelfall in der Weise abgeben zu lassen, daß das Versicherungsunternehmen den Kunden jeweils bittet, die Fragen an den Arzt zusammen mit einer individuell auszustellenden Schweigepflichtentbindung weiterzugeben, so daß der Arzt dann direkt gegenüber dem Versicherungsunternehmen Stellung nehmen kann, wird von der Versicherungswirtschaft abgelehnt. Dies sei problematisch, weil in diesem Fall der Kunde/Patient über alle gesundheitlichen Einzelheiten informiert werde. Es seien jedoch auch Fälle denkbar, in denen der Arzt aus bestimmten Gründen Informationen von dem Kunden/Patienten fernhalten wolle (Krebs, Aids u.ä.). Dies sei nicht mehr möglich, wenn das Versicherungsunternehmen die an den Arzt zu stellenden Fragen dem Kunden/Patienten offenlegen müsse.

Die Versicherungswirtschaft hat erklärt, in jedem Fall löse der Versicherte durch seinen Versicherungs- oder Leistungsantrag mit Angaben und Unterlagen die Risikoprüfung bzw. die Leistungsprüfung aus. Soweit eine Rückfrage erforderlich werde, richte sie sich im medizinischen Bereich an den angegebenen Behandler. Die Schweigepflichtentbindung für die Zukunft und auch über den Tod hinaus in der Kranken- und Unfallversicherung sei auch rechtlich erforderlich, da anderenfalls eine Leistungsfrage nicht geklärt werden könne und die bestehenbleibende Unklarheit wegen fehlender Leistungspflicht des Versicherers zu Lasten der Versicherten bzw. seiner Erben gehe:

Zum einen könne der Versicherte infolge Erkrankung oder Unfall für längere Zeit bewußtlos oder sonst in einem Zustand sein, in dem er keine wirksame Schweigepflichtentbindung erklären kann. Im entsprechenden Einzelfall wäre dann die Zwischenrechnung des Krankenhauses über z.B. einen Krankenhausaufenthalt von vier Wochen wegen des Komas des Patienten, soweit dies in Betracht kommt, nicht prüfbar und daher der Versicherer bis zur Klärung nicht leistungspflichtig.

Zum anderen könne jeder Leistungsfall zum Tod des Versicherten führen. Nach seinem Tod seien nach herrschender Meinung seine Erben nicht mehr in der Lage, eine wirksame Schweigepflicht-Entbindungserklärung abzugeben. Liege also keine Entbindungserklärung des Versicherten über den Tod hinaus vor, so könne im Einzelfall nach seinem Tod eine für die Leistungspflicht des Versicherers klärungsbedürftige Frage nicht mehr durch Rückfrage bei dem behandelnden Arzt geklärt werden.

Schließlich komme es leider nicht ganz selten vor, daß der Versicherte unzutreffende Angaben macht und versucht, unberechtigt Leistungen in Anspruch zu nehmen. Dies gehe bis zur Verfälschung bzw. Fälschung von Rechnungen.

Würde für die Nachprüfung jeweils eine Schweigepflichtentbindung konkretisiert auf den betreffenden Fall erforderlich sein, so würde der Versicherte vorher von der vorgesehenen Prüfung Kenntnis erhalten und hätte dann die Möglichkeit, vor Abgabe der Entbindungserklärung Schwachpunkte des geltend gemachten Anspruches zu bereinigen, insbesondere auf denjenigen Einfluß zu nehmen, der voraussichtlich vom Krankenversicherer um Auskunft gebeten wird. Insbesondere auch ein nachträglicher Ver-

dacht der unberechtigten Leistungsinanspruchnahme könnte kaum geklärt werden, da der Versicherte eine Schweigepflichtentbindung für den bereits abgerechneten Fall vermutlich verweigern würde.

Auch das jetzt schon von mehreren Unternehmen der Privaten Krankenversicherung eingeführte Krankenhaus-Ausweisverfahren sei ohne die generelle Entbindungserklärung nicht durchführbar. Übernehme nämlich der Krankenversicherer eine Leistungsverpflichtung unmittelbar gegenüber dem Krankenhaus, so müsse er auch die Möglichkeit haben, im Einzelfall eine Rückfrage ganz kurzfristig zu halten, um erforderlichenfalls dann seine Leistungsverpflichtung gegenüber dem Krankenhaus durch Widerruf zeitlich zu begrenzen. Eine für die Rückfrage notwendige Einzelentbindung würde die Möglichkeit der Rückfrage wesentlich verzögern.

Mit den datenschutzrechtlichen Aspekten des sogenannten Krankenhaus-Ausweisverfahrens (Medicard) haben sich die Datenschutz-Aufsichtsbehörden bislang noch nicht befaßt. Ich kann jedoch nicht erkennen, daß die Besonderheiten dieses direkten Abrechnungsverfahrens eine andere Beurteilung der Zukunftswirkung der Schweigepflicht-Entbindungsklausel als in anderen Fällen datenschutzrechtlich nahelegen oder gar zwingend erfordern würden.

Eine Einigung in der Frage der Zukunftswirkung in der Kranken- und Unfallversicherung konnte somit bislang nicht erzielt werden. Das Thema wird weiter mit der Versicherungswirtschaft erörtert.

Der Forderung der Datenschutz-Aufsichtsbehörden, die Schweigepflichtentbindung für Sozialversicherungsträger aus den Klauseln herauszunehmen, ist in den Entwürfen der Versicherungswirtschaft Rechnung getragen worden.

Die Kritik der Datenschutz-Aufsichtsbehörden im Hinblick auf die gleichzeitige Schweigepflichtentbindung für mitzuversichernde minderjährige Kinder ist in den Vorschlägen der Versicherungswirtschaft im wesentlichen nicht berücksichtigt worden. Die Datenschutz-Aufsichtsbehörden halten an ihren Forderungen fest, daß die Schweigepflicht-Entbindungserklärung für mitzuversichernde minderjährige Kinder separat und nur von den Inhabern des Sorgerechts abgegeben wird und daß sie auf den Zeitraum bis zum Vorliegen der Volljährigkeit der Kinder begrenzt wird.

In den Vorschlägen der Versicherungswirtschaft wird jetzt nicht mehr auf die Minderjährigkeit, sondern auf die Einsichtsfähigkeit abgestellt. Sie stützt sich dabei auf die Ansicht des Bundesaufsichtsamts für das Versicherungswesen, daß Anknüpfungspunkt allein die Einsichtsfähigkeit sein könne. Bei der Schweigepflicht-Entbindungserklärung handele es sich um eine höchstpersönliche Erklärung, für deren Wirksamkeit es nicht auf die Volljährigkeit oder Geschäftsfähigkeit ankomme, sondern allein auf die Einsichtsfähigkeit. Dies entspreche der herrschenden Meinung in Rechtsprechung und Literatur. Die Datenschutz-Aufsichtsbehörden vertreten dagegen die Auffassung, daß wegen besserer Abgrenzbarkeit und Handhabbarkeit auf die Minder- bzw. Volljährigkeit abgestellt werden sollte.

Die noch offenen Probleme werden weiter mit der Versicherungswirtschaft erörtert.

5.4.4 Datenübermittlungen im Zusammenhang mit Vertrauensschadenversicherungen

Von einigen Versicherungsunternehmen werden sogenannte Vertrauensschaden- und Computer-Mißbrauchsversicherungen angeboten, mit denen sich Unternehmen gegen Schäden versichern können, die ihnen ihre eigenen Mitarbeiter durch Diebstahl, Unterschlagung, Buchhaltungsmanipulationen, Computer-Mißbrauch oder anderes ungetreues Verhalten zufügen können. Dabei werden entweder alle Mitarbeiter, bestimmte Mitarbeitergruppen oder namentlich genannte einzelne Arbeitnehmer in diese Versicherung einbezogen. Bei dem Einschluß namentlich zu benennender Vertrauenspersonen kann dies mit oder ohne Wissen des Betroffenen geschehen.

Wenn namentlich benannte Arbeitnehmer in die Vertrauensschadenversicherung eingeschlossen werden sollen, müssen z.B. bei einem Hamburger Versicherungsunternehmen u. a. folgende Angaben über den Betroffenen gemacht werden:

Name und Vorname, Wohnanschrift, Geburtsdatum und -ort, seit wann für den Versicherungsnehmer tätig? Art der Tätigkeit für den Versicherungsnehmer, Angestellter oder nicht. Geschieht diese Antragstellung auf Abschluß einer Vertrauensschadenversicherung mit Wissen des Betroffenen oder nicht? Liegen Lohn- und Gehaltspfändungen vor (ja, nein, Höhe)? Sind Ihnen Umstände bekannt, die für die Beurteilung der Vertrauenswürdigkeit und Zuverlässigkeit des Betroffenen nachteilig sein könnten? Lückenloser Tätigkeitsnachweis für die letzten drei Jahre (Schulbesuch, sämtliche Arbeitgeber, selbständige Tätigkeit, etwaige Arbeitslosigkeit ist durch Bescheinigung des Arbeitsamtes nachzuweisen), Referenzen (Angabe von Personen, bei denen sich das Versicherungsunternehmen über die einzuschließende Person erkundigen kann; keine Verwandten und früheren Arbeitgeber).

Diese Angaben können die Grundlage für weitere Ermittlungen über die Vertrauenswürdigkeit des betroffenen Arbeitnehmers durch das Versicherungsunternehmen sein, z. B. durch Einholung von Auskünften bei Handels- und Wirtschaftsauskunfteien. Wenn die Vertrauensschadenversicherung mit Wissen des betroffenen Arbeitnehmers beantragt wird, kann davon ausgegangen werden, daß er über die Datenweitergabe an das Versicherungsunternehmen zumindest informiert ist. Ob auch seine Einwilligung in die Datenübermittlung an das Versicherungsunternehmen und die möglichen weiteren Verarbeitungen eingeholt wird, ist dem Hamburger Versicherungsunternehmen, das mir Auskünfte gegeben hat, nicht bekannt.

Diese Gesellschaft teilt im Falle der Ablehnung eines Vertragsabschlusses dem Arbeitgeber des betroffenen Arbeitnehmers den Grund der Ablehnung nicht mit. Auch auf Nachfragen des Antragstellers wird nicht offengelegt, welche besonderen Risiken gesehen wurden.

In einem Schadenfall meldet der Versicherungsnehmer neben dem Schaden auch den Namen des Schadenverursachers. Der Schadenersatzanspruch des Versicherungsnehmers gegen den Schädiger geht bei Schadensregulierung kraft Gesetzes auf das Versicherungsunternehmen über. Damit dieses den Anspruch gegen den Schädiger dann verfolgen kann, muß bekannt sein, welche rechtlichen Maßnahmen der Versicherungsnehmer bereits gegen ihn eingeleitet hat. Dies muß also auch gemeldet werden.

Es gibt nach Auskunft des von mir befragten Versicherungsunternehmens keine zentrale Datei, an die Schädiger gemeldet werden.

Die Datenübermittlungen im Zusammenhang mit dem Abschluß von Vertrauensschadenversicherungen mit Einschluß namentlich benannter Vertrauenspersonen halte ich für problematisch, insbesondere wenn dies ohne Wissen des Betroffenen geschieht. Da die Beeinträchtigung schutzwürdiger Belange der betroffenen Arbeitnehmer angesichts des recht detaillierten Datenaustausches und der Ermöglichung weiterer Recherchen durch das Versicherungsunternehmen leicht denkbar ist, sollten namentlich benannte Vertrauenspersonen in derartige Versicherungen nur einbezogen werden dürfen, wenn sie in die dadurch notwendige Datenweitergabe eingewilligt haben.

Das Argument, das Vertrauensverhältnis zwischen Arbeitgeber und Mitarbeitern könne beeinträchtigt werden, wenn diese von dem Abschluß einer derartigen Versicherung erfahren, überzeugt micht nicht. Wenn ein Arbeitgeber zu einem Mitarbeiter, den er in einer besonderen Vertrauensstellung beschäftigen will oder beschäftigt, ein doch nur so eingeschränktes Vertrauen hat, daß er eine Vertrauensschadenversicherung für nötig hält, stellt sich die Frage, ob dem Mitarbeiter nicht zu viel Verantwortung übertragen werden soll oder worden ist. Jedenfalls ist diese Leichtfertigkeit nicht so schutzwürdig, daß sie einen detaillierten Informationsaustausch hinter dem Rücken des Betroffenen rechtfertigen könnte.

Das bereits erwähnte Hamburger Versicherungsunternehmen hat mir erklärt, in den letzten Jahren seien praktisch alle Vertrauensschadenversicherungen mit Einschluß namentlich benannter Personen mit deren Wissen abgeschlossen worden. Für dieses Unternehmen sind die Überlegungen also praktisch gegenstandslos. Bei anderen Versicherungsunternehmen treten die Fälle, in denen der Betroffene nichts von dem Abschluß der Vertrauensschadenversicherung weiß, dagegen offenbar häufiger auf.

Weiter erscheint es mir notwendig, die Meldung an das Versicherungsunternehmen auf solche Informationen zu beschränken, die der Arbeitgeber nach den arbeitsrechtlichen Grundsätzen zum Fragerecht bei Einstellungen von dem Betroffenen erfragen dürfte. Diese Grundsätze würden umgangen, wenn der Arbeitgeber/Versicherungsnehmer mehr Angaben über den Arbeitnehmer an das Versicherungsunternehmen geben müßte, als er von diesem erfragen darf. Eine derartige Verpflichtung bringt die Gefahr mit sich, daß der Arbeitgeber entweder durch (unzulässige) Befragung des Arbeitnehmers oder hinter dessen Rücken auf andere Weise versucht, die Angaben zu erhalten, die das Versicherungsunternehmen haben will.

Die Problematik der Datenübermittlungen im Zusammenhang mit Vertrauensschadenversicherungen ist bislang noch nicht mit der Versicherungswirtschaft diskutiert worden.

5.4.5 Auskunftsstelle über den Versicherungsaußendienst e.V. (AVAD)

5.4.5.1 Stand der Automation

Seit dem Herbst 1986 ist die AVAD dazu übergegangen, ihr Archiv auf ein modernes automatisiertes Verfahren umzustellen.

Dabei ist sie davon ausgegangen, daß im Außenverhältnis zu den Versicherungsgesellschaften und Bausparkassen weiterhin mit denselben Formularen gearbeitet werden soll. Lediglich die interne Archivbearbeitung — das Heraussuchen einer Akte/Auskunft, das Kopieren und andere manuelle Tätigkeiten — werden durch das neue Verfahren ersetzt.

Die Umstellung erfolgt in der Weise, daß nach außen hin praktisch nur noch das neue Verfahren angewendet wird. Bei jedem Anlaß, einen Vorgang zu bearbeiten, werden die Informationen aus den vorhandenen Auskünften oder Akten sofort übernommen. Die Antwort der AVAD auf eine Anfrage besteht schon aus einem Computerbrief, der im Rahmen des neuen Verfahrens erstellt worden ist.

Die gespeicherten Datensätze sind inhaltlich genauso aufgebaut wie die verwendeten Formulare. Zusätzlich wird das Datum der Eingabe festgehalten.

Zur Kontrolle am Bildschirm oder bei einem Ausdruck wird von einem Programm der entsprechende Vordruck dazugesteuert, damit der Leser die Zusammenhänge erkennen kann.

Nach einem Eingabevorgang (Übernahme, Eingang einer Tätigkeitsmeldung, Eingang oder Abforderung einer Auskunft) werden die Originalbelege in ein Archiv gegeben, in dem sie chronologisch nach dem Eingabedatum abgelegt und für Auskunftszwecke nicht mehr verwendet werden. Dieses Archiv dient lediglich dazu, etwaige Übertragungsfehler bei der Eingabe später noch aufklären zu können. Ansonsten bleibt nach der Übernahme keine Akte mehr bestehen. Ausnahmen ergeben sich nur, wenn der Betroffene in einen Schriftverkehr mit der AVAD eingetreten ist. Bei der üblichen Routine, einer anfragenden Gesellschaft Auskunft zu erteilen, kann jedoch keine Information aus der Akte in die Auskunft gelangen, weil bei dem starr ablaufenden Verfahren ein Zugriff auf die Akte nicht vorgesehen ist.

Die Bearbeitung des Archivs erfolgt ausschließlich am Bildschirm. Dazu bietet das Verfahren eine vorgegebene Menü-Auswahl an.

Zunächst ist der Name des Betroffenen einzugeben, dann ist zu wählen zwischen der Bearbeitung von Tätigkeitsmeldungen, Anfragen nach einer Auskunft oder Eingabe einer neuen Auskunft. Sonderauswertungen sind darüber hinaus am Bildschirm nicht möglich.

Die praktisch-technische Verarbeitung der Daten hat die AVAD einer externen Stelle übertragen, die zuvor nach den entsprechenden Vorgaben auch die Programme erstellt hat. Zu ihren Aufgaben gehört neben der täglichen Auftragsverarbeitung auch

die weitere Programmpflege. Auch der Auftragnehmer unterliegt der ständigen Aufsicht durch die Datenschutz-Aufsichtsbehörde nach den Vorschriften des 4. Abschnittes des BDSG. Dabei gehe ich davon aus, daß alle Weisungen des Auftraggebers in Schriftform ergehen.

Die Umstellung auf das neue Verfahren bedeutet keine Verschlechterung des Datenschutzes für den Betroffenen. Die ihm erteilte Auskunft enthält sogar mehr Daten als bisher. Da im neuen EDV-Verfahren nicht nur das eigentliche Auskunftsformular, sondern alle per Vordruck gemeldeten Daten gespeichert werden, erstreckt sich der Anspruch auf die Selbstauskunft nunmehr auch auf die Tätigkeitsmeldungen und die Auskunftsgesuche. Der betroffene Außendienstmitarbeiter erhält also auch Antwort auf die oft gestellte Frage, welche Gesellschaft über ihn angefragt hat oder welche Gesellschaft eine Tätigkeitsmeldung abgegeben hat und mit welchen konkreten Angaben die begonnene Tätigkeit angezeigt wurde.

5.4.5.2 Auskünfte über Versicherungsmakler

In meinem letzten Tätigkeitsbericht hatte ich über die Behandlung von Versicherungsmaklern im AVAD-Verfahren berichtet (5.TB, 6.5.6.3, S. 127 f.). Die AVAD hat inzwischen ein spezielles Auskunftsformular für Makler entworfen, das sie in den Gremien der Versicherungswirtschaft abgestimmt und mir vorgestellt hat. Sie hat weiter darauf hingewirkt, daß in Zukunft beim Abschluß von Courtagevereinbarungen mit Versicherungsmaklern die Zustimmung zu den Datenübermittlungen im Rahmen des AVAD-Verfahrens Bestandteil der getroffenen Vereinbarungen wird.

5.5 Handels- und Wirtschaftsauskunfteien

5.5.1 Angebot von bonitätsgeprüften Adressen

In meinem letzten Tätigkeitsbericht (5. TB, 6.6.1, S. 128 ff.) hatte ich ausführlich über meine datenschutzrechtlichen Bedenken gegenüber dem Vertrieb bonitätsgeprüfter Adressen durch Handels- und Wirtschaftsauskunfteien berichtet.

Eine Einigung mit der Hamburger Auskunftei, die derartige Adressen anbietet, konnte leider auch in diesem Berichtsjahr nicht erzielt werden. Diese Auskunftei setzt trotz meiner rechtlichen Bedenken den Vertrieb bonitätsgeprüfter Adressen fort. Sie ist der Auffassung, daß dies nach dem geltenden BDSG nicht verboten ist. Da mir Eingriffsmöglichkeiten nach dem Gesetz nicht zustehen, kann ich die Auskunftei nicht hindern, ihre von mir für unzulässig gehaltene Praxis fortzusetzen.

5.5.2 Automation bei Auskunfteien

Die fortschreitende Automation bei Handels- und Wirtschaftsauskunfteien führt dazu, daß auch immer mehr Kunden die Möglichkeit erhalten, mit einem Online-Anschluß direkt auf die Daten der Auskunftei zuzugreifen.

Unter den Datenschutz-Aufsichtsbehörden wird derzeit diskutiert, ob dies zur Folge hat, daß die Handels- und Wirtschaftsauskunfteien gem. § 39 Abs. 2 Nr. 8 BDSG alle Online-Nutzer zum Register bei der Aufsichtsbehörde melden müssen, da diese Kunden Empfänger regelmäßiger Übermittlungen sind. Für die Auskunfteien wäre die Meldung aller Online-Nutzer nicht unproblematisch, da sie gezwungen wären, ihre Kunden an das jedermann — also auch der Konkurrenz — zur Einsicht offenstehende Register zu melden. Die Wahrscheinlichkeit, daß die Konkurrenzunternehmen sich dann über die Online-Kunden der anderen Auskunfteien durch Einsichtnahme in das Register informieren, dürfte zwar nicht sehr groß sein. Die Aufsichtsbehörden überlegen dennoch, ob auf diese Meldungen nicht verzichtet werden kann. Dieser Meinungsbildungsprozeß ist noch nicht abgeschlossen.

5.6 Arbeitnehmer-Datenschutz

5.6.1 Frage- und Auskunftsrechte des Arbeitgebers

Das Bundesarbeitsgericht zum Fragerecht des Arbeitgebers

Zum Fragerecht des Arbeitgebers gegenüber Bewerbern habe ich zuletzt im 5. TB unter Nr. 6.7.2 ausführlich Stellung genommen. Dabei konnte die Entscheidung des Bundesarbeitsgerichts vom 22. 10. 1986 (5 AZR 660/85) noch nicht berücksichtigt werden. Sie bestätigt noch einmal die grundsätzliche Grenze des Fragerechts: „Der Schutz des Persönlichkeitsrechts des Arbeitnehmers läßt nur solche Fragen des Arbeitgebers zu, an denen der Arbeitgeber zur Beurteilung der Eignung und Befähigung des Arbeitnehmers ein objektives gerechtfertigtes Interesse hat." Das Gericht hat zugleich abgelehnt, bereits die Datenerhebung in einem Personalfragebogen — auch bei nachfolgender elektronischer Speicherung — nach dem Bundesdatenschutzgesetz zu bewerten. Erst bei der Frage, welche Daten auch noch für die Durchführung des Arbeitsverhältnisses erforderlich sind und damit gespeichert bleiben dürfen, hat das BAG § 23 BDSG herangezogen. Fazit: Die Speicherung von Geschlecht, Familienstand und Ausbildungsdaten sei bereits im Bewerbungsverfahren zulässig und liege — nach einer Einstellung — „im Rahmen der Zweckbestimmung des Arbeitsverhältnisses". Für die Frage nach Konfession und Wehrdienst hatte die Vorinstanz dies rechtskräftig verneint und den Arbeitgeber zur Löschung verurteilt.

Die Frage nach dem Familienstand eines Bewerbers rechtfertigt das BAG damit, daß hiervon die Versetzungsmöglichkeit oder die Auswahl des Beschäftigungsortes mit Folgeproblemen (Wohnraumbedarf, Schulproblem usw.) abhängen könne. Wie in meinem 5. TB festgestellt, halte ich die Frage nach dem Familienstand schon bei Bewerbern — anders ist es nach einer Einstellung — nicht für zulässig. Ob jemand geschieden oder verwitwet ist, ist für seine Arbeitsleistung unerheblich. (Kinderlos) Verheiratete können ebenso mobil und einsatzfähig sein wie (verlobte) Unverheiratete mit Kindern. Würde aus der Antwort „verheiratet" auf eine Nichteignung des Bewerbers geschlossen, verstieße das meines Erachtens gegen das Diskriminierungsverbot und den Schutz der Ehe.

Frage nach schwebenden Strafverfahren

Die Begrenzung des Arbeitgeber-Fragerechts auf die konkreten Arbeitsplatz-Anforderungen wirkt sich auch aus auf die Frage nach Strafverfahren des Bewerbers. Das Verlangen eines allgemeinen Führungszeugnisses, das keine Beschränkung auf bestimmte Deliktarten kennt, ist damit in der Regel ebenso unzulässig wie die undifferenzierte Frage nach anhängigen strafrechtlichen Ermittlungs- oder Gerichtsverfahren. Die datenschutzrechtlich beste Lösung hinsichtlich einer Frage nach schwebenden Strafverfahren wäre die ausdrückliche Freiwilligkeit der Beantwortung. Um naheliegende negative Schlüsse aus einer Nicht-Beantwortung zu vermeiden, müßte dann aber auch eine falsche Antwort akzeptiert werden. Will man diese einfachste Lösung nicht, bedarf es wegen der rechtsstaatlichen Unschuldsvermutung zumindest einer starken Einschränkung der Frage nach anhängigen Verfahren. Sie ist erst nach einer grundsätzlichen positiven Einstellungsentscheidung in einem persönlichen Gespräch zu stellen und zu begrenzen auf arbeitsplatzrelevante Straftatvorwürfe von einigem Gewicht, denn auch ein Führungszeugnis offenbart keine Bagatellstraftaten. Nur im Rahmen eines solchen Gesprächs mit einem Einzustellenden darf der Arbeitgeber auch nach einer drohenden Freiheitsstrafe fragen, die den Arbeitnehmer möglicherweise an der Erbringung der vereinbarten Arbeitsleistung hindern wird. Demgegenüber muß das allgemeine Interesse des Arbeitgebers daran, daß der Arbeitnehmer nicht wegen einer Haftstrafe ausfällt, die aufgrund einer nicht arbeitsplatzrelevanten Straftat verhängt wurde, meines Erachtens zurücktreten hinter dem Interesse des Arbeitnehmers aus der Unschuldsvermutung. Die Schwierigkeit, zuverlässig zu beurteilen, ob das Gericht eine Freiheitsstrafe verhängen wird, darf sich dabei nicht zulasten des/der Einzustellenden auswirken. Denn anders als bei krankheits- oder

schwangerschaftsbedingter Arbeitsunfähigkeit hat der Arbeitgeber bei einer Arbeitsverhinderung durch Verbüßen einer Freiheitsstrafe viel weitergehende Kündigungsmöglichkeiten und keine Lohnfortzahlungspflicht. Zumindest das materielle Risiko des Arbeitgebers ist hier gering.

Änderung eines Personalfragebogens

Das (bundesweit agierende) Unternehmen, dessen Personalfragebogen ich im letzten Tätigkeitsbericht vorgestellt und zum Teil kritisiert hatte, hat sich nun zu Änderungen bereiterklärt — nachdem ich auch den Betriebsrat im Hinblick auf sein Mitbestimmungsrecht bei Personalfragebogen auf meine Beanstandungen aufmerksam gemacht habe. Während die Frage nach dem Rentenbezug in Zukunft differenziert, die nach der Konfession und einem allgemeinen Führungszeugnis gestrichen werden soll, will das Unternehmen die Frage nach Familienstand und Kinderzahl jedoch mit der oben dargestellen Begründung des BAG beibehalten.

Auskünfte des früheren Arbeitgebers an den zukünftigen Arbeitgeber über einen Bewerber

Im Berichtszeitraum erreichten mich wieder Anfragen zum Recht des zukünftigen Arbeitgebers, beim früheren Arbeitgeber des Bewerbers Auskünfte einzuholen (vgl. ausführlich 5. TB, Nr. 6.7.7). In einem Fall lehnte ein Petent es ab, sich bei einem vom Arbeitsamt vermittelten Unternehmen zu bewerben, von dem er aus früheren geschäftlichen Kontakten wußte, daß es regelmäßig Bewerber- bzw. Personaldaten mit anderen „befreundeten" Unternehmen derselben Branche austauscht. Ich halte eine solche Praxis nicht für zulässig. Sie zeigt, daß das von der herrschenden Arbeitsrechtsliteratur und -rechtsprechung eingeräumte Auskunftsrecht des Arbeitgebers bei extremer Handhabung zu einer erheblichen Einschränkung der freien Arbeitsplatzwahl führen kann. Der tatsächliche Umfang der Auskünfte und damit die Einhaltung der von der Rechtsprechung festgelegten Grenzen ist bei den üblichen telefonischen Rückfragen weder für den Bewerber noch für die Personen zu kontrollieren, die für den Datenschutz im Betrieb verantwortlich sind. Ich habe deswegen Zweifel, ob die Rechtsprechung des Bundesarbeitsgerichts, nach der Auskünfte auch gegen den Willen des Bewerbers eingeholt werden dürfen, den heutigen Anforderungen des Datenschutzes noch gerecht wird. Die „Lagertheorie" des BAG (Arbeitgeber dürfen sich untereinander ebenso unterstützen wie Arbeitnehmer dies tun) führt in Bewerbungsverfahren, in denen der potentielle Arbeitnehmer dem Arbeitgeber weitgehend allein gegenübersteht, zu einem Ungleichgewicht und angesichts des Arbeitsplatzmangels für den Bewerber zu einer Situation des Ausgeliefertseins.

Zu begrüßen ist deswegen, daß einige Unternehmen schon heute grundsätzlich auf Anfragen bei früheren Arbeitgebern verzichten, wenn der Bewerber das nicht wünscht. Dies sollte nach dem Volkszählungsurteil des Bundesverfassungsgerichts allgemein zur arbeitsrechtlichen Praxis werden. In Bremen und Hessen ist dies im übrigen — für den Bereich des öffentlichen Dienstes — bereits Gesetz: „Die Übermittlung (der Daten von Beschäftigten) an einen künftigen Dienstherrn oder Arbeitgeber ist nur mit Einwilligung des Betroffenen zulässig" (§ 16 b Abs. 3 Satz 2 BrDSG, § 34 Abs. 2 HessDSG). Dasselbe sieht der nordrhein-westfälische Referentenentwurf zur Novellierung des Landesdatenschutzgesetzes vor. Gerade noch vertretbar wäre die Regelung, daß der spätere Arbeitgeber die telefonische Auskunft nur in Anwesenheit des Bewerbers und mit dessen Möglichkeit mitzuhören einholt oder wenn er ausschließlich schriftliche Auskünfte anfordert und diese dem Bewerber zur Kenntnis gibt. Ich meine, daß es heute an der Zeit ist, neben den in meinem 5. TB (Nr. 6.7.7) umschriebenen inhaltlichen Grenzen, das Auskunftsrecht selbst an die Zustimmung, zumindest aber an eine Beteiligung des Bewerbers zu binden.

5.6.2 Auskünfte an und durch einen Branchenauskunftsdienst

Im letzten Tätigkeitsbericht (Nr. 6.7.7) hatte ich Auskünfte eines Branchenauskunftsdienstes an zukünftige Arbeitgeber mit der Rechtsprechung des Bundesarbeitsge-

richts verglichen und Zweifel an der Zulässigkeit folgender Datenübermittlungen geäußert, da eine Einwilligung des Betroffenen fehle:

— Form der Vertragsbeendigung

— Kündigung erfolgt durch Mitarbeiter oder Unternehmen

— Grund des Ausscheidens

— Einspruch oder Klage erhoben?

— Erkenntnisse über ungünstige Einkommensverhältnisse

— Bestand beim Ausscheiden ein rückforderbarer Saldo aus nicht verdienter Provision (bei Handesvertretern)?

Nach Erklärungen des Branchenauskunftsdienstes wird heute wie folgt verfahren: Wer sich erstmals um eine Anstellung oder selbständige Mitarbeit bei einem Unternehmen der Branche bewirbt, wird in einem Merkblatt darüber aufgeklärt, daß bei seinem/ihrem Ausscheiden dem Branchenauskunftsdienst bestimmte Daten gemeldet werden, die dieser bei späteren Bewerbungen an zukünftige Arbeitgeber/Auftraggeber weitergibt. In Zukunft sollen die Betroffenen bei der Bewerbung auch ein Blanko-Formular dieser Meldung an den Branchenauskunftsdienst erhalten. Bei Beendigung des Vertragsverhältnisses wird der/dem Betroffenen mitgeteilt, welche Angaben dem Branchenauskunftsdienst konkret gemacht werden bzw. wurden. Mit diesem Verfahren erklärt sich der Bewerber einverstanden durch seine Unterschrift unter den Arbeitsvertrag bzw. den Handelsvertretervertrag, als dessen Teil das Auskunftsverfahren vereinbart wird.

Da das Einverständnis der/des Betroffenen zum Auskunftsverfahren in engem Zusammenhang mit der Vereinbarung eines Arbeits- bzw. eines Auftragsverhältnisses gegeben wird, ist sie nicht als selbständige Einwilligung im Sinne des § 3 Abs. 1 Ziff. 2 BDSG zu werten. Als Bestandteil eines umfassenden Vertrages soll sie dessen Schicksal teilen und keine eigenständige, isolierte Bedeutung erhalten. Sie kann z.B. nicht unabhängig vom Vertrag widerrufen werden. Maßstab zur Beurteilung des Verfahrens ist die Übermittlungsvorschrift des § 24 BDSG — und zwar in seiner ersten Variante: „Zweckbestimmung eines Vertragsverhältnisses". (Die im letzten Tätigkeitsbericht geäußerten Zweifel bezogen sich auf die 2. Alternative: „Wahrung berechtigter Interessen ohne Beeinträchtigung schutzwürdiger Belange des Betroffenen".) Auch als unselbständiges Einverständnis im Rahmen eines Vertragsabschlusses muß die Erklärung des/der Betroffenen allerdings den inhaltlichen Anforderungen der formellen Einwilligung des § 3 BDSG genügen. Der/die Betroffene muß die Einwilligung in Kenntnis ihrer Bedeutung und freiwillig abgegeben haben.

Das Merkblatt, für das mir der Branchenauskunftsdienst noch einzelne Modifikationen zusagte, sowie das Blanko-Formular der Meldung an den Branchenauskunftsdienst gewährleisten zusammen, daß der Bewerber tatsächlich weiß, was er mit seiner Unterschrift unter den Vertrag billigt.

Hinsichtlich der notwendigen Freiwilligkeit des Einverständnisses bestehen die allgemeinen Bedenken gegen die Annahme einer wirklichen Vertrags„freiheit" zwischen Partnern mit sehr unterschiedlicher Verhandlungsmacht. Angesichts des gegenwärtigen Arbeitsplatzmangels mag der Bewerber keine realistische Alternative zu einer Einverständniserklärung sehen. Ich meine jedoch, daß hier auch die Tragweite der Zustimmung mit in die Beurteilung der Freiwilligkeit einbezogen werden muß: In äußerst einschneidende oder etwa nicht sachbezogene Datenverarbeitung wird man nur unter Druck einwilligen. Je einleuchtender die angekündigte Datenverarbeitung aber erscheint, desto eher wird die Einwilligung auch ohne den Zwang, auf den in Aussicht stehenden Arbeitsplatz angewiesen zu sein, erteilt werden. Dabei verläuft die Grenze der Freiwilligkeit aber nicht genau dort, wo auch die Abwägung nach § 24, 2. Alt. (Wahrung berechtigter Interessen ohne Beeinträchtigung schutzwürdiger Belange des Betroffenen) Zulässigkeit und Unzulässigkeit von Datenübermittlungen voneinander scheidet. Im Rahmen eines komplexen Vertragsverhältnisses des gegenseitigen

Gebens und Nehmens wird der Beroffene zur Erlangung anderer Vorteile eher großzügig sein, als es eine abstrakte Güterabwägung ohne diese Zusammenhänge sein kann. Der Einwilligung käme sonst entgegen der gesetzlichen Differenzierung auch keine eigenständige Rechtfertigungsfunktion zu.

Die dem Branchenauskunftsdienst mitgeteilten Auskünfte sind sachbezogen — auch soweit sie über den möglichen Zeugnis-Inhalt hinausgehen und nur einen mittelbaren Bezug zu Verhalten und Leistung des Betroffenen während des Arbeitsverhältnisses aufweisen. Die Auskünfte dienen der Überprüfung der Zuverlässigkeit der Mitarbeiter, die die zuständige Fachaufsichtsbehörde von dem Unternehmen und dem Branchenauskunftsdienst ausdrücklich fordert. Sie sind aus der Sicht der Branche und der Kunden auch nachvollziehbar. Ich neige deswegen dazu, ohne Vorliegen besonderer Umstände auch die Freiwilligkeit der vertraglichen Einverständniserklärung anzunehmen.

Nach meiner Auffassung kollidiert das Auskunftsverfahren, wie es künftig praktiziert werden soll, also nicht mit der Rechtsprechung des Bundesarbeitsgerichts zum Auskunftsrecht des Arbeitgebers. Ich habe diese Meinung den Datenschutz-Aufsichtsbehörden der Länder zur Diskussion gestellt. Wenn dort eine einheitliche Auffassung erarbeitet ist, werde ich gegenüber dem Branchenauskunftsdienst abschließend Stellung nehmen.

5.6.3 Personaldatenverarbeitung und Rechte des Betriebsrates

Das Bundesarbeitsgericht zu den Informationspflichten des Arbeitgebers

In einer neueren Entscheidung vom 17. 3. 1987 macht das Bundesarbeitsgericht grundsätzliche Ausführungen zum Anspruch des Betriebsrates, vom Arbeitgeber über alle Formen der Verarbeitung personenbezogener Arbeitnehmerdaten unterrichtet zu werden (1 ABR 59/85, Der Betrieb 87, 1491). Dabei bezeichnet das Gericht das BDSG ausdrücklich als ein zugunsten der Arbeitnehmer geltendes Gesetz, dessen Überwachung dem Betriebsrat nach § 80 Abs. 1 Nr. 1 BetrVG obliegt. Der hieraus abzuleitende Auskunfts- und Unterrichtungsanspruch über die Personaldaten-Verarbeitung im Betrieb setze auch nicht voraus, daß bereits ein Verstoß gegen das Datenschutzgesetz behauptet wird. Der Betriebsrat benötige vielmehr „Kenntnisse darüber, welche personenbezogenen Daten der Arbeitnehmer gespeichert und zu welchen Zwecken sie verarbeitet werden"; er sei „zu unterrichten über die zum Schutz dieser Datenverarbeitung getroffenen Maßnahmen"; weiter sei es „erforderlich, daß der Betriebsrat hinsichtlich aller Programme, mit denen personenbezogene Daten verarbeitet werden, unterrichtet wird". Mit diesen Leitsätzen hat das Bundesarbeitsgericht einen wertvollen Beitrag geleistet zur Befähigung der Betriebsräte, ihre Aufgabe, den Datenschutz der Arbeitnehmer zu überwachen, auch tatsächlich zu erfüllen.

Eine mögliche Form der Kontrolle von Computerprogrammen ist die Einsichtnahme in Rechner-Protokolle. Hierzu erreichte mich eine Eingabe mit der Frage, ob der Arbeitgeber den Betriebsrat auch dann entsprechend einer Betriebsvereinbarung Protokolle aus einer Personaldatenbank zugänglich machen muß, wenn diese sowohl als Log-Protokoll (wer benutzte wann und wie das System) als auch als Recovery-Protokoll mit Angabe der geänderten personenbezogenen Daten selbst ausgestaltet sind. Ich habe dies verneint und eine technisch mögliche Trennung beider Funktionen empfohlen. Ein Betriebsrat darf auch bei einer weitergefaßten Betriebsvereinbarung Datenbankprotokolle nur im Rahmen seiner betriebsverfassungsrechtlichen Kontrollbefugnis einsehen und ist jederzeit an die Einhaltung der Datenschutzrechte der Arbeitnehmer gebunden.

Pflicht zur rechtzeitigen und verständlichen Information

In dem genannten Urteil vom 17. 3. 1987 führt das BAG weiter aus, daß der Unterrichtungsanspruch des Betriebsrates rechtzeitig, d.h. in einem Zeitpunkt erfüllt werden müsse, in dem der Betriebsrat „seine Aufgaben am sinnvollsten noch wahrnehmen

kann und daran nicht faktisch dadurch gehindert wird, daß eine Änderung bestehender und als endgültig betrachteter Zustände regelmäßig nur schwer und unter zusätzlichen Kosten möglich ist". Die Hinzuziehung eines Sachverständigen durch den Betriebsrat nach § 80 Abs. 3 BetrVG komme erst nach einer Unterrichtung durch den Arbeitgeber in Betracht. Die Unterrichtung habe nämlich — schon wegen des Prinzips der vertrauensvollen Zusammenarbeit — in einer Form zu erfolgen, daß der Betriebsrat „die erhaltene Information auch verstehen kann. Das mag angesichts der Schwierigkeit und Komplexität der Materie einen größeren Zeitaufwand, Wiederholungen und Einzelerklärungen erforderlich machen".

In meiner Beratungspraxis für Betriebsräte hat sich die Form der Auskunftserteilung über Personaldaten durch den Arbeitgeber noch in anderer Weise als problematisch erwiesen: So scheute sich ein Betriebsrat, den Kolleginnen und Kollegen einen seitenlangen Computer-Ausdruck zuzumuten, den der Arbeitgeber den Arbeitnehmern zur Erfüllung eines Auskunftsanspruches anbot, der in einer Betriebsvereinbarung festgelegt war. Auch wenn hier nicht das betriebsverfassungsrechtliche Gebot der vertrauensvollen Zusammenarbeit eine „lesbare" Auskunft fordert, so macht der vereinbarte Auskunftsanspruch auch im Verhältnis Arbeitgeber/Arbeitnehmer nur dann Sinn, wenn die gespeicherten Personaldaten unverschlüsselt und allgemein verständlich dem Betroffenen mitgeteilt werden. Ich habe dem Betriebsrat aber davon abgeraten, darüber hinaus mit dem Arbeitgeber eine übersichtliche Kurzfassung der Datenausdrucke zu vereinbaren (ohne die Betriebsvereinbarung entsprechend zu modifizieren). Vorzuziehen ist vielmehr ein Angebot des Betriebsrates, den Kolleginnen und Kollegen bei Bedarf die Bedeutung der einzelnen Datenarten allgemein oder jeweils personenbezogen zu erläutern.

Weitergabe von Arbeitnehmerdaten durch Betriebsratsmitglied an die Gewerkschaft

Ebenfalls in den Bereich „Personaldatenverarbeitung und Betriebsratsrechte" fällt die Beschwerde eines Arbeitnehmers darüber, daß ein Mitglied „seines" Betriebsrates eine Liste von Arbeitnehmer-Adressen an die eigene Gewerkschaft weitergab. In persönlichen Schreiben an die Privatadressen warb die Gewerkschaft dann für ihre Kandidaten zur bevorstehenden Betriebsratswahl. Das Betriebsratsmitglied hatte die Listen vom Arbeitgeber für die Betriebsratsarbeit erhalten. Die Datenübermittlung erfolgte hier nicht im Rahmen der Zweckbestimmung des Arbeitsverhältnisses und war zur Wahrung berechtigter Interessen weder für das einzelne Betriebsratsmitglied, den Betriebsrat insgesamt noch für die Gewerkschaft erforderlich (§ 24 BDSG). Das Recht der Gewerkschaft auf Werbung (Art. 9 GG) fordert ebenfalls keine solche Datenübermittlung, da die Arbeitnehmer auch innerhalb oder vor dem Betrieb hätten angesprochen oder durch Flugblätter informiert werden können. Vielmehr hat hier ein Betriebsratsmitglied seine betriebliche Stellung für gewerkschaftliche Zwecke ausgenutzt. Im konkreten Fall teilen inzwischen alle Beteiligten diese Rechtsauffassung.

5.7 Sonstige Probleme

5.7.1 Überwachungstätigkeit — Registermeldungen

Im März 1987 habe ich alle 226 Unternehmen angeschrieben, die nach § 39 BDSG zum Register der Aufsichtsbehörde gemeldet waren. Ich habe sie darauf hingewiesen, daß der Aufsichtsbehörde alle Veränderungen der ursprünglich gemeldeten Angaben innerhalb einer Frist von einem Monat anzuzeigen sind. Ich hatte in der Vergangenheit den Eindruck, daß viele Firmen ihre Änderungen nicht meldeten und deshalb die Angaben in dem öffentlichen Register zum Teil unrichtig geworden waren.

Diese Vermutung bestätigte sich allein schon dadurch, daß mein Schreiben in 37 Fällen (16 %!) von der Post nicht einmal zugestellt werden konnte. Daraufhin mußte erst einmal ermittelt werden, ob das angeschriebene Unternehmen nicht mehr existierte oder nur seinen Sitz verlegt hatte. Als weitere Reaktion auf mein Schreiben erhielt ich eine Fülle von Änderungsmeldungen. Im Ergebnis waren bei 91 Firmen (36 %) Än-

derungen nötig und 37 Firmen wurden ganz aus dem Register gelöscht. Das bedeutet, daß nicht einmal die Hälfte der Registerkarten richtig war und jedes zweite Unternehmen seine Meldepflicht nicht ernstgenommen hatte.

Ich habe nach dieser Registerbereinigung nicht im Einzelfall nachgeforscht, wann die Veränderung eingetreten war. An dieser Stelle muß ich jedoch deutlich darauf hinweisen, daß eine Fristüberschreitung auch bei Änderungsmeldungen eine Ordnungswidrigkeit ist und mit einem Bußgeld geahndet werden kann.

5.7.2 Auskünfte von Fluggesellschaften an Dritte

In meinem letzten Tätigkeitsbericht hatte ich berichtet, daß die von einer Fluggesellschaft geübte Praxis der Auskunftserteilung an Dritte datenschutzrechtliche Probleme aufwarf (5. TB, 6.8.1, S. 142 f.). Ich hatte auch dargestellt, daß ich zusammen mit der Fluggesellschaft die Lösung dieser Problematik darin gefunden habe, daß den Fluggästen die Möglichkeit eingeräumt wird, Auskünfte an Dritte generell zu untersagen.

Die Fluggesellschaft hat ihre interne Dienstanweisung jetzt unter meiner Mitwirkung geändert. Ihr können die Mitarbeiter des Unternehmens jetzt entnehmen, daß jeder Fluggast die Möglichkeit hat, bei seiner Buchung einen Sperrvermerk in das EDV-System der Fluggesellschaft aufnehmen zu lassen, wonach seine Reservierungsdaten nicht an Dritte zu Auskunftszwecken weitergegeben werden dürfen. Den Mitarbeitern wird in der Dienstanweisung aufgegeben, vor Erteilung einer Auskunft zu überprüfen, ob ein Sperrvermerk vorliegt oder nicht.

Die Fluggäste werden auch durch einen Hinweis im Taschenflugplan dieses Unternehmens darauf aufmerksam gemacht, daß sie einen Sperrvermerk anbringen lassen können. Dieser Hinweis war zunächst so ungünstig plaziert worden, daß er mit Sicherheit von keinem Passagier gelesen worden wäre. Auf meine Anregung hat die Fluggesellschaft den Hinweis nunmehr vorne im Taschenflugplan angeordnet. Dadurch und durch den Fettdruck wird die Chance, daß er von den Flugpassagieren zur Kenntnis genommen wird, zumindest vergrößert.