BÜRGERSCHAFT
DER FREIEN UND HANSESTADT HAMBURG

Drucksache 11/1864

11. Wahlperiode

12.01.84

Der Hamburgische Datenschutzbeauftragte

An den
Herrn Präsidenten der Bürgerschaft

Betr.: Zweiter Tätigkeitsbericht
des Hamburgischen Datenschutzbeauftragten zum 1. Januar 1984

Gemäß § 20 Absatz 2 Satz 2 des Hamburgischen Datenschutzgesetzes übersende ich der Bürgerschaft meinen Zweiten Tätigkeitsbericht, den ich zum 1. Januar 1984 erstellt habe.*

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 46

Zweiter Tätigkeitsbericht
des
Hamburgischen Datenschutzbeauftragten

vorgelegt zum 1. Januar 1984
gemäß § 20 Absatz 2 Satz 2 des Hamburgischen Datenschutzgesetzes

Inhaltsverzeichnis / Abkürzungsverzeichnis

1.	**Zur Lage des Datenschutzes**	1
1.1	Folgerungen aus der Auseinandersetzung um die Volkszählung	1
1.2	Verhältnis zur Verwaltung	3
1.3	Information über Datenschutz	4
2.	**Überblick über die Tätigkeit der Dienststelle**	5
2.1	Neue Aufgabe Bildschirmtext	5
2.1.1	Beschreibung der Aufgabe	5
2.1.2	Stand in Hamburg	5
2.2	Entwicklung der Dienststelle	6
2.3	Eingaben	6
2.3.1	Allgemeines	6
2.3.2	Statistik	8
2.4	Beratungen und Prüfungen	8
2.4.1	Öffentlicher Bereich	8
2.4.1.1	Beratungen	8
2.4.1.2	Prüfungen	9
2.4.2	Beratungen und Prüfungen im nicht-öffentlichen Bereich	10
2.5	Datenschutzregister	10
2.5.1	Aufgaben, Aufbau und Inhalt	10
2.5.1.1	Aufgaben	10
2.5.1.2	Aufbau und Inhalt	11
2.5.2	Stand, Qualität, Fortschreibung	12
2.5.3	Dateienübersicht	13
2.5.4	Registerverordnung	13
2.6	Beobachtung der automatisierten Datenverarbeitung (ADV)	13
2.6.1	Allgemeine Vorbemerkung	13
2.6.2	Zentralisierung der ADV	15
2.6.2.1	Situation in Hamburg	15
2.6.2.2	Zentrale und dezentrale ADV aus der Sicht des Datenschutzes	16
2.6.2.3	Konzentration von Daten	17
2.6.2.4	Vormarsch der Dialogverarbeitung	17
2.6.2.5	Stand der Datensicherung	18
2.6.3	Entwicklung der Datenverarbeitungstechnik	19

2.6.3.1 Gefährdungspotential der gegenwärtigen Datenverarbeitungstechnik ... 19

2.6.3.2 Gefährdungen durch die neue Entwicklung ... 20

2.6.4 Neue Medien ... 22

2.6.4.1 Übersicht über die neuen Medien ... 22

2.6.4.2 Datenschutzspezifische Gefährdungen ... 22

2.6.5 Mitwirkung an Automationsvorhaben ... 25

2.6.5.1 Einzelne Verfahren ... 25

2.6.5.2 Landeseigene Sozialhilfestatistik ... 26

3. Einzelprobleme im öffentlichen Bereich ... 29

3.1 Neue Medien ... 29

3.1.1 Bildschirmtext ... 29

3.1.1.1 Darstellung des Systems ... 29

3.1.1.2 Situation in Hamburg ... 30

3.1.1.3 Gefahren für den Datenschutz ... 30

3.1.1.4 Regelungsdefizite des Bundesdatenschutzgesetzes und Notwendigkeit bereichsspezifischer Regelungen ... 33

3.1.1.5 Datenschutzregelungen im Staatsvertrag über Bildschirmtext ... 36

3.1.1.6 Überwachung durch den Datenschutzbeauftragten ... 39

3.1.2 Andere Medien ... 40

3.1.2.1 Kabelkommunikation ... 40

3.1.2.2 Fernwirkdienste ... 41

3.1.2.3 Der Staatsvertrag über Bildschirmtext als Vorbild ... 41

3.2 Archivwesen ... 41

3.2.1 Archivgesetz ... 42

3.2.1.1 Notwendigkeit eines Archivgesetzes ... 42

3.2.1.2 Stand der Überlegungen bei den Datenschutzbeauftragten ... 42

3.2.2 Einsicht in Archivgut durch die ROM und CINTI Union e. V. ... 43

3.2.2.1 Darstellung des Sachverhalts ... 43

3.2.2.2 Bewertung aus Datenschutzsicht ... 44

3.3 Personalwesen ... 47

3.1.1 Prüfungsamt für den öffentlichen Dienst ... 47

3.3.1.1 Aufgaben und Arbeitsabläufe ... 47

3.3.1.2 Datenschutzrechtliche Bewertung ... 49

3.4 Steuerwesen ... 51

3.4.1 Novellierung der Abgabenordnung (AO) ... 51

3.4.1.1 Regelung des Kontrollrechts im Bereich der Steuerverwaltung in der AO? ... 51

3.4.1.2 Datenschutzrelevante Regelungen im Entwurf ... 52

3.4.2 Probleme in Hamburg ... 53

3.5 Schulwesen ... 53

3.5.1 Probleme im Schulbereich ... 53

3.5.1.1 Bergriff der meldepflichtigen Datei in Abhängigkeit vom Stellen- und Übermittlungsbegriff ... 53

3.5.1.2 Bedeutung des Stellenbegriffs im Schulbereich im Hinblick auf § 6 Abs. 1 Nr. 4 ... 54

3.5.2 Umsetzung der Datenschutzbestimmungen im Schulbereich ... 55

3.5.3 Schülerbogen für Berufsschüler ... 55

3.6 Bauwesen ... 56

3.7 Statistik ... 57

3.7.1 Volkszählung 1983 ... 57

3.7.1.1 Beteiligung an der Auseinandersetzung ... 57

3.7.1.2 Stellungnahme zu Problemen der Volkszählung 1983 ... 57

3.7.2 Mikrozensus, EG-Stichprobenerhebung über Arbeitskräfte ... 59

3.7.2.1 Mikrozensus ... 59

3.7.2.2 EG-Stichprobenerhebung über Arbeitskräfte ... 60

3.8 Einwohnerwesen ... 60

3.8.1 Meldewesen ... 61

3.8.1.1 Regelmäßige Datenübermittlungen aus dem Melderegister ... 61

3.8.1.1.1 Vorgesehene Übermittlungsempfänger ... 61

3.8.1.1.2 Regelung des automatisierten Datenabgleichs ... 62

3.8.1.1.3 Übermittlungen zwischen den hamburgischen Meldebehörden ... 62

3.8.1.1.4 Übermittlungen an die Kirchen ... 63

3.8.1.1.5 Übermittlung durch Übersendung von Meldescheinen ... 63

3.8.1.1.6 Datenübermittlungsverordnungen des Bundes ... 63

3.8.1.2 Probleme bei der Umsetzung des Meldegesetzes in die Praxis ... 63

3.8.1.2.1 Löschung von Haftmitteilungen ... 63

3.8.1.2.2 Auskunft an den Betroffenen ... 65

3.8.1.2.3 Melderegisterauskunft an Dritte ... 65

3.8.1.3 Automation im Meldewesen ... 65

3.8.2 Personalausweis-/Paßwesen ... 66

3.8.2.1 Gefahren des neuen Ausweises ... 67

3.8.2.2 Unklarheiten und Defizite im Bundespersonal-ausweis-Gesetz ... 68

3.8.2.2.1 Protokollierung von Anfragen in polizeilichen Informationssystemen ... 68

3.8.2.2.2 Verwendung der Serien-Nr. durch die Polizei ... 68

3.8.2.2.3 Nutzung des Personalausweises im nicht-öffentlichen Bereich ... 69

3.8.2.2.4 Internationale Lesbarkeit ... 69

3.8.2.3 Anforderungen an ein Landespersonalausweis-Gesetz ... 69

3.8.2.4 Entwurf eines neuen Paßgesetzes ... 70

3.8.3 Ausländerwesen ... 70

3.8.4 Personenstandswesen ... 71

3.8.4.1 Neufassung der Dienstanweisung für die Standesbeamten ... 71

3.8.4.2 Durchführung des Transsexuellengesetzes ... 71

3.9 Allgemeine Bemerkungen zum Sicherheitsbereich ... 72

3.9.1 Zur Prüfkompetenz des Datenschutzbeauftragten ... 72

3.9.1.1 Der Umfang der Kontrollaufgabe ... 72

3.9.1.2 Allgemeine Befugnisse des HmbDSG ... 72

3.9.1.3 Zum Umfang des Akteneinsichtsrechts ... 73

3.9.1.4 Die Bedeutung des Sicherheitsvorbehalts ... 73

3.9.1.5 Keine Einschränkung der Prüfkompetenz durch Berufs- oder Amtsgeheimnisse ... 74

3.9.1.6 Resümee ... 74

3.9.2 Zum Auskunftsverhalten der Sicherheitsbehörden gegenüber dem Bürger ... 74

3.9.2.1 Auskünfte der Polizei ... 75

3.9.2.2 Auskünfte des Verfassungschutzes ... 75

3.9.2.3 Auskünfte der Staatsanwaltschaft ... 76

3.9.2.4 Resümee ... 76

3.10 Polizei ... 77

3.10.1 Überblick ... 77

3.10.2 Informationsverarbeitung außerhalb von Dateien ... 77

3.10.2.1 Akten zur Bearbeitung von Kriminalfällen ... 77

3.10.2.2 Anhaltemeldungen ... 78

3.10.2.3 Sonstige Kurzberichte ... 78

3.10.3 Entwicklung der automatisierten Datenverarbeitung bei der Polizei ... 79

3.10.3.1 Quantitative Ausweitung automatisierter Dateien ... 79

3.10.3.2 Bundesweite Zentralisierung der ADV ... 79
3.10.3.3 Ausweitung des Anwendungsbereiches ... 79
3.10.3.3.1 Fahndungs- und Aktennachweissysteme ... 79
3.10.3.3.2 PIOS-Dateien ... 79
3.10.3.3.3 Spurendokumentationssysteme ... 80
3.10.3.3.4 Falldateien ... 80
3.10.3.4 Ausblick ... 81
3.10.4 Stand des Datenschutzes bei der Polizei ... 81
3.10.4.1 KpS-Richtlinien ... 81
3.10.4.2 Dateien-Richtlinien ... 81
3.10.4.3 Zugriffsregelungen ... 82
3.10.4.4 Rückmeldungen von der Staatsanwaltschaft an die Polizei ... 82
3.10.5 Problemfälle bei Speicherungen ... 83
3.10.5.1 Speicherung „anderer Personen" ... 83
3.10.5.2 Suizidversuche ... 84
3.10.5.3 Hinweise auf Sinti und Roma ... 85
3.10.5.4 Straftaten von überregionaler Bedeutung im bundesweiten Kriminalaktennachweis (KAN) ... 86
3.10.6 Problemfälle bei Übermittlungen an die Polizei ... 87
3.10.6.1 Sozialdaten ... 87
3.10.6.2 Feuerwehr-Einsatz-Daten ... 87
3.10.6.3 Kraftfahrzeug-Register-Daten ... 89
3.10.6.4 Sonstige Problemfälle ... 90
3.11 Landesamt für Verfassungsschutz ... 90
3.12 Staatsanwaltschaft ... 91
3.12.1 Zentralkartei ... 91
3.12.2 Persönlichkeitsschutz bei der Datenverarbeitung in Akten ... 92
3.13 Justizverwaltung und Strafvollzug ... 93
3.13.1 Überarbeitung von Justizverwaltungsvorschriften ... 94
3.13.1.1 Anordnungen über Mitteilungen in Strafsachen (MiStra) ... 94
3.13.1.2 Anordnung über Mitteilungen in Zivilsachen (MiZi) ... 94
3.13.1.3 Schuldnerverzeichnis ... 94
3.13.2 Strafvollzug ... 95
3.14 Gesundheitswesen ... 95
3.14.1 Prüfung von Kliniken des Universitäts-Krankenhauses Eppendorf (UKE) ... 95
3.14.2 Beratungen zum „Datenschutz in Krankenhäusern" ... 96
3.14.3 Zum Verhältnis zwischen dem Schutz des Patientengeheimnisses nach § 203 StGB und den

	Datenschutzgesetzen	96
3.14.4	Übermittlungen von Patientendaten an die Kirchen	98
3.15	Sozialwesen	98
3.15.1	Problemfälle bei der Anwendung der Übermittlungsvorschriften des SGB X	99
3.15.1.1	§ 69 Abs. 1 Nr. 1 SGB X	99
3.15.1.2	§ 76 SGB X	99
3.15.2	Bestellung von betrieblichen Datenschutzbeauftragten gem. § 79 SGB X	100
3.15.2.1	Sachstand	100
3.15.2.2	Vorschläge zur Organisation des betrieblichen Datenschutzbeauftragten	100
3.15.2.3	Betriebliche DSB auch bei den Personalverwaltungen?	101
3.15.3	Ausführung des Bundeskindergeldgesetzes	102
3.16	Wissenschaft und Forschung	103
3.16.1	Modelle zur Lösung des Konflikts zwischen Forschung und Datenschutz	103
3.16.2	Forschung im Gesundheitswesen	104
3.16.2.1	Allgemeine Probleme bei der Forschung mit Patientendaten	104
3.16.2.2	Hamburgisches Krebsregister	105
3.16.2.3	Basisdokumentation Psychiatrie	106
3.16.3	Forschung und Sozialdaten	107
3.16.4	Forschung im Justizwesen	107
4.	**Einzelne Probleme des Datenschutzes im nicht-öffentlichen Bereich**	109
4.1	Handel	109
4.1.1	Umtauschzettel bei Kaufhäusern	109
4.1.2	Versandhandel	109
4.1.3	Direktwerbung	110
4.1.3.1	„Robinsonliste"	110
4.1.3.2	Übermittlung listenmäßiger oder sonst zusammengefaßter Daten	110
4.2	Kreditwirtschaft	111
4.2.1	Erteilung von Bankauskünften	111
4.2.2	Girokontenführung auf Guthabenbasis	112
4.2.3	Ermittlung der Anschriften von Kindergeldempfängern für Werbezwecke	113
4.3	Versicherungswirtschaft	113
4.3.1	Zentrale Dateien der Versicherungsverbände	113
4.3.1.1	Zentrale Registrierstelle Rechtsschutz	114

4.3.1.2 Sonderwagnisdatei der Lebensversicherer ... 115

4.3.1.3 Meldeverfahren des Deutschen Transport-versicherungsverbandes (DTV) ... 116

4.3.1.4 Malus-Datei des HUK-Verbandes für die Kfz-Haftpflicht-Versicherer ... 116

4.3.2 Herkunft von Werbeadressen ... 118

4.3.3 Datenübermittlungen im Rahmen von fakultativen Gruppenversicherungsverträgen ... 119

4.4 Auskunfteien ... 120

4.4.1 Handels- und Wirtschaftsauskunfteien ... 120

4.4.1.1 Regeln zur Umsetzung des Datenschutzes ... 120

4.4.1.2 Eingaben ... 121

4.4.1.3 Prüfungen ... 121

4.4.2 Auskunftsstelle über den Versicherungsaußendienst e. V. Hamburg (AVAD) ... 123

4.4.3 Schufa ... 124

4.4.3.1 Interner Datenverkehr zwischen den Schufagesellschaften ... 124

4.4.3.2 Identitätsprüfung bei fehlendem Geburtsdatum ... 125

4.4.3.3 Aussagekraft von Negativdaten ... 126

4.5 Datenschutz auf dem Wohnungsmarkt ... 127

4.5.1 Fragebögen zur Wohnungsbewerbung ... 127

4.5.2 Zusammenarbeit von Vermietern mit Auskunfteien ... 128

4.5.2.1 Zusammenarbeit mit der Schufa ... 128

4.5.2.2 Zusammenarbeit mit Handels- und Wirtschaftsauskunfteien ... 129

4.6 Datenschutz bei Verkehrsbetrieben ... 129

4.6.1 Sogenannte „Schwarzfahrerdatei" der HHA ... 129

4.6.2 Speicherung personenbezogener Daten im Rahmen von Fahrgeldbeanstandungen ... 130

4.7 Öffentliche Bekanntgabe von Lotteriegewinnern ... 131

4.8 Arbeitnehmer-Datenschutz ... 131

4.8.1 Zum Verhältnis von BDSG und BetrVG ... 131

4.8.2 Die Position des betrieblichen Datenschutzbeauftragten ... 131

4.8.2.1 Kann der bDSB zugleich Mitglied der Geschäftsleitung oder Leiter der EDV-Abteilung sein? ... 132

4.8.2.2 Zur Kompetenzüberlagerung zwischen betrieblichem Datenschutzbeauftragten und Betriebsrat ... 132

4.8.2.3 Mitwirkung des Betriebsrats bei der Bestellung des betrieblichen Datenschutzbeauftragten ... 132

4.8.3 Personalfragebögen ... 133

4.8.4 Personalinformationssysteme ... 134

4.8.4.1 Das Mitbestimmungsrecht des Betriebsrates nach § 87 Abs. 1 Nr. 6 BetrVG ... 134
4.8.4.2 Dem Mitbestimmungsrecht vorgelagerte Informationsrechte des Betriebsrates ... 136
4.8.4.3 Elemente einer Betriebsvereinbarung ... 136
4.8.4.4 Systembenutzungskontrolle ... 137
4.8.5 Probleme der Konzerndatenverarbeitung ... 137
4.9 Datenübermittlungen zwischen nicht-öffentlichem und öffentlichem Bereich ... 138
4.9.1 Erteilung von Auskünften durch die Schufa an Strafverfolgungsbehörden ... 139
4.9.2 Datenübermittlung Hamburger Wasserwerke (HWW) - Polizei ... 139
4.9.3 Errichtung von Fahrraddateien ... 139
4.9.4 Datenübermittlung des Amtes für Arbeitsschutz an Betriebsräte ... 141

5. Ausblick ... 143
5.1 Rechtsentwicklung in Hamburg ... 143
5.1.1 Hamburgisches Datenschutzgesetz (HmbDSG) ... 143
5.1.2 Krebsregistergesetz und Archivgesetz ... 143
5.1.3 Novellierung des HmbSOG ... 143
5.2 Rechtsentwicklung im Bund ... 146
5.2.1 Spezifische Regelungen für den Sicherheitsbereich ... 146
5.2.2 Arbeitnehmerdatenschutz ... 146
5.2.3 Novellierung des BDSG ... 147

Anlage 1

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum Datenschutz im Personenstandswesen 151

Anlage 2

Abgestimmte Stellungnahmen der Landesbeauftragten für den Datenschutz zur „Anordnung über Mitteilung in Strafsachen (MiStra)"
- Auszug - 153

Übersicht über die Organisation der Dienststelle des Hamburgischen Datenschutzbeauftragten
- Nachtrag - 159

Abkürzungsverzeichnis

ADV	=	Automatisierte Datenverarbeitung
AGBB	=	Allgemeine Geschäftsbedingungen der Banken
AGBG	=	Gesetz zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen
AGBSp	=	Allgemeine Geschäftsbedingungen der Sparkassen
AO	=	Abgabenordnung
ARB	=	Allgemeine Bedingungen über die Rechtsschutzversicherungen
ArbGG	=	Arbeitsgerichtsgesetz
AVAD	=	Auskunftsstelle über den Versicherungsaußendienst e.V., Hamburg
AZO	=	Arbeitszeitordnung
BAG	=	Bundesarbeitsgericht
BAV	=	Bundesaufsichtsamt für das Versicherungswesen
BDSG	=	Bundesdatenschutzgesetz
bDSB	=	betrieblicher Datenschutzbeauftragter
BetrVG	=	Betriebsverfassungsgesetz
BfD	=	Bundesbeauftragter für den Datenschutz
BGB	=	Bürgerliches Gesetzbuch
BGBl.	=	Bundesgesetzblatt
BGH	=	Bundesgerichtshof
BKA	=	Bundeskriminalamt
BKGG	=	Bundeskindergeldgesetz
BMeldDÜV	=	Bundesmeldedatenübermittlungsverordnung
BMJFG	=	Bundesministerium für Jugend, Familie, Gesundheit
BPAG	=	Bundespersonalausweisgesetz
BR	=	Betriebsrat
BremPolG	=	Bremisches Polizeigesetz
BGS-G	=	Bundesgrenzschutz-Gesetz
BT-Drs.	=	Bundestags-Drucksache
Btx	=	Bildschirmtext
BVerfG	=	Bundesverfassungsgericht
DA	=	Dienstanweisung für die Standesbeamten und ihre Aufsichtsbehörden
dpa	=	Deutsche Presseagentur
DS	=	Datenschutz
DSB	=	Datenschutzbeauftragter
DTV	=	Deutscher Transportversichererverband
DV	=	Datenverarbeitung
DVZ	=	Datenverarbeitungszentrale

ed	=	erkennungsdienstlich
EPaßG	=	Entwurf eines Paßgesetzes
FHH	=	Freie und Hansestadt Hamburg
GG	=	Grundgesetz
HmbSOG	=	Hamburgisches Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung
HHA	=	Hamburger Hochbahn Aktiengesellschaft
HmbBG	=	Hamburgisches Beamtengesetz
HmbDSB	=	Hamburgischer Datenschutzbeauftragter
HmbDSG	=	Hamburgisches Datenschutzgesetz
HmbKrebsRG-E	=	Entwurf des Hamburgischen Krebsregistergesetzes
HmbLVO	=	Hamburgische Laufbahnverordnung
HmbMeldDÜV	=	Hamburgische Meldedatenübermittlungsverordnung
HmbMG	=	Hamburgisches Meldegesetz
HUK-Verband	=	Verband der Haftpflicht-, Unfall-, Auto- und Rechtsschutzversicherer e.V.
HVV	=	Hamburger Verkehrsverbund
HWW	=	Hamburger Wasserwerke GmbH
IMK	=	Innenminister-Konferenz
INPOL	=	Informationssystem der Polizei
JGG	=	Jugendgerichtsgesetz
JVA	=	Justizvollzugsanstalt
KAN	=	Kriminalaktennachweis
KBA	=	Kraftfahrtbundesamt
Kps-Richtlinien	=	Richtlinien über kriminalpolizeiliche personenbezogene Sammlungen
LPAG	=	Landespersonalausweisgesetz
MiStra	=	Anordnung über Mitteilungen in Strafsachen
MiZi	=	Anordnung über Mitteilungen in Zivilsachen
MRRG	=	Melderechtsrahmengesetz
NADIS	=	Nachrichtendienstliches Informations- und Verbundsystem
NJW	=	Neue Juristische Wochenschrift
NS	=	Nationalsozialismus
NVwZ	=	Neue Zeitung für Verwaltungsrecht
OLG	=	Oberlandesgericht
OVG	=	Oberverwaltungsgericht
PIOS	=	Inpol-Anwendung Personen, Institutionen, Objekte, Sachen
POLAS	=	Polizeiliches Auskunftssystem
RCU	=	ROM und CINTI Union e. V.
RiStBV	=	Richtlinien für das Straf- und Bußgeldverfahren

SGB	=	Sozialgesetzbuch
Schufa	=	Schutzgemeinschaft für allgemeine Kreditsicherung
SchulG	=	Schulgesetz der Freien und Hansestadt Hamburg
SchVG	=	Schulverfassungsgesetz
SOG		s. HmbSOG
SPUDOK	=	Spurendokumentationssystem
StA	=	Staatsanwaltschaft
StGB	=	Strafgesetzbuch
StPO	=	Strafprozeßordnung
StaLa	=	Statistisches Landesamt
TB	=	Tätigkeitsbericht
TSG	=	Transsexuellengesetz
TV	=	Fernsehen
Tz	=	Teilziffer
UKE	=	Universitäts-Krankenhaus Eppendorf
VG	=	Verwaltungsgericht
VO	=	Verordnung
VVAV	=	Verwaltungsvorschriften für das automatisierte Verfahren im Anordnungs-, Kassen- und Rechnungswesen
VVG	=	Versicherungsvertragsgesetz
VZ	=	Volkszählung
VZG	=	Volkszählungsgesetz
ZEVIS	=	Zentrales Verkehrsinformationssystem
ZPO	=	Zivilprozeßordnung

1. Zur Lage des Datenschutzes

1.1 Folgerungen aus der Auseinandersetzung um die Volkszählung

Ende 1982 werden nur wenige vorausgesehen haben, daß 12 Monate später Veranlassung bestehen werde, 1983 im Rückblick zum Jahr des Datenschutzes zu erklären. Ganz im Gegenteil, viele – auch ich gehörte dazu – hatten befürchtet, im nunmehr abgelaufenen Jahr werde sich die Wende im Datenschutz vollziehen, würden Positionen, die der Datenschutz in den 70-er Jahren erobert hatte, wieder zurückgenommen werden. Statt dessen setzte gleich zu Beginn des Jahres eine leidenschaftliche Diskussion ein über Grundfragen des Daten- und Grundrechtsschutzes unter den gewandelten technischen Bedingungen des Computer-Zeitalters, die alle Schichten der Bevölkerung erfaßte und die mit großer Heftigkeit ausgetragen wurde.

Die Beantwortung dieser Fragen, die in der Auseinandersetzung um die Volkszählung 1983 aufgeworfen wurden, oblag dem Bundesverfassungsgericht; seine Entscheidung lag bei Redaktionsschluß für diesen Tätigkeitsbericht noch nicht vor. Ich gehe davon aus, daß das Gericht die Maßstäbe für die Datenerhebung und Datenverarbeitung mit Eingriffs-und Gefährdungscharakter, die es selbst Ende der 60-er/Anfang der 70-er Jahre in mehreren Entscheidungen aufgestellt hat, in einer Weise fortschreiben wird, die die zwischenzeitlichen Entwicklungen berücksichtigt und auch dem Phänomen des Widerstandes gegen die Volkszählung Rechnung trägt, wie wir es heute zu übersehen vermögen.

In der mündlichen Verhandlung des Bundesverfassungsgerichts hatte es den Anschein, als ob einzelne Verfahrensbeteiligte dieses Phänomen noch immer nicht verstanden haben. Sie sehen politische Systemgegner am Werk, die in Wahrheit ganz andere Ziele verfolgen. Sie weisen auf das groteske Mißverhältnis hin zwischen dem konkreten Anlaß und der Erbitterung, mit der die Volkszählung bekämpft wurde. Die Erkenntnis bleibt ihnen verschlossen, daß die Furcht des Menschen vor der undurchschaubaren und unkontrollierbaren Elektronik selbst dann ernst genommen werden müßte, wenn sie ganz unbegründet wäre. Diese Furcht beruht auf dem Gefühl, zunehmend von anonymen staatlichen und gesellschaftlichen Apparaturen abhängig und immer stärker elektronisch erfaßt zu werden und damit der Möglichkeit eigenverantwortlicher Lebensgestaltung beraubt zu sein. Skepsis gegenüber der eingeschlagenen Richtung des Fortschritts macht sich breit. Widerstand gegen die Technik, gegen staatliche und gesellschaftliche Planungen ist die Folge.

Ganz unabhängig von den Grundsätzen, die das Bundesverfassungsgericht für den Grundrechtsschutz bei statistischen Erhebungen und Verarbeitungen aufstellen wird, hat der Streit über die Volkszählung gezeigt, daß nie wieder eine Großzählung, vielleicht nicht einmal eine kleinere Repräsentativerhebung routinemäßig vorbereitet und abgewickelt werden kann unter Berufung darauf, daß sich das Verfahren seit Jahrzehnten bewährt habe, weniger Fragen gestellt würden als beim letztenmal, die Geheimhaltungsvorschriften verbessert worden seien und im übrigen die Datenschutzbeauftragten alle Vorgänge kontrollieren könnten. Zu einzelnen Anforderungen, die aus der Sicht des Datenschutzes an eine künftige Volkszählung zu stellen sind, werde ich mich an anderer Stelle (Nr. 3.7) äußern. Hier möchte ich nur auf zwei Beobachtungen von allgemeinerer Bedeutung eingehen:

1. Vereinbarungen zwischen den Datenschutzbeauftragten und den Regierungen, die dem Zweck dienen, ein in hohem Maße interpretationsbedürftiges Gesetz in verfassungskonformer Weise auszulegen und gesetzliche Erlaubnisse noch weiter einzuschränken, können ein Gesetz mit präzisen und zugleich restriktiven Bestimmungen nicht ersetzen. Die Forderungen, die ich Mitte Februar erhoben und deren Erfüllung der Senat in der nächsten Sitzung der Bürgerschaft zugesagt hatte, der Forderungs-

---

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

katalog, den die Konferenz der Datenschutzbeauftragten Ende März vorlegte und auf den sich die meisten Innenminister bereitwillig einließen, wurden in der Öffentlichkeit als untaugliche Versuche bewertet, Mängel des Gesetzes zu beseitigen und Regelungslücken zu schließen. Zur Beruhigung der Bevölkerung trugen sie nur wenig bei. Nicht allein um verfassungsrechtlichen Anforderungen zu genügen, sondern auch um die Bürger zu überzeugen und zur Mitwirkung zu gewinnen, wird der Gesetzgeber künftig also, wenn er etwa erneut eine Volkszählung durchführen will und auf ein zuverlässiges Ergebnis Wert legt, über eine klare Normierung der Auskunftsverpflichtung und der vorgesehenen Verwendung der Daten hinaus auch Form und Inhalt der Fragebögen, die Grundzüge des Erhebungsverfahrens und die zu treffenden Sicherheitsvorkehrungen exakt regeln müssen.

2. Je heftiger der Widerstand gegen die Volkszählung wurde, desto häufiger beriefen sich Politiker, die die Bürger von der Ungefährlichkeit des Vorhabens überzeugen wollten, darauf, daß es schließlich auch noch die Datenschutzbeauftragten gäbe. Diese würden alle Stellen, die an der Erhebung und Auswertung der Volkszählungsdaten beteiligt seien, streng kontrollieren und könnten dafür garantieren, daß jeglicher Verstoß gegen Datenschutzvorschriften aufgedeckt würde. Von diesem Argument ließen sich die Bürger nur wenig beeindrucken. Sie trauten den Datenschützern einfach nicht zu, daß sie mit ihrem kleinen Kontrollapparat in der Lage seien, Tausende von Zählern, Hunderte von Statistikmitarbeitern und die ganze bei der Volkszählung eingesetzte Technik wirksam zu überwachen. In Diskussionen wurde mir immer wieder vorgehalten, Datenschutzbeauftragte seien doch bloße Papiertiger und auf eine Feigenblattfunktion beschränkt.

   Für diese Skepsis gibt es einleuchtende Gründe. Natürlich kann eine Dienststelle mit sechs Prüfern nicht eine Totalerhebung, von der 1,5 Mill. Bürger betroffen sind, in jeder ihrer Phasen und an allen Stellen überwachen und zugleich ihre sonstigen Aufgaben erledigen. Das Vertrauen in die Fähigkeit eines Datenschutzbeauftragten, auch komplexe DV-Vorgänge fortlaufend zu beobachten und zu kontrollieren, wird sicherlich zunehmen, wenn er der Öffentlichkeit mitteilen kann, daß die personelle Ausstattung seiner Dienststelle verbessert worden ist.

   Vor allem aber kommt es darauf an, daß der Datenschutzbeauftragte eindeutige und umfassende Kontrollbefugnisse hat. Zwar trifft es nicht zu, daß die Datenschutzbeauftragten bei der Überwachung bestimmter Behörden, z. B. im Sicherheitsbereich Beschränkungen unterworfen sind, wie manche Bürger meinen. Jedenfalls ist in Hamburg von der Staatswohlklausel, die allein die Möglichkeit böte, einzelne Vorgänge der Überprüfung durch den Datenschutzbeauftragten zu entziehen, bislang in keinem Fall Gebrauch gemacht worden. Die Öffentlichkeit hat aber aufmerksam registriert, daß über den Umfang der Kontrollbefugnisse der Datenschutzbeauftragten heftig gestritten wird. Kontroversen gibt es über die Frage, ob die Datenschutzbeauftragten die Einhaltung „anderer" Datenschutzvorschriften nur in den Fällen kontrollieren dürfen, in denen Daten in Dateien gespeichert oder aus ihnen übermittelt werden. Nur in Baden-Württemberg hat der Gesetzgeber eine eindeutige Regelung getroffen – zuungunsten der Landesbeauftragten für den Datenschutz. Der Hamburgische Datenschutzbeauftragte ist bislang nicht behindert worden. Doch ist ihm mehrfach entgegengehalten worden, eigentlich sei er ja nicht zuständig; gleichwohl habe man geruht, seine Meinung anzuhören. Der Senat hat sich noch nicht festgelegt. Vielleicht tut er es eines schönen Tages – und tritt der Auffassung des Datenschutzbeauftragten entgegen, weil dessen Kontrolle und dessen Kritik in einem bestimmten Fall unerwünscht sind. Gerade im Interesse der betroffenen Bürger ist es nicht hinnehmbar, daß die Kontrollinstanz vom Wohlwollen der zu kontrollierenden Einrichtung abhängig ist. Es muß Klarheit geschaffen werden – zugunsten des Datenschutzbeauftragten –, wenn dessen Stellung als Bürgeranwalt nicht entscheidend geschwächt und das Vertrauen der Öffentlichkeit nicht minimiert werden soll. Die Besorgnis der Bürger über eine mögliche Rechtsbeeinträchtigung dürfte in aller Regel unabhängig davon bestehen, ob ihre Daten in Akten oder in Dateien verarbeitet wer-

den. Es würde sicherlich nicht ganz einfach sein, ihm begreiflich zu machen, daß er den Datenschutzbeauftragten nur anrufen darf, wenn der von ihm ausgefüllte Fragebogen in dateimäßiger Form gestapelt wird, ihm dieses Recht aber nicht zusteht, wenn der gleiche Fragebogen in eine Akte eingeheftet wird.

Nichts anderes gilt, wenn der Datenschutzbeauftragte prüfen will, ob Amtsgeheimnisse, die besonders sensitive Daten schützen (z. B. das Steuergeheimnis), eingehalten worden sind. Es ist geradezu absurd, daß eben dieses Amtsgeheimnis der Kontrollinstanz entgegengehalten wird, um eine Kontrolle zu verhindern. Ebenso abwegig wäre es schließlich, wenn der Datenschutzbeauftragte nicht uneingeschränkt sollte alle Akten einsehen dürfen, die mit der Verarbeitung personenbezogener Daten im Zusammenhang stehen, sondern die zu kontrollierende Stelle die Aktenteile aussortieren könnte, welche ihr für die Kontrolle geeignet erscheinen.

1.2 Verhältnis zur Verwaltung

In der Praxis sind es vor allem zwei Rahmenbedingungen, die für die Sicherung und Fortentwicklung des Datenschutzes von entscheidender Bedeutung sind: zum einen ist es die Resonanz, die der Datenschutzgedanke bei den mit der Datenverarbeitung befaßten Personen findet, zum anderen das Problembewußtsein, daß die Bürger für den Datenschutz entwickeln.

Innerhalb der Verwaltung hat allein die Existenz eines Datenschutzbeauftragten nach meinem Eindruck schon dazu geführt, daß eigene Aktivitäten in Bezug auf die Sammlung, Weiterleitung und Sicherung von Daten kritischer gesehen und manche Verhaltensweisen geändert wurden. In aller Regel stand die Verwaltung meinen Bedenken und Forderungen aufgeschlossen gegenüber: für fast alle praktischen Probleme konnten bislang einvernehmliche Lösungen gefunden werden. Dabei spielt sicherlich auch eine Rolle, daß immer mehr Beamte die These bestätigen müssen (Nr. 5.2.3 meines letzten TB), die zunächst nur Kopfschütteln ausgelöst hat: Der Datenschutz muß durchaus nicht immer das Verwaltungshandeln erschweren; er sorgt in der Regel für mehr Transparenz und damit Klarheit in der Verantwortlichkeit; häufiger als die Beteiligten es wahrhaben wollen, führt er auch zu einer Rationalisierung der Informationsverarbeitung. Jedenfalls habe ich nicht feststellen müssen, daß Behörden mehr Mühe darauf verwendet haben, die Datenschutzvorschriften zu umgehen, als zu ihrer Befolgung notwendig wäre.

Diese durchaus positiven Erfahrungen dürfen jedoch nicht über ein generelles Problem hinwegtäuschen: die eigenen Initiativen für den Datenschutz sind in der Verwaltung zu wenig ausgeprägt. Zu oft noch geht der Anstoß für bestimmte Datenschutz-Aktivitäten nicht von der Verwaltung selbst aus. Allzu häufig bin ich – zufällig – erst durch Bürger, Pressemeldungen oder Kollegen aus den anderen Ländern auf einzelne Probleme aufmerksam gemacht worden. Dieses Defizit hat verschiedene Ursachen: Wenn die BAJS mich z. B. nicht in die Vorbereitung von datenschutzrechtlich sehr wichtigen Verwaltungsvorschriften für die Ausführung des Sozialgesetzbuches nicht einbezogen hat, liegt dies m. E. daran, daß das Bewußtsein für Probleme des Datenschutzes insgesamt noch nicht sehr ausgeprägt ist oder daß die Möglichkeit, sich durch den Datenschutzbeauftragten beraten zu lassen, nicht hinreichend bekannt ist. Ob der Rat des Datenschutzbeauftragten eingehalten und ob er gar befolgt wird, hängt in großem Maß immer noch von der persönlichen Einstellung des gerade zuständigen Mitarbeiters ab.

Zum Teil können sich die zuständigen Stellen nicht vorstellen, daß Regelungen in Bundesgesetzen auch für den Datenschutz im Lande von Bedeutung sind (so daß ich etwa vor dem Erlaß wichtiger Änderungen der Gewerbeordnung oder vor der Verabschiedung des Bundespersonalausweisgesetzes nicht beteiligt wurde). Auch über datenschutzrechtlich relevante Tagesordnungspunkte von Ministerkonferenzen und ihrer Arbeitskreise werde ich in aller Regel nicht informiert und kann mich in den Verfahrensgang erst einschalten, nachdem ich von anderer Seite Hinweise erhalten habe.

Nur in seltenen Fällen habe ich den Eindruck, daß die Verwaltung mich über bestimmte Probleme deswegen nicht von sich aus unterrichtet, weil sie den Datenschutzbeauftragten nach Möglichkeit aus der Diskussion heraushalten möchte.

Die Diskussion dieses Berichts wird hoffentlich dazu beitragen, daß mehr Initialzündungen für Datenschutzaktivitäten von der Verwaltung selbst ausgehen werden und der Rat des Datenschutzbeauftragten bei wichtigen Problemen früher und gezielter in Anspruch genommen wird. Außerdem hoffe ich, daß die Bereitschaft, die Anliegen des Datenschutzbeauftragten nicht als nachrangig zu behandeln, sondern seine Fragen schnell und umfassend zu beantworten, bei einigen Stellen noch zunehmen wird. Auch wenn Auskunftsersuchen des DSB als lästig empfunden werden, muß es nicht einige Monate dauern, ehe die erbetene Auskunft erteilt wird. In aller Regel wäre es auch zu begrüßen, wenn ich im neuen TB ausführen könnte, daß die Diskussion über ein Problem, über das ich bereits im vorangegangenen Bericht informiert habe, inzwischen – mit welchem Ergebnis auch immer – abgeschlossen ist.

Soeben hat mich eine Stellungnahme der Finanzbehörde zu einem von mir aufgeworfenen Übermittlungsproblem erreicht – gerade noch rechtzeitig, um darüber berichten zu können. Die Finanzbehörde meint, unabhängig von der Beurteilung des jeweiligen Sachproblems seien auch bei Fragen des Datenschutzes immer verwaltungsökonomische Gesichtspunkte anzuwenden, und es erscheine fraglich, ob der Verwaltungsaufwand, der mit einer – von mir geforderten – Unterrichtung des Betroffenen verbunden wäre (nämlich Personalkosten, Porto- und Materialkosten für eine kurze Mitteilung), in der jetzigen wirtschaftlichen Situation mit neuerlichen Belastungen für den hamburgischen Haushalt tragbar sei; es seien hier auch die schutzwürdigen Belange des Bürgers auf umsichtige Verwaltung seiner Steuergelder zu berücksichtigen.

Dieser Auffassung trete ich ganz entschieden entgegen. Eine **rechtlich gebotene** Datenverarbeitung läßt sich nicht durch verwaltungsökonomische Gesichtspunkte relativieren. Eine unrechtmäßige Datenverarbeitung wird nicht dadurch zu einer rechtmäßigen, daß sie die für die Verwaltung kostengünstigere Lösung für eine bestimmte Verwaltungsaufgabe darstellt. Auf den Vorgang bezogen, über den Finanzbehörde und DSB nicht einer Meinung sind (vgl. auch Nr. 3.4.2), heißt das: Wird in einer Verwaltungsvorschrift die regelmäßige Unterrichtung einer öffentlichen Stelle durch eine andere verlangt, also eine Datenübermittlung **ohne Prüfung der Erforderlichkeit im Einzelfall**, und liegt dieser Verwaltungsvorschrift keine gesetzliche Regelung zugrunde, so stellt diese Übermittlung einen Eingriff in die Grundrechtssphäre des Betroffenen dar, der nur dann – für eine Übergangszeit – hingenommen werden kann, wenn der Betroffene hierüber wenigstens informiert wird.

Kostengesichtspunkte spielen nur dort eine Rolle, wo zu prüfen ist, welche technischen und organisatorischen Maßnahmen zur Datensicherung erforderlich sind. Hierfür – und nur hierfür – kommt es nach § 8 darauf an, daß der Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht.

1.3 Information über Datenschutz

Eine positive Entwicklung hat insgesamt das Problembewußtsein der Bürger für den Datenschutz genommen: dies zeigt insbesondere die intensive Diskussion über die mit der Volkszählung und mit der Einführung des maschinenlesbaren Personalausweises verbundenen Probleme und Gefahren, die sich auch in zahlreichen Anfragen und Eingaben niedergeschlagen haben. Überhaupt scheint mir die stark gestiegene Anzahl an Eingaben und der darin enthaltenen wertvollen Hinweise und begründeten Beschwerden ein guter Gradmesser für die wachsende Sensibilisierung der Bevölkerung zu sein. Trotz dieser positiven Tendenzen ist die Zahl der Bürger, die ihre Rechte nach den Datenschutzgesetzen aktiv wahrnehmen, insgesamt noch gering. Um diesem abzuhelfen und die Bürger zu befähigen, sich gegen Einbrüche in ihre private Sphäre besser zur Wehr zu setzen, habe ich im Sommer den „Hamburger Wegweiser zum Datenschutz" (gemeinsam mit dem NDR) herausgegeben. Mit dieser Broschüre, deren 1. Auflage (12.500) bei

Abschluß dieses Berichts schon vergriffen war, habe ich nicht nur versucht, den Lesern einen theoretischen Überblick über das verschlungene System der Datenschutzregelungen zu geben. Gleichzeitig war es mein Anliegen, ihnen auch praktische Hilfestellungen zu geben: Ein vorgedruckter Postkartenteil, für den das Scheckheft des Berliner Datenschutzbeauftragten als Vorbild diente, sowie ein Verzeichnis der Anschriften aller anderen Datenschutzkontrollinstanzen erleichtern den Bürgern – wie ich in vielen Anfragen bestätigt gefunden habe – die Wahrnehmung ihrer Rechte erheblich. Daneben habe ich selbstverständlich alle anderen mir zur Verfügung stehenden Möglichkeiten genutzt, den Bürger zu informieren: Ich habe weitere Broschüren verteilt, meine Mitarbeiter und ich sind auf unzähligen Veranstaltungen von Parteien, Gewerkschaften, Bürgerinitiativen und anderen Organisationen aufgetreten und – last not least – habe ich den Kontakt zu den Medien weiter ausgebaut.

Diese Öffentlichkeitsarbeit wird auch im Jahre 1984 einer der Schwerpunkte meiner Tätigkeit sein, denn die Unterstützung durch die Bevölkerung wird weiterhin von besonderer Bedeutung für den Erfolg meiner Tätigkeit sein.

2. Überblick über die Tätigkeit der Dienststelle

2.1 Neue Aufgabe Bildschirmtext

2.1.1 Beschreibung der Aufgabe

Bildschirmtext ist ein neuer Dienst der Deutschen Bundespost. Vereinfachend gesagt wird damit Computerleistung im Wohnzimmer verfügbar gemacht, ohne daß ein Computer beschafft werden muß. Das System wird unter Nr. 3.1.1 näher beschrieben.

Nach Beendigung der Feldversuche in Berlin und Düsseldorf soll Bildschirmtext – nachdem der ursprüngliche Termin 1.9.1983 aus technischen Gründen verschoben werden mußte – im Laufe des Jahres 1984 bundesweit eingeführt werden.

Mit dem Bildschirmtext sind neue Gefährdungen für die Privatsphäre verbunden (s. Nr. 3.1.1.3). Daher sieht ein von den Ländern am 18.3.1983 geschlossener Staatsvertrag, der Bildschirmtext umfassend rechtlich regelt, u. a. bereichsspezifische Datenschutzvorschriften (s. Nr. 3.1.1.5) und die Überwachung ihrer Einhaltung durch eine Verwaltungsbehörde vor.

2.1.2 Stand in Hamburg

Der Staatsvertrag bedarf der Ratifizierung. Ein entsprechendes Gesetz hat der Senat am 17.5.1983 (Drucksache 11/668) in die Bürgerschaft eingebracht. Das Einführungsgesetz enthält zusätzliche Vorschriften über die Datenschutzkontrolle. Es befindet sich in den parlamentarischen Beratungen. Seine Verabschiedung und damit das Inkrafttreten des Staatsvertrages sind Anfang nächsten Jahres zu erwarten.

In der Senatsdrucksache wird angekündigt, daß dem Hamburgischen Datenschutzbeauftragten – neben der Überwachung im öffentlichen Bereich, für die er nach dem Hamburgischen Datenschutzgesetz ohnehin zuständig ist – auch die Überwachung im nicht-öffentlichen Bereich durch Zuständigkeitsanordnung des Senats übertragen werden soll. Damit wird der Datenschutz auch für Bildschirmtext in einer Hand liegen – eine für den Bürger nützliche Regelung, wie die bisherigen Erfahrungen mit der Zusammenfassung der Kontrollaufgaben nach dem HmbDSG und dem BDSG zeigen.

Da die Überwachung der Anbieter auch nach den Erfahrungen in den Feldversuchen in Berlin und Düsseldorf ohne aktive Teilnahme am System nicht möglich ist, habe ich die Bereitstellung von Mitteln für die Beschaffung einer Teilnehmerausstattung (Tastatur mit integriertem Decoder, Monitor, Drucker – zur Beweissicherung –) beantragt und die Anmeldung zunächst als Teilnehmer in die Wege geleitet.

2.2 Entwicklung der Dienststelle

Mit dem Haushaltsplan 1983 hat die Bürgerschaft die beiden von mir beantragten Stellen (A 15, A 12) bewilligt. Ich bin ihr sehr dankbar dafür. Die Zuweisung der A 15-Stelle hatte keine Auswirkung auf den Personalbestand der Dienststelle, weil ich schon seit Ende 1982 einen zusätzlichen Beamten des höheren Dienstes auf einer „Leihstelle" des Senatsamtes für den Verwaltungsdienst hatte einsetzen und damit den allerdringendsten Bedarf hatte decken können. Die A 12-Stelle habe ich zum 1.12.83 besetzen und damit den Aufbau der Dienststelle entsprechend den bei Aufnahme meiner Tätigkeit entwickelten Vorstellungen abschließen können.

Ich hatte schon im Vorjahr darauf hingewiesen, daß auch eine Verstärkung der Dienststelle im beantragten Umfang bei weitem nicht ausreichen würde, um die wünschenswerte Kontrolldichte zu erzielen. Meine Erwartungen, daß – unter Berücksichtigung meiner sonstigen Aufgaben – die Dienststelle ihren Kontrollauftrag nur in unzulänglicher Weise werde erfüllen können, haben sich bestätigt. Trotz großen Einsatzes aller Mitarbeiter, der über bloße Pflichterfüllung weit hinausgeht und den ich ihnen auf Dauer nicht zumuten kann, wird unsere Arbeitskapazität durch Erfüllung der an uns herangetragenen Beratungswünsche und durch Einzelfallprüfungen, die durch Eingaben ausgelöst werden, so stark in Anspruch genommen, daß für eigene Initiativen und systematische Prüfungen keine Zeit bleibt.

Ich gehe davon aus, daß nach Inkrafttreten des Btx-Staatsvertrages in Hamburg zu Beginn des nächsten Jahres dem Hamburgischen Datenschutzbeauftragten die Datenschutzkontrolle über die Hamburger Anbieter übertragen wird. Das Einführungsgesetz zum Staatsvertrag über Bildschirmtext sieht vor, daß eine Kontrolle nicht nur – wie nach § 30 BDSG – durchgeführt wird, wenn die Beschwerde eines Betroffenen vorliegt, sondern von Amts wegen stattfindet. Bei der Beratung des Staatsvertages in der Bürgerschaft ist die Erwartung ausgesprochen worden, daß – um einer unbefugten oder gar mißbräuchlichen Nutzung der durch das neue Informations- und Kommunikationsmittel geschaffenen Möglichkeiten wirksam zu begegnen – gerade in der Anfangszeit eine umfassende Überwachung aller Anbieter erfolgen werde. Ich kann diese hochgespannten Erwartungen allerdinmgs nur erfüllen, wenn mir die für die Wahrnehmung der neuen Aufgabe benötigte Verstärkung der Dienststelle zugestanden wird. Nach den bisherigen – sicherlich unzuverlässigen – Schätzungen ist in Hamburg nach dem bundesweiten Start von Bildschirmtext mit etwa 500 Anbietern zu rechnen.

2.3 Eingaben

2.3.1 Allgemeines

Im zweiten Jahr meiner Tätigkeit stieg die Anzahl der Eingaben erheblich an. Dies ist sicher auf die Berichterstattung über Datenschutzprobleme in den Medien (Volkszählung 1983!), auf die Veröffentlichungen der Datenschutzbeauftragten, insbesondere ihre Tätigkeitsberichte, und – wie ich hoffe – nicht zuletzt auf die Herausgabe des „Hamburger Wegweisers zum Datenschutz" im September zurückzuführen. Die Art der Eingaben zeigt, daß die Sensibilisierung der Bürger für Fragen des Datenschutzes und ihre Bereitschaft zur Kritik an der Verwaltung in Fällen von unzulässiger oder zumindest bedenklicher Datenverarbeitung durchaus zugenommen hat, während andererseits die Umsetzung der Datenschutzvorschriften in die Verwaltungspraxis noch nicht allenthalben gelungen ist. Bürger machen mit ihren Eingaben in aller Regel Einwände gegen einen speziellen – sie persönlich betreffenden – Datenverarbeitungsvorgang geltend; doch häufig geben sie mir damit nützliche Hinweise auf generelle datenschutzrechtlich relevante Verfahrensweisen, die anläßlich der Eingabenbearbeitung näher untersucht und – falls erforderlich – korrigiert werden. Interessant ist, daß auch Mitarbeiter von Verwaltungsdienststellen eine Tätigkeit, die sie z. T. schon seit langem in dieser Form ausgeübt haben, nunmehr kritisch an Datenschutzbestimmungen messen. Sie haben sich an mich

gewandt, weil sie Zweifel an der Unbedenklichkeit bestimmter Usancen bekommen haben. Die Datenverarbeitung im öffentlichen wie im nicht-öffentlichen Bereich hat im übrigen nicht nur Betroffene veranlaßt, mit Eingaben an mich heranzutreten, sondern auch viele interessierte Bürger und Interessenvertretungen haben mich auf Datenschutzprobleme aufmerksam gemacht.

Beispiele:

1. Der Vater eines Schülers rügte den „Schülerbogen für Berufsschüler" (s. Nr. 3.5.3). Die Eingabe gab Anlaß,
   - die Prüfung der Frage zu beschleunigen, welcher Datenumfang für die betreffende Frage tatsächlich erforderlich ist, und
   - die Behörde auf ihre Verpflichtung nach § 9 Abs. 2 hinzuweisen. Danach ist der Betroffene über die für die Datenerhebung maßgebliche Rechtsvorschrift bzw. auf die Freiwilligkeit seiner Angaben hinzuweisen.

2. Durch eine Eingabe wurde ich darauf aufmerksam gemacht, daß die Staatsanwaltschaft in einem Ermittlungsverfahren gegen einen Polizeibeamten die Akten offen mit der Behördenpost über dessen Dienststelle an die für Amtsdelikte/Polizeisachen zuständige Dienststelle versandt hatte, so daß Kollegen des Beschuldigten Einzelheiten zur Kenntnis nehmen konnten und dies auch getan hatten. Nachdem der Aktenversand aufgrund meiner Bedenken neu organisiert worden war (besonderer Fahrdienst direkt zwischen StA und der für Amtsdelikte/Polizeisachen zuständigen Dienststelle der Polizei – Ps 3), wurde ich durch einen weiteren Hinweis auf eine zweite Schwachstelle aufmerksam gemacht, nämlich darauf, daß der nach Beendigung des Verfahrens an die Polizei zurückzusendende Laufzettel ebenfalls offen über die Beschäftigungsdienststelle an die Dienststelle Ps 3 geleitet wird, wodurch wiederum die Kollegen des Betroffenen unzulässigerweise von dem Ausgang des Ermittlungsverfahrens Kenntnis nehmen konnten. Die Laufzettel werden nunmehr in verschlossenen Umschlägen zurückgesandt.

3. Einem Bürger war aufgefallen, daß Besucher der JVA Vierlande bei Besichtigungen in bedenklich einfacher Weise von den Namen der einsitzenden Gefangenen Kenntnis erhalten können, weil die Namen zum einen an einem Holzbrett bei der Stationsaufsicht, zum anderen an jeder Saaltür groß und deutlich angebracht sind. Durch folgende Maßnahmen wird dies nunmehr verhindert: In der Stationsaufsicht wird die Holztafel vor der Ankunft der Besucher verhängt, von den Saaltüren werden die Namensschilder für die Dauer der Besichtigung entfernt.

4. Ein in der Buchbinderei der JVA Fuhlsbüttel beschäftigter Gefangener wandte sich an mich, weil er einen Verstoß gegen die ärztliche Schweigepflicht darin sah, daß der Buchbinderei Sektionsprotokolle und Operationsberichte aus dem UKE zum Binden übergeben worden waren. Die Ermittlungen in dieser Sache führten zu der Feststellung, daß gegen § 203 StGB verstoßen wurde. Ich konnte erreichen, daß das UKE künftig derartige Unterlagen nicht mehr an die JVA Fuhlsbüttel zum Binden geben wird.

5. Ein Fahrgast der HHA rügte die Speicherung der Personalausweis-Nr. durch die HHA im Rahmen von Fahrgeldbeanstandungen nach Versagen von Fahrkartenautomaten. Ich habe empfohlen, künftig nur noch die Tatsache, daß ein Ausweis vorgelegen hat, in dem Formular „Automaten-Fahrgeldbeanstandung" zu notieren (vgl. Nr. 4.6.2).

6. Von einer Gewerkschaft erfuhr ich, daß ein Kreditinstitut zur Unterstützung einer Marketing-Aktion die Adressen der Kunden, die Kindergeldzahlungen erhalten, zusammenstellen wollte. Aufgrund meiner Intervention hat das betreffende Kreditinstitut die Auswertung für Werbezwecke gestoppt und ihre EDV-Zentralen angewiesen, die zur Verarbeitung bereits erstellten Selektionsbänder zu löschen (vgl. Nr. 4.2.3).

2.3.2 Statistik

Bis zum 30.11.1983 gingen 243 Eingaben bei mir ein, von denen ca. 45% auf den öffentlichen Bereich und ca. 55% auf den nicht-öffentlichen Bereich entfielen. Im einzelnen betrafen die – bislang erledigten – Eingaben folgende Bereiche:

Bereiche	Anzahl	gesamt
A Öffentlicher Bereich		
– Sicherheitsbereich	37	
– Gesundheits- und Sozialbereich	17	
– übrige Bereiche	37	91
B Nicht-öffentlicher Bereich		
– Versandhandel	6	
– Versicherungen	15	
– Kreditinstitute	11	
– Sonstige, die dem 3. Abschnitt des BDSG unterliegen	32	
– Creditreform	20	
– AVAD	15	
– Schimmelpfeng	4	
– Schufa	5	
– Sonstige, die dem 4. Abschnitt des BDSG unterliegen	3	111
	202	202

2.4 Beratungen und Prüfungen

2.4.1 Öffentlicher Bereich

2.4.1.1 Beratungen

Die Arbeit meiner Dienststelle war im Berichtszeitraum weniger durch systematische Prüfungen als vielmehr durch eine zunehmende Beratungstätigkeit geprägt. Den stärksten Beratungsbedarf habe ich in den Bereichen Gesundheits- sowie Arbeits- und Sozialwesen festgestellt. Während z. B. die Polizei von Anfang an relativ gut auf die Anforderungen des Datenschutzes vorbereitet war, stieß ich in den o. g. Bereichen noch auf weit verbreitete Unsicherheiten in grundsätzlichen Fragen. Dies hing im Arbeits- und Sozialbereich vor allem mit Problemen zusammen, die sich aus der Anwendung des relativ jungen Zehnten Buches des Sozialgesetzes (SGB X) und aus der Konkurrenz zwischen den bereichsspezifischen Regelungen des SGB X mit anderen Datenschutzvorschriften ergeben. Diesen Problemen sollte bei der Aus- und Fortbildung der Bediensteten mehr Aufmerksamkeit geschenkt werden.

Im Gesundheitswesen tauchte immer wieder die grundsätzliche Frage nach dem Verhältnis der ärztlichen Schweigepflicht zu den Datenschutzgesetzen auf. Nachdem ich diese Problematik aus eigener Initiative aufgegriffen hatte, haben die zuständigen Behörden jedoch beachtliche eigene Aktivitäten zur Abarbeitung bestehender Defizite entfaltet und insbesondere in allen Krankenhäusern Datenschutzverantwortliche bestimmt.

Fast alle Behörden scheinen inzwischen davon Kenntnis zu haben, daß es auch in Hamburg einen Datenschutzbeauftragten gibt, und nehmen – soweit Bedarf besteht – meine Dienste in Anspruch; ich bin den Wünschen gern nachgekommen. Nach wie vor stehe ich auf dem Standpunkt, daß es im Interesse der Bürger effektiver ist, datenschutzrechtliche Mängel vorher zu verhindern als sie nachher zu beanstanden.

Lediglich in einem Fall sah ich mich gezwungen, eine Beratung in der gewünschten Form aus grundsätzlichen Erwägungen abzulehnen: Ein Bezirksamt hatte mir die Große Anfrage einer Bezirksfraktion zu einem umfassenden Thema übersandt und mich gebeten, ihm die für die Beantwortung der Anfrage erforderlichen Angaben übermitteln zu lassen. Diese Dienstleistung habe ich abgelehnt, denn sie würde die gesetzlich klar geregelte Aufteilung der Kompetenzen auf dem Gebiet des Datenschutzes unterlaufen. Nach § 16 Abs. 1 S. 1 haben zunächst einmal alle Behörden selbst jeweils für ihren Bereich die Ausführung des Datenschutzgesetzes sowie anderer Vorschriften über den Datenschutz sicherzustellen. Diese grundsätzliche Verantwortlichkeit kann ihnen der Datenschutzbeauftragte nicht abnehmen. Seine Beratungstätigkeit kann stets nur unterstützenden Charakter haben.

Besondere Erwähnung verdient die Auseinandersetzung um die Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung (Volkszählung 1983 – im folgenden VZ genannt). Sie hat bis zur einstweiligen Anordnung des Bundesverfassungsgerichts und auch darüber hinaus einen großen Teil der personellen Kapazitäten meiner Dienststelle gebunden. Schwerpunkte meiner Tätigkeit waren

- die Formulierung und Durchsetzung von Forderungen zur Gewährung des Datenschutzes,
- die Beteiligung an Diskussionsveranstaltungen unterschiedlicher Träger (Parteien, Verbände, Kirchengemeinden u. a.m.),
- zahlreiche Einzelgespräche mit Besuchern oder am Telefon und eine Vielzahl von Briefen, die beantwortet werden mußten,
- die Stellungnahmen gegenüber dem Bundesverfassungsgericht im Vorverfahren und in der Hauptsache sowie die Teilnahme an der mündlichen Verhandlung in der Hauptsache,
- ein umfassender Bericht über meine Erfahrungen aus der VZ gegenüber dem Innenausschuß der Hamburger Bürgerschaft.

2.4.1.2 Prüfungen

In meinem 1. TB (Nr. 8.1, S. 5a) hatte ich umfassende Prüfungen von ausgewählten speichernden Stellen und Rechenzentren für das Jahr 1983 angekündigt. Leider konnte ich systematische Prüfungen nicht durchführen; die Gründe hierfür liegen

- in der nichtvorhersehbaren Inanspruchnahme durch die VZ 1983 und
- in dem – verglichen mit meinen Schätzungen – weitaus höheren Kapazitätsbedarf für die Aufstellung des Datenschutzregisters (insbesondere für die Beratung der meldepflichtigen Stellen und die Korrektur der Meldungen) sowie
- in einer unerwartet starken Beanspruchung durch die Bearbeitung von Beratungsersuchen und Eingaben.

Im Berichtszeitraum konnte ich daher lediglich – im Zusammenhang mit Eingaben oder sonstigen Ermittlungen – Teilprüfungen in einigen Dienststellen vornehmen, z. B.

- im Prüfungsamt für den öffentlichen Dienst,
- im Statistischen Landesamt,
- im UKE,
- in diversen Dienststellen der Polizei.

Ich habe mir die in diesem Berichtszeitraum ausgefallenen Prüfungen für das nächste Jahr vorgenommen.

2.4.2 Beratungen und Prüfungen im nicht-öffentlichen Bereich

Meine Beratung im nicht-öffentlichen Bereich beschränkt sich nicht auf die – gesetzlich vorgesehene – Unterstützung betrieblicher Datenschutzbeauftragter. Vielmehr sehe ich meine Aufgabe – auch im nicht-öffentlichen Bereich – darin, die Bürger über Datenschutzprobleme aufzuklären und ihnen zu helfen, ihre Rechte wahrzunehmen. Daneben stehe ich auch allen Personen zur Verfügung, die für den Umgang mit personenbezogenen Daten verantwortlich sind.

Viele Fragen wurden – gerade nach der Veröffentlichung meines 1. TB und des „Hamburger Wegweisers zum Datenschutz" – auch telefonisch an mich gerichtet. Einige Angaben gaben Anlaß für eine Überprüfung, andere konnte ich in schon bestehende Kontakte zu den speichernden Stellen einflechten. Bei meinen Überprüfungen fand ich in den datenverarbeitenden Stellen i. d. R. aufgeschlossene Gesprächspartner, die bereitwillig – z. T. weit über den Einzelfall hinaus – Auskunft gaben. Solche offenen Gespräche bieten mir die Möglichkeit, aufgrund weiterer Hintergrundinformationen die Interessen sowohl des Betroffenen als auch der speichernden Stelle oder Dritter besser zu beurteilen. Die Prüfung des Einzelfalls orientiert sich zwar an dem jeweiligen vom Petenten vorgetragenen Problem; es ist jedoch nicht ausgeschlossen, daß die Aufsichtsbehörde im Laufe des Gesprächs in die Rolle des Beraters schlüpft, der auch zu anderen Fragen Stellung nimmt.

Lediglich in einem Fall hat mir eine Schufa-Anschlußfirma Auskünfte über den Hintergrund einer Datenübermittlung verweigert. Die zugrundeliegende Beschwerde richtete sich gegen die Schufa, und die Anschlußfirma wollte sich aus der Auseinandersetzung zwischen dem eigenen Kunden und der Schufa heraushalten. Diese Haltung mußte ich akzeptieren, da sich nach der jetzigen Rechtslage mein Auskunftsanspruch nur gegen die Stelle richtet, die für die fragliche Datenverarbeitung verantwortlich ist.

Zur Überwachung der datenverarbeitenden Stellen des Vierten Abschnitts des BDSG hatte ich mir vorgenommen, wöchentlich eine Prüfung durchzuführen. Wegen einiger aktueller Vorhaben habe ich jedoch streckenweise die Schwerpunkte verlagert. So habe ich zwar mit den turnusmäßigen Überprüfungen begonnen, das mir selbst vorgegebene Ziel aber nicht ganz erreicht. Unter den geprüften Datenverarbeitern befand sich u. a. auch eine große Handels- und Wirtschaftsauskunftei; über das Ergebnis wird unter Nr. 4.4.1 berichtet.

Daneben habe ich eine Reihe von Datenerfassungsbetrieben und Service-Rechenzentren überprüft. Schwerpunktmäßig habe ich die zum Register nach § 40 BDSG gemeldeten Entsorgungsunternehmen kontrolliert, die in Werbung und Vertragstext weniger die Rohstoffgewinnung als die Sicherheit der Datenlöschung betonen. Bei keiner der geprüften Stellen habe ich gravierende Mängel festgestellt.

2.5 Datenschutzregister

2.5.1 Aufgaben, Aufbau und Inhalt

2.5.1.1 Aufgaben

Das nach § 13 vom Hamburgischen Datenschutzbeauftragten zu führende Datenschutzregister, über dessen Rechtsgrundlagen ich in meinem 1. TB unter Nr. 4.4.1 bis 4.4.3 Ausführungen gemacht habe, dient sowohl als Informationsquelle für den Bürger als auch mir als Arbeitsgrundlage für meine Kontrolltätigkeit. Das HmbDSG räumt dem Bürger in den §§ 6, 14 und 15 Kontroll-, Abwehr- und Gestaltungsrechte ein. Da der Bürger nicht in jedem Falle wissen wird, wo und durch wen Daten zu seiner Person gespeichert

sind, soll er sich anhand des Datenschutzregisters umfassend darüber unterrichten können, gegenüber welchen öffentlichen Stellen er von seinen Datenschutzrechten Gebrauch machen kann. Das Datenschutzregister bildet somit die praktische Grundlage für die Verwirklichung seiner Datenschutzrechte.

Mit den in meinem 1. TB genannten Einschränkungen (hinsichtlich der Dateien des Landesamtes für Verfassungsschutz [§ 13 Abs. 4], der Staatsanwaltschaft, der Polizei, der Landesfinanzbehörden, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung in Dateien speichern [§ 13 Abs. 3 Nrn. 1 und 2], der öffentlich-rechtlichen Kreditinstitute [§ 2 Abs. 2] sowie der öffentlich-rechtlichen Wettbewerbsunternehmen [§ 2 Abs. 3]) wird die Datenverarbeitung im öffentlichen Bereich durch das Datenschutzregister für den Bürger transparent gemacht. Dies ist vor allem deshalb geboten, weil die öffentlichen Stellen nicht – wie die privaten Unternehmen – zur individuellen Benachrichtigung jedes Betroffenen verpflichtet sind.

Ich selbst gewinne durch das Register Einblick in die Infrastruktur der Informationsverarbeitung im öffentlichen Bereich und habe dadurch die Möglichkeit, Entwicklungen, Veränderungen, kritische Phasen zu beobachten und meine Kontrolltätigkeit entsprechend zu planen.

2.5.1.2 Aufbau und Inhalt

Das Datenschutzregister besteht aus zwei Teilen, und zwar dem öffentlich zugänglichen „allgemeinen Teil" und dem nicht öffentlichen „besonderen Teil". Der allgemeine Teil enthält die Dateien mit personenbezogenen Daten derjenigen Behörden und sonstigen in § 2 Abs. 1 genannten öffentlichen Stellen, die ohne Einschränkung meldepflichtig sind. Gem. § 13 Abs. 2 kann jedermann diesen Teil des Registers einsehen, daraus Auskünfte und – wenn er ein berechtigtes Interesse darlegt – Auszüge erhalten. Der allgemeine Teil enthält insbesondere Angaben über

1. die speichernde Stelle (Bezeichnung, Anschrift),

2. die Datei (Bezeichnung, Art der gespeicherten personenbezogenen Daten),

3. die Aufgaben, zu deren Erfüllung die Kenntnis dieser Daten erforderlich ist, sowie die Rechtsvorschriften, aufgrund derer die jeweilige Aufgabe zu erfüllen ist,

4. den betroffenen Personenkreis,

5. regelmäßige Übermittlungen aus der Datei (Übermittlungsempfänger, Art der zu übermittelnden Daten, Zweck und Rechtsgrundlage der Übermittlung).

Das Datenschutzregister enthält jedoch nicht – wie häufig angenommen wird – **Individualdaten von Bürgern.**

Über die im allgemeinen Teil des Registers enthaltenen Dateien ist mindestens einmal jährlich eine Übersicht zu veröffentlichen (s. Nr. 2.5.3).

Der besondere Teil enthält die Dateien mit personenbezogenen Daten der in § 13 Abs. 3 genannten Stellen. Hinsichtlich dieser Dateien besteht kein Recht auf Einsicht und auf Auszüge, und über diese Dateien ist keine Übersicht zu veröffentlichen. Die Angaben im Register sind auf die nach obigen Nummern 1. bis 3. beschränkt.

Neben den beiden vorgenannten Teilen des Datenschutzregisters habe ich noch eine interne Ergänzung aufgebaut, die nur meiner Kontrolltätigkeit dient: Dieser Teil enthält Dateien von öffentlich-rechtlichen Wettbewerbsunternehmen, die gem. §§ 2 Abs. 2, 13 zum

Register keine Meldungen abzugeben haben (s. dazu Nr. 4.4.2 meines 1. TB), die mir aber gleichwohl – weil sie auch gem. § 2 Abs. 2 Satz 1 meiner Kontrolle unterliegen – ihre Dateien gemeldet haben.

2.5.2 Stand, Qualität, Fortschreibung

Bis zum 30. Juni 1983 hatten alle meldepflichtigen Behörden und öffentlichen Stellen der Freien und Hansestadt Hamburg (A) sowie die der Aufsicht der FHH unterstehenden juristischen Personen des öffentlichen Rechts (B) Meldungen bzw. Fehlanzeigen abgegeben. Zu melden sind alle automatisierten Dateien und manuelle Dateien dann, wenn sie nicht ausschließlich „intern" sind. „Intern" ist eine Datei, deren Daten nicht zur Übermittlung bestimmt sind.

Die statistische Auswertung der Meldungen ergibt folgende Übersicht (Stand: 30.6.1983):

	A	B	insgesamt
meldepflichtige Stellen gem. § 2 Abs. 1 HmbDSG (A+B s. oben)	19	28	47
Fehlanzeige erfolgte durch	1	8	9
Dateien gemeldet haben	18	20	38
speichernde Stellen (funktionaler Stellenbegriff)	605	54	659
davon Schulen	485		
Finanzämter	18		
Amtsgerichte	6		
Bezirksämter, Ortsämter, Ortsdienststellen	23		
zum allgemeinen Teil des Registers gemeldete Dateien (§ 13 Abs. 3 HmbDSG)	8.895	300	9.195
davon automatisierte Dateien	53	170	223

Seit dem 1.7.1983 sind bisher (21.11.1983) eingegangen:

Änderungsmeldungen (einschl. Korrekturen)	25
Neumeldungen von Dateien	34
Löschungsanzeigen	7

Diese Anzahl von Veränderungen (insgesamt 66) dürften noch nichts darüber aussagen, wie häufig Veränderungen im Dateienbestand tatsächlich sind, denn ein erheblicher Teil der vorstehenden Meldungen ist wohl noch im Zusammenhang mit den Anfangsschwierigkeiten bei der Einrichtung des Datenschutzregisters zu sehen.

Während die Ermittlung der in § 2 Abs. 1 genannten Behörden und juristischen Personen keine Probleme aufwarf, gestaltet sich wegen der Vielfalt der wahrzunehmenden Verwaltungsaufgaben die Prüfung schwierig, ob die speichernden Stellen alle meldepflichtigen Dateien erfaßt und zum Register gemeldet haben. Die notwendige Abgrenzung des Begriffs **„speichernde Stelle"**, die unmittelbare Auswirkungen hat auf die Frage, wann die Weitergabe von Daten aus einer Datei als „Übermittlung" zu qualifizieren ist, und da-

mit auf die Einstufung einer manuellen Datei entweder als meldepflichtige oder „interne" Datei, hat in der Praxis nicht selten längere Diskussionen ausgelöst und Ausführungen zum im Datenschutzrecht anzuwendenden **Stellenbegriff** (s. dazu Nr. 3.5) erforderlich gemacht. Während einige Stellen wegen dieser Schwierigkeiten vorsorglich alle Dateien gemeldet und die Beurteilung durch meine Dienststelle abgewartet haben, haben andere Stellen in Verkennung des Übermittlungsbegriffs manuelle Dateien für nicht meldepflichtig gehalten. Dies ist mir insbesondere im Schulbereich aufgefallen. Weiter bestanden Zweifel hinsichtlich des Begriffs der Übermittlung von Daten **„aus einer Datei"**. Diese Feststellung läßt sich am Beispiel der Personalkarteien für die Angehörigen des öffentlichen Dienstes darstellen: Neben den Personalakten, die z. Z. gem. § 4 Abs. 4 Nr. 3, 2. Halbsatz nicht als Datei anzusehen sind, werden für alle Bediensteten Personalkarteikarten geführt, auf denen ein erheblicher Teil der in den Personalakten enthaltenen Daten gespeichert ist. Zwar war die Dateieigenschaft der Personalkarteien unbestritten; doch bestand teilweise die Auffassung, daß – weil Auskünfte über Bedienstete stets aus den Personal**akten** gegeben werden sollen und nicht aus den Personal**karteikarten** – die Daten in den Personalkarteien nicht zur Übermittlung bestimmt und diese Dateien mithin intern und nicht meldepflichtig sind. Tatsächlich werden – zumindest wenn die Akten versandt sind, aber auch in anderen Fällen – in der Praxis doch Daten aus den Karteikarten übermittelt. Ein Teil der Meldungen nach dem 30.6.1983 entfiel daher auf Personalkarteien.

Die abgegebenen Dateimeldungen konnten wegen der großen Anzahl vor ihrer Einstellung in das Datenschutzregister nur einer globalen Plausibilitätsprüfung unterzogen werden. Die **inhaltliche Prüfung**, insbesondere hinsichtlich der Angaben zu den Rechtsgrundlagen der Speicherung, zu den Übermittlungen und zu deren Rechtsgrundlagen, muß ebenso wie die **Kontrolle der Vollzähligkeit** der abgegebenen Dateimeldungen nach und nach erfolgen. Für die systematische Überprüfung der Dateimeldungen wird z. Z. ein Konzept erarbeitet, nach dem während des nächsten Berichtszeitraumes vorgegangen werden soll.
Im übrigen habe ich die meldepflichtigen Stellen aufgefordert, meldepflichtige Vorgänge (Neueinrichten, Verändern, Löschen von Dateien) zeitnah mitzuteilen.

2.5.3 Dateienübersicht

Nach § 13 Abs. 1 Satz 3 habe ich mindestens einmal im Jahr eine Übersicht über die im Datenschutzregister enthaltenen Dateien zu veröffentlichen. Mit der Bekanntmachung im Amtlichen Anzeiger vom 7. September 1983 Seite 1501 ff habe ich erstmals eine solche Dateienübersicht veröffentlicht. Aus dieser gehen nicht nur die Dateien mit Angabe der speichernden Stelle und der betroffene Personenkreis hervor, sondern ich habe in der Veröffentlichung auch die Aufgaben, zu deren Wahrnehmung die Dateien von den speichernden Stellen eingerichtet sind, und die Empfänger regelmäßiger Übermittlungen dargestellt. Darüber hinaus habe ich die Dateienübersicht auch in dem „Hamburger Wegweiser zum Datenschutz" veröffentlicht, wodurch eine breitere Bevölkerungsschicht unterrichtet werden konnte (1. Auflage insges. 12.500 Exemplare).

2.5.4 Registerverordnung

Die Erfahrungen bei der Einrichtung des Datenschutzregisters sollen eingebracht werden in die Vorbereitungsarbeiten für eine Registerverordnung gem. § 13 Abs. 5.

2.6 Beobachtung der automatisierten Datenverarbeitung (ADV)

2.6.1 Allgemeine Vorbemerkung

Die ADV wird in der Öffentlichkeit überwiegend mit kritischem Mißtrauen oder mit Furcht betrachtet. Dazu trägt bei, daß in den Medien über die technischen Möglichkeiten, weniger aber über die – die technischen Möglichkeiten stark begrenzenden – praktischen Anwendungsprobleme und über den tatsächlichen Anwendungsstand berichtet wird. Ein

gutes Beispiel hierfür ist die Diskussion über die Volkszählung. In ihr wurden die Anwendung modernster Techniken und raffiniertester Auswertungsverfahren bei der Verarbeitung der Volkszählungsdaten unterstellt. Hinweise, daß solche Techniken und Verfahren der amtlichen Statistik nicht zur Verfügung stehen, daß vielmehr mit der lokalen Stapelverarbeitung eine Technik eingesetzt werden sollte, die weit hinter den Möglichkeiten der modernen Datenverarbeitungstechnologie zurückbleibt, gleichwohl aber zur Erledigung der gestellten statistischen Aufgaben ausreicht, wurden kaum zur Kenntnis genommen. Versicherungen der Datenschutzbeauftragten, angesichts der geringen Attraktivität der Daten und der eingesetzten Datensicherungsmaßnahmen seien bei der Verarbeitung im Rechenzentrum Mißbrauchsmöglichkeiten so gut wie ausgeschlossen, wurden bestenfalls mit freundlicher Skepsis aufgenommen. Andererseits hat die Diskussion über die Volkszählung auch sichtbar gemacht, wie groß die Furcht vor der ADV in weiten Bevölkerungskreisen ist und wie tief sie sitzt. Die Ursachen hierfür sehe ich in ganz persönlichen Erfahrungen des Bürgers mit der ADV:

- Die Datenverarbeitungstechnik ist für den Außenstehenden nicht durchschaubar.

- Sie verstärkt den Mangel an Bürgerfreundlichkeit, der die Verwaltung wegen ihrer Komplexität kennzeichnet, durch technisch erklärbare, aber vermeidbare Zumutungen an den Bürger (z. B. Verwendung von Schlüsselzahlen, die an anderer, umständlich zu suchender Stelle erklärt sind).

- Bei der weit verbreiteten Direktwerbung mit Hilfe ausgesuchter Adressensammlungen beunruhigt es viele betroffene Bürger, daß sie häufig sehr persönlich angesprochen werden. Eine einleuchtende Erklärung meinen sie in der scheinbaren Omnipotenz der Computer finden zu können.

- Viele Bürger werden von Kreditauskunfteien darüber benachrichtigt, daß Daten über sie gespeichert werden; die Chance, den Bürger über die Umstände zu informieren und über seine Rechte nach den Datenschutzgesetzen aufzuklären, wird nicht genutzt.

- Überhaupt kann der Bürger leicht das Gefühl bekommen, er sei für die zahlreichen Institutionen in Verwaltung und Wirtschaft nur eine Informationsquelle; ihn aufzuklären, hielten sie für überflüssig; seine Versuche, seine Rechte wahrzunehmen, werden als lästige Störungen abgewehrt.

- Natürlich spielt auch eine Rolle, daß der Computer oder – allgemeiner – die Mikroelektronik in der Arbeitswelt als Bedrohung empfunden und erlebt wird.

Datenverarbeitung wird als feindlich erfahren; sie potenziert unfreundliche oder sogar abweisende Züge, die Großorganisationen wie die öffentliche Verwaltung ohnehin schon aufgrund ihrer Größe haben. Hinzu kommen Momente, die in der Technik der automatisierten Datenverarbeitung selbst begründet sind. Da ist zum einen die Versuchung, das technisch Machbare auch anzustreben, weil es – jedenfalls auf den ersten Blick – Rationalisierungsmöglichkeiten bietet. Ein Beispiel hierfür ist die Zielvorstellung der integrierten Datenverarbeitung, die die öffentliche Verwaltung Anfang der 70-iger Jahre beherrschte; die benötigten Daten sollten nur einmal erhoben und nur einmal gespeichert, aber vielfach verwendet werden. Diese Zielvorstellung ist sehr früh schon aus technischen Gründen, aber auch aus Datenschutzerwägungen aufgegeben worden; denn die integrierte Datenverarbeitung würde durch ihren Zwang zur Normierung, insbesondere zur Einführung übergreifender Verknüpfungsmerkmale, die faktisch als freiheitssichernd wirkende Vielfalt der Datenspeicherung je für besondere Zwecke aufheben und die durch unterschiedliche Zuständigkeiten geregelte Aufgabenteilung in Frage stellen. Es ist die Aufgabe des Datenschutzes, das Aufleben der Idee der integrierten Datenverarbeitung zu verhindern.

Zum anderen hält sich die technische Entwicklung nicht an die Kategorien, die der Gesetzgeber zur Beschreibung der Datenverarbeitung in den Datenschutzgesetzen geprägt hat. Bei bestimmten Entwicklungen der Informationstechnik, z. B. der Textverarbeitung oder bei intelligenten Fernsprecheinrichtungen, ist es fraglich, ob der Dateibegriff noch erfüllt ist, der heute die Anwendung der Datenschutzgesetze begründet. Die Bedeutung der Verknüpfung von maschinell gespeicherten Daten ohne inhaltliche Veränderung (häufig auch als Abgleich bezeichnet) nimmt mit fortschreitender Automatisierung zu; diese Verarbeitungsform ist aber den von den Datenschutzgesetzen normierten Phasen der Datenverarbeitung nicht ausdrücklich zugeordnet. Es bedarf erheblicher interpretatorischer Anstrengungen, um den – internen – Datenabgleich unter das Gesetz zu subsumieren. Aufgabe der Datenschutzbeauftragten ist es, das den Datenschutzgesetzen zugrundeliegende Konzept ständig zu überprüfen und rechtzeitig Vorschläge für eine Anpassung der Datenschutzgesetze zu machen, wenn die Entwicklung der Technik es erfordert. Der vorliegende Referentenentwurf aus dem Bundesinnenministerium zur Novellierung des BDSG wird den Anforderungen, die sich aus der technischen Entwicklung der letzten Jahre ergeben, nur in sehr unzureichender Weise gerecht. Es ist zu hoffen, daß die Vorschläge der Datenschutzbeauftragten im weiteren Gesetzgebungsverfahren wenigstens teilweise aufgegriffen werden.

2.6.2 Zentralisierung der ADV

Mit diesem Thema hatte ich mich in der Auseinandersetzung über die Volkszählung 1983 intensiver zu beschäftigen; Anlaß waren die Behauptungen, jedenfalls in Hamburg seien die Gefahren einer mißbräuchlichen Nutzung der Daten aus der Volkszählung deswegen größer, weil sie

- zusammen mit anderen Daten der Verwaltung (insbesondere aus dem Sicherheitsbereich) in einem Rechenzentrum verarbeitet werden, das zudem
- im Polizeihochhaus untergebracht ist.

Nach meinen Feststellungen – die ich auch dem Bundesverfassungsgericht in dem Verfahren über die Volkszählung 1983 mitgeteilt habe – hätte die Verarbeitung der Volkszählungsdaten im Verwaltungsrechenzentrum die Gefahr des Mißbrauchs nicht erhöht. Da ich dieser Frage aber grundsätzliche Bedeutung beimesse, scheint mir die Aufnahme der wesentlichen Gedanken und Feststellungen in den Bericht angebracht.

2.6.2.1 Situation in Hamburg

Die Begriffe „Rechenzentrum", „autonome" oder „isolierte" DV-Anlage und „zentral" sowie „dezentral" sind nicht eindeutig und werden mit unterschiedlichem Inhalt verwendet. Die „DV-Landschaft" in der hamburgischen Verwaltung kann jedoch auch ohne vorherige Klärung der Begriffe pragmatisch erklärt werden.

1. Für die maschinelle Durchführung der automatisierten Verfahren, die in den Behörden und Ämtern der Freien und Hansestadt Hamburg (unmittelbare Staatsverwaltung) angewendet werden, steht die **Datenverarbeitungszentrale** (DVZ) als Verwaltungsrechenzentrum zur Verfügung. In der DVZ sind insgesamt 6 große Datenverarbeitungsanlagen von IBM und Siemens mit jeweils umfangreicher Peripherie installiert. In der DVZ werden rd. 200 verschiedene Anwendungen durchgeführt, darunter die gesamte Statistik und das polizeiliche Auskunftssystem (jedoch **keine** Anwendung des Verfassungsschutzes – das „Nachrichtendienstliche Informations- und Verbundsystem" NADIS wird als Gemeinschaftseinrichtung des Bundesamtes für Verfassungsschutz und der Verfassungsschutzbehörden der Länder außerhalb Hamburgs betrieben). Die meisten Anwendungen in der DVZ werden in der Form der Stapelverarbeitung (Verarbeitung zu bestimmten Terminen oder nach Bedarf; nur während der Verarbeitung sind die Daten in der DV-Anlage; die Verarbeitung findet nur unter Beteiligung des Personals der DVZ statt) durchgeführt; nur wenige, allerdings z. T. sehr komplexe Verfahren, in denen besonders sensible Daten verarbeitet werden, sind Dialogverfahren (unmittelbare Kommunikation des Benutzers mit der DV-

Anlage über eine Benutzerstation und ein Datenfernverarbeitungsnetz; die Daten sind ständig in der DV-Anlage präsent; Verarbeitung ohne Beteiligung des DVZ-Personals), nämlich das polizeiliche Auskunftssystem, das Auskunftssystem der Steuerverwaltung, die Datenerfassung für das Personalabrechnungssystem (in der Einführung), die Anwendungsprogrammierung (in der Einführung). Weitere Dialoganwendungen, z. B. die Automation des Einwohnerwesens, sind in Vorbereitung (zur Auswirkung auf die Datensicherung vgl. Nr. 2.6.2.4).

Die DVZ wird von der Finanzbehörde betrieben. (Vgl. im einzelnen die Niederschrift über die Sitzungen des Unterausschusses Stellenplan am 6. und 19.2.1981, als Broschüre „Automation in der hamburgischen Verwaltung" herausgegeben vom Senatsamt für den Verwaltungsdienst; die Feststellungen des Unterausschusses treffen – abgesehen von Details z. B. der maschinellen Ausstattung – auch heute noch zu.)

2. In der erwähnten Broschüre werden die in der DVZ installierten DV-Anlagen als „zentrale Maschinerie" bezeichnet (vgl. Anlage 12 der Broschüre). Die außerhalb der DVZ in der unmittelbaren Staatsverwaltung Hamburgs installierten DV-Anlagen werden „dezentrale autonome Maschinerie" genannt (vgl. Anlage 14 der Broschüre). Sie umfaßt mehrere DV-Anlagen meist geringer Größe, die in der Regel für die Erledigung nur einer bestimmten Aufgabe im allgemeinen mit geringem Umfang eingesetzt werden; (in der Fachliteratur werden sie häufig als dedicated systems bezeichnet). Diese Anlagen sind meistens „neben dem Arbeitsplatz" aufgestellt und werden nicht als Rechenzentrum betrieben (keine Produktionssteuerung, keine spezielle Bedienung, sondern Steuerung durch die Anwendungen).

3. Die der Aufsicht der Freien und Hansestadt Hamburg unterstehenden juristischen Personen des öffentlichen Rechts (mittelbare Staatsverwaltung) haben ebenfalls DV-Anlagen unterschiedlicher Größenordnung installiert, über die ich durch die Meldungen zum Datenschutzregister informiert bin.

   Eine Sonderstellung nimmt das Rechenzentrum der Universität Hamburg ein, in dem nach einem Beschluß des Senatsausschusses für das Rechenzentrum grundsätzlich keine personenbezogenen Daten verarbeitet werden dürfen; z. Z. kann jedoch nach Angaben der zuständigen Gremien keine Gewähr dafür übernommen werden, daß dieser Beschluß eingehalten wird.

   Auch das Universitäts-Krankenhaus Eppendorf betreibt ein Rechenzentrum, das in der Broschüre des Senatsamtes aber zur dezentralen autonomen Maschinerie gezählt wird.

2.6.2.2 Zentrale und dezentrale ADV aus der Sicht des Datenschutzes

Im Vordergrund der folgenden Betrachtungen stehen die in der umittelbaren Staatsverwaltung installierten DV-Anlagen (zentrale und dezentrale autonome Maschinerie in der Terminologie der Broschüre „Automation in der hamburgischen Verwaltung").

Die Entscheidung, auf welcher DV-Anlage eine bestimmte Anwendung durchgeführt wird, hängt von vielen Faktoren ab (vgl. Anlage 16 der Broschüre). Aber auch bei weiter voranschreitender Entwicklung der DV-Anlagen, die als dezentrale autonome Maschinerie betrieben werden können, wird es auf absehbare Zeit weiterhin Rechenzentren geben, in denen mehrere Anwendungen durchgeführt werden. Der Betrieb von Rechenzentren wird damit begründet, daß in ihnen

- leistungsfähige große DV-Anlagen installiert werden können, die für bestimmte Aufgaben notwendig sind und nur durch Zusammenfassung mehrerer Anwendungen wirtschaftlich genutzt werden können,

- bestimmte vor- und nachgelagerte Dienste (z. B. Belegverarbeitung, Papiernachbearbeitung) und unterstützende Funktionen (z. B. Datenbankverwaltung) wirtschaftlich vorgehalten werden können.

Ein Blick auf die anderen Bundesländer, die Kommunalverwaltungen und die private Wirtschaft zeigt, daß auch dort aufgrund derselben Überlegungen Rechenzentren wie die DVZ betrieben werden. Rechenzentren und dezentrale autonome DV-Anlagen sind nach heutiger Auffassung keine Alternativen, sondern sinnvolle Ergänzungen.

2.6.2.3 Konzentration von Daten

Für den Hamburgischen Datenschutzbeauftragten ist die Form, in der DV-Anlagen installiert werden, allein unter dem Aspekt der Datensicherung relevant. Die Erwägungen zur Wirtschaftlichkeit sind nur als ein Grund (unter mehreren) für die Entstehung der gegenwärtigen Organisation mitgeteilt worden und nur insofern interessant, als die – nach der Schutzbedürftigkeit der Daten zu beurteilenden – Maßnahmen der Datensicherung als (Kosten-) Faktor in die Entscheidung eingehen und angemessen zu berücksichtigen sind (insofern muß die Anlage 16 in der Broschüre ergänzt werden).

Es wäre verfehlt, in einer der erörterten Organisationsformen – Zentralisierung der Datenverarbeitungskapazität in einem Rechenzentrum oder dezentrale autonome DV-Kapazität – ein erhöhtes Datenschutzrisiko zu vermuten. Beide Organisationsformen verursachen unterschiedliche Risiken und es bestehen auch unterschiedliche Möglichkeiten, den Risiken durch Datensicherungsmaßnahmen zu begegnen. Die Zentralisierung von Datenverarbeitungskapazität in einem Rechenzentrum hat die Konzentration von Daten aller dort betriebenen Anwendungen zur Folge; dem Risiko erhöhter Mißbrauchsgefahr kann durch die Organisation des Rechenzentrumbetriebs und durch die bei großen DV-Anlagen zahlreichen und ausgefeilten technischen Maßnahmen der Datensicherung (angefangen bei modernen Betriebssystemen bis zu speziellen Programmsystemen für die Datensicherung) begegnet werden. Auf einer autonom betriebenen DV-Anlage befinden sich wesentlich weniger Daten, im allgemeinen nur aus einer Anwendung; der Stand der Datensicherung ist aber in der Regel niedriger als bei großen DV-Anlagen (vgl. den 11. TB des Hessischen Datenschutzbeauftragten S. 50 ff, in dem auch auf die Erschwerung der Datenschutzkontrolle bei dezentralen autonomen DV-Anlagen hingewiesen wird, ein Problem, das allerdings in einem Flächenland wie Hessen größere Bedeutung hat). Die Angemessenheit der Datensicherung kann daher nur im konkreten Einzelfall nach der Vorschrift des § 8 Abs. 1 Satz 2 beurteilt werden.

2.6.2.4 Vormarsch der Dialogverarbeitung

Die Organisation der automatisierten Datenverarbeitung steht gegenwärtig in einem Wandlungsprozeß. Während bis vor wenigen Jahren die automatisierten Verfahren nahezu ausschließlich in der Form der lokalen Stapelverarbeitung (die zu verarbeitenden Fälle werden gesammelt – gestapelt – und zum Rechenzentrum transportiert; die Verarbeitungsergebnisse werden vom Rechenzentrum zurück in die Fachabteilung gebracht) in Rechenzentren durchgeführt wurden, wird heute – auch in der öffentlichen Verwaltung – zunehmend „Computerleistung am Arbeitsplatz" zur Verfügung gestellt. Hierbei werden die Aufgaben in der Form der Dialogverarbeitung über Benutzerstationen erledigt; die Benutzerstationen sind entweder über Datenfernverarbeitung an die zentrale Maschinerie in der DVZ oder lokal an eine dezentrale autonome Maschine (DV-Anlage) angeschlossen.

Es ist zu erwarten, daß mit der Zunahme der Dialoganwendungen die Bestrebungen stärker werden, Daten auch im on-line-Betrieb zu **übermitteln**; (an eine Dialoganwendung sind zunächst nur die Benutzer angeschlossen, die für die Erledigung der automatisierten Aufgabe zuständig sind; hinzutreten können auch andere Stellen, die an regelmäßigen Datenübermittlungen interessiert sind). Der direkte Zugriff auf automatisierte

Daten über on-line-Anschlüsse ist für die Bürger mit besonderen Risiken verbunden, denen der Gesetzgeber mit erhöhten Anforderungen an die Zulässigkeit solcher Abrufverfahren begegnen muß.

Wie bereits in meinem ersten TB ausgeführt (s. Nr. 4.3.1, S. 22 f), muß die bei der Dialogverarbeitung leichter mögliche mißbräuchliche Benutzung durch umfassende technische und organisatorische Maßnahmen, beginnend z. B. bei der Zugangssicherung durch Schlösser oder Ausweisleser an den Benutzerstationen über moderne Betriebssysteme mit Datensicherungskomponenten und Vorkehrungen in den Anwendungsprogrammen (insbesondere Identifikation der Benutzer und Zugriffsbeschränkungen über Kenn- und Paßwörter) bis zum Einsatz spezieller, der Datensicherung dienender Programmsysteme, verhindert werden. Diesem Problem wird im kommenden Berichtszeitraum meine besondere Aufmerksamkeit gelten.

2.6.2.5 Stand der Datensicherung

Im Zusammenhang mit der Diskussion über die Volkszählung 1983 habe ich mich besonders mit dem Stand der Datensicherung in der DVZ befaßt. Hierbei stand die Frage im Vordergrund, ob der mit der Zentralisierung sehr vieler Verfahren zwangsläufig verbundenen höheren Gefährdung wirksam begegnet wird.

Das in meinem ersten TB als Basis der Datensicherung beschriebene Konzept der physischen Trennung von Verfahren im Stapelbetrieb, Verfahren im Dialogbetrieb und Testbetrieb der Anwendungsprogrammierung ist im Berichtszeitraum für den IBM-Bereich aufgegeben worden, weil sich die Aufgaben ungleich entwickeln (starke Zunahme der Verfahren im Dialogbetrieb). Für den Stand der Datensicherung ergibt sich:

- Im Siemensbereich ist nach wie vor das Konzept der physischen Trennung gültig. Das polizeiliche Auskunftssystem und einige Verfahren im Stapelbetrieb, der Testbetrieb der Anwendungsprogrammierung und die technischen Anwendungen (ohne personenbezogene Daten) werden auf physisch getrennten DV-Anlagen verarbeitet. Die Verfahren im Stapelbetrieb, in denen personenbezogene Daten verarbeitet werden, werden in den IBM-Bereich übertragen.

- Im IBM-Bereich ist das Programmsystem SECURE installiert worden, ein umfassendes Datensicherungssystem, das nur den durch Paßwort ausgewiesenen Berechtigten den Zugang zu den Dateien im Stapel- und Dialogbetrieb gestattet. Da SECURE erst vor kurzem installiert worden ist, werden die Erfahrungen mit dem System erst im nächsten TB ausgewertet werden können.

Die zahlreichen Datensicherungsmaßnahmen der DVZ können hier – auch zur Vermeidung von Ausforschungen – nicht vollständig und im Detail dargestellt werden. Ich beschränke mich auf einige relevante Punkte:

- Nachdem die DVZ auch die Verwaltung der Magnetbänder übernommen hat, die in den programmierenden Stellen für Testzwecke verwendet werden, dürfen (außer in den Fällen, in denen automatisierte Verfahren den Austausch von Magnetbändern vorsehen; der Magnetbandaustausch wird von der DVZ betrieben und kontrolliert) keine Datenträger aus der DVZ entfernt werden. Bis vor kurzem noch durften Magnetbänder mit Testdaten „aus- und eingeführt" werden. Da niemand von außen erkennen kann, ob sich auf einem Magnetband auch tatsächlich Testdaten befinden, bestand hier eine Lücke im Datensicherungssystem. Sie ist nunmehr geschlossen worden.

- Die innere Organisation der DVZ ist geändert worden. Die Abteilung „Planung und Steuerung" ist aufgelöst worden; ihre Aufgaben sind auf die „Technische Arbeitsvorbereitung" übertragen worden. Für diese organisatorische Änderung sprechen vor

allem wirtschaftliche Gründe, weil bisherige Doppelarbeiten entfallen. Andererseits bewirkt Redundanz auch mehr Sicherheit. Durch die Auflösung der Abteilung „Planung und Steuerung" ist die „Komplottstrecke" (das ist die Zahl derjenigen, die bei einer mißbräuchlichen Benutzung in Stapelverfahren zusammenwirken müssen) qualitativ verändert worden: Vorher konnte der allein auftragsberechtigte Angehörige der Abteilung „Planung und Kontrolle" nur innerhalb der durch die automatisierten Verfahren vorgegebenen Arbeitsstruktur handeln, weil er keine neuen, in den Dokumentationen bisher nicht vorgesehenen Arbeiten ohne Komplizen in der „Technischen Arbeitsvorbereitung" einführen konnte. Dadurch waren die Mißbrauchsmöglichkeiten begrenzt. Jetzt ist derjenige, der die Arbeiten einführt, auch auftragsberechtigt.

Die DVZ will das erhöhte Risiko durch
- die personelle Verstärkung der Innenrevision, die stichprobenweise die Verarbeitungen prüft, und
- die – vorgesehene – maschinelle Auftragserteilung mit einem maschinellen Soll-Ist-Vergleich

ausgleichen.

- Im Berichtszeitraum ist damit begonnen worden, im IBM-Bereich die interaktive Programmierung im größeren Maßstab einzuführen. Auch hier soll das Programmsystem SECURE Mißbrauch verhindern.

Die hier aufgeführten wichtigen Veränderungen geben mir Veranlassung, das Datensicherungssystem der DVZ im nächsten Jahr umfassend zu prüfen. Entsprechende Vereinbarungen mit der DVZ sind getroffen worden.

Es gibt keine absolute Sicherheit gegen Mißbrauch; aber durch Datensicherungsmaßnahmen kann die versehentliche unberechtigte Nutzung fremder Daten so gut wie ausgeschlossen und die Schwelle für die absichtliche unberechtigte Nutzung fremder Daten (der eigentliche Mißbrauch) so hoch gelegt werden, daß der mögliche Ertrag aus dem Mißbrauch den Aufwand für die Überwindung der Datensicherungsmaßnahmen nicht lohnt. Unter dieser Prämisse werde ich den Stand der Datensicherung in der DVZ prüfen. Ein weiterer Schwerpunkt meiner Arbeit 1984/1985 wird sein, mir einen Überblick über die Datensicherungsmaßnahmen bei dezentralen autonomen DV-Anlagen zu verschaffen und bei ausgewählten autonomen DV-Anlagen zu überprüfen.

2.6.3 Entwicklung der Datenverarbeitungstechnik

In der Diskussion über die Volkszählung 1983 habe ich mich auch intensiver mit dem Argument auseinandergesetzt, daß vielleicht die heute zur Verfügung stehenden und angewendeten Datenverarbeitungstechniken hinsichtlich ihrer Risiken und Gefährdungen beherrschbar sind, nicht jedoch die sich abzeichnende Datenverarbeitungstechnik (zu den Gefährdungen durch neue Medien siehe Nr. 2.6.4). Ich habe meine Feststellungen hierzu ausführlich in meinem Bericht „Die Volkszählung – Erfahrungen und Resümee" an den Innenausschuß der Hamburger Bürgerschaft dargestellt.

2.6.3.1 Gefährdungspotential der gegenwärtigen Datenverarbeitungstechnik

Die mit der **gegenwärtigen** Datenverarbeitungstechnik verbundene neue Qualität der Datenverarbeitung und die sich daraus ergebenden Gefährdungen haben nicht zuletzt zum Erlaß der Datenschutzgesetze geführt. Die Regelungen der Datenschutzgesetze haben das Ziel, die Anwendung der Datenverarbeitungstechnik zu begrenzen, sie zu „zähmen", und der durch die Datenverarbeitungstechnik erhöhten Mißbrauchsgefahr durch entsprechende Datensicherungsmaßnahmen zu begegnen.

Wenn heute im großen und ganzen davon ausgegangen werden kann, daß zumindest in der öffentlichen Verwaltung die von der automatisierten Datenverarbeitung ausgehenden Gefährdungen beherrscht werden, dann liegt das nicht zuletzt an dem technisch-

organisatorischen (Rück-) Stand der automatisierten Datenverarbeitung in der öffentlichen Verwaltung. Die vorherrschende Verarbeitungsform ist auch heute noch die Stapelverarbeitung, deren Risiken beherrscht werden (s. Nr. 2.6.2). Das wird sich mit zunehmenden Dialoganwendungen ändern, wie ich schon mehrfach betont habe. Aber auch der Geschwindigkeit dieses Wandlungsprozesses sind Grenzen gesetzt durch den Aufwand, der für die Umstellung der heutigen Stapelverfahren auf Dialoganwendungen zu leisten ist.

2.6.3.2 Gefährdungen durch die neue Entwicklung

Die sich abzeichnenden technischen Entwicklungen sind daher vor dem Hintergrund der Gefährdungen zu sehen, die bereits heute mit der automatisierten Datenverarbeitung verbunden sind. Meine Analyse dreier Kernbereiche der technischen Entwicklung befaßt sich daher mit der Frage, ob der Einsatz der neuen Technik zusätzliche und neue Gefahren mit sich bringt.

1. Speicherkapazität

   Es ist nicht zu erwarten, daß die Kapazität der externen Speicher (das sind die Speicher, auf denen die jeweils zu verarbeitenden Daten aufbewahrt werden, bis sie zur Aufgabenerfüllung nicht mehr notwendig sind und gelöscht werden können) in der nächsten Zukunft wesentlich steigen wird. Auch die für die Verarbeitungsmöglichkeiten wichtigen Übertragungsraten (gemessen in Bytes/sec.), mit denen Daten vom Magnetband oder von der Magnetplatte in die Zentraleinheit übertragen werden, werden sich nicht wesentlich ändern. Allenfalls von grundsätzlich neuen Speichern (z. B. optische Speicher) sind Sprünge in der Speicherkapazität (Bildplatte z. B. 6.000 Mio. Bytes, das ist mehr als das 10fache der hamburgischen Volkszählungsdaten) und in der Übertragungsgeschwindigkeit zu erwarten. Da diese Speicher als externe Speicher für DV-Anlagen noch keine Anwendungsreife haben, sind sie z. Z. nicht relevant.

   Es bleiben natürlich die mit der heutigen Speicherkapazität verbundenen Gefährdungen (Speicherung großer Datenmengen auf geringem Raum für lange Dauer, flexible und – im Rahmen der gewählten Organisation – schnelle Verfügbarkeit der gespeicherten Daten).

2. Retrieval

   Das Wiederauffinden (Retrieval) von gespeicherten Daten auf einem externen Datenträger und das Bereitstellen eines bestimmten Datensatzes für die Verarbeitung in der Zentraleinheit einer DV-Anlage setzen eine geeignete Datenorganisation und eine darauf abgestimmte Verarbeitungstechnik voraus. Da ein bestimmter Datensatz für Außenstehende in Sekundenschnelle, häufig im Wortsinne „auf Knopfdruck" erscheint, entsteht der Eindruck, das Wiederauffinden der Daten bereite keinerlei Schwierigkeiten, alle gespeicherten Daten seien beliebig verfügbar. Dabei wird übersehen, daß die schnelle Bereitstellung eines bestimmten Datensatzes das Ergebnis langer Überlegungen und aufwendiger Detailarbeiten ist und zudem nur **die** Datensätze mit der gewünschten Schnelligkeit zur Verfügung gestellt werden, deren Bedarf im Rahmen der Verfahrens-Entwicklung vorgesehen war, so daß die Datenorganisation sich darauf einstellen konnte.

   Stark vereinfacht kann man, soweit auf die Verarbeitungstechnik abgestellt wird, grundsätzlich zwischen
   - Verfahren mit sequentiellem Zugriff und
   - Verfahren mit Direktzugriff unterscheiden.

Dabei ist die Verarbeitungstechnik in erster Linie von der Organisation der Daten, nicht von dem gewählten Speichermedium abhängig. Bei den Verfahren mit Direktzugriff können wiederum

- einfache Direktzugriffsverfahren und
- Datenbankverfahren

unterschieden werden.

Die Datenorganisation und die Verarbeitungstechnik werden nach den Erfordernissen der zu erledigenden Aufgaben ausgewählt. In Stapelverfahren werden die Dateien sequentiell, in Dialogverfahren so organisiert, daß ein Direktzugriff möglich ist. Das hat im wesentlichen wirtschaftliche Gründe; denn die Organisation mit Direktzugriff ist wesentlich teurer als mit sequentiellem Zugriff (höherer Aufwand für den Entwurf der Organisation, höhere laufende Speicherkosten).

Im Rahmen der nach den Notwendigkeiten der jeweiligen Aufgabenerfüllung gewählten Datenorganisation und Verarbeitungstechnik werden benötigte Daten sehr schnell bereitgestellt. Außerhalb dieses Rahmens ist die Bereitstellung von Daten mühsam und mit großem Aufwand verbunden.

Bei allen heute verwendeten Verarbeitungstechniken muß jemand, der bestimmte Daten in einem Datenbestand wiederfinden will, die konkrete Datenorganisation und die Zugriffsmethode genau kennen. Es gibt nach meiner Kenntnis auch keine Systeme, die jede Suche einfach und ohne nennenswerten Aufwand realisieren.

3. Vernetzung

Unter Vernetzung werden hier Netze mit Terminals verstanden, die zu mehreren DV-Anlagen Zugang haben; der Ausdruck „Vernetzung" enthält eine wertende Komponente, die den Zusammenschluß nahezu aller DV-Anlagen suggeriert.

Datenfernverarbeitung kann heute nur in Form von geschlossenen Netzen realisiert werden, d. h. es ist vor Konzeption und Realisierung des Netzes bekannt, welche DV-Anlagen einbezogen und welche Nachrichten ausgetauscht werden. Beispiele für geschlossene Netze sind POLAS/INPOL (das Verbundsystem der Polizeiauskunftssysteme von Bund und Ländern) oder die Abfrage der Steuerkonten in der Freien und Hansestadt Hamburg. An dem Charakter als geschlossenem Netz ändert sich nichts, wenn statt Punkt-zu-Punkt (Datex-L) -Leitungen solche benutzt werden, bei denen der Betreiber (die Deutsche Bundespost) das sichere Ankommen von Nachrichten in Form von „Datenpaketen" garantiert, sich aber die Disposition vorbehält, auf welchem Wege die Nachricht im konkreten Einzelfall transportiert wird (Datex-P). Entscheidend ist, daß weitere DV-Anlagen nur angeschlossen werden können, nachdem das vorhandene (geschlossene) Netz entsprechend erweitert worden ist. Offene Netze hingegen gestatten den jederzeitigen Anschluß zusätzlicher DV-Anlagen dadurch, daß die DV-Anlage eine Verbindung zum Netz erhält, so wie heute beispielsweise ein neues Telefon angeschlossen wird. Offene Netze setzen Normung voraus, technische (physikalische Eigenschaften der Netze und DV-Anlagen) und organisatorische (äußerer Aufbau der Nachrichten) Normungen. Dieser Normungsprozeß ist national und international noch nicht abgeschlossen. Zwar besteht über einige grundlegende, insbesondere technische Normen (sog. V. 24 bzw. X. 21-Schnittstellen) völlige, über die organisatorischen Normen aber nur teilweise Übereinstimmung. Das zeigt z. B. der überaus harte Kampf, den sich z. Z. Hersteller von DV-Anlagen im Bürocomputerbereich um die Durchsetzung ihrer Firmenstandards liefern. Es ist z. Z. nicht absehbar, wann die für offene Netze erforderliche Normung abgeschlossen sein wird.

Gelegentlich wird in der Diskussion das Bildschirmtextsystem (Btx-System, s. Nr. 3.1) als ein offenes Netz bezeichnet. Tatsächlich ist es offen zur Benutzung durch jedermann, seiner Natur nach jedoch ein geschlossnes Netz (wenn auch ein sehr großes); denn alle Teilnehmer müssen sich an die von der Deutschen Bundespost festgelegten Konventionen halten. Daher können auch andere, bestehende Netze nicht ohne weiteres mit dem Btx-System verbunden werden; Voraussetzung hierfür wäre, daß die Netze sich nach den von der Deutschen Bundespost festgelegten Konventionen richten. Am Btx-System läßt sich außerdem veranschaulichen, daß ein solches Netz nur dann mit Gefährdungen für den einzelnen Bürger verbunden ist, wenn er sich aus eigener Initiative in das System einschaltet: Selbst wenn sehr viele (externe im Sprachgebrauch des Btx-Systems) DV-Anlagen angeschlossen sind, können alle nur dann in Kontakt mit dem einzelnen Teilnehmer treten, wenn dieser es wünscht; denn nur der Teilnehmer kann die Verbindung zur Btx-Vermittlungsstelle herstellen, und die Btx-Vermittlungsstelle stellt eine Verbindung zu einer externen DV-Anlage nur dann her, wenn der Teilnehmer es verlangt. Von einer externen DV-Anlage aus kann keine Verbindung zu einem Teilnehmer aufgebaut werden oder – mit anderen Worten etwas salopp ausgedrückt – das Versandhaus xy kann nicht unverlangt von der Mattscheibe grüßen.

Zusammenfassend bin ich der Ansicht, daß von der gegenwärtig absehbaren Entwicklung der Datenverarbeitungstechnik keine qualitativ neuen Gefährdungen ausgehen; sicherlich werden sich einige Gefährdungen, die schon in der gegenwärtigen Datenverarbeitungstechnik angelegt sind, verstärken. Ich bin aber zuversichtlich, daß diesen Gefährdungen mit dem jetzigen Datenschutzinstrumentarium wirksam begegnet werden kann; die Instrumente müssen allerdings scharf gehalten werden. Diese Feststellung entbindet nicht von der Verpflichtung, die Entwicklung aufmerksam zu beobachten und rechtzeitig neue Instrumente herzustellen, wenn neue Gefährdungen erkannt werden, gegebenenfalls muß dann das vorhandene Datenschutzkonzept durch ein neues ersetzt werden.

2.6.4 Neue Medien

Die Neuen Medien spielen in der öffentlichen Diskussion eine bedeutende Rolle. Auch wenn dabei gesellschaftspolitische Fragestellungen (Auswirkungen auf den Arbeitsmarkt und auf das menschliche Zusammenleben) im Vordergrund stehen, gibt es gewichtige Datenschutzprobleme, die durch die Verbindung von automatisierter Datenverarbeitung und Kommunikation entstehen. Auf die Datenschutzprobleme insbesondere bei Bildschirmtext und einigen anderen Medien gehe ich unter Nr. 3.1 näher ein. Hier soll lediglich ein zusammenfassender Überblick gegeben werden.

2.6.4.1 Übersicht über die Neuen Medien

In Abb. 1 sind die gegenwärtig vorhandenen und die künftig möglichen Medien und Transport-(Kommunikations-) Wege zusammengestellt. Daraus ergibt sich, daß die mögliche Entwicklung im Nutzungsbereich private Wirtschaft und öffentliche Verwaltung – abgesehen vom Bildschirmtext, auf den ich gleich näher eingehen werde – im jetzigen Zeitpunkt noch sehr unbestimmt ist. Weitere Analysen werden erforderlich sein, um die Gefährdungen zu erkennen, die sich aus dem Zusammenschluß von konventioneller Bürotechnik, automatisierter Datenverarbeitung und Kommunikation (Stichwort: „Büro 2.000") und aus dadurch möglichen gravierenden Veränderungen im Geschäftsleben ergeben. Als Beispiel sei nur erwähnt, daß die Kredit- und Scheckkarten möglicherweise das Bargeld nahezu ganz verdrängen und damit bisher anonyme Vorgänge individualisieren werden. Dagegen wird sich die Situation im Nutzungsbereich Unterhaltung, private Information schon heute absehbar revolutionär entwickeln.

2.6.4.2 Datenschutzspezifische Gefährdungen

In Abb. 2 ist für die Medien, die gegenwärtig und künftig im privaten Haushalt zur Verfügung stehen, untersucht worden, welche Daten bei welcher Stelle gespeichert werden

Abb. 1: Übersicht über die gegenwärtig vorhandenen und künftig möglichen Medien und Transportwege

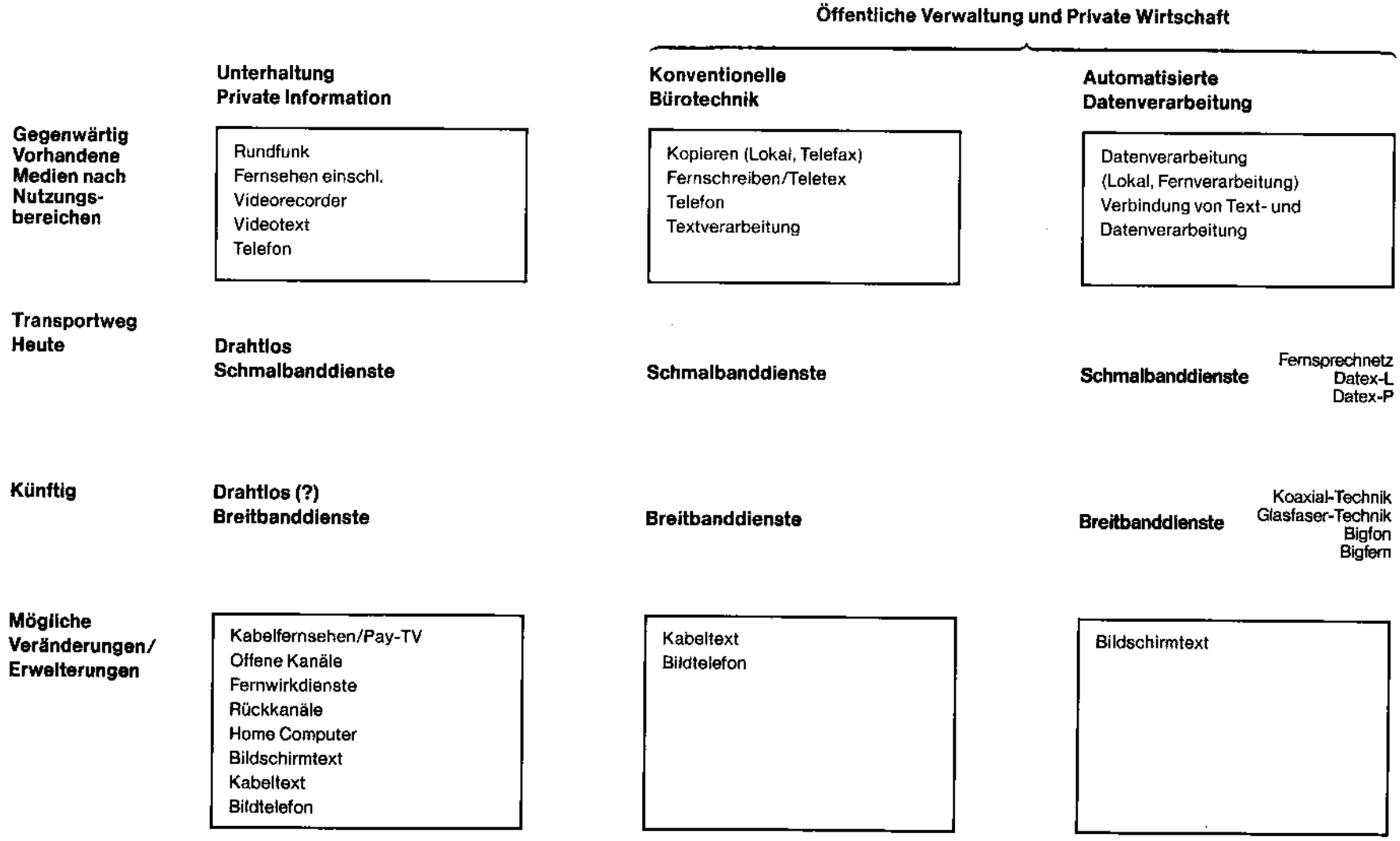


Abb. 2: Übersicht über die mit den vorhandenen und künftigen Medien verbundene Datenspeicherung

Speicherung / Medium	Welche Daten werden gespeichert?	Welche Stelle speichert die Daten?	Hat der Teilnehmer Kenntnis von der Speicherung?
Rundfunk	Daten über die Person (Name, Anschrift usw.)	Gebühreneinzugszentrale	Ja (Anmeldung)
Fernsehen	– " –	– " –	– " –
Videotext	– " –	– " –	– " –
Bildschirmtext	Daten über die Person Daten über die in Anspruch genommenen Dienste Daten über Einkommens- und Vermögensverhältnisse Daten über Einkaufsverhalten Daten über Reiseverhalten	Betreiber – " – Anbieter – " – – " –	Ja (Anmeldung) Nein Ja (Dispositionen) Ja (Einkäufe) Ja (Buchungen)
Telefon/Bildtelefon	Daten über die Person	Betreiber	Ja (Anmeldung)
Kabelfernsehen/ Pay – TV	Daten über die Person Daten über Sehgewohnheiten	Veranstalter? – " –	Ja (Anmeldung) Ja? (Buchung)
Offene Kanäle	Daten über die Person?	Veranstalter?	Ja (Anmeldung)
Rückkanäle	Daten über die Person Daten über Meinungen und dgl.	Veranstalter? – " –	Ja? (Anmeldung)
Kabeltext	Daten über die Person? Daten über in Anspruch genommene Texte	Betreiber? – " –	Ja (Anmeldung) Nein
Fernwirkdienste	Daten über die Person und ihr Verhalten	Veranstalter? Anbieter	Ja?
Home Computer	Es handelt sich um eine andere Problematik (Speichern von personenbezogenen Daten durch Private für private Zwecke – Geltung des BDSG)		

und ob der Benutzer oder Teilnehmer von der Datenspeicherung Kenntnis hat. Aus diesen Angaben soll auf das Gefährdungspotential der Medien geschlossen werden.

In der Frage, ob der Benutzer oder Teilnehmer von der Datenspeicherung Kenntnis hat, bin ich davon ausgegangen, daß der Mehrzahl der Teilnehmer die wesentliche neue Eigenschaft der Vermittlungstechnik nicht bewußt ist. Künftig wird die Vermittlung der Dienste über Datenverarbeitungsanlagen zwangsläufig dazu führen, daß bei der Inanspruchnahme der Dienste teilnehmerbezogene Nutzungsdaten entstehen (es ist eine andere Frage, ob sie auf Dauer gespeichert werden).

Mit den heute vorhandenen Medien Rundfunk, Fernsehen, Videotext und Telefon ist – jedenfalls in der gegenwärtigen Betriebsform – keine datenschutzspezifische Gefährdung verbunden. Änderungen können sich durch die Einführung neuer Techniken ergeben:

- Beim Telefon können computergestützte Vermittlungseinrichtungen die Aufzeichnung von Nutzungsdaten (Gesprächsteilnehmer, Dauer des Gesprächs) ermöglichen.

- Beim künftigen Kabelfernsehen ist ebenfalls die Aufzeichnung von Nutzungsdaten (welche Programme wurden wann und wie lange empfangen) möglich, wenn die technischen Einrichtungen, die die gewünschten Programme zur Verfügung stellen, aus wirtschaftlichen Gründen außerhalb des Teilnehmerbereichs eingerichtet werden.

Die Gefährdungen durch das Medium Bildschirmtext und durch die Fernwirkdienste werden unter Nr. 3.1.1 bzw. Nr. 3.1.2.2 im Detail behandelt. Bei den weiter aufgeführten Neuen Medien besteht die Gefährdung ebenfalls in der Speicherung von Daten über Nutzungsvorgänge; es ist z. Z. noch schwierig einzuschätzen, ob die Teilnehmer sich bewußt sind, daß Daten über Nutzungsvorgänge **gespeichert** werden, auch wenn sie – wie z. B. beim Pay-TV (d. h. Abnahme bestimmter **Sendungen**) – diese Daten selbst dem Veranstalter übergeben haben. Maßgebend für die Einschätzung ist auch die konkrete technische und organisatorische Gestaltung der einzelnen Dienste, über die gegenwärtig keine gesicherten Erkenntnisse vorliegen.

Konkrete Gefährdungen entstehen mit der tatsächlichen Realisierung der Neuen Medien. Bildschirmtext wird bundesweit im Laufe des Jahres 1984 eingeführt werden; daher sind bereichsspezifische Datenschutzvorschriften geschaffen worden (vgl. Nr. 3.1.1). Der Realisierungsstand bei den anderen Medien ist regional unterschiedlich; in Hamburg hat die Post begonnen, in größerem Umfang zu verkabeln und damit die Voraussetzungen, nämlich die Transportwege, für die Einführung neuer Dienste zu schaffen. Die tatsächliche Einführung neuer Dienste hängt auch von den wirtschaftlichen Erfolgsaussichten ab, die in jüngster Zeit unterschiedlich beurteilt werden. Ich werde die Entwicklung aufmerksam beobachten und mich rechtzeitig um die erforderlichen bereichsspezifischen Datenschutzvorschriften bemühen.

2.6.5 Mitwirkung an Automationsvorhaben

Im Berichtszeitraum habe ich bei folgenden – noch in der Planungsphase befindlichen – Projekten mitgewirkt:

2.6.5.1 Beim Verfahren

- „Abbau der Fehlsubventionierung im Wohnungswesen" durch Stellungnahmen, in denen ich Einwendungen gegen den Umfang der vorgesehenen Datenspeicherung erhoben und mich mit den beabsichtigten Übermittlungen auseinandergesetzt habe (s. dazu Nr. 3.6);

- „Automation im Einwohnerwesen" durch Teilnahme an Sitzungen der Arbeitsgruppe für fachliche Fragen (AG I) und der Lenkungsgruppe Automation im Einwohnerwesen (s. dazu Nr. 3.8);

- „Automatisierung der Zentralkartei der Staatsanwaltschaft" durch Stellungnahme zu dem Bericht über die Detailplanung zur „Automatisierten Führung der Zentralkartei", in der ich Bedenken gegen die Speicherung einzelner Daten äußerte und in der ich unter Hinweis auf § 8 HmbDSG und die Anlage dazu forderte, zusätzliche Datensicherungsmaßnahmen zu planen und zu definieren sowie die Frage der Löschungsfristen befriedigend zu regeln (s. auch Nr. 3.12).

- „Krankenhausverwaltungssystem KVS" durch Stellungnahme zu einem Konzept betreffend den Einsatz von dezentralen ADV-Anlagen für kaufmännische und Verwaltungsaufgaben in den Krankenhäusern des Landesbetriebes Krankenhäuser. Da das Konzept in der mir zur Stellungnahme vorgelegten Form nicht weiter verfolgt wird, sehe ich davon ab, auf Einzelheiten einzugehen.

- „Emissionskataster (Luft) für Hamburg" durch ein Gutachten zu den mit diesem Verfahren zusammenhängenden Datenschutzfragen. In dem Gutachten habe ich u. a. dargelegt, daß das HmbDSG auf das Verfahren Anwendung findet, weil in einer Datei – auch – personenbezogene Daten, daß heißt Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren **natürlichen Person**, gespeichert werden sollen. Ich habe zu einigen grundsätzlichen Fragen, wie Umfang der Datenspeicherung, Übermittlungen durch Zugriff auf einen Datenbestand im Dialogbetrieb sowie Paßwortschutz, Erläuterungen abgegeben.

2.6.5.2 Landeseigene Sozialhilfestatistik

Beim Verfahren „Landeseigene Sozialhilfestatistik" habe ich an Besprechungen der Arbeitsgruppe „Sozialhilfestatistik" teilgenommen. Seit 1980 sind die Ausgaben für Sozialhilfeleistungen sprunghaft angestiegen. Diese Entwicklung beruht nicht nur auf einer wachsenden Zahl von Leistungsempfängern, sondern auch auf einer strukturellen Veränderung des Empfängerkreises. Die schon seit längerem erhobene Forderung nach aussagekräftigem Zahlenmaterial für eine realistische Haushaltsplanung ist dadurch immer dringlicher geworden, daß Nachforderungen für Mehraufwendungen in einem viel kritisierten Umfang notwendig wurden. Auch hat der sachliche und politische Rechtfertigungsdruck gegenüber der Öffentlichkeit, den parlamentarischen Gremien und dem Senat in starkem Maße zugenommen.

Vor diesem Hintergrund ist der am 2.3.1982 der Behörde für Inneres (BfI) und der Behörde für Arbeit, Jugend und Soziales (BAJS) erteilte Auftrag des Senates zu sehen, die „Entwicklung eines auf Dauer angelegten, aussagefähigen Instrumentariums der Analyse im Bereich der Sozialhilfe" zu prüfen. Nach Abschluß der Vorarbeiten hat der Senat sodann am 2.11.1982 die BfI beauftragt, „zusammen mit der BAJS und der Behörde für Bezirksangelegenheiten, Naturschutz und Umweltgestaltung (BBNU) und dem Senatsamt für den Verwaltungsdienst die Arbeiten an der Einführung einer landeseigenen Sozialhilfestatistik so zu beschleunigen, daß diese von 1984 an eingeführt werden kann." Die aufgrund dieser Beschlüsse eingesetzte Arbeitsgruppe „Sozialhilfestatistik" hat in der Folgezeit mehrere Konzepte entwickelt.

Im Zusammenhang mit der Sozialhilfestatistik galt meine Aufmerksamkeit sowohl dem z. Z. praktizierten Verfahren zur Erstellung der Bundessozialhilfestatistik als auch der geplanten Erweiterung der Sozialhilfestatistik, d. h. den Aktivitäten zur Entwicklung des neuen Verfahrens „Landeseigene Sozialhilfestatistik."

Bisher wird die bundesgesetzlich vorgeschriebene Sozialhilfestatistik (§§ 10, 11 Bundesstatistikgesetz – BStatG – vom 14.3.1980, BGBl. I Seite 289, §§ 1 – 5 des Gesetzes über die Durchführung von Statistiken auf dem Gebiet der Sozialhilfe, der Kriegsopferfürsorge und der Jugendhilfe vom 15.1.1963, BGBl. I Seite 49) in der Weise erstellt, daß die Sozialdienststellen ihre den Namen und die Anschrift des Hilfeempfängers enthaltenden Leistungskarten dem Statistischen Landesamt von Zeit zu Zeit zur Auswertung zur Verfügung stellen. Das Statistische Landesamt wertet diese Karten entweder selbst

aus oder vergibt die Arbeit an Heimarbeiter. Die Auswertung besteht darin, daß die aus den Karten entnommenen Daten nunmehr anonym in zur automatisierten Verarbeitung geeignete Signierlisten (Lesebelege) übertragen werden. Die Leistungskarten gehen nach Auswertung an die Sozialdienststellen zurück und werden dort wieder zu den jeweiligen Sachakten genommen.

Schon in einem Vermerk vom 5. Januar 1981 setzte sich die BAJS mit der Frage auseinander, ob dieses Verfahren nach Inkrafttreten des SGB X am 1.1.1981 im Hinblick auf die Vorschriften über den Schutz des Sozialgeheimnisses (§§ 67 – 78 SGB X) noch zulässig sei. Die BAJS kam zu einem positiven Ergebnis, und zwar im wesentlichen aufgrund folgender Überlegungen:

Sozialhilfeträger ist die Freie und Hansestadt Hamburg. Unzweifelhaft müssen Daten, die den Bereich des Sozialhilfeträgers verlassen, anonymisiert sein. Das Sozialgeheimnis ist aber auch bzgl. der verschiedenen Dienststellen und Behörden eines Rechtsträgers untereinander zu wahren. Das heißt jedoch nur, daß die in den Sozialdienststellen bekannten personenbezogenen Daten nicht an Dienststellen weitergegeben (übermittelt) werden dürfen, die keine Aufgaben von Sozialdienststellen wahrnehmen. Zu den Aufgaben des Sozialhilfeträgers gehört es auch, den mit der Durchführung der Statistik befaßten Dienststellen die erforderlichen Daten zur Verfügung zu stellen. Dies könnte zwar in der Weise geschehen, daß die Daten bereits im Sozialamt anonymisiert werden. Hierfür könnten besondere Sachbearbeiter bei den Sozialämtern eingesetzt werden. Das wäre im Sinn des Geheimschutzes die sauberste Lösung. Daß diese Sachbearbeiter beim Sozialhilfeträger Freie und Hansestadt Hamburg nicht in den Sozialämtern sitzen, sondern beim Statistischen Landesamt zusammengefaßt sind, weil sie nicht nur die Anonymisierung, sondern auch die datenverarbeitungstechnische Aufbereitung der Daten vornehmen, ist lediglich eine Organisationsfrage, deren Regelung dem Sozialhilfeträger freisteht. Jedenfalls werden hier auch Aufgaben des Sozialhilfeträgers wahrgenommen, so daß der Geheimnisschutz der Weitergabe der Leistungskarten nicht entgegensteht. Aufgrund dieser Rechtsauffassung wurde das Verfahren in der beschriebenen Weise fortgesetzt.

In einem Beitrag zum Protokoll über die Besprechung des Arbeitskreises Sozialhilfestatistik am 9.3.1983 bin ich der Auffassung der BAJS entgegengetreten. Ich habe dargelegt, daß die Sozialhilfedienststellen als für die Wahrnehmung der Aufgaben des Sozialleistungsträgers Freie und Hansestadt Hamburg zuständige Stellen mit dem Statistischen Landesamt als in Hamburg für statistische Aufgaben zuständige Stelle keine Einheit bilden, sondern daß sie verschiedene speichernde Stellen sind und die Bekanntgabe von personenbezogenen Daten durch die Sozialdienststellen an das Statistische Landesamt eine Übermittlung im Sinne von § 2 Abs. 2 Nr. 2 BDSG ist. Erforderlich ist nach den Statistikbestimmungen nur die Übermittlung von anonymisierten bzw. aggregierten Daten. Wenn – wie im vorliegenden Fall – die Leistungskarten übergeben werden, werden personenbezogene Daten, und zwar Sozialdaten, übermittelt. Eine Offenbarung von Sozialdaten ist aber nur zulässig unter den Voraussetzungen der §§ 67 – 77 SGB X. Falls keine Einwilligung der Betroffenen vorliegt, muß einer der gesetzlichen Offenbarungstatbestände gegeben sein (§ 67 SGB X), von denen hier nur § 75 Abs. 1 Nr. 2, Abs. 2 SGB X in Frage kommen kann, wonach eine Offenbarung personenbezogener Daten zulässig ist, soweit sie erforderlich ist für die Planung im Sozialleistungsbereich durch eine öffentliche Stelle im Rahmen ihrer Aufgaben. Zur Zeit fehlt ein konkretes Planungsvorhaben im Sozialleistungsbereich und darüber hinaus die nach § 75 Abs. 2 SGB X erforderliche Genehmigung durch die zuständige oberste Bundes- oder Landesbehörde.

Die Konsequenz ist, daß – solange keine Einwilligung der Betroffenen vorliegt – eine Übermittlung von Daten aus der Sozialhilfe nur in anonymisierter Form zulässig ist; d. h., die für die Statistik erforderlichen Daten dürfen nur ohne Namen (streng genommen auch ohne Geschäftszeichen) übermittelt werden. Die gegenwärtige Praxis ist deshalb bedenklich.

Im Hinblick darauf, daß das neue – automatisierte – Verfahren beschleunigt entwickelt und schon zum 1.1.1984 eingeführt werden sollte, habe ich die kurzfristige Fortsetzung des praktizierten rechtswidrigen Verfahrens hingenommen.

Die Entwicklung eines Konzepts für die „Landeseigene Sozialhilfestatistik" gestaltete sich aber so schwierig, daß mit der Einführung des Verfahrens am 1.1.1984 nicht zu rechnen ist. Bisher liegt erst der Rohentwurf eines Konzepts vor, der zwei alternative Lösungsmöglichkeiten aufzeigt. Beide Varianten sehen die Signierung der Statistikdaten durch die zuständigen Sozialhilfesachbearbeiter vor. Dem StaLa wird zur Auswertung mit den Statistikprogrammen lediglich ein Magnetband mit statistischen Daten (ohne Personenbezug) zur Verfügung gestellt. Die im Verhältnis zur Bundesstatistik zusätzlich in die statistische Auswertung einbezogenen Daten müssen nicht besonders erhoben werden, sondern sind auf den Leistungskarten bereits vorhanden.

Zwar habe ich gegen das Konzept – so wie es mir hier vorliegt – keine datenschutzrechtlichen Bedenken; aber es kann nicht hingenommen werden, daß das zu beanstandende bisher praktizierte Verfahren auf unabsehbare Zeit fortgesetzt wird, weil das neue Verfahren nicht oder erst sehr spät realisiert wird. Ich wiederhole hier meinen Hinweis, daß im Rahmen von § 80 SGB X die Möglichkeit besteht, die Auswertung der Leistungskarten durch das StaLa bzw. durch für das StaLa arbeitende Heimarbeiter auf der Grundlage einer Vereinbarung über die „Verarbeitung personenbezogener Daten im Auftrag" zu organisieren. Dafür ist erforderlich, daß der Auftraggeber (hier Sozialhilfedienststellen) dem Auftragnehmer, dessen Zuverlässigkeit im Sinne von § 80 SGB X, § 8 Abs. 1 BDSG der Auftraggeber zu prüfen hat, detaillierte Anweisungen für die Verarbeitung und für die vom Auftragnehmer zu treffenden technischen und organisatorischen Maßnahmen erteilt. Insbesondere hat der Auftraggeber darüber zu entscheiden, ob der für zuverlässig erachtete öffentliche Auftragnehmer seinerseits die Verarbeitung auf Stellen oder Personen, die nicht zum öffentlichen Bereich gehören, übertragen darf. Dies folgt aus § 80 Abs. 5 SGB X, wonach die Verarbeitung personenbezogener Daten im Auftrag durch nicht-öffentliche Stellen nur zulässig ist, wenn anders Störungen im Betriebsablauf nicht vermieden oder Teilvorgänge der automatischen Datenverarbeitung hierdurch erheblich kostengünstiger besorgt werden können. Da das Sozialgeheimnis von den **Sozialdienststellen** zu wahren ist, haben **sie** für alle Regelungen im Zusammenhang mit einer Auftragserteilung zur Datenverarbeitung durch andere die Verantwortung und **sie** haben darzulegen, ob die Voraussetzungen von § 80 Abs. 5 SGB X erfüllt sind, damit eine Verarbeitung durch Private überhaupt in Frage kommt. Die Auftragnehmer (StaLa und ggf. Heimarbeiter) dürfen nur im Rahmen der Weisungen handeln. Es versteht sich, daß die Organisation der Auftragsdatenverarbeitung schriftlich fixiert werden muß.

3. Einzelprobleme im öffentlichen Bereich

3.1 Neue Medien

3.1.1 Bildschirmtext

3.1.1.1 Darstellung des Systems

Das Bildschirmtextsystem bringt „Computerleistung in das Wohnzimmer"; es greift auf Einrichtungen zurück, die nahezu in jedem Haushalt vorhanden sind, nämlich Farbfernseher und Telefonanschluß sowie das Fernsprechnetz und bietet – nach Installation neuer Bildschirmtexteinrichtungen der Deutschen Bundespost (Leitzentrale und regionale Vermittlungsstellen) – folgende Dienste an:

- Abruf von Informationen z. B. Nachrichten, Lokales, Notdienste, kulturelle Programme
- Teilnahme an Computerspielen
- Dienstleistungen externer Rechner z. B. Warenbestellungen, Bankgeschäfte, Reisebuchungen
- Mitteilungen an Einzelne oder Mehrere (electronic mail)

Da die Kosten für die Zusatzeinrichtungen in den privaten Haushalten (Decoder, u. U. alphanumerische Tastatur) verhältnismäßig gering sein sollen (z. Z. noch um 1.500 , später um 500 DM), erwartet die Deutsche Bundespost rasch hohe Teilnehmerzahlen. Auch für geschäftliche Anwendungen (z. B. kann ein Reisender seine Geschäftsabschlüsse täglich an seine Firma übermitteln; das Bildschirmtextsystem kann sogar als firmeneigenes Datenverarbeitungsnetz – inhouse-Netz – benutzt werden) ist das Bildschirmtextsystem interessant. Aus datenschutzrechtlicher Sicht stehen jedoch die mit der Benutzung durch private Haushalte verbundenen Probleme im Vordergrund. Als Voraussetzung für die Erörterung der Datenschutzprobleme soll die Arbeitsweise des Bildschirmtextsystems stark vereinfacht beschrieben werden:

1. Für die Beteiligten am Bildschirmtextsystem werden folgende Begriffe verwendet:

   Der **Teilnehmer** nutzt das Bildschirmtextsystem, indem er Angebote abruft oder Einzelmitteilungen anderen Teilnehmern übermittelt.

   Der **Anbieter** stellt Informationen (Seiten) oder Leistungen externer Rechner zur Verfügung.

   Der **Betreiber** stellt die technische Infrastruktur für das Bildschirmtextsystem zur Verfügung und vermittelt die angebotenen Dienste (z. Z. nur die Deutsche Bundespost).

2. Der Teilnehmer wählt die nächstgelegene Vermittlungsstelle an. Beim Aufbau der Verbindung werden zur Vermeidung von Mißbrauch Kennungen abgefragt, u. a. ein vom Teilnehmer selbst vergebenes persönliches Kennwort.

3. Nach Aufbau der Verbindung bezeichnet der Teilnehmer die Dienste, die er in Anspruch nehmen möchte:

   - Abruf von Information oder Teilnahme an Computerspielen:
     In diesem Falle werden die entsprechenden „Seiten", wie die Informationen genannt werden, entweder aus der Vermittlungsstelle zur Verfügung gestellt, wenn der Anbieter sie dort eingespeichert hat, oder der Teilnehmer wird, wenn die Seiten in dem externen Rechner eines Anbieters gespeichert sind, zu diesem Rechner durchgeschaltet.

- Dienstleistungen externer Rechner:
  Der Teilnehmer wird zum externen Rechner des Anbieters, z. B. seiner Bank, durchgeschaltet.

- Mitteilungen an Einzelne oder Mehrere:
  Die Mitteilung wird gespeichert und ihr Vorhandensein dem Empfänger angezeigt, sobald er eine Verbindung zum Bildschirmtextsystem aufgebaut hat.

4. Während der Abwicklung der Dienste entstehen Daten:

   - über hergestellte Verbindungen bei der Deutschen Bundespost als Betreiber,

   - über abrechnungsrelevante Sachverhalte (die Deutsche Bundespost berechnet Gebühren, der Anbieter kann Seiten entgeltpflichtig machen) ebenfalls bei der Deutschen Bundespost,

   - im externen Rechner des Anbieters,

   - in der Form abgesandter Mitteilungen.

Das Bildschirmtextsystem wird ausführlich in der Broschüre „Bildschirmtext – Beschreibung und Anwendungsmöglichkeiten" der Deutschen Bundespost erläutert.

3.1.1.2 Situation in Hamburg

Das Bildschirmtextsystem ist in den Jahren 1980 bis 1983 in Feldversuchen in Berlin und Düsseldorf erprobt worden. Nach Sammlung ausreichender Erfahrungen hat die Deutsche Bundespost 1981 die Entscheidung für die bundesweite Einführung getroffen. Nach den ursprünglichen Planungen der Deutschen Bundespost sollte die bundesweite Einführung im September 1983 beginnen; Hamburg sollte nach diesen Planungen unter den ersten Ortsnetzen sein, die angeschlossen werden. Durch Verzögerungen in der Konzeption und Realisierung des Systems (für das bundesweite System konnten die in den Feldversuchen verwendeten Systeme nicht übernommen werden) verzögert sich der Beginn der bundesweiten Einführung bis etwa Mitte 1984. Nach den Planungen soll Hamburg weiterhin unter den ersten angeschlossenen Ortsnetzen sein. Bis zu diesem Termin hat die Deutsche Bundespost die Möglichkeit eröffnet, daß im norddeutschen Raum über einen in Hamburg installierten Einwählknoten bis zu 1.000 Teilnehmer an den Berliner Feldversuch angeschlossen werden.

3.1.1.3 Gefahren für den Datenschutz

Abb. 3 gibt eine Übersicht über die Gefahren, die von Bildschirmtext für die Privatsphäre ausgehen. In der ersten Spalte werden die Daten beschrieben, die im Bildschirmtextsystem erhoben und gespeichert werden. In der zweiten Spalte wird angegeben, welche Stelle die Daten speichert. In der dritten Spalte werden die Gefährdungen analysiert, die mit den Datenerhebungen und -speicherungen verbunden sind. In der vierten Spalte werden Vermutungen darüber angestellt, ob und in welchem Ausmaß der Teilnehmer Kenntnis von der Datenspeicherung hat und sich der Gefährdungen bewußt ist. Die Abbildung nimmt den in Nr. 2.6.4.2 entwickelten Ansatz auf und konkretisiert ihn für das Bildschirmtextsystem.

Die gespeicherten Daten und die Gefährdungspotentiale werden im folgenden – soweit nicht aus sich heraus verständlich – näher erläutert. Dabei muß zur Vermeidung von Mißverständnissen darauf hingewiesen werden, daß es sich um abstrakte und zudem maximale Annahmen handelt, die die Notwendigkeit der in den folgenden Schritten darzustellenden bereichsspezifischen Datenschutzregelungen belegen sollen. Aus der Darstellung dieser Datenschutzregelungen und der technischen Realisierung wird sich ergeben, daß diesen Gefahren bis auf wenige Ausnahmen wirksam begegnet wird.

Abb. 3: Übersicht über die Gefahren, die vom Bildschirmtextsystem für den Datenschutz ausgehen

Analyse der Gefahren / angebotene Dienste	gespeicherte Daten	speichernde Stelle	Gefährdungspotential	Kenntnis des Betroffenen
Mitteilungen an Einzelne oder Mehrere (electronic mail)	private und geschäftliche Mitteilungen	Betreiber (Deutsche Bundespost)	Offenbarung privater und geschäftlicher Geheimnisse, Kommunikationsmatrix	wenig wahrscheinlich
Abruf von Informationen (Seiten)	personenbezogene Daten (z.B. Biographien, Werbeaussagen)	Betreiber oder Anbieter (im externen Rechner)	Bekanntgabe an viele Teilnehmer	wahrscheinlich
Teilnahme an Spielen	Angaben über den Teilnehmer (z.B. Name, Anschrift, Alter, Beruf)	Betreiber und Anbieter	Verwendung für andere Zwecke, z.B. Werbung größere Offenbarungsbereitschaft in häuslicher Umgebung	nein nein
Dienstleistungen externer Rechner	Angaben über den Teilnehmer Daten über das Nutzungsverhalten	Anbieter	Verwendung für andere Zwecke, z.B. Werbung Persönlichkeitsprofil Individualisierung bisher anonymer Vorgänge größere Bereitschaft in häuslicher Umgebung	nein nein wenig wahrscheinlich nein
Bereitstellung aller Dienste	Angaben über den Teilnehmer Daten über vermittelte Dienste Daten über abrechnungsrelevante Sachverhalte	Betreiber	Persönlichkeitsprofil	nein

1. Mitteilungen an Einzelne oder Mehrere

   Dieser Dienst entspricht dem Transport von Briefen, also einem traditionellen Dienst der Post. Im Unterschied hierzu befindet sich der Inhalt jedoch nicht in einem verschlossenen Umschlag, sondern wird offen, den beteiligten Postbediensteten zugänglich, transportiert und gespeichert, vergleichbar der Postkarte und dem Telegramm. Die hierdurch entstehende höhere Gefahr der Offenbarung privater und geschäftlicher Geheimnisse wird dadurch relativiert, daß der Inhalt in magnetisierter Form gespeichert und transportiert wird und die mißbräuchliche Kenntnisnahme daher beträchtlichen Aufwand für das Sichtbarmachen erfordert.

   Eine andere Gefahr besteht darin, daß festgehalten wird, wann ein Teilnehmer welchem anderen Teilnehmer eine Mitteilung gesandt hat. Damit entsteht eine Kommunikationsmatrix (Ansatz zu einem Persönlichkeitsprofil).

2. Teilnahme an Spielen

   Die Gefahr, persönliche Daten im Zusammenhang mit der Teilnahme an Spielen mitzuteilen, wird dadurch erhöht, daß dies in der gewohnten häuslichen Umgebung und ohne nennenswerten Aufwand, hier im Wortsinne mit Knopfdruck, geschieht; denn auf Anforderung eines Anbieters setzt die Deutsche Bundespost den Namen und die Anschrift des Teilnehmers in die Seiten ein. Der Teilnehmer muß die Übersendung dieser Daten an den Anbieter zwar durch eine zusätzliche Entscheidung und Aktivität (Drücken der Tasten „1" und „9") veranlassen; das wird ihm aber sehr leicht gemacht. (Nur zur Klarstellung sei nochmals bemerkt, daß die Deutsche Bundespost von sich aus keine Daten des Teilnehmers an den Anbieter übermittelt.)

3. Dienstleistung externer Rechner

   Für die Verwendung von Daten für andere Zwecke gilt, daß es dem Anbieter bei geschicktem Vorgehen gelingen kann, dem Teilnehmer Daten zu entlocken, ohne daß dieser es bemerkt. Diese Gefahr ist nicht nur theoretisch, sondern in den Feldversuchen tatsächlich beobachtet worden. Die Deutsche Bundespost hat zwar aus diesen Erfahrungen heraus im neuen Btx-System Vorkehrungen vorgesehen, die den Teilnehmer vor Übervorteilung schützen sollen (z. B. weiße Taste, die alle Farben verschwinden läßt; kein Überschreiben der untersten Zeile); dennoch halte ich es auch weiterhin für notwendig, das Anbieterverhalten aufmerksam zu beobachten. Gerade für die Inanspruchnahme von Dienstleistungen externer Rechner gilt, daß die gewohnte häusliche Umgebung die Hemmschwelle herabsetzt und damit eine größere Bereitschaft vorhanden ist, etwas zu tun, was man sich sonst noch einmal überlegt.

   - Der Anbieter kann die abrufbaren Seiten auch in seinem externen Rechner speichern, anstatt sie in die Btx-Zentralen der Deutschen Bundespost einzuspeichern. Wenn er den Teilnehmer dazu veranlassen konnte, seine Daten zu übermitteln, so daß er ihn identifizieren kann, kann der Anbieter personenbezogen speichern, in welcher Weise der Teilnehmer die Seiten nutzt, z. B. welche Seiten hat er wie lange betrachtet, welche Geschicklichkeit hat er bei seinem Weg durch das Angebot bewiesen. Über längere Zeit hinweg können daraus Persönlichkeitsprofile entstehen, die der Anbieter für seine Geschäftsbeziehungen mit dem Teilnehmer nutzen kann.

     Diese Gefahr wird dadurch relativiert, daß der Aufwand an Speicherkapazität für die beschriebenen detaillierten Aufzeichnungen beträchtlich ist, ohne daß ihm ein entsprechend hoher Nutzen aus der Datenspeicherung gegenüber stehen dürfte.

   - Wenn bisherige Geschäfte künftig über Btx abgewickelt werden, werden diese bisher anonymen Vorgänge individualisiert; z. B. wird beim Lesen der Zeitung über Btx nicht nur erkennbar, welche Zeitung ein Teilnehmer liest, sondern auch, wel-

chen Artikel er wie lange liest, was bisher in der persönlichen Sphäre blieb. Auf die geschilderte Art kann, wenn Btx die bisher gewohnten Barkäufe verdrängt, ein bedeutender Teil des Lebensverhaltens der einzelnen Bürger transparent werden.

4. Für alle Dienste gilt, daß bei der Deutschen Bundespost als Betreiber neben den Daten über den Teilnehmer Daten über alle vermittelten Dienste und über abrechnungsrelevante Sachverhalte entstehen. Diese Daten beschreiben das Nutzungsverhalten jedes Teilnehmers:
   Welche Dienste werden wann in Anspruch genommen, welche Seiten werden wann wie lange abgerufen, welcher Weg wurde durch das Angebot genommen.

Im Vergleich zu den eben beschriebenen Möglichkeiten eines Anbieters ist jedoch der Umfang der Datensammlungen, die bei der Deutschen Bundespost entstehen, ungleich größer, weil Daten über die Kommunikation **eines** Teilnehmers mit **allen** Anbietern, deren Dienste er in Anspruch nimmt, anfallen: Bevorzugt abgerufene Angebotsseiten, Konsumgewohnheiten, Geldgeschäfte, Anwesenheitszeiten im Haus, besondere Hobbys, die Geschicklichkeit beim Weg durch das Angebot u. a. m. Es besteht die Gefahr, daß hieraus umfassende und aussagekräftige Persönlichkeitsprofile entwickelt werden; diese Gefahr wird aber durch den großen Aufwand für die (dauerhafte) Speicherung der Daten relativiert.

3.1.1.4 Regelungsdefizite des Bundesdatenschutzgesetzes und Notwendigkeit bereichsspezifischer Regelungen

In der Abb. 4 sind den in Abb. 3 dargestellten Gefährdungen die entsprechenden Regelungen des Bundesdatenschutzgesetzes gegenübergestellt worden. Dabei war das BDSG zugrundezulegen, weil die Deutsche Bundespost (Betreiber) als Bundesbehörde unter das BDSG fällt und auch die privaten Anbieter unter das BDSG fallen. Das HmbDSG wäre auf die öffentlichen Anbieter anzuwenden, die Behörden der Freien und Hansestadt Hamburg oder der Aufsicht der Freien und Hansestadt Hamburg unterstehende juristische Personen des öffentlichen Rechts sind; diese Anbieter werden voraussichtlich weder nach der Zahl noch nach der Menge oder des Inhalts ihrer Angebote ins Gewicht fallen.

Die entsprechenden Regelungen des BDSG konnten nur summarisch beschrieben werden; die Angaben werden im folgenden erläutert:

1. Mitteilungen an Einzelne oder Mehrere

   Es ist schon fraglich, ob das BDSG anzuwenden ist, weil andere Rechtsvorschriften gem. § 45 BDSG vorgehen. In Betracht kommen könnten das in § 45 Nr. 1 genannte Fernmeldeanlagengesetz und die Fernmeldeordnung. Diese Frage wird an anderer Stelle wieder aufgenommen.

   Weiterhin ist fraglich, ob das BDSG gilt, weil die Einzelmitteilungen möglicherweise nicht in Dateien gespeichert sind. Aber selbst wenn das BDSG anzuwenden wäre, bliebe die in § 14 vorgesehene Regelung der Sperrung und Löschung unbefriedigend.

2. Abruf von Informationen

   Die Aufnahme von personenbezogenen Daten in ein Angebot erfüllt für sich genommen nicht den datenschutzrechtlichen Tatbestand des Speicherns in Dateien. Weder die einzelne Angebotsseite noch die Angebotsseiten eines Anbieters zusammengenommen und auch nicht die Vielzahl der von einem Betreiber zum Abruf bereitgehaltenen Angebote genügen allen Merkmalen des Dateibegriffs. Daher wird die Speicherung von personenbezogenen Daten in Angeboten vom BDSG nicht erfaßt.

Abb. 4: Regelungen des Bundesdatenschutzgesetzes für die aufgezeigten Sachverhalte

Analyse der Gefahren / angebotene Dienste	gespeicherte Daten	speichernde Stelle	Gefährdungspotential	Kenntnis des Betroffenen	Regelungen des BDSG
Mitteilungen an Einzelne oder Mehrere (electronic mail)	private und geschäftliche Mitteilungen	Betreiber (Deutsche Bundespost)	Offenbarung privater und geschäftlicher Geheimnisse Kommunikationsmatrix	wenig wahrscheinlich	nur, wenn in Dateien gespeichert: § 9 Abs. 1 Speicherbefugnis § 14 Abs. 2 Satz 2 Sperrung § 14 Abs. 3 Löschung
Abruf von Informationen (Seiten)	personenbezogene Daten (z.B. Biographien, Werbeaussagen)	Betreiber oder Anbieter (im externen Rechner)	Bekanntgabe an viele Teilnehmer	wahrscheinlich	wird vom BDSG nicht erfaßt, weil keine Speicherung in einer Datei
Teilnahme an Spielen	Angaben über den Teilnehmer (z.B. Name, Anschrift, Alter, Beruf)	Betreiber und Anbieter	Verwendung für andere Zwecke, z.B. Werbung größere Offenbarungsbereitschaft in häuslicher Umgebung	nein nein	Erhebung wird vom BDSG nicht erfaßt; bei Speicherung in Dateien: §23 (weitgehende) Speicherbefugnis
Dienstleistungen externer Rechner	Angaben über den Teilnehmer Daten über das Nutzungsverhalten	Anbieter	Verwendung für andere Zwecke, z.B. Werbung Persönlichkeitsprofil Individualisierung bisher anonymer Vorgänge größere Bereitschaft in häuslicher Umgebung	nein nein wenig wahrscheinlich nein	Erhebung wird vom BDSG nicht erfaßt; bei Speicherung in Dateien: § 23 (weitgehende) Speicherbefugnis § 27 Abs. 2 S. 2 Sperrung § 27 Abs. 3 Löschung
Bereitstellung aller Dienste	Angaben über den Teilnehmer Daten über vermittelte Dienste Daten über abrechnungsrelevante Sachverhalte	Betreiber	Persönlichkeitsprofil	nein	fraglich, ob vom BDSG erfaßt; wenn Speicherung in Dateien: § 9 Abs. 1 Speicherbefugnis § 14 Abs. 2 Satz 2 Sperrung § 14 Abs. 3 Löschung

3. Teilnahme an Dienstleistungen externer Rechner

Die Speicherung personenbezogener Daten in einer Datei ist nach dem BDSG nur zulässig, wenn entweder ein gesetzlicher Erlaubnistatbestand erfüllt ist oder wenn der Betroffene eingewilligt hat.

Ob diese Voraussetzungen vorliegen, hat die speichernde Stelle (hier der Anbieter) jeweils vor der Speicherung zu prüfen. Nach der Vorstellung des Gesetzgebers ist der Vorgang des Erhebens von Daten bei dem Betroffenen von dem Vorgang des Erfassens, Aufnehmens und Aufbewahrens von Daten auf einem Datenträger zum Zwecke weiterer Verwendung (Speicherung) zu unterscheiden. Auf diese Weise wird zwischen dem nicht geschützten Vorgang der Datenerhebung und dem geschützten Vorgang des Speicherns eine Filterfunktion geschaltet, die den Betroffenen davor bewahrt, daß Daten, die zwar erhoben wurden, aber nicht gespeichert werden dürfen, gleichwohl gespeichert werden. Diese Funktion fällt aus, wenn der Betroffene selbst seine Daten in das Verarbeitungssystem einbringt und damit automatisch der datenschutzrechtliche Tatbestand des Speicherns erfüllt wird, etwa wenn er erstmals mit einem Anbieter Kontakt aufnimmt, zu diesem Zweck seine Daten in eine Antwortseite einfügt, die Seite absendet und diese Daten sodann vom Anbieter in Dateiform gespeichert werden.

Das aus § 3 BDSG abzuleitende prinzipielle Verbot, personenbezogene Daten in Dateien zu speichern oder aus Dateien zu übermitteln, sofern es nicht schon durch tatbestandmäßig fixierte Erlaubnisse durchbrochen ist, steht letztlich unter dem allgemeinen datenschutzrechtlichen Abwägungsvorbehalt. Das heißt, die Speicherung oder die Übermittlung ist erlaubt, wenn sie zur Wahrung berechtigter Interessen der speichernden Stelle oder eines Dritten oder der Allgemeinheit erforderlich ist und schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden (§§ 23, 24 BDSG).

Der Schutz der im Bildschirmtextsystem gespeicherten Daten hätte hier eine breite offene Flanke, wenn sich nicht die Ansicht durchsetzte, daß das Interesse des Betroffenen einer Verarbeitung seiner im Bildschirmtextsystem anfallenden Daten ausnahmslos oder doch wenigstens grundsätzlich entgegensteht. Sonst ginge der Teilnehmer, der Daten abgibt oder die Erhebung von Daten in sonstiger Weise ermöglicht, ein erhebliches Risiko ein.

Das BDSG stellt die Einwilligung des Betroffenen den gesetzlichen Erlaubnistatbeständen gleich, läßt aber im Hinblick auf den Schutz des Betroffenen, der durch seine Einwilligung einen eigenständigen Rechtsgrund für die Verarbeitung seiner Daten schafft, vieles offen. Ungeklärt ist vor allem, in welchem Verhältnis die Einwilligung zu den Erlaubnistatbeständen steht und welche Anforderungen an die Einsicht des Einwilligenden in die Bedeutung und Tragweite seiner Erklärung und der Versagung von Leistungen zu stellen sind, falls er die begehrte Einwilligung verweigert. Wäre es mangels entsprechender Schutzvorschriften den Anbietern erlaubt, ihre Leistungen im Bildschirmtextsystem von einer Einwilligung des Betroffenen in die Verarbeitung seiner Daten abhängig zu machen und zugleich die Anforderungen an eine zureichende Aufklärung des Betroffenen niedrig zu halten, so könnte damit der Datenschutz weitgehend unterlaufen werden.

Das BDSG sieht für eine wirksame Einwilligung des Betroffenen in die Verarbeitung seiner Daten die Schriftform vor, gestattet aber wegen besonderer Umstände eine andere angemessene Form. Es läßt sich nicht von vornherein ausschließen, daß auch die Art der Kommunikation einen besonderen Umstand i. S. dieser Vorschrift bildet. Demgegenüber dürfte es schwerfallen, das Gebot der Schriftform bei der Bildschirmkommunikation allein mit ihrer Warnfunktion zu begründen. Doch muß man sehen, daß, wenn man die Erklärung der Einwilligung sinnvollerweise über Bildschirmtext zuläßt, die Warnfunktion entfällt. Dies ist im Hinblick auf Datenverarbeitungsvorgänge,

bei denen der Betroffenen nicht zuletzt wegen der Umstände und der Tragweite der Einwilligungserklärung auf eine entsprechende Warnung besonders angewiesen ist, besonders bedenklich.

4. Bereitstellung aller Dienste

   Nach § 3 BDSG ist Voraussetzung für die Speicherung unter anderem eine gesetzliche Erlaubnis. Keiner der gesetzlichen Erlaubnistatbestände eignet sich indessen dazu, die Besonderheit der Bildschirmtextkommunikation in sich aufzunehmen, die in der Notwendigkeit vorübergehender, d. h. zum Aufbau bzw. der Abwicklung des Kommunikationsvorgangs erforderlicher, Speicherung personenbezogener Daten liegt. Sie sind vielmehr so gefaßt, daß sie die Speicherung entweder auf Dauer erlauben oder daß es bei dem Verbot jeglicher Speicherung bleibt.

   Entschiedener als bei anderen DV-Anwendungen, deren Mißbrauchsrisiko für den Betroffenen geringer eingeschätzt werden kann, ist bei den im Rahmen von Btx erhobenen und gespeicherten Daten zu fordern, daß sie gelöscht werden, sobald sie ihren Zweck erfüllt haben und nicht mehr benötigt werden (z. B. nach Beendigung der Kommunikation, nach Eingang geschuldeter Entgelte). Anders als das HmbDSG schreibt das BDSG für solche Fälle die Löschung nicht zwingend vor, sondern die speichernde Stelle ist zur Löschung nur dann verpflichtet, wenn die Daten zur Erfüllung des Speicherungszwecks nicht mehr erforderlich sind und der Betroffene die Löschung ausdrücklich verlangt oder wenn die Speicherung unzulässig war. Sonst sind die Daten lediglich zu sperren.

Aus dieser Analyse ergibt sich, daß das als Auffangnorm anzuwendende BDSG erhebliche Regelungsdefizite hat; bereichsspezifische Datenschutzvorschriften sind mithin unabdingbar.

3.1.1.5 Datenschutzregelungen im Staatsvertrag über Bildschirmtext

Die Notwendigkeit bereichsspezifischer Datenschutzregelungen für den Bildschirmtext wurde frühzeitig erkannt. Der am 18.3.1983 von den Bundesländern abgeschlossene Staatsvertrag enthält neben anderen Vorschriften (z. B. Begriffsbestimmungen, Beteiligung am Btx, Geltungsbereich, Entgelt, Anbieterkennzeichnung, Sorgfaltspflicht, Gegendarstellung, Werbung und Angebotszuordnung, Meinungsumfragen, Verwaltungsbehörden einschl. Zuständigkeit, Ordnungswidrigkeiten) auch Bestimmungen über den Datenschutz. Die Datenschutzbeauftragten haben bei der Erarbeitung dieser Bestimmungen mitgewirkt.

In Abb. 5 sind – entsprechend dem Vorgehen in der Abb. 4 – den Gefährdungen durch Btx (s. Abb. 3) die entsprechenden Regelungen des Staatsvertrags gegenübergestellt. Aus der Gegenüberstellung ergibt sich, daß die Regelungen des Staatsvertrages die Defizite weitgehend ausgleichen, die sich aus der Anwendung des BDSG ergeben würden.

Die Datenschutzbestimmungen des Staatsvertrages werden im folgenden näher erläutert. Dabei wird auch – soweit erforderlich – darauf eingegangen, inwieweit das von der Deutschen Bundespost entwickelte System den Bestimmungen des Staatsvertrages entspricht (hierzu muß jedoch der Vorbehalt gemacht werden, daß die Kenntnis der technischen Vorgänge auf mündlichen Erläuterungen der Deutschen Bundespost beruht; Zusagen, daß ergänzende schriftliche Unterlagen nachgereicht werden, hat die Deutsche Bundespost bis zum Redaktionsschluß dieses Tätigkeitsberichtes nicht eingehalten).

1. Generell, d. h. für alle Dienste und für Betreiber und Anbieter gilt folgendes:

   - Art. 9 Abs. 1 bestimmt, daß die jeweils geltenden Vorschriften über den Schutz personenbezogener Daten anzuwenden sind, soweit der Staatsvertrag nichts an-

Abb. 5: Regelungen des Staatsvertrages über Bildschirmtext für die aufgezeigten Sachverhalte

Analyse der Gefahren / angebotene Dienste	gespeicherte Daten	speichernde Stelle	Gefährdungspotential	Kenntnis des Betroffenen	Regelungen des Staatsvertrages generell:	
					Art. 9 Abs. 1	subsidiäre Geltung des allgemeinen Datenschutzrechts
					Art. 9 Abs. 7	Rechte des Betroffenen
					Art. 9 Abs. 8	Verpflichtung zu Datensicherungsmaßnahmen
					Art. 10	Geheimhaltung
Mitteilungen an Einzelne oder Mehrere (electronic mail)	private und geschäftliche Mitteilungen	Betreiber (Deutsche Bundespost)	Offenbarung privater und geschäftlicher Geheimnisse Kommunikationsmatrix	wenig wahrscheinlich	Art. 10 Art. 9 Abs. 4	Geheimhaltung Speicherung und Löschung der Verbindungs- und Abrechnungsdaten (§ 38b Abs. 5 Fernmeldeordnung, Löschung der Mitteilungen nach max. 60 Tagen)
Abruf von Informationen (Seiten)	personenbezogene Daten (z. B. Biographien, Werbeaussagen)	Betreiber oder Anbieter (im externen Rechner)	Bekanntgabe an viele Teilnehmer	wahrscheinlich	Art. 9 Abs. 5	Btx-Angebot gilt als Datei Die für Übermittlungsvorgänge geltenden Vorschriften des Datenschutzes sind anzuwenden und vom Anbieter zu beachten
Teilnahme an Spielen	Angaben über den Teilnehmer (z. B. Name, Anschrift, Alter, Beruf)	Betreiber und Anbieter	Verwendung für andere Zwecke, z. B. Werbung größere Offenbarungsbereitschaft in häuslicher Umgebung	nein nein	Art. 9 Abs. 6	Abfrage (= Erhebung) und Speicherung von Daten nur - soweit dies für das Erbringen der Leistung, den Abschluß oder die Abwicklung eines Vertrages erforderlich ist. Verarbeitung dieser Daten nur - im Rahmen der Zweckbestimmung des Vertrages oder der Leistung; darüberhinaus nur aufgrund Einwilligung Aufklärung über die Bedeutung der Einwilligung Mit Ausnahme der Kreditgeschäfte: Die Leistung, der Abschluß oder die Abwicklung eines Vertragsverhältnisses dürfen nicht von der Einwilligung abhängig gemacht werden. Einwilligung über Bildschirmtext wird nur nach Bestätigung wirksam.
Dienstleistungen externer Rechner	Angaben über den Teilnehmer Daten über das Nutzungsverhalten	Anbieter	Verwendung für andere Zwecke, z. B. Werbung Persönlichkeitsprofil Individualisierung bisher anonymer Vorgänge Größere Bereitschaft in häuslicher Umgebung	nein nein wenig wahrscheinlich nein	Art. 9 Abs. 8 Nr. 2	Sicherstellung, daß der Teilnehmer Daten nur durch eine bewußte und eindeutige Handlung übermitteln kann
Bereitstellung aller Dienste	Angaben über den Teilnehmer Daten über vermittelte Dienste Daten über abrechnungsrelevante Sachverhalte	Betreiber	Persönlichkeitsprofil	nein	Art. 9 Abs. 2	Abfrage und Speicherung von Daten nur, soweit und so lange für - Vermittlung des Abrufs von Angeboten (Verbindungsdaten), - Abrechnung von Gebühren und Entgelten (Abrechnungsdaten) erforderlich.
					Art. 9 Abs. 3	Speicherung der Abrechnungsdaten nur mit Einverständnis des Teilnehmers in detaillierter Form. Übermittlung der Abrechnungsdaten nur aufgrund besonderer Rechtsvorschrift oder an den Anbieter zur Betreibung. Übermittlung der Verbindungsdaten unzulässig. Löschung der Abrechnungsdaten, wenn für Zwecke der Abrechnung nicht mehr erforderlich. Löschung der Verbindungsdaten nach Ende der jeweiligen Verbindung.
					Art. 9 Abs. 7 Satz 4	Anspruch des Betroffenen auf Löschung der Verbindungs- und Abrechnungsdaten
					Art. 9 Abs. 8 Nr. 1	Sicherstellung, daß Verbindungsdaten gelöscht werden

deres bestimmt. Infrage kommen vor allem die Vorschriften über die Rechte des Betroffenen.

- Art. 9 Abs. 7 wiederholt, daß die Rechte des Betroffenen nach dem allgemeinen Datenschutzrecht unberührt bleiben, und regelt, wer Adressat der Ansprüche ist.

- Art. 10 verpflichtet – vergleichbar dem Datengeheimnis nach § 5 BDSG und entsprechenden Bestimmungen der Landesdatenschutzgesetze – die bei den Btx-Einrichtungen der Anbieter und Betreiber tätigen Personen zur Geheimhaltung der ihnen bei ihrer Tätigkeit bekanntgewordenen Tatsachen, soweit diese nicht offenkundig sind oder ihrer Natur nach der Geheimhaltung nicht bedürfen. Diese Geheimhaltungsverpflichtung geht über das Datengeheimnis z. B. nach § 5 BDSG hinaus, weil es nicht an die Verarbeitung in Dateien gebunden ist; sie bleibt hinter dem Datengeheimnis zurück, weil sie offenkundige und solche Daten, die ihrer Natur nach nicht geheimhaltungsbedürftig sind, ausnimmt. Die Notwendigkeit der Ausnahme wird auch in der amtlichen Begründung zum Staatsvertrag nicht erläutert; ich werde die Praxis aufmerksam beobachten und mich dazu äußern, ob Anlaß zu einer Revision dieser Bestimmung besteht.

- Infolge der subsidiären Geltung des allgemeinen Datenschutzrechts sind die Betreiber und Anbieter verpflichtet, Datensicherungsmaßnahmen zu treffen (§ 6 BDSG und entsprechende Bestimmungen der Landesdatenschutzgesetze). Art. 9 Abs. 8 verpflichtet Betreiber und Anbieter **darüber hinaus** zu speziellen, Btx-spezifischen Datensicherungsmaßnahmen. Art. 9 Abs. 8 Nr. 3 fordert, daß zum Zwecke der Datensicherung vergebene Codes dem Stand der Technik entsprechen müssen. Hieraus ergibt sich zweierlei: a) Es müssen Codes vergeben werden, z. B. beim Verbindungsaufbau, b) die Code-Verfahren sind ständig darauf zu überprüfen, ob sie entsprechend der technischen Entwicklung verbessert werden müssen.

2. Mitteilungen an Einzelne oder Mehrere

   § 38b der Fernmeldeordnung schreibt die Löschung der Mitteilungen nach spätestens 60 Tagen vor.

   Art. 9 Abs. 4 schreibt in Verbindung mit Art. 9 Abs. 2 und 3 vor, daß

   - Verbindungs- und Abrechnungsdaten nur so lange gespeichert werden dürfen, wie dies für den Verbindungsaufbau und die Abrechnung erforderlich ist (Verbindungsdaten sind Adressat und Absender sowie der Zeitpunkt der Absendung – zur Berechnung der Löschungsfrist; Abrechnungsdaten sind der Absender und die Seitenzahl – nach ihr richtet sich die Gebühr);

   - Verbindungsdaten zu löschen sind, wenn der Adressat die Mitteilung gespeichert oder gelöscht hat, spätestens nach 60 Tagen entsprechend § 38b Fernmeldeordnung;

   - Abrechnungsdaten nicht detailliert gespeichert werden dürfen und gelöscht werden müssen, sobald der Absender die Gebühren bezahlt hat.

   Durch diese Vorschriften wird das Entstehen einer Kommunikationsmatrix verhindert.

3. Abruf von Informationen

   Art. 9 Abs. 5 schreibt die Anwendung und Beachtung der Vorschriften des BDSG für die Übermittlung vor; durch die Fiktion, das Btx-Angebot gelte als Datei, ist ein Regelungs-Defizit des BDSG ausgeglichen.

4. Teilnahme an Dienstleistungen externer Rechner (Art. 9 Abs. 6)

Die empfindlichen Defizite des BDSG sind ausgeglichen:

- Die Abfrage, d. h. die btx-spezifische Form der Erhebung, ist ausdrücklich in die Regelung einbezogen worden.

- Die erhobenen Daten unterliegen einer bestimmten Zweckbindung (Verarbeitung nur zulässig, soweit für das Erbringen der Leistung, den Abschluß oder die Abwicklung eines Vertragsverhältnisses erforderlich).

- Außerhalb der Zweckbindung dürfen **keine** Daten erhoben und gespeichert werden.

- Die Verwendung der Daten außerhalb der Zweckbindung bedarf der Einwilligung des Betroffenen.

- Die Einwilligung darf nicht erzwungen werden; Ausnahme: Kreditgeschäfte.

- An die Einwilligung werden besondere Anforderungen gestellt; insbesondere muß sie vom Betroffenen auf andere Weise (z. B. schriftlich) bestätigt werden, wenn sie über Btx abgegeben worden ist.

Bedenken habe ich gegen die Ausnahme bei Kreditgeschäften. Für die Abfrage der Kreditwürdigkeit bei Abschluß eines Kreditvertrages bedarf es keiner Einwilligung. Die Ausnahme hat nur den Zweck, den Betroffenen zur Einwilligung in die Übermittlung der Daten über die Abwicklung des Kreditgeschäftes an die Schufa zu zwingen. Damit wird das derzeit praktizierte Informationssystem der Schufa gesetzlich bestätigt, das ich indessen für überprüfungsbedürftig halte. Meine Bedenken richten sich nicht prinzipiell gegen die Übermittlung von Daten über die Abwicklung von Kreditgeschäften, sondern gegen eine Absicherung der gegenwärtigen Praxis.

Bedenken bestehen auch dagegen, daß die Daten des Teilnehmers nach Erbringen der Leistung oder nach Abwicklung des Vertragsverhältnisses nur gesperrt und nicht gelöscht werden **müssen** (§ 27 Abs. 2 Satz 2, § 27 Abs. 3 Satz 1 BDSG, die subsidiär gelten). Es wäre nach meiner Ansicht besser gewesen, Art. 9 Abs. 6 des Staatsvertrages hätte die Löschung dieser Daten vorgeschrieben.

5. Bereitstellung aller Dienste

Die Bestimmungen des Staatsvertrages für die Speicherung der Verbindungs- und Abrechnungsdaten gleichen die Defizite des BDSG insgesamt aus, wenn man darüber hinaus die technische Lösung des Btx-Systems berücksichtigt.

- Die Regelungen für die Verbindungsdaten sind eindeutig und streng:

  Speicherung nur für den Verbindungsaufbau.
  Keine Übermittlung.
  Löschung nach Ende der Verbindung.

  Damit wird der Gefahr wirksam begegnet, daß umfassende und aussagekräftige Persönlichkeitsprofile entstehen. Diese Gefahr war – das darf ich in Erinnerung rufen – bei den Verbindungsdaten besonders groß, weil beim Betreiber Daten über alle in Anspruch genommenen Dienste anfallen.
  Die technische Lösung des Btx-Systems sieht überdies vor, daß die Verbindungsdaten nur als Prozeßdaten während der Verbindung im Hauptspeicher und daß auch nur die jeweils aktuellen Daten gespeichert werden.

- Die Regelung für die Abrechnungsdaten ist weiter gefaßt. Die technische Lösung des Btx-Systems nutzt jedoch diesen Spielraum nicht aus. Die Abrechnungsdaten werden – gerade bei entgeltpflichtigen Angeboten – so pauschal gespeichert, daß Persönlichkeitsprofile nicht entstehen können. Die Deutsche Bundespost kann das Angebot des Staatsvertrages (Art. 9 Abs. 3 Satz 1) nicht einlösen, auf Wunsch des Teilnehmers Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit bestimmter in Anspruch genommener Angebote zu speichern.

- Die Übermittlung der Abrechnungsdaten ist u. a. aufgrund besonderer Rechtsvorschriften zulässig. Besondere Rechtsvorschriften sind nach meiner Auffassung nur solche, die ausdrücklich auf den Btx-Staatsvertrag Bezug nehmen. Aufgrund der bisherigen Durchbrechungen des Fernmeldegeheimnisses etwa dürften Übermittlungen von Daten aus den technischen Einrichtungen der Bundespost nicht erfolgen.

- Die Übermittlung an den Anbieter ist zulässig, soweit eine Forderung auch nach Mahnung nicht beglichen wird. Die Deutsche Bundespost übernimmt das Inkasso der den Anbietern zustehenden Entgelte nur bis zur Beitreibung. Meine Bedenken gegen diese Regelung sind dadurch geringer geworden, daß die Deutsche Bundespost in diesen Fällen dem Anbieter nur den Namen des Teilnehmers und den Betrag der Forderung in einer Summe mitteilt. Nur wenn es zu einer streitigen Auseinandersetzung kommt, teilt die Deutsche Bundespost nicht den Anbietern, sondern dem Gericht den Zeitpunkt der Entstehung der Forderung mit.

Während der materielle Gehalt der Datenschutzbestimmungen über die Verbindungs- und Abrechnungsdaten nach meiner Ansicht ausreichend ist, sehe ich die Sonderstellung der Deutschen Bundespost als problematischer an. Als Bundesbehörde fühlt sie sich durch die Bestimmungen des Staatsvertrages – als Landesrecht – nicht gebunden. Der Staatssekretär im Bundesministerium für das Post- und Fernmeldewesen hat aber erklärt, daß sich die Deutsche Bundespost an die Bestimmungen des Staatsvertrages halten und sie in entsprechende Bestimmungen der Fernmeldeordnung und interner Verwaltungsvorschriften umsetzen werde. Die Fernmeldeordnung ist inzwischen geändert worden; weitere Regelungen stehen noch aus.

Auch wenn die Bundespost dadurch und durch die technische Gestaltung des Btx-Systems die Zusage einhält, sie werde sich an die Bestimmungen des Staatsvertrages halten, bleibt bedenklich, daß die Bindung von der Bereitwilligkeit der Deutschen Bundespost abhängig ist.

3.1.1.6 Überwachung durch den Datenschutzbeauftragten

Insgesamt sind die Datenschutzbestimmungen des Staatsvertrages ein Beispiel für gelungene bereichsspezifische Datenschutzvorschriften, das sich durchaus auch als Vorbild für entsprechende Regelungen bei anderen neuen Medien eignet (vgl. Nr. 3.1.2.3 in diesem Bericht).

Meine Aufgabe liegt jetzt darin, die Umsetzung und Einhaltung dieser Vorschriften in der Praxis zu überwachen. Ich werde meine Aufmerksamkeit insbesondere auf folgende Punkte lenken:

- Keine unzulässige Erhebung von Daten des Teilnehmers, z. B. beim Abruf von Katalogen oder dgl.

- Trennung von Angeboten und Bestelldiensten

- Kein „Überlisten" der Teilnehmer

- Erfüllung der Anforderungen an die Einwilligung

Allgemein gebe ich allen Btx-Teilnehmern den Rat, bei der Inanspruchnahme aller Dienste stets überlegt zu handeln und bei der Preisgabe von Daten Zurückhaltung zu üben.

3.1.2 Andere Medien

3.1.2.1 Kabelkommunikation

Der neue Dienst Bildschirmtext benutzt als Transportweg vorhandene Netze, nämlich das Fernsprechnetz für die Verbindung zu den Teilnehmern und das Datex-P-Netz für den Anschluß externer Rechner. Da Bildschirmtext vorhandene Infrastruktur nutzt, kann das System so preiswert sein.

Die weiteren Dienste,
- Kabelfernsehen,
- Pay-TV,
- offene Kanäle,
- Rückkanäle,
- Kabeltext,
- Fernwirkdienste (s. Nr. 3.1.2.2),

benötigen neue Transportwege, weil die vorhandene Infrastruktur nicht ausreicht. Dieser neue Transportweg sind die Breitbandkabel (Kupferkoaxial- oder Glasfaserkabel), bekannt unter dem Schlagwort „Verkabelung".

In der Vergangenheit sind Kabel überwiegend verlegt worden, um den Fernsehempfang in benachteiligten Gebieten („Abschattungsgebiete") zu verbessern. In den letzten Jahren sind zunehmend auch andere Nutzungen auf der Basis von Kabeln diskutiert worden, eben die oben erwähnten weiteren Dienste. Da die – im weitesten Sinne – gesellschaftspolitischen Auswirkungen der Kabelkommunikation umstritten sind, gibt es – vergleichbar den Feldversuchen bei Btx – Kabelpilotprojekte in Berlin, Dortmund, Ludwigshafen und München. Mit den Pilotprojekten sollen die Erkenntnisse gewonnen werden, die für die Entscheidung über eine bundesweite Einführung notwendig sind. Die Deutsche Bundespost betreibt unabhängig hiervon die Verlegung von Kupferkoaxialkabeln z. B. auch in Hamburg.

Die wirtschaftlichen Aussichten der Kabelkommunikation und der auf ihr basierenden neuen Dienste werden zunehmend kontrovers diskutiert. Es mehren sich skeptische Stimmen, die angesichts hoher Anschluß- und auch laufender Kosten davor warnen, das Teilnehmerpotential zu überschätzen. Hohe Teilnehmerzahlen sind aber eine notwendige Voraussetzung für die Rentabilität der Kabel und der Dienste.

Die Risiken für die Privatsphäre, die mit der Einführung der neuen Dienste verbunden sind, sind in der Abb. 2 skizziert. Wie bereits unter Nr. 2.6.4.2 ausgeführt, sind die konkreten Gefährdungen von der technischen Gestaltung abhängig. Bei den verwandten Diensten Kabelfernsehen und Pay-TV z. B. ist die Gefährdung davon abhängig, wo die „Verteileinrichtung" (d. h. die Einrichtung, die die über Kabel ankommenden Sendungen nach den Wünschen der Teilnehmer auf diese verteilt) installiert wird. Bei den heutigen Fernsehgeräten befindet sich die Verteileinrichtung im Gerät; dort wird aus den über die Luft und die Antenne transportierten Programmen das ausgewählt, das empfangen werden soll. Bei der Kabelkommunikation scheint sich das Modell durchzusetzen, daß die Verteileinrichtung außerhalb des Teilnehmerbereichs für mehrere Teilnehmer zusammengefaßt wird. Dann wären die Verteileinrichtungen mit den Btx-Vermittlungsstellen vergleichbar; in ihnen entstehen Verbindungs- und Abrechnungsdaten wie im Btx-System. Aus der Sicht des Datenschutzes sind daher auch die Gefährdungen vergleichbar (Entstehung von Persönlichkeitsprofilen). Ihnen kann mit dem BDSG oder mit den Landesdatenschutzgesetzen nicht wirksam begegnet werden, wie die eingehende Analyse am Beispiel Btx gezeigt hat (s. Nr. 3.1.1.4). Deshalb sind auch für die Kabelkommunikation bereichsspezifische Datenschutzbestimmungen erforderlich.

3.1.2.2 Fernwirkdienste

Unter den sich abzeichnenden weiteren Diensten nehmen die Fernwirkdienste wegen des damit verbundenen Eindringens in die private Sphäre eine besondere Stellung ein. Unter Fernwirkdiensten (Fernwirken, Fernmessen) werden Dienste verstanden, die von außen in der Wohnung eines Teilnehmers

- Wirkungen auslösen, z. B. Unterbrechen des laufenden Programms oder Anschalten des Fernsehers für wichtige Meldungen;

- Messungen anstellen, z. B. Ablesen des Strom-, Gas-, Wasserverbrauchs, gesundheitliche Messungen;

- Beobachtungen machen, z. B. überwachen Eltern von unterwegs das Wohlbefinden ihres Säuglings.

In München sind die Fernwirkdienste für die Endphase des Kabelpilotprojektes vorgesehen.
Die Fernwirkdienste haben ohne Zweifel positive Aspekte, z. B. für Kranke und Behinderte, zur Rationalisierung. Mit ihnen sind aber auch erhebliche Gefährdungen verbunden:

- Verstoß gegen die Unverletzlichkeit der Wohnung (Art. 13 GG)

- Eindringen in die Privatsphäre (Art. 1 Abs. 1, 2 Abs. 1 GG)

Insbesondere das Eindringen in die Privatsphäre wirft schwerwiegende Fragen auf, weil der Zugang zum innersten Bereich privater Lebensgestaltung eröffnet werden kann.
Die Realisierung der Fernwirkdienste hängt in erster Linie von den wirtschaftlichen Erfolgsaussichten der Kabelkommunikation ab. Eine konkrete Gefahr zeichnet sich noch nicht ab. Dennoch müssen – insbesondere wegen der im Vergleich zu den anderen Diensten neuen Qualität der Fernwirkdienste, nämlich der aktiven, von **außen** gesteuerten Kommunikation – rechtzeitig Vorkehrungen getroffen werden.

Hinzu kommt, daß die Deutsche Bundespost erwägt, die Realisierung von Fernwirkdiensten durch private Anbieter über das Fernsprechnetz zu ermöglichen. Damit könnten sich die Fernwirkdienste auch unabhängig von der Kabelkommunikation entwickeln.

3.1.2.3 Der Staatsvertrag über Bildschirmtext als Vorbild

Die Notwendigkeit bereichsspezifischer Datenschutzvorschriften für die Kabelkommunikation ist offenkundig. Auch wenn die wirtschaftlichen Erfolgsaussichten nicht eindeutig sind, muß rechtzeitig Vorsorge getroffen werden. Vorbild für solche Regelungen kann in weiten Teilen der Staatsvertrag über Bildschirmtext sein.

Eine Arbeitsgruppe der Datenschutzbeauftragten beschäftigt sich mit Überlegungen für bereichsspezifische Datenschutzvorschriften für die Kabelkommunikation. An dieser Arbeitsgruppe beteilige ich mich. Die Überlegungen in dieser Arbeitsgruppe werden in erster Linie von den Datenschutzbeauftragten der Länder beeinflußt, in denen Kabelpilotprojekte durchgeführt werden.

3.2 Archivwesen

In diesem Abschnitt werden die Probleme staatlicher (öffentlicher) Archive behandelt. In Hamburg ist als staatliches Archiv hauptsächlich das Staatsarchiv betroffen. Die Datenschutzprobleme bei Medien- und Pressearchiven fallen in meine Zuständigkeit als Aufsichtsbehörde nach §§ 30, 40 BDSG. Mit diesem Thema werde ich mich in meinem nächsten Tätigkeitsbericht beschäftigen.

3.2.1 Archivgesetz

3.2.1.1 Notwendigkeit eines Archivgesetzes

Ich habe in meinem 1. Tätigkeitsbericht (Nr. 6.2 auf S. 32) auf die Problematik hingewiesen, die sich aus der Löschungspflicht gem. § 15 Abs. 3 für den Zugang des Staatsarchivs zu Dateien ergibt, und die Lösung des Problems durch die Einfügung einer Archivklausel in das HmbDSG vorgeschlagen. Ich habe weiter festgestellt, daß die Einfügung einer Archivklausel nicht dringend ist, weil das Staatsarchiv gegenwärtig keine Dateien übernimmt. Auch im Jahre 1983 ist kein Fall bekanntgeworden, in dem die Übernahme einer Datei an der Vorschrift des § 15 Abs. 3 gescheitert ist. In dem Bericht habe ich ferner deutlich gemacht, daß eine Archivklausel nicht alle Probleme löst, und die Empfehlung der Datenschutzbeauftragten zur Sicherstellung des Datenschutzes im Archivwesen erwähnt.

Der Senat hat in meiner Stellungnahme zu meinem ersten Tätigkeitsbericht (s. Drucksache 11/455, Nr. 2.5) eine Archivklausel für wünschenswert erklärt und eine Entscheidung, ob der Erlaß eines Archivgesetzes der Einfügung einer Archivklausel in das HmbDSG vorzuziehen ist, nach Auswertung der z. Z. in Bund und Ländern laufenden Vorbereitungen für ein Archivgesetz angekündigt.

Ich bin zu der Auffassung gelangt, daß eine umfassende Regelung durch ein Archivgesetz notwendig ist, und fasse die wesentlichen Argumente im folgenden zusammen:

- Der Streit um die Akteneinsicht durch die ROM und CINTI Union e. V. hat gezeigt, daß die Nutzung von Archivgut schwerwiegende Probleme des Persönlichkeitsschutzes aufwirft. Diese Konflikte müssen durch den Gesetzgeber entschieden werden; die gegenwärtigen Regelungen in Verwaltungsvorschriften sind keine tragfähige Grundlage.

- Ohne ein Archivgesetz sind die Rechte des Betroffenen insbesondere auf Auskunft und Gegendarstellung nur unzureichend geregelt, weil auf Auffangnormen zurückgegriffen werden muß, die nur eingeschränkt gelten (z. B. HmbDSG nur bei Dateien) oder auf andere Sachverhalte zugeschnitten sind (z. B. Verwaltungsverfahrensgesetz).

- Auch die Anbietung, Übernahme und Sicherung des Archivguts bedürfen einer gesetzlichen Regelung. Dabei gibt es Schwierigkeiten vor allem bei der Übernahme solcher Unterlagen, die besonderen Geheimnissen unterliegen (z. B. Steuer-, Statistikgeheimnis).

Die Notwendigkeit eines Archivgesetzes wird auch dadurch unterstrichen, daß im internationalen Vergleich neben der Bundesrepublik nur wenige Länder kein Archivgesetz haben.

3.2.1.2 Stand der Überlegungen bei den Datenschutzbeauftragten

Ein Arbeitskreis der Datenschutzbeauftragten hat die Arbeiten an einem Musterentwurf für ein Archivgesetz weitgehend abgeschlossen. Der Entwurf umfaßt im wesentlichen folgende Regelungsbereiche:

- Aufgaben der staatlichen Archive

- Begriff des Archivgutes
  (technische und inhaltliche Definition)

- Aussonderung und Anbietung von Archivgut
  (Pflichten der Stellen, die archivwürdiges Material führen;
  Möglichkeit von Vereinbarungen zwischen abgebender Stelle und Archiv)

- Übernahme von Archivgut
  (Übernahmeverfahren, Funktion des Zwischenarchivs;
  Einsichtsrecht des Archivs)

- Sicherung des Archivguts

- Nutzung des Archivguts
  (Voraussetzungen und Einschränkungen des Rechts auf Nutzung;
  Sperrfristen, Verbot von Persönlichkeitsprofilen)

- Recht auf Auskunft und Gegendarstellung.

Schwierige Probleme sind mit der Formulierung einer Vorschrift verbunden, die den staatlichen Archiven den Zugang zu Unterlagen eröffnet, die unter dem Schutz der oben erwähnten besonderen Geheimnisse stehen. Landesgesetze können Ausnahmen nur zulassen, soweit auch die Berufs- und besonderen Amtsgeheimnisse landesrechtlich geregelt sind.

3.2.2 Einsicht in Archivgut durch die ROM und CINTI Union e. V.

3.2.2.1 Darstellung des Sachverhalts

1. Nach dem Bericht eines Richters, den der Senat mit der Durchsicht des hier in Rede stehenden Archivgutes beauftragt hatte, lagern im Staatsarchiv folgende Materialien:

   - 1.120 sog. Landfahrerakten, die jeweils einen bestimmten Landfahrer betreffen und in fast allen Fällen auch Vorgänge über seine engere Sippe enthalten. Die Akten haben unterschiedlichen Umfang (bis zu 40 Blatt) und enthalten hauptsächlich Urkunden. Der Akteninhalt erweckt nicht den Eindruck zielstrebigen Sammelns, sondern eher den Eindruck, die aktenführende Stelle habe zum fraglichen Namen alles Greifbare – ob gewichtig oder belanglos – beigezogen.

   - Verwaltungsakten der früheren Landfahrerdienststelle der Polizei.

   In dem Bericht werden die für diesen Fall relevanten Feststellungen in folgenden Aussagen zusammengefaßt:

   - Alle Akten stammen aus der Zeit nach dem 8. Mai 1945. In keinem Fall handelt es sich um die Fortsetzung oder Fortschreibung alter NS-Akten.

   - Die Landfahrerakten enthalten keine Originalbestandteile aus der NS-Zeit – abgesehen von Formalurkunden wie Geburts-, Heirats- und Sterbeurkunden. Sie führen ausnahmslos keine (also auch keine Original-) Beiakten.

   - In zahlreichen Akten befinden sich indessen Photokopien und Abschriften von Urkunden oder – meist nur bruchstückhaften – Vorgängen aus der NS-Zeit.

   In dem Bericht wird ferner mitgeteilt, daß eine von der Landfahrer-Dienststelle früher geführte (Landfahrer-)Kartei nicht an das Staatsarchiv abgegeben, sondern im November 1982 von der Polizei vernichtet worden ist.

2. Die ROM und CINTI Union e. V. (im folgenden mit RCU abgekürzt) wollte die im Staatsarchiv vorhandenen Akten für die Darstellung der Geschichte ihres Volkes auswerten. Das Staatsarchiv lehnte ihren Antrag auf Einsichtnahme ab, weil die Einsichtnahme durch Vertreter der RCU die Persönlichkeitsrechte andererZigeuner, über die die Akten Vorgänge enthalten, verletzen könnte. Das Staatsarchiv berief sich auf die durch Beschluß des Senats festgelegte Sperrfrist von 60 Jahren nach Schließung der Akten, die dem Persönlichkeitsschutz dient.

Die RCU nahm die Ablehnung der Einsichtnahme nicht hin. Sie erhob Klage vor dem Verwaltungsgericht. Daneben wurde das Thema in der Presse und mehrfach in der Hamburger Bürgerschaft behandelt. In der Auseinandersetzung spielten insbesondere folgende Argumente eine Rolle:

- Der Hinweis auf den Schutz der Persönlichkeitsrechte anderer Betroffener wurde von der RCU (und ihr folgend weitgehend auch von der Presse) als Diskriminierung empfunden („Will man uns vor uns selber schützen?" lautete eine Überschrift in einer Wochenzeitung). Es wurde häufig übersehen, daß die antragstellende RCU ein Verein ist, der im Zweifel nur für seine Mitglieder sprechen kann.

- Die Verweigerung der Einsicht wurde auch deswegen als ungleiche und diskriminierende Behandlung empfunden, weil der Senat „Sexualforschern" Einsicht gewährt hatte. Tatsächlich wurde im Rahmen eines von der Deutschen Forschungsgemeinschaft geförderten Forschungsprojektes namentlich benannten und besonders verpflichteten Kräften der Psychiatrischen Klinik des Universitäts-Krankenhauses Eppendorf Einsicht in die Erbgesundheitsakten aus der NS-Zeit – das sind andere als die Landfahrerakten, in die die RCU einsehen wollte – gewährt. Die Akten durften nur unter Aufsicht eingesehen, Aufzeichnungen nur in anonymer Form gemacht werden.

- Es wurde vermutet, daß die Akten eine Fortführung von entsprechenden Akten aus der NS-Zeit darstellen und Vorgänge auch aus der Zeit nach dem 8.5.1945 enthalten, die zu verbergen der Senat ein Interesse hat. Diese Vermutung ist durch den oben zitierten Bericht nicht bestätigt worden.

Insgesamt hätte die z. T. sehr emotional geführte Auseinandersetzung vermieden werden können, wenn der oben erwähnte Bericht nicht erst Mitte Juli, sondern früher in Auftrag gegeben worden wäre. Nachdem dpa am 28.9.1983 den Bericht ausführlich referiert hatte, fand die Auseinandersetzung ein schnelles Ende.

3. Am 17.10.1983 verglichen sich die RCU und der Senat in dem anhängigen Verwaltungsrechtstreit. Danach

   - dürfen die Vorsitzenden der RCU in Begleitung ihrer Prozeßbevollmächtigten die Landfahrerakten als personenbezogene Akten und die zu diesem Bereich vorliegenden Sachakten einsehen und die Akten und Aktenteile bezeichnen, an denen die RCU zur Aufarbeitung der Geschichte ihrer Völker interessiert ist;

   - werden die bezeichneten Akten der RCU in anonymisierter Form zur Verfügung gestellt (Schwärzung der Namen oder andere Verfahren, die den Persönlichkeitsschutz der in den Akten genannten Personen wahren). Von der Verpflichtung zur Anonymisierung sind die Namen der Bediensteten ausgenommen, die bis 1945 in dem fraglichen Bereich tätig waren;

   - verpflichten sich die Vorsitzenden der RCU zur Verschwiegenheit über die ihnen bei der Durchsicht bekanntgewordenen Namen. Nur mit ausdrücklicher Zustimmung des Staatsarchivs darf ein Name veröffentlicht oder in sonstiger Weise Gebrauch von der Kenntnis der anonymisierten Namen gemacht werden.

3.2.2.2 Bewertung aus Datenschutzsicht

1. Die Auseinandersetzung hat nach meiner Meinung unterstrichen, daß ein Archivgesetz notwendig ist. Die Position des Senats war schon dadurch geschwächt, daß die Benutzung durch Verwaltungsvorschriften und durch diese nicht erschöpfend geregelt ist. So konnte der Eindruck entstehen, der Senat berufe sich auf Persönlichkeitsschutz, um andere Interessen zu kaschieren.

2. Der Musterentwurf der Datenschutzbeauftragten für ein Archivgesetz hätte für diesen Fall folgende Regelungen vorgesehen:

   - Die Sperrfrist für die Nutzung des Archivguts beträgt 30 Jahre nach dem Tod der Person, auf die sich die Akte bezieht.

   - Die Sperrfrist kann mit Zustimmung der abgebenden Stelle verkürzt werden.

   - Das Archivgut darf nach Ablauf der Sperrfrist für wissenschaftliche Zwecke oder zur Wahrung berechtigter persönlicher Belange eingesehen werden.

3. Bevor es zu dem Vergleich kam, hatte der Senat folgendes Verfahren für die Akteneinsicht vorgeschlagen:

   - Kräfte des Staatsarchivs sehen die Akten durch und zeichnen alle Namen auf, die in den Akten vorkommen.

   - Die RCU stellt anhand der Namenslisten fest, welche Personen noch leben und welche verstorben sind, und befragt die noch lebenden Personen, ob sie mit der Einsicht einverstanden sind.

   - Das Staatsarchiv gewährt Einsicht, soweit Einwilligungserklärungen vorliegen.

   Dieser Vorschlag war mit mir abgestimmt. Die geplante Übermittlung der Namenslisten hätte nach meiner Ansicht keine schutzwürdigen Belange der Betroffenen verletzt, weil jedenfalls unter den Betroffenen die Tatsache allgemein bekannt ist, daß sie in den Vorgängen der Polizei erfaßt waren. Wenn die RCU von der Mehrzahl ihrer Mitglieder eine Einwilligungserklärung erhalten hätte, so hätte sie durch die Einsicht in die entsprechenden Akten einen repräsentativen Überblick über das Material bekommen.

   Ausführlich hatte ich mich zu dem Verfahren für die bereits Verstorbenen und für diejenigen, bei denen nicht festgestellt werden kann, ob sie noch leben, geäußert.
   In die Unterlagen verstorbener Personen darf auch Einsicht genommen werden, wenn eine Einwilligung Hinterbliebener, also enger Familienangehöriger vorliegt.
   Soweit keine Einwilligung vorliegt, ist eine allgemeine Einsicht nach Ablauf bestimmter Schutzfristen zulässig. Die Bestimmung dieser Schutzfristen beruht entsprechend den Gründen des „Mephisto-Urteils" darauf, daß der grundsätzliche Vorrang der Belange des Betroffenen vor den Informationsinteressen Dritter und der Allgemeinheit (wissenschaftliche Forschung) zeitlich begrenzt sein muß. In allen vorliegenden Entwürfen für ein Archivgesetz wird eine Schutzfrist von 30 Jahren nach dem Tode des Betroffenen für angemessen gehalten.

   Ist ein Todestag nicht oder nur mit unvertretbarem Aufwand festzustellen, so ist eine Sperrfrist auf den Zeitpunkt der Geburt des Betroffenen zu beziehen. Darüber, welche Länge für eine solche Sperrfrist festzulegen ist, konnte in der bisherigen Diskussion noch keine Einigkeit erzielt werden. Zum Teil wird eine Frist von 100 Jahren nach der Geburt für ausreichend gehalten; andere Entwürfe sehen eine Frist von 120 Jahren vor. Für eine Begrenzung der Frist auf 100 Jahre spricht der Umstand, daß die durchschnittliche Lebenserwartung bei 70 Jahren liegt. Weil aber ein Teil der Betroffenen älter wird als 70 Jahre, sollte sicherheitshalber eine Frist von 120 Jahren gewählt werden.

   Über die Behandlung solcher Fälle, in denen weder ein Todes- noch ein Geburtsdatum mit vertretbarem Aufwand feststellbar ist, wird man eine Schutzfrist m. E. auf den Zeitpunkt der Entstehung bzw. des Abschlusses der Vorgänge beziehen müssen (z. B. 60 Jahre nach Abschluß eines Vorgangs).

In besonderen Fällen führt die Interessenabwägung dazu, daß eine Einsichtnahme durch Dritte auch ohne Einwilligung der Betroffenen oder der Hinterbliebenen bzw. unter Verkürzung der Schutzfristen möglich ist. Dies ist namentlich dann der Fall, wenn Einsichtnahme

- zur Erreichung eines wissenschaftlichen Zwecks,
- zur Behebung einer Beweisnot oder
- aus sonstigen im überwiegenden Interesse der abgebenden Stelle oder eines Dritten liegenden Gründen

erforderlich ist.

In diesen Fällen ist jedoch durch Anonymisierung oder auf andere Weise sicherzustellen, daß schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden. Ob eine Beeinträchtigung schutzwürdiger Belange gegeben ist, hängt insbesondere von der Sensibilität der gespeicherten Unterlagen in Relation zum Zweck der Einsichtnahme ab.

4. Der Vergleich zwischen dem Senat und der RCU trägt meinen Überlegungen Rechnung.
   Nach dem unter 3.2.2.1, Tz 1 erwähnten Bericht enthalten die Akten überwiegend nur Urkunden und nur zu einem geringen Teil andere Unterlagen wie Anträge, Schriftsätze, Handschreiben, Berichte, abschriftlich beigebrachte Verwaltungs- und Polizeivorgänge, Anklagen, Urteile. Mithin ist die Gefahr gering, daß durch die Einsicht Persönlichkeitsrechte Dritter verletzt werden, zumal sich die Einsicht nehmenden Vertreter der RCU zur Verschwiegenheit und zum Verzicht auf eigenmächtige Nutzung verpflichtet haben. Das Material, an dem die RCU für die Aufarbeitung der Geschichte ihrer Völker interessiert ist und das sie bei der Einsichtnahme bezeichnet, wird ihr in anonymisierter Form zur Verfügung gestellt.

5. Angehörige der ROM und CINTI haben sich während der Auseinandersetzungen an mich um Hilfe gewandt, weil das Staatsarchiv ihnen die Einsicht in die ihre Person betreffenden Akten verwehrt hatte. Ich habe dem Staatsarchiv mitgeteilt, daß das Auskunftsrecht einzelner Betroffener von der grundsätzlichen Auseinandersetzung über die Einsichtnahme durch die RCU unberührt bleibt und auch nicht wegen des Aufwands, der mit seiner Realisierung möglicherweise verbunden ist (z. B. Entheftung bei fadengehefteten Akten), abgewehrt werden darf.

6. Zu der im November 1982 vernichteten Kartei habe ich die Behörde für Inneres zu folgenden Fragen um eine Stellungnahme gebeten:

   - Welchem Zweck diente die Kartei? Hatte die Kartei – nach Einführung von POLAS – noch die Funktion, Hinweise auf Kriminalakten zu geben?
   - Welche Art von Daten wurden in ihr gespeichert?
   - Wie lange wurde die Kartei genutzt?
   - Warum wurde diese Kartei im Rahmen der Ablieferungsaktion im Jahre 1980 nicht mit an das Staatsarchiv abgeliefert?
   - Welchen Zweck hatte sie nach der Ablieferung der Landfahrerakten?
   - Wodurch wurde die Löschung im November 1982 veranlaßt?
   - Wer hat die Kartei vernichtet?

   Eine Antwort steht noch aus.

3.3 Personalwesen

3.3.1 Prüfungsamt für den öffentlichen Dienst

Eine Eingabe gab mir Veranlassung, mich umfassend über die Datenverarbeitung im Prüfungsamt für den öffentlichen Dienst zu unterrichten.

3.3.1.1 Aufgaben und Arbeitsabläufe

1. Das Prüfungsamt für den öffentlichen Dienst ist vom Senat eingerichtet worden. Nach den „Bestimmungen über die Einrichtung des Prüfungsamtes für den öffentlichen Dienst" in der Fassung des Senatsbeschlusses vom 18.6.1974 hat es die Aufgabe, die Eignung aller Bewerber bestimmter, vom Senat vorgegebener Gruppen in Eignungsuntersuchungen festzustellen. Ziel dieser Organisation ist die Professionalisierung der Eignungsfeststellung, d. h. sie wird nicht dem gesunden Menschenverstand oder dem Zufall mehr oder weniger ausreichender psychologischer Kenntnisse der Personalleiter oder -sachbearbeiter in den Behörden und Ämtern überlassen, sondern einem objektivierenden Verfahren durch geschulte Kräfte unterworfen. In diesem Verfahren wird die allgemeine Eignung festgestellt; es liegt weiterhin in der Verantwortung der jeweiligen Behörden und Ämter, die Eignung für spezielle fachliche Anforderungen (z. B. einer Tätigkeit als Programmierer) festzustellen.

   Das Prüfungsamt besteht aus

   - dem Vorstand, der die Objektivität des Verfahrens bei den Eigungsuntersuchungen sicherstellt,

   - den Prüfungsausschüssen, die aufgrund der Ergebnisse der psychologischen Eignungsuntersuchung durch die Prüfungsstelle in bestimmten Fällen über die Eignung oder Nichteignung der Bewerber entscheiden, und

   - der Prüfungsstelle, die die psychologische Eignungsuntersuchung durchführt. Ihre Tätigkeit wird im folgenden näher beschrieben. Dabei ist festzuhalten, daß die Prüfungsstelle unselbständiger Teil des Prüfungsamtes ist. Das Prüfungsamt ist als speichernde Stelle für die Einhaltung der Datenschutzvorschriften zuständig.

2. Datenerhebung

   Die Bewerber werden am Prüfungstermin über Sinn und Zweck, Ablauf und Auswertung der Eignungsuntersuchung mündlich informiert. Die Prüfungsstelle ist sich darüber im klaren, daß diese Informationen und entsprechende Aushänge im Prüfungsraum von den Bewerbern wegen der nervlichen Belastung der bevorstehenden Eignungsuntersuchung kaum wahrgenommen werden. Der Ablauf der Prüfung ist nach Bewerbergruppen und den entsprechenden Eignungsanforderungen differenziert.

   Die während der Prüfung angefertigten Arbeitsproben (Testergebnisse) werden quantitativ ausgewertet; aufgrund dieser Auswertungen werden die Fähigkeiten beurteilt und auf einem Arbeitsbogen notiert. Diese und die Feststellungen in einem Gespräch mit dem Bewerber sind die Ergebnisse der Eignungsuntersuchung und Grundlage für die zusammenfassende Feststellung: geeignet oder nicht geeignet. Das Votum geht an den zuständigen Prüfungsausschuß, der es in einem späteren Termin bestätigt oder verwirft und seine abschließende Entscheidung bekanntgibt, oder an die zuständige Behörde, die die Eignung abschließend feststellt.

3. Datenspeicherung

   Die Prüfungsstelle speichert die erhobenen Daten in folgenden Dateien:

a) Bewerberkartei mit Angaben zur Person des Bewerbers und zum Ablauf des Bewerbungsverfahrens; mit ihr sollen Doppel- und Nachbewerbungen erkannt und der jeweilige Bearbeitungsstand nachgewiesen werden.

b) Beurteilungsbögen mit Angaben zur Person und Feststellungen zur Eignung des Bewerbers; sie dienen der Begründung des Ergebnisses der Eignungsuntersuchung und als Grundlage für weitere Beurteilungen.

c) Automatisierte Datei der Prüfungsergebnisse mit Angaben zur Person des Bewerbers (ohne Namen) und den Ergebnissen der einzelnen Tests; diese Datei wird mit Hilfe statistischer Verfahren für Zwecke der Testkonstruktion und -analyse und für die Bewährungskontrolle der Einzeltests und des Gesamtverfahrens ausgewertet.

d) Testantwortbögen und schriftliche Arbeiten (Arbeitsproben).

e) Signierbeleg für die Eingabe in die automatisierte Datei (s. o.) und zugleich für Arbeitsaufzeichnungen des Psychologen.
Die Datei enthält Angaben zur Person des Bewerbers (ohne Namen), die Ergebnisse einzelner Tests und die Beurteilung der Fähigkeiten. Sie dient als Grundlage für die weitere Bearbeitung der Eingabe in die automatisierte Datei und als Nachweis der Beurteilung.

Rechtsgrundlage für die Speicherung sind §§ 6 und 7 HmbBG und § 2 HmbLVO sowie § 9 Abs. 1 HmbDSG. Art. 33 Abs. 2 GG gewährt dem Einzelnen – innerhalb der durch die Organisationsgewalt gegebenen Möglichkeiten – Anspruch auf gleichen Zugang zu allen öffentlichen Ämtern nach Eignung; der Anspruch gilt nicht nur für Beamte, sondern auch für Angestellte und Arbeiter. Aus diesem Anspruch ergibt sich für die Freie und Hansestadt Hamburg die Aufgabe, die Eignung so objektiv wie möglich festzustellen. Die beamtenrechtlichen Vorschriften enthalten keine Regelungen über den zulässigen Umfang der Datenverarbeitung. Deshalb muß § 9 Abs. 1 HmbDSG als Befugnisnorm herangezogen werden. Das Prüfungsamt darf nur die Daten speichern, die für die rechtmäßige Erfüllung der Aufgabe „Gewährleistung des gleichen Zugangs zu öffentlichen Ämtern nach Eignung" erforderlich sind. Nach meinen Feststellungen sind die gespeicherten Daten nach Art und Umfang für die Aufgabenerfüllung erforderlich.
Die Daten werden je Datei unterschiedlich lange aufbewahrt:
Bewerberkartei, Beurteilungsbögen 10 Jahre,
automatisierte Datei 15 Jahre,
Signierbelege 7 Jahre,
Testantwortbögen und schriftliche Arbeiten 1 Jahr.

4. Datenverarbeitung, insbesondere Datenübermittlung

Die Auswertung der Daten mit dem Ziel, die Eignung des Bewerbers festzustellen, ist für die Erfüllung der dem Prüfungsamt übertragenen Aufgaben notwendig.

Ein besonderes Problem – das auch der Anlaß für die Eingabe war – ist die mehrfache Verwendung der Ergebnisse einer Eignungsuntersuchung bei mehreren Bewerbungen einer Person (z. B. als Anwärter für den gehobenen allgemeinen Verwaltungsdienst und den Steuerdienst). Dabei können dieselben Ergebnisse durchaus zu unterschiedlichen Eignungsfeststellungen führen, weil unterschiedlich scharfe Maßstäbe angelegt werden. Die Ergebnisse einer Eignungsfeststellung werden mehrfach verwendet, um

- die Arbeitsbelastung für die Prüfungsstelle gering zu halten und

- den Bewerber nicht unnötig mit Zeit- und Energieaufwand für Tests zu belasten.

Das Prüfungsamt hat die Aufgabe, für die Behörden die psychologische Eignung der Bewerber festzustellen.
Bei den Bewerbergruppen „Beamtenanwärter", „Bewerber für den gehobenen Polizeidienst" und „Polizeikommissar-Anwärter" trifft das Prüfungsamt allerdings keine abschließende Entscheidung (daher werden z. B. auch die Prüfungsausschüsse nicht eingeschaltet). Es leitet den zuständigen Behörden den Beurteilungsbogen mit der strengen Auflage zu, ihn nicht zu kopieren. Die Behörden geben den Bogen nach Kenntnisnahme zurück. Die Behörden selbst stellen in diesen Fällen die Eignung abschließend fest; das Prüfungsamt liefert nur die Grundlagen dafür.

Bei allen anderen Bewerbern entscheiden die Prüfungsausschüsse abschließend über die Eignung; dabei wird den Behörden in diesen Fällen nur die zusammenfassende Feststellung „geeignet" oder „nicht geeignet" mitgeteilt.

3.3.1.2 Datenschutzrechtliche Bewertung

1. Datenerhebung

Umfang und Intensität der Datenerhebung richten sich nach psychologischen Erkenntnissen, die sich meiner Beurteilung entziehen. Es ergeben sich aber keine Anhaltspunkte dafür, daß das Testprogramm überzogen ist.

M. E. hat das Prüfungsamt mit dem bisherigen Hinweisverfahren seiner Verpflichtung gem. § 9 Abs. 2 nur unzureichend genügt. Die beteiligten Stellen haben mir zugestimmt, daß der Prüfungstag wegen der besonderen nervlichen Belastung des Bewerbers für diese Hinweise nicht geeignet ist. Künftig sollen daher die Hinweise gem. § 9 Abs. 2 in das Einladungsschreiben aufgenommen werden.
Dabei soll auch auf die mehrfache Verwendung der Ergebnisse der Eignungsuntersuchung hingewiesen werden (s. nachstehend Tz 3).

2. Datenspeicherung

Die gespeicherten Daten sind nach Art und Umfang erforderlich,um die dem Prüfungsamt gestellte Aufgabe zu erfüllen; (dabei wiederhole ich den Vorbehalt, daß sich Umfang und Intensität des Testprogramms und der Ergebnisse daraus meiner Beurteilung entziehen).

Die Dauer der Aufbewahrung oder Speicherung muß zunächst nach der Wahrscheinlichkeit einer erneuten Eignungsuntersuchung beurteilt werden.

- Von den nicht eingestellten Bewerbern (Bewerbung zurückgezogen, nicht geeignet) bewerben sich rund 40% innerhalb von 6 Jahren erneut.

- Auch bei eingestellten Bewerbern ergibt sich bei bestimmten Wechseln in der Beschäftigung, z. B. durch Aufstieg vom mittleren Dienst (und vergleichbaren Angestelltenpositionen) in den gehobenen Dienst, die Notwendigkeit einer erneuten Eignungsuntersuchung.

Der Zeitraum, in dem eine erneute Eignungsuntersuchung anfallen kann, umfaßt nach empirisch belegbaren Erfahrungen 10 Jahre. Während der ersten 5 Jahre wird aufgrund der Ergebnisse der 1. Eignungsuntersuchung entschieden, ob eine erneute Eignungsuntersuchung durchgeführt werden soll (immer dann, wenn die Nicht-Eignung nicht auf gravierenden Mängeln beruht oder die Eignung gerade noch erreicht worden ist) oder ob aufgrund der 1. Eignungsuntersuchung entschieden werden soll (bei gravierenden Mängeln, also Nicht-Eignung, und bei klarer Eignung wird das frühere Urteil übernommen).

Vom 6. bis zum 10. Jahr wird in jedem Falle eine erneute Eignungsuntersuchung durchgeführt. Ihre Ergebnisse werden mit denen der früheren Eignungsuntersuchung

verglichen; damals gute Ergebnisse können dazu führen, daß ein aktuelles Urteil in kritischen Kategorien nach oben korrigiert wird. Da nach der Praxis der Prüfungsstelle im Zweifel immer gegen den Bewerber entschieden wird, kann die alte Eignungsuntersuchung mithin in den Fällen Zweifel ausräumen, in denen sie eine klare Eignung auswies. Die Aufbewahrung wirkt mithin in diesen Fällen zugunsten des Bewerbers.

Solange die Prüfungsstelle nach einer Eignungsuntersuchung eine erneute geforderte Entscheidung in wesentlichem Umfang von den Ergebnissen der ersten Eignungsuntersuchung abhängig macht, sind diese Unterlagen für die Erfüllung ihrer Aufgaben erforderlich. Der Zeitraum von 5 Jahren steht allerdings im Widerspruch zu der Frist von 4 Jahren, nach der gem. § 15 Abs. 4 alle gespeicherten Daten auf ihre Erforderlichkeit hin zu überprüfen sind. Da es jedenfalls z. Z. keine empirisch belegbaren Gründe für die 5-jährige Aufbewahrung der Daten gibt, habe ich empfohlen, die Daten nur 4 Jahre lang aufzubewahren. Das Prüfungsamt will meiner Empfehlung folgen.

Ab dem 5. Jahr ist nur noch die Aufbewahrung der Unterlagen erforderlich und damit zulässig, in denen eine klare Eignung festgestellt wird; denn nur diese Unterlagen haben eine Relevanz. Entsprechend der in § 15 Abs. 4 festgelegten Frist ist die Speicherung dieser Fälle für weitere 4 Jahre zulässig, danach sind auch diese Daten zu vernichten.

Für die unter Nr. 3.3.1.1, Tz 3, aufgeführten Dateien ergeben sich nunmehr folgende Fristen:

Bewerberkartei Beurteilungsbögen Signierbeleg	Aufbewahrung aller Fälle 4 Jahre; danach Aufbewahrung nur der Fälle mit klarer Eignung für weitere 4 Jahre.
Automatisierte Datei	Sie enthält nur die Prüfnummer. Die Verbindung von der Prüfnummer zum Namen wird über die Beurteilungsbögen hergestellt. Wenn diese vernichtet werden, sind die Daten in der automatisierten Datei hinreichend anonymisiert, weil aus den sonstigen Angaben zur Person nur mit außerordentlich hohem Aufwand auf eine bestimmte Person zurückgeschlossen werden kann. Die 15-jährige Aufbewahrung ist daher zulässig, wenn mit den Beurteilungsbögen so verfahren wird wie oben angegeben.
Testantwortbögen usw.	Die einjährige Aufbewahrung ist erforderlich, weil während dieser Zeit der Bewerber Widerspruch erheben kann.

3. Datenverarbeitung, insbesondere Datenübermittlung

Die mehrfache Verwendung derselben Ergebnisse einer Eignungsuntersuchung für verschiedene Zwecke wäre dann unzulässig, wenn die Chancen des Bewerbers geschmälert würden, weil er bei einer zweiten Eignungsuntersuchung besser abschneidet.
Das wäre ihm – wegen der im Zeitablauf nachlassenden Erinnerung – allenfalls im ersten Jahr nach der Eignungsuntersuchung möglich. Nach den Erfahrungen der Prüfungsstelle verändert sich das Testergebnis bei Wiederholung innerhalb eines Jahres nicht signifikant. Das deckt sich nach meinen Feststellungen mit den Erfahrungen aus anderen Tests. Die mehrfache Verwendung ist daher zulässig.

Die Übermittlung von Daten aus der Eignungsuntersuchung an die einstellenden Behörden ist nach § 10 Abs. 1 Satz 1, 1. Alternative zulässig; denn das Prüfungsamt ist

eingerichtet worden, um für die Behörden die psychologische Eignung der Bewerber festzustellen.
Die Datenübermittlung ist nach § 10 Abs. 1 Satz 1 auf den für die Aufgabenerfüllung notwendigen Datenumfang zu beschränken.

- Die Übermittlung der zusammenfassenden Feststellungen ist erforderlich.

- Die Übermitttlung der Beurteilungsbögen (d. h. Einzelfeststellungen) bei bestimmten Bewerbergruppen ist ebenfalls erforderlich, weil das Prüfungsamt in diesen Fällen die Eignung nicht selbst abschließend beurteilt – das tun die zuständigen Behörden –, sondern nur die Unterlagen für diese Beurteilung liefert. Auch wenn in Betracht gezogen wird, daß Personalverwaltungen den Umgang mit sensitiven Daten gewohnt sind, wird durch diese Übermittlung das Risiko einer unbefugten Verwendung erhöht. Die Entscheidung des Senats, durch die die Zuständigkeiten zur abschließenden Eignungsfeststellung auf das Prüfungsamt und bestimmte Behörden verteilt worden sind, habe ich nicht überprüft.

Die Zulässigkeit mehrfacher Verwendung muß dem Betroffenen bekannt sein (§ 10 Abs. 1 Satz 2). Diese Voraussetzung soll für den Betroffenen größtmögliche Transparenz herstellen, damit er z. B. sein Recht auf Sperrung der Übermittlung nach § 6 Abs. 1 Nr. 4 – z. Z. noch nicht in Kraft – wahrnehmen kann. Daher ist, wenn die mehrfache Verwendung der Daten bereits bekannt ist, schon bei der Datenerhebung auf diese Tatsache hinzuweisen (s. Abel, Peters, Hamburgisches Datenschutzgesetz, Rdnr. 3 zu § 10).

Bei den Einladungen wurde bisher kein ausdrücklicher Hinweis auf die mehrfache Verwendung gegeben; das Argument, daß schon die Bezeichnung „Prüfungsamt für den öffentlichen Dienst" einen ausreichenden Hinweis auf die mehrfache Verwendung bietet, vermag nicht zu überzeugen.
Es besteht Übereinstimmung, diesen Hinweis künftig in das Einladungsschreiben aufzunehmen.

3.4 Steuerwesen

3.4.1 Novellierung der Abgabenordnung (AO)

3.4.1.1 Regelung des Kontrollrechts im Bereich der Steuerverwaltung in der AO?

Im August hat der Bundesminister der Finanzen den überarbeiteten Referentenentwurf eines Gesetzes zur Änderung der Abgabenordnung und anderer Gesetze vorgelegt. Dieser Entwurf stellt gegenüber der ersten Fassung (Stand: 15.10.1982) eine wesentliche Verbesserung in datenschutzrechtlicher Hinsicht dar; er berücksichtigt weitgehend die gegen den ersten Entwurf von den Datenschutzbeauftragten erhobenen Einwände. Allerdings bringt auch dieser Entwurf nicht die wünschenswerte Klarstellung des Konkurrenzverhältnisses zwischen Steuergeheimnis und Kontrollrecht der Datenschutzbeauftragten.

Wie schon in meinem 1. TB dargestellt (6.3), geben die Steuerverwaltungen den Datenschutzbeauftragten nur dann Auskünfte und Akteneinsicht über unter das Steuergeheimnis fallende Vorgänge, wenn die Datenschutzbeauftragten aufgrund von Bürgereingaben tätig werden. Im übrigen lassen die Steuerverwaltungen Kontrollen nicht zu, soweit das Steuergeheimnis berührt ist. Die Datenschutzbeauftragten haben ihren Rechtsstandpunkt dazu am 28.9.1982 in einer Entschließung formuliert, deren wesentlichen Inhalt ich bereits in meinem 1. TB wiedergegeben habe.
Da beide Seiten auf ihrem Rechtsstandpunkt beharren, streben die Datenschutzbeauftragten eine klarstellende Regelung an, die aus Gründen der Gesetzessystematik allerdings in die Datenschutzgesetze (BDSG, HmbDSG) einzubauen wäre und sich auf alle speziellen Geheimhaltungsvorschriften erstrecken sollte. Aber auch der Referentenentwurf zur Novellierung des BDSG vermeidet eine entsprechende Klarstellung.

3.4.1.2 Datenschutzrelevante Regelungen im Entwurf

Nach § 30 Abs. 2 AO 1977 verletzt ein Amtsträger das Steuergeheimnis, wenn er Daten eines anderen bzw. fremde Betriebs- und Geschäftsgeheimnisse, die ihm im Rahmen der in Abs. 2 genannten Verfahren/Vorgänge befugt (in seiner Eigenschaft als mit der Sache befaßter Amtsträger) bekanntgeworden sind, unbefugt an Dritte offenbart oder selbst zum Zwecke privater Nutzung verwertet. Der Referentenentwurf schafft einen weiteren Tatbestand für die Verletzung des Steuergeheimnisses, nämlich die Variante, daß ein Amtsträger, der nicht an dem betreffenden Verfahren/Vorgang beteiligt ist, kraft der ihm zur Verfügung stehenden tatsächlichen Möglichkeiten (z. B. weil er Zugang zu den entsprechenden technischen Einrichtungen hat und mit den Verfahrenskonventionen vertraut ist) Daten aus einer Datei im automatisierten Verfahren unbefugt abruft. Auf eine Offenbarung an Dritte oder die Verwertung der so erlangten Kenntnisse soll es dann nicht ankommen.

Dies ist eine Erweiterung des Tatbestandes der Verletzung des Steuergeheimnisses, die den Belangen des Datenschutzes entgegenkommt. Allerdings stellt diese Regelung nur auf automatisierte Verfahren ab, während das unbefugte Lesen von Daten in Akten und Karteien nicht als Bruch des Steuergeheimnisses behandelt wird. Diese Beschränkung halte ich für akzeptabel im Hinblick auf die mit der automatisierten Datenverarbeitung verbundenen besonderen Risiken. Die neue Regelung in der AO wäre eine bereichsspezifische Ergänzung des in §§ 5 Abs. 1 BDSG, 7 Abs. 1 HmbDSG geregelten Datengeheimnisses.

In § 93 des Entwurfs werden zwei datenschutzrelevante Komplexe geregelt: die Auskunftspflicht Nichtbeteiligter (Abs. 1) sowie die Übersendung von sogenannten Kontrollmitteilungen durch Behörden und Gerichte (Abs. 7). Die Problematik der in § 93 geregelten Auskunftspflichten besteht darin, daß ein angemessener Ausgleich geschaffen werden muß zwischen dem unabweisbaren Bedürfnis der Finanzverwaltung nach Aufdekkung unbekannter Steuerfälle und dem grundlegenden Prinzip des Datenschutzes, daß Daten beim Betroffenen selbst und nicht „hinter seinem Rücken" erhoben werden sollen. Die Forderung, daß Nichtbeteiligte, d. h. andere als der Steuerpflichtige selbst, durch Auskunftsersuchen nicht über das unbedingt erforderliche Maß hinaus in Anspruch genommen werden sollen, resultiert aus dem Eingriffscharakter steuerbehördlicher Aufklärungsmaßnahmen.

Die Datenschutzbeauftragten streben eine Fassung des § 93 Abs. 1 AO an, durch die Nichtbeteiligte erst dann zur Auskunftserteilung herangezogen werden dürfen, wenn die Sachverhaltsaufklärung durch die Beteiligten nicht zum Ziele führt oder keinen Erfolg verspricht. Sie räumen auch ein, daß die Finanzbehörden – im Rahmen einer Kann-Bestimmung – das Recht haben müssen, vom Steuerpflichtigen Auskunft über die in § 160 AO genannten Gläubiger und Empfänger von Zahlungen zu verlangen, damit im privaten Bereich Einkünfte, die dem Finanzamt nicht ohne weiteres bekannt werden, zur Besteuerung herangezogen werden können.
Das Prinzip der Datenerhebung beim Betroffenen kann nicht so weit gehen, daß keine Auskunft bei Nichtbeteiligten eingeholt werden darf, wenn der Betroffene den Finanzbehörden gar nicht bekannt ist, weil in diesem Falle die Daten de facto bei ihm nicht erhoben werden können.

Die Neufassung des § 93 Abs. 1 entspricht diesen Forderungen, wenn sie – entsprechend der Begründung zum Entwurf – so zu verstehen ist, daß die Heranziehung Nichtbeteiligter neben den Fällen erfolgloser Sachverhaltsermittlung beim Betroffenen auf Fälle des § 160 AO beschränkt ist.

Durch die Einführung des neuen § 93 Abs. 7 AO wird endlich eine Rechtsgrundlage für Kontrollmitteilungen geschaffen, womit die bedenkliche Einordnung des Kontrollmitteilungsverfahrens unter dem Begriff der Amtshilfe aufgegeben wird. Kontrollmitteilungen von Behörden und Gerichten an Finanzbehörden über steuerlich relevante Sachverhalte

(z. B. Zahlungen von Sachverständigenentschädigungen, Vergütungen für Vortragstätigkeit usw.) lassen sich wohl weder aus den Besteuerungsgrundsätzen des § 85 AO, der lediglich eine Aufgabenzuweisung enthält, noch – im öffentlichen Bereich – allein aus den Amtshilfevorschriften der §§ 111 ff AO rechtfertigen. Auch die bisherige Fassung des § 93 AO stellt keine Rechtsgrundlage für Kontrollmitteilungen dar. Ob und in welchem Umfang Kontrollmitteilungen in Zukunft erlaubt sind, muß durch Rechtsverordnung des Bundesministers der Finanzen konkretisiert werden.

Nicht berücksichtigt wird die Forderung der Datenschutzbeauftragten nach einer Unterrichtung der Betroffenen über die Versendung der Kontrollmitteilungen durch die mitteilende Stelle. Durch eine solche Information könnten die schutzwürdigen Belange des Betroffenen angemessen berücksichtigt werden, ohne daß dadurch der Zweck der Kontrollmitteilungen – die Erfassung aller steuererheblichen Vorgänge – vereitelt würde. Im Gegenteil: Aufgrund der Information wird der steuerpflichtige Betroffene geradezu angehalten, von sich aus die notwendigen Erklärungen abzugeben. Die Erfahrung, daß nicht hinter seinem Rücken Erkenntnisse über ihn gesammelt werden, kann nur dazu beitragen, Mißtrauen und falsche Vorstellungen über Datenflüsse in der Verwaltung abzubauen.

3.4.2 Probleme in Hamburg

In meiner Praxis wurde bisher nur die Frage der Kontrollmitteilungen und der Benachrichtigung des Betroffenen relevant, und zwar durch eine Anfrage der Gesundheitsbehörde, die unter Hinweis auf § 10 Abs. 1 Satz 2 Bedenken geltend machte gegen Nr. 3.3.1.4 der Verwaltungsvorschriften der Finanzbehörde für das Automatisierte Verfahren im Anordnungs-, Kassen- und Rechnungswesen (VVAV). Hiernach müssen die hamburgischen Behörden unter bestimmten Voraussetzungen über Zahlungen ab 1.000,– DM dem Finanzamt auf einem besonderen Vordruck Mitteilung machen. Ich habe die Gesundheitsbehörde über die derzeitige Rechtslage informiert und erklärt, daß für eine begrenzte Übergangszeit Kontrollmitteilungen übersandt werden können, wenn der Betroffene über die Kontrollmitteilung unterrichtet wird. Die Finanzbehörde habe ich gebeten, Nr. 3.3.1.4 der VVAV dahingehend zu ergänzen, daß der Betroffene zu benachrichtigen ist.

Die Frage meiner Kontrollkompetenz unabhängig von einer konkreten Beschwerde eines Steuerpflichtigen ist bisher nicht akut geworden, da ich noch keine routinemäßige Kontrolle im Bereich der Finanzbehörde durchgeführt habe.

3.5 Schulwesen

3.5.1 Probleme im Schulbereich

Im Zuge der Überprüfung der Dateimeldungen für das Datenschutzregister sind einige klärungsbedürftige Rechtsfragen zutage getreten, die nachstehend erörtert werden sollen.

3.5.1.1 Begriff der meldepflichtigen Datei in Abhängigkeit vom Stellen- und Übermittlungsbegriff

Neben den im Verwaltungsbereich der BSB bestehenden Dateien wird eine Reihe von Dateien zur Erledigung von Schulverwaltungsaufgaben in den über 500 staatlichen Schulen Hamburgs geführt. Zum größten Teil handelt es sich bei diesen Daten um manuell geführte Karteikartensammlungen bzw. um Aktensammlungen (Schülerbogen der Jahrgangsstufen 1 – 10), die wegen ihrer vordruckmäßigen Umschlaggestaltung einer Karteikartensammlung entsprechen und deshalb – ungeachtet des eigentlichen Aktenhalts – als Datei anzusehen sind. Daneben meldeten 33 Schulen automatisierte Dateien, die auf schulischen Kleinrechenanlagen verarbeitet werden.

Während die Dateieigenschaft dieser Datensammlungen verhältnismäßig schnell geklärt werden konnte, besteht noch Uneinigkeit über die Frage, ob einige der manuellen Dateien in Schulen „intern" sind oder nicht. Intern sind bekanntlich solche manuellen Dateien, deren Daten nicht zur Übermittlung bestimmt sind. Unstreitig sind solche Dateien nicht intern, aus denen Daten im Einzelfall oder regelmäßig an Stellen außerhalb des Schulbereichs übermittelt werden. Bei den Dateien, aus denen Daten von Schulen nur an die BSB – z. B. für Zwecke der Schulaufsicht oder im Rahmen eines Widerspruchsverfahrens – weitergegeben werden, kommt es darauf an, ob die Schulen nur Teile einer umfassenden speichernden Stelle BSB sind oder ob jede Schule für sich eine eigene speichernde Stelle neben der BSB ist.
Die BSB vertritt die Auffassung einer einheitlichen speichernden Stelle mit der Konsequenz, daß die Weitergabe von personenbezogenen Daten innerhalb des Schulbereichs keine Übermittlung darstellt, weil die BSB im Verhältnis zu den Schulen nicht Dritter ist.
Dieser Auffassung kann ich nicht zustimmen. Selbst wenn man nicht von dem – dem Datenschutzrecht wohl angemesseneren – funktionalen Stellenbegriff, sondern von dem weitergefaßten organisatorischen Stellenbegriff des Verwaltungsverfahrensgesetzes ausgeht, wird deutlich, daß die Schulen jeweils für ihre Dateien eigene speichernde Stellen sind:
Wie aus § 1 Abs. 2 des Hamburgischen Verwaltungsverfahrensgesetzes folgt, ist Behörde jede organisatorisch selbständige Stelle, der Aufgaben der öffentlichen Verwaltung zur eigenverantwortlichen Wahrnehmung übertragen sind. Äußeres Zeichen der organisatorischen Selbständigkeit ist insbesondere die Befugnis zu eigenverantwortlichem Auftreten im eigenen Namen nach außen. Dienststellen, die nach den maßgeblichen organisatorischen Bestimmungen nur im Namen und mit Wirkung für und gegen andere Stellen handeln können, z. B. Sachgebiete, Dezernate und Abteilungen einer Behörde, sind nicht selbst Behörde, sondern bloß Teile einer solchen. Anders verhält es sich bei nicht rechtsfähigen Anstalten wie den Schulen. Innerhalb des gem. § 41 SchulG, § 2 SchVG vorgegebenen Rahmens verwalten sich die Schulen selbst. Der Schulleiter vertritt die Schule nach außen, § 3 Abs. 4 SchVG. In der „Gliederung der BSB und ihrer Ämter" (Organigram vom Juli 1980) sind die Schulen nicht enthalten. Sie sind also keine unselbständigen Dienststellen der BSB, sondern organisatorisch selbständige Stellen.
Diese Ansicht vertritt übrigens auch das Senatsamt für den Verwaltungsdienst in seinen – mit der Justizbehörde abgestimmten – Hinweisen zur Durchführung des Hamburgischen Datenschutzgesetzes (HmbDSG) in der hamburgischen Verwaltung (MittVw 1982 Seite 55). In der Anlage 1 zu den Hinweisen sind die Schulen als selbständige speichernde Stellen genannt.

3.5.1.2 Bedeutung des Stellenbegriffs im Schulbereich im Hinblick auf § 6 Abs. 1 Nr. 4

Am 1.5.1984 wird die Bestimmung des § 6 Abs. 1 Nr. 4 in Kraft treten. Die Auswirkungen der Vorschrift erstrecken sich auf den gesamten öffentlichen Bereich in Hamburg, sie sollen hier nur beispielhaft für den Schulbereich erörtert werden.

Die Vorschrift eröffnet dem Betroffenen das Recht, die Übermittlung seiner Daten an Behörden und sonstige öffentliche Stellen zu sperren, soweit die Übermittlung nicht durch Gesetz zugelassen ist. Das bedeutet: Bevor eine Stelle des öffentlichen Bereichs personenbezogene Daten aus einer Datei an eine andere Stelle des öffentlichen Bereichs übermittelt, hat sie zu prüfen, ob die Übermittlung nach § 10 Abs. 1 Satz 1 zulässig ist. Sie hat dann weiter zu prüfen, ob der von der beabsichtigten Übermittlung Betroffene eine Übermittlungssperre ausgesprochen hat. Liegt ein Sperrvermerk vor, darf die Übermittlung nicht erfolgen. Wenn hingegen ein – besonderes – Gesetz die Übermittlung zuläßt, kann der Betroffene eine Übermittlungssperre nicht erwirken. § 10 Abs. 1 ist keine spezialgesetzliche Regelung i. S. des § 6 Abs. 1 Nr. 4. Ich stimme insoweit der Justizbehörde zu, die dazu im Mai 1981 ausgeführt hat:
„Wäre als Gesetz i. S. des § 6 Abs. 1 Nr. 4 auch § 10 anzusehen, dann würde zu den ohnehin durch § 5 Abs. 1 Nr. 1 i. V. mit § 10 begründeten Verwaltungspflichten im Bereich der Datenübermittlung innerhalb des öffentlichen Bereichs lediglich eine Bekräftigung hinzutreten. Nach dem erklärten – und der Auslegung zugrunde zu legenden – Willen der

Bürgerschaft sollen unterdessen unter diesen Gesetzesbegriff nur bereichsspezifische gesetzliche Regelungen fallen, nicht auch § 10."

Durch das hinausgeschobene Inkrafttreten der Vorschrift sollte die Verwaltung in die Lage versetzt werden zu prüfen, ob Datenflüsse, die zur Aufgabenerfüllung der übermittelnden oder der empfangenden Stelle unabdingbar sind, durch Sperrvermerke von Betroffenen unterbunden werden können, weil keine spezialgesetzlichen Grundlagen für die betreffenden Übermittlungen bestehen.

Wenn nun – anders als die BSB meint – die Schulen selbständige speichernde Stellen sind, dann könnten betroffene Schüler/Eltern die Datenübermittlungen an die BSB sperren, es sei denn, daß in das Schulgesetz eine Regelung über zulässige Datenübermittlungen im Schulbereich aufgenommen wird. Diese Konsequenz zwingt aber nicht zu einer anderen Beurteilung des Stellenbegriffs im Schulbereich, sie kann vielmehr nur dazu führen, daß die Datenflüsse überprüft und ggf. im Schulgesetz geregelt werden.

3.5.2 Umsetzung der Datenschutzbestimmungen im Schulbereich

Im Zusammenhang mit den vorstehend erörterten Rechtsfragen habe ich der BSB empfohlen, die Datenschutzbestimmungen für die Praxis der Schulen näher zu erläutern, weil die am Schulbetrieb beteiligten Personen von Datenschutzproblemen zu weit entfernt sind. Die BSB bereitet z. Z. eine Zusammenfassung der für die Hamburger Schulen relevanten Datenschutzbestimmungen mit konkreten Hinweisen für die Anwendung vor. Das Ergebnis wird als generelle Datenschutzrichtlinie in das Verwaltungshandbuch für Schulen aufgenommen werden.

3.5.3 Schülerbogen für Berufsschüler

Aus den Eingaben, die die Datenverarbeitung in den Schulen zum Gegenstand haben, habe ich einen – in der Diskussion abgeschlossenen – Fall herausgegriffen. Der Petent sieht einen Verstoß gegen den Datenschutz darin, daß an Haupt- und Realschulen von den Schülern der Abgangsklassen die Ausfüllung des Vordrucks „Schülerbogen für Berufsschüler" verlangt wird. Seine Einwendungen richten sich hauptsächlich gegen den Umfang der mit dem Vordruck erhobenen Daten, aber auch dagegen, daß der Klassenlehrer seines Sohnes den Schülern nicht erklären konnte, welchem Zweck die Datenerhebung im einzelnen dient.

Der „Schülerbogen für Berufsschüler" enthält auf einem mehrseitigen Karteikartenvordruck diejenigen Schülerdaten, die nach Meinung der BSB erforderlich sind, um

- die Einhaltung der zwölfjährigen Schulpflicht zu überwachen,
- die Organisation der Berufsschulen durchführen zu können (Bildung von Klassen, Lehrerstundenzuteilung u. a.),
- der für den Schüler aufgrund der Organisation zuständigen Schule die benötigten Personalien zur Verfügung zu stellen.

Das Verfahren „betreffend die Erfassung der berufsschulpflichtigen Schulabgänger" ist durch Rundschreiben vom 5.4.1977 (Bestandteil des Verwaltungshandbuches für Schulen) geregelt. Erst die Eingabe hat Veranlassung gegeben, den Umfang der in dem „Schülerbogen für Berufsschüler" gespeicherten Daten in datenschutzrechtlicher Hinsicht zu überprüfen.
Aus der Sammlung der „Schülerbogen für Berufsschüler" werden Daten an Stellen der BSB (Schulaufsicht, Schülerhilfe, Rechtsabteilung) sowie an die für die Überwachung der Schulpflicht zuständigen Meldeschulen weitergegeben. Die BSB nimmt zu der Frage, ob diese Datenflüsse als Übermittlungen zu qualifizieren sind, den unter Nr. 3.5.1 dargestellten Standpunkt ein mit der Folge, daß sie die Datei als interne betrachtet.

Aus den unter Nr. 3.5.1 genannten Gründen bin ich dieser Auffassung entgegengetreten und habe die BSB aufgefordert,

- die Datei zum Datenschutzregister zu melden,
- einige zur Aufgabenerfüllung nicht erforderliche Daten nicht mehr zu erheben und zu speichern,
- die Vorschrift des § 9 Abs. 2 zu beachten, wonach bei der Datenerhebung ein Hinweis auf die die Erhebung rechtfertigende Rechtsvorschrift bzw. auf die Freiwilligkeit der Datenpreisgabe zu geben ist.

Ungeachtet ihres derzeitigen Rechtsstandpunktes hat die BSB den Vordruck „Schülerbogen für Berufsschüler" inzwischen überarbeitet. Der Entwurf des neuen Vordrucks enthält nicht mehr die Angaben
- Krankenkasse,
- Geburtstag und -ort der gesetzlichen Vertreter,
- Noten des letzten Zeugnisses, Regelmäßigkeit des Schulbesuchs, Stenokenntnisse, Angabe, ob das Klassenziel voraussichtlich erreicht wird, Bemerkungen.

Inhaltlich habe ich gegen den Vordruck-Entwurf keine Einwände mehr; er genügt jedoch noch immer nicht den Anforderungen aus § 9 Abs. 2. Die BSB hat die Aufnahme der erforderlichen Hinweise zugesagt.

3.6 Bauwesen

In meinem 1. TB hatte ich unter Nr. 6.4 über das geplante Automationsverfahren zur Erhebung der Fehlbelegungsabgabe nach dem Gesetz zum Abbau der Fehlsubventionierung und der Mietverzerrung im Wohnungswesen berichtet. Die weitere Verfahrensentwicklung ruht z. Z. Die Gründe dafür hat der Senat in seiner Antwort auf die schriftliche Kleine Anfrage eines Abgeordneten im Mai mitgeteilt (Drucksache 11/687).

Von dem geplanten Automationsverfahren „Fehlbelegungsabgabe" ist z. Z. nur der Teil realisiert, der dem Aufbau einer automatisierten Wohnraumkartei dient. Nach grober Schätzung ist etwa ein Drittel des Bestandes in den Wohnungsämtern erfaßt und in der Form der automatisiert ausgedruckten neuen Wohnraumkartei-Karten vorhanden. Der Änderungsdienst der Wohnraumkartei erfolgt anhand einer Liste aus dem ADV-Verfahren „Änderungs- und Mitteilungsdienst" der Einwohnerämter. Die Diskussion über den Umfang der mit dieser Liste von den Einwohnerämtern an die Wohnungsämter übermittelten Daten konnte in meinem Sinne abgeschlossen werden. Ich hatte gegen die Übermittlung der Daten „Mietverhältnis" (Angabe ob Haupt- oder Untermieterverhältnis), „Anzahl der ausgestellten Lohnsteuerkarten" und „Anzahl der zugeordneten Familienangehörigen" Einwendungen erhoben. Statt dieser Daten wird jetzt nur die „Anzahl der Erwachsenen und Kinder in der Wohnung" sowie – im Falle eines echten Untermietverhältnisses – der Name des Vermieters als „Adressenzusatz" übermittelt.

Offen sind nach wie vor zwei Fragen: Ist für Aufgaben der Baubehörde auf dem Gebiet der Wohnungsversorgung ein Doppel der Hauskarteikarten erforderlich?
In welcher Form benötigt die Clearingstelle die Angaben über ausländische Mieter (personenbezogen, wie im Entwurf der Meldedaten-Übermittlungsverordnung vorgesehen, oder in tabellarischer Form, d. h. weitgehend anonymisiert, wie ich es vorgeschlagen habe)?

Weitere Probleme aus dem Bereich des Bauwesens sind erst kürzlich durch Eingaben an mich herangetragen worden:

- Vermieter von Sozialwohnungen beanstanden, daß die Bezirksämter die Mieter dieser Wohnungen informieren, sobald eine Abgeschlossenheitsbescheinigung für die Wohnungen erteilt wurde.

- Ein Vermieter von Sozialwohnungen wendet sich dagegen, daß er bei Mieterhöhungsverlangen den Mietern – wenn sie es verlangen – eine Wirtschaftlichkeitsberechnung vorlegen muß, die so detailliert sei, daß die Mieter und andere aus dieser Unterlage Schlüsse über seine persönlichen Vermögensverhältnisse ziehen könnten.

- Die Baubehörde beabsichtigt, für eine Untersuchung über die Situation von Wohnungssuchenden eine Erhebung bei den Antragstellern von Bescheinigungen nach § 5 Wohnungsbindungsgesetz und von Dringlichkeitsscheinen durchzuführen. Sie hat mir die Entwürfe der Erhebungsbögen zur Stellungnahme zugeleitet.

Die Diskussion dieser Probleme ist noch nicht abgeschlossen. Eine ausführliche Darstellung muß meinem nächsten Tätigkeitsbericht vorbehalten bleiben.

3.7 Statistik

3.7.1 Volkszählung 1983

3.7.1.1 Beteiligung an der Auseinandersetzung

Es würde den Rahmen dieses Berichts sprengen, wenn ich über die Auseinandersetzung um die Volkszählung im Detail berichtete. Mein Beitrag bestand in der Mitwirkung an zahlreichen Veranstaltungen und in

- Presseerklärungen vom 22.2. und 24.3.1983,
- Stellungnahmen im Vorverfahren und zur Hauptsache gegenüber dem Bundesverfassungsgericht,
- einem umfangreichen Bericht an den Innenausschuß der Hamburger Bürgerschaft und
- Teilnahme an der mündlichen Verhandlung vor dem Bundesverfassungsgericht in der Hauptsache.

3.7.1.2 Stellungnahme zu Problemen der Volkszählung 1983

Bis zur einstweiligen Anordnung des Bundesverfassungsgerichts vom 13.4.1983, mit der der Vollzug des Volkszählungsgesetzes einstweilen ausgesetzt worden ist, galten meine Bemühungen dem Ziel, eine Anwendung des Volkszählungsgesetzes durchzusetzen, die den Belangen des Datenschutzes in größtmöglichem Umfang Rechnung trug. Um dieses Ziel zu erreichen, habe ich seit Anfang Februar mit der Behörde für Inneres über eine verfassungskonforme, d. h. eine nicht nur den Informationsbedarf der Verwaltung, sondern auch die Persönlichkeitsrechte der Bürger berücksichtigende Auslegung des in hohem Maße auslegungsbedürftigen Volkszählungsgesetzes verhandelt. Darüber hinaus ging es mir von vornherein auch darum, den – gemessen an ihren technischen Möglichkeiten allzu weiten – gesetzlichen Handlungsspielraum der Verwaltung noch stärker einzuengen. Erstes Zwischenergebnis war ein aus 13 Punkten bestehender Forderungskatalog, dessen Erfüllung der Innensenator am 23.2.1983 zusagte. Es folgten weitere Vereinbarungen, die es mir ermöglichten, für Hamburg zu erklären, daß – unbeschadet grundsätzlicher Bedenken insbesondere gegen die Melderegisterberichtigung in der vorgesehenen Form – bei der Durchführung der Volkszählung die Beeinträchtigung schutzwürdiger Belange der Bürger nicht zu befürchten sei. Der Hamburger Fragenkatalog war wesentliche Grundlage der Erklärung, die die Konferenz der Datenschutzbeauftragten am 23.3.1983 zur Volkszählung abgab.

Mit der einstweiligen Anordnung des Bundesverfassungsgerichts fand die leidenschaftliche und erbitterte Auseinandersetzung ein jähes Ende; die Entscheidung des Bundesverfassungsgerichts hatte die beabsichtigte friedensstiftende Wirkung. In diesem Lichte betrachtet wäre es wünschenswert gewesen, wenn schon die Initiative des Senats, die Volkszählung um zwei Jahre zu verschieben, Erfolg gehabt hätte. Nach der einstweiligen Anordnung des Bundesverfassungsgerichts bestand Gelegenheit, die durch die Volkszählung 1983 aufgeworfenen Probleme losgelöst von der Hektik der tagespolitischen Auseinandersetzung grundsätzlich zu analysieren. Sichtbaren Ausdruck fanden diese Bemühungen in meinem Bericht an den Innenausschuß der Hamburger Bürgerschaft und in der Stellungnahme in der Hauptsache gegenüber dem Bundesverfassungsgericht.

In der mündlichen Verhandlung vor dem Bundesverfassungsgericht am 18. und 19.10.1983 habe ich meine Haltung zum Volkszählungsgesetz nochmals umrissen:

- Von einer Ausnahme abgesehen, stellt der Fragenkatalog keine übermäßige Belastung für den Bürger dar. Weder dringen die einzelnen Fragen in den unantastbaren Bereich privater Lebensgestaltung ein noch wird durch die Gesamtheit der Fragen ein umfassendes Persönlichkeitsbild geschaffen. Die Ausnahme betrifft die Frage nach der Eigenschaft als „Insasse" einer Anstalt. In Anbetracht der Diskriminierungsgefahr, die mit der namentlichen Erhebung – selbst bei frühzeitiger Trennung von Identifikationsmerkmalen und statistischen Angaben – verbunden ist, belastet diese Frage den betroffenen Bürger übermäßig.

- Eignung und Erforderlichkeit der namentlichen Erhebung halte ich für fraglich, weil die dafür ins Feld geführte Möglichkeit der Rückfrage beim Auskunftspflichtigen angesichts der personellen Kapazitäten in den Statistischen Ämtern kaum genutzt werden wird. Sie belastet den Bürger jedenfalls dann übermäßig, wenn

  - Identifikationsmerkmale untrennbar mit den statistischen Angaben verbunden werden und
  - mithin Identifikationsmerkmale und statistische Angaben nicht schon nach Prüfung auf Vollständigkeit und Plausibilität getrennt werden können, wie es das Bundesstatistikgesetz vorschreibt.

  Mit dem vom Hamburger Senat vorgesehenen Mantelbogen wäre wenigstens den Forderungen des Bundesstatistikgesetzes entsprochen worden.

- Der Melderegisterabgleich wird so, wie er durch § 9 des Volkszählungsgesetzes (VZG 1983) zugelassen wird, den verfassungsrechtlichen Anforderungen nicht gerecht, weil der Inhalt des sog. Benachteiligungsverbots (§ 9 Abs. 1 Satz 2 VZG) nicht präzise bestimmt werden kann.

- Die Vorschriften für die (ausnahmsweise) Übermittlung von Einzelangaben (§ 9 Abs. 2 – 4 VZG) müssen präzisiert werden:

  1. Einzelangaben dürfen nur ausnahmsweise, wenn die Auswertung durch das Statistische Landesamt nicht möglich ist, übermittelt werden.

  2. Sie dürfen nur zu statistisch-planerischen Zwecken weitergegeben werden. Die zulässigen Zwecke müssen präzise beschrieben werden.

  3. Daten dürfen nur in dem Umfang übermittelt werden, der für den jeweiligen Zweck erforderlich ist (d.h. z.B. ohne Anschrift, wenn die vorhandenen räumlichen Aggregationen ausreichen).

- Schwerpunktmäßig habe ich mich mit der Frage befaßt, welche Teile der Organisation und des Verfahrens der Volkszählung in dem Volkszählungsgesetz selbst geregelt werden müssen. Ich halte weitergehende Regelungen für erforderlich, weil auch das Erhebungsverfahren in die grundrechtlich geschützte Rechtssphäre eingreift.
  Die folgenden zusätzlichen Sachverhalte müßten in einem neuen Volkszählungsgesetz oder in Ausführungsgesetzen der Länder oder in Rechtsverordnungen aufgrund dieser Gesetze geregelt werden:

  Form und Inhalt der Fragebögen, insbesondere
  1. Trennung von Identifikationsmerkmalen und statistischen Angaben,
  2. Hinweis darauf, daß Identifikationsmerkmale nicht gespeichert werden,
  3. Verzicht auf freiwillige Angaben, zumindest aber Hinweis auf die Freiwilligkeit der Angaben,
  4. Belehrung des Bürgers über seine Rechte;

  Rechte des Bürgers im Erhebungsverfahren, insbesondere
  5. das Recht, die geforderten Angaben in einem eigenen Fragebogen zu machen, insbesondere für die Auskunftspflichtigen, die zusammen mit anderen in einem Haushalt leben,

6. das Recht, den ausgefüllten Fragebogen unmittelbar der Erhebungsdienststelle zuzuleiten, damit der Zähler keinen Einblick in den Inhalt nehmen kann;

Grundzüge der Erhebungsorganisation, insbesondere
7. Einrichtung und Aufgaben der Erhebungsdienststellen,
8. Grundsätze für die Auswahl der Zähler (Eignung, Vertrauenswürdigkeit etc.),
9. Grundsätze für den Einsatz des Zählers (örtliches Einsatzgebiet, Ausschluß von Interessenkonflikten),
10. Grundsätze für die Entschädigung der Zähler (keine „Erfolgsprämien");

Aufbewahrungs- und Löschungsfristen für
11. die Identifikationsmerkmale,
12. die Angaben aus der Zählungsorganisation (z. B. Kenn-Nr.),
13. die Erhebungsunterlagen (Fragebogen, Zählerlisten);

Grundzüge der automatisierten Datenverarbeitung, insbesondere
14. Speicherung der Einzelangaben in sequentieller Organisation und ohne, daß sie in ständigem Zugriff stehen.

Die Forderung, die Grundzüge der automatisierten Verarbeitung gesetzlich zu regeln, dringt tiefer in die Organisationshoheit der Executive ein. Ich halte ein Tätigwerden des Gesetzgebers gleichwohl für notwendig, weil die Speicherung der Einzelangaben einen Eingriff in die durch Art. 2 Abs. 1 i. V. mit Art. 1 Abs. 1 GG geschützte Rechtssphäre darstellt, der nur hinnehmbar ist, wenn das Risiko einer mißbräuchlichen Nutzung so gering wie möglich gehalten wird.

Der Aufwand für die Reidentifizierung einzelner Betroffener als Voraussetzung für eine mißbräuchliche Benutzung ist wegen der für statistische Auswertungen eingesetzten Datenverarbeitungstechnik, die mit dem Stichwort Stapelverarbeitung gekennzeichnet werden kann, gegenwärtig relativ hoch. Da die Stapelverarbeitung für statistische Aufbereitungen (Eingabekontrollen und Herstellung von Tabellen) ausreichend, zweckmäßig und wirtschaftlich ist, müssen die Strukturprinzipien dieser Verarbeitungsform gesetzlich festgeschrieben werden. Es besteht von der Aufgabe her, die der amtlichen Statistik bei der Verarbeitung von Einzelangaben gestellt ist, keine Notwendigkeit, die Daten in anderer Weise zu speichern.

Selbst wenn das Bundesverfassungsgericht das Volkszählungsgesetz 1983 nicht in wesentlichen Teilen für verfassungswidrig erklären sollte, bedarf es für eine spätere Volkszählung eines neuen Gesetzes. Ich gehe davon aus, daß der Gesetzgeber – wie auch immer das Gericht auf die Verfassungsbeschwerde entscheiden wird – aus den Erfahrungen bei der Vorbereitung der Volkszählung 1983 gelernt hat.

3.7.2 Mikrozensus, EG-Stichprobenerhebung über Arbeitskräfte

3.7.2.1 Mikrozensus

Der Bundestag hat am 15.12.1982 das Gesetz über die Durchführung einer Repräsentativerhebung der Bevölkerung und des Erwerbslebens (Mikrozensusgesetz) beschlossen. Nachdem der Bundesrat zugestimmt hatte, ist das Mikrozensusgesetz am 21.2.1983 verkündet worden. Da das vorangegangene Mikrozensusgesetz nur bis einschließlich 1982 galt (die Mikrozensusgesetze haben eine befristete Gültigkeit), sind damit die rechtlichen Grundlagen geschaffen worden, um auch 1983 einen Mikrozensus durchzuführen.

Hierauf hat der Bundesinnenminister aber verzichtet, weil er die Entscheidung des Bundesverfassungsgerichts über die Volkszählung abwarten wollte, die wegen der zu erwartenden grundsätzlichen Feststellungen zu statistischen Erhebungen sicherlich auch für den Mikrozensus Bedeutung hat. Z. Z. wird eine Rechtsverordnung gem. § 6 Abs. 4 des Bundesstatistikgesetzes vorbereitet, mit der der Mikrozensus für 1983 ausgesetzt wird.

Der Bundestag hat das neue Mikrozensusgesetz sehr ausführlich beraten und dabei insbesondere den Umfang der vorgesehenen Erhebungen geprüft. Aufgrund dieser Prüfung ist der von der Bundesregierung vorgelegte Gesetzentwurf in einzelnen Punkten geändert worden (Verzicht auf einzelne Fragen). Auf Empfehlung des federführenden Innenausschusses hat der Bundestag die Bundesregierung in einer Entschließung ersucht, „dem Deutschen Bundestag bis zum 31. Dezember 1985 über die bisherigen Erfahrungen bei der Durchführung des Gesetzes zu berichten und dabei auch darzulegen,

1. in welchem Umfang auf Erhebungen nach dem Mikrozensusgesetz wegen Reduzierung oder Wegfalls der sachlichen Notwendigkeit dieser Erhebung verzichtet werden kann,
2. in welchem Umfang Erhebungen nach dem Mikrozensusgesetz durch weniger kostenintensive und gleichwertige oder bessere Umfragemethoden ersetzt werden können.

Dabei sollen auch die neuesten Erkenntnisse der empirischen Sozialforschung und die Erfahrung mit statistischen Erhebungen im Ausland bewertet und sofern sie auf anderen Systemen beruhen, ihre Geeignetheit für die Bundesrepublik Deutschland geprüft werden."

Der mit diesem Ersuchen angeforderte Bericht der Bundesregierung wird Grundlage nicht nur für die Überprüfung des Mikrozensus sein; da der Mikrozensus eine zentrale Bedeutung im statistischen System hat, wird der Bericht weitgreifende Auswirkungen auf die Statistik insgesamt haben.

3.7.2.2 EG-Stichprobenerhebung über Arbeitskräfte

Die Erhebung beruht auf der Verordnung (EWG) Nr. 603/83 des Rates vom 14.3.1983 zur Durchführung einer Stichprobenerhebung über Arbeitskräfte im Frühjahr 1983 (Amtsblatt der Europäischen Gemeinschaft Nr. 2 72/1 vom 18.3.1983). Nach dem Recht der Europäischen Gemeinschaft gilt diese Verordnung unmittelbar in den Mitgliedstaaten, ohne daß es einer Übernahme durch Rechtsetzung in den einzelnen Mitgliedstaaten bedarf.

Die EG-Stichprobenerhebung über Arbeitskräfte hat es auch in früheren Jahren schon gegeben; sie wurde zusammen mit dem Mikrozensus durchgeführt. Da es 1983 keinen Mikrozensus gab, mußte die EG-Stichprobenerhebung über Arbeitskräfte allein, für sich erhoben werden. Wegen der zeitlichen Nähe zur Auseinandersetzung um die Volkszählung – die Vorbereitungen für die Erhebung liefen im Mai 1983 an – wurde die EG-Stichprobenerhebung für kurze Zeit in der Presse als eine Art „Ersatz-Volkszählung" diskutiert. Nach meinen Feststellungen verweigerten in Hamburg ca. 70 Auskunftspflichtige ihre Mitwirkung; in dem anschließenden Verwaltungszwangsverfahren änderten ca. 50 Auskunftspflichtige ihre Haltung und beantworteten die Fragen. Aus den verbleibenden Fällen sind acht Verfahren vor dem Verwaltungsgericht anhängig, das noch nicht entschieden hat.

Für mich stellt sich nur die Frage, wie die Durchführung der Erhebung aus der Sicht des Datenschutzes zu beurteilen ist. Nach meinen Feststellungen wurden die Angaben zur Indentifikation des Auskunftspflichtigen auf einem Mantelbogen bzw. auf einer abreißbaren Leiste des Fragebogens erhoben, so daß sie nach der Plausibilitätskontrolle von den eigentlichen statistischen Angaben getrennt und vernichtet werden konnten. Die Abreißleiste ist bereits vernichtet worden, der Mantelbogen wird noch vernichtet. Die mit der Erhebung gewonnenen statistischen Angaben werden anonym an die Europäische Gemeinschaft zur Auswertung gegeben.

3.8. Einwohnerwesen

Dem Einwohnerwesen kommt bei meiner Arbeit eine besondere Bedeutung zu. Dieser Bereich, der organisatorisch beim Einwohner-Zentralamt der Behörde für Inneres sowie bei den Bezirksämtern angesiedelt ist und der im einzelnen die – funktional und organi-

satorisch – voneinander getrennten Aufgabenbereiche Meldewesen, Personalausweis-/Paßwesen, Ausländerangelegenheiten und Personenstandswesen umfaßt, zeichnet sich durch folgende Besonderheiten aus:
Zum einen werden nicht nur Gruppen der Bevölkerung, sondern sämtliche Einwohner Hamburgs mit einer relativ großen Anzahl ständig aktuell gehaltener personenbezogener Daten erfaßt; zum zweiten ist die Verwaltungstätigkeit in diesem Bereich – im Gegensatz zu anderen Behörden – in starkem Maße darauf gerichtet, Daten gerade für die Nutzung durch andere Behörden bereitzuhalten.

Auch in diesem Bereich erlaubten es meine begrenzten Kapazitäten nicht, eine über die Einzelfallprüfung hinausgehende Kontrolltätigkeit zu entfalten. Die Schwerpunkte meiner Beratungstätigkeit in diesem Bereich lagen bei den Problemen:
- Einführung des neuen maschinenlesbaren Personalausweises
- Entwurf einer Meldedaten-Übermittlungs-VO
- Automation des Meldewesens
- Neufassung der Dienstanweisung für die Standesbeamten und ihre Aufsichtsbehörden

3.8.1 Meldewesen

Das Meldewesen wird rechtlich strukturiert durch das Hamburgische Meldegesetz (HmbMG) mit seinen detaillierten Regelungen zur Speicherung und Übermittlung von Meldedaten, zu Meldepflichtigen sowie spezifisch geregelten Schutzrechten für Betroffene. Am Gesetzgebungsverfahren für das Meldegesetz in den Jahren 1981/82 war ich noch nicht beteiligt. Ich bin nicht in der Lage, heute schon abschließende Feststellungen darüber zu treffen, ob das Gesetz allen datenschutzrechtlichen Anforderungen gerecht wird. In der Praxis, insbesondere bei Diskussionen mit der Verwaltung im Zusammenhang mit dem Entwurf einer Meldedatenübermittlungsverordnung (HmbMeldDÜV) haben sich jedoch einige Probleme gezeigt, die durch das Meldegesetz noch nicht gelöst worden sind (s. Nr. 3.8.1.1). Die insoweit aufgetretenen Fragen sollten Anlaß sein, zu gegebener Zeit – nach Vorliegen weiterer praktischer Erfahrungen – grundsätzlich zu prüfen, wieweit das Gesetz den selbst gestellten hohen Anforderungen gerecht wird.

Schwierigkeiten haben sich ferner bei der Umsetzung einzelner gesetzlicher Bestimmungen (z. B. über Auskunft und Löschung) in die Praxis ergeben (s. Nr. 3.8.1.2).

3.8.1.1 Regelmäßige Datenübermittlungen aus dem Melderegister

In § 31 Abs. 5 HmbMG wird der Senat ermächtigt, durch Rechtsverordnung die regelmäßige Übermittlng der in § 31 Abs. 1 und 2 HmbMG genannten Daten zuzulassen. Er hat dabei Anlaß und Zweck der Übermittlung, die Datenempfänger und die zu übermittelnden Daten festzulegen. Die Behörde für Inneres hat einen Verordnungsentwurf erarbeitet. Eine endgültige Verabschiedung durch den Senat stand bei Abschluß dieses Berichts noch aus.

3.8.1.1.1 Vorgesehene Übermittlungsempfänger

Nach dem derzeitigen Sachstand sind die nachstehenden Stellen als Empfänger regelmäßiger Datenübermittlungen mit einem jeweils genau definierten Datensatz vorgesehen:

- für Zwecke des Meldewesens: andere Hamburger Meldebehörden
- zur Führung der Wohnraumkartei: Bezirksämter
- für Zwecke der Familienbuchführung: Standesämter
- zur Durchführung von allgemeinen Wahlen: Statistisches Landesamt – Landeswahlamt – und Wahldienststellen der Bezirksämter
- zur allgemeinen Ausschreibung von Lohnsteuerkarten: Behörde für Inneres
- zur Vorbereitung der Wehrerfassung: Bezirksämter

- für statistische Zwecke: Statistisches Landesamt
- zur Fortführung von Paßsperrakten: Behörde für Inneres
- zur Erfüllung von Aufgaben auf dem Gebiet des Ausländerwesens: Behörde für Inneres
- zur Durchsetzung der Schulpflicht: Behörde für Schule und Berufsbildung
- für Zwecke der Säuglings- und Kleinkinderfürsorge: Bezirksgesundheitsämter
- für kirchliche Zwecke: öffentlich-rechtliche Religionsgesellschaften
- zur Ehrung von Altersjubilaren: Senatskanzlei
- zur Aufklärung von Straftaten: Datenabgleich mit der Polizei

3.8.1.1.2 Regelung des automatisierten Datenabgleichs

Der vorgesehene Abgleich von Daten des Melderegisters mit dem Informationssystem der Polizei ist nicht frei von Bedenken. Im Falle eines Abgleichs übermittelt die Meldebehörde erheblich mehr Daten an den Empfänger als – streng genommen – zur Aufgabenerfüllung erforderlich sind. Daran ändert auch die Tatsache nichts, daß die beiden Bestände innerhalb einer Stelle, der DVZ, die gleichzeitig Auftragnehmerin der Meldebehörde und des vorgesehenen Empfängers ist, miteinander verglichen werden. Dem versucht der Verordnungsentwurf mit folgender Regelung entgegen zu wirken:

> „Wird in dieser Verordnung die Datenübermittlung beschränkt auf die Form des automatisierten Datenabgleichs zugelassen, ist durch technische und organisatorische Maßnahmen sicherzustellen, daß durch den Vergleich der Datenbestände des Empfängers und der Meldebehörde dem Empfänger nur personenbezogene Daten derjenigen Personen zur Kenntnis gebracht oder sonst wahrnehmbar gemacht werden können, die in dem Datenbestand bereits vorhanden sind, welcher bei dem Empfänger zu dem in der Übermittlungsvorschrift genannten Zweck geführt wird."

Die Polizei soll mithin nur die Daten speichern – also erfassen und zur weiteren Verwendung aufbewahren – können, die zur Aufgabenerfüllung erforderlich sind.

Mit dieser Maßgabe habe ich meine Bedenken gegen regelmäßige Übermittlungen in der Form des automatisierten Datenabgleichs zurückgestellt. Eine entsprechende Regelung soll in das Krebsregistergesetz aufgenommen werden. Auf einen Abgleich mit den Datenbeständen anderer Stellen ist im Laufe der Diskussion verzichtet worden.

Ich lege aber Wert darauf, daß die Notwendigkeit eines Abgleichs für polizeiliche Zwecke im Zusammenhang mit der geplanten Novellierung des SOG noch einmal erörtert wird. Hierüber besteht mit der Behörde für Inneres Einverständnis.

3.8.1.1.3 Übermittlungen zwischen den hamburgischen Meldebehörden

Gem. § 31 Abs. 5 Satz 1 HmbMG wird der Senat nur ermächtigt, durch Rechtsverordnung die regelmäßige Übermittlung der in § 31 Abs. 1 und 2 HmbMG genannten Daten zuzulassen. Empfänger dieser Übermittlungen können nur andere Behörden und sonstige öffentliche Stellen der FHH sein. Nicht erfaßt von der Verordnungsermächtigung werden Datenübermittlungen gem. §§ 30, 32 und 33 HmbMG, also zwischen den Meldebehörden, an den Suchdienst und an öffentlich-rechtliche Religionsgesellschaften. Dementsprechend ist eine Regelung der Datenübermittlungen zwischen den örtlichen Meldedienststellen (der Bezirksämter) und der zentralen Meldebehörde (Einwohner-Zentralamt) – wie sie die Behörde für Inneres im Verordnungs-Entwurf vorgesehen hat – nicht von der Verordnungsermächtigung gedeckt. Da die hamburgischen Meldebehörden jedoch organisatorisch verschiedenen Behörden angehören (Behörde für Inneres, Bezirksämter) finden auch insoweit Datenübermittlungen (i. S. des Datenschutzgesetzes) statt, die einer rechtlichen Regelung – etwa ebenfalls durch eine Verordnung – bedürfen. Diese Übermittlungen werden vom Meldegesetz nicht berücksichtigt. Dies ergibt sich schon daraus, daß das Gesetz – ohne den organisatorischen Gegebenheiten Rech-

nung zu tragen – von einer Meldebehörde spricht (vgl. z. B. § 1 Abs. 2 HmbMG). Da ich davon ausgehe, daß der Gesetzgeber die vorhandene Organisation des Meldewesens nicht ändern wollte, rege ich an, durch eine Änderung des Meldegesetzes klare Grundlagen für die Datenflüsse zwischen den Meldebehörden zu schaffen.

3.8.1.1.4 Übermittlungen an die Kirchen

Wie oben bereits erwähnt, ist vorgesehen, daß in der HmbMeldDÜV auch zusätzlich die – in § 33 HmbMG nicht detailliert genannten – Anlässe für die Datenübermittlung an öffentlich-rechtliche Religionsgesellschaften geregelt werden. Auch diese Regelung ist von der VO-Ermächtigung des § 31 Abs. 5 HmbMG nicht gedeckt. Wenn die konkreten Anlässe einer Datenübermittlung für kirchliche Zwecke im einzelnen per Rechtsvorschrift eingegrenzt werden sollten – wofür zumindest die Gleichbehandlung mit den sonstigen regelmäßigen Datenübermittlungen spricht –, so sollte eine solche Regelung durch den Gesetzgeber in § 33 HmbMG, der die Datenübermittlungen an öffentlich-rechtliche Religionsgesellschaften abschließend regelt, erfolgen.

3.8.1.1.5 Übermittlung durch Übersendung von Meldescheinen

Aus Gründen der Praktikabilität soll in der vorgesehenen HmbMeldDÜV in drei Fällen eine Datenübermittlung durch Übersendung einer Ausfertigung des Meldescheins zugelassen werden, obwohl dieser mehr Daten enthält, als die empfangenden Stellen zur rechtmäßigen Aufgabenerfüllung benötigen. Ich habe der Behörde für Inneres mitgeteilt, daß ich diese Art der Übermittlung für datenschutzrechtlich bedenklich halte. Ich könne sie – wenn überhaupt – allenfalls für eine Übergangszeit und nur dann tolerieren, wenn sichergestellt sei, daß die Meldescheine nach ihrer Auswertung unverzüglich zurückgegeben würden. Diese Forderungen hat die Behörde für Inneres in zwei Fällen akzeptiert. In einem Fall (Ausländerbehörde) sieht sie sich nicht in der Lage, die Meldescheine nach Auswertung zurückzusenden, sondern will sie wie bisher in den jeweiligen Akten ablegen. Eine solche Datenübermittlung verstößt eindeutig gegen § 31 Abs. 5 i. V. m. Abs. 1 HmbMG.

3.8.1.1.6 Datenübermittlungsverordnungen des Bundes

Für hamburgische Meldebehörden relevante Vorschriften über regelmäßige Datenübermittlungen sind nach § 20 Melderechtsrahmengesetz (MRRG) auch auf Bundesebene vorgesehen: Am 1. Oktober 1983 ist die „Verordnung zur Durchführung von regelmäßigen Datenübermittlungen zwischen Meldebehörden verschiedener Länder" (1. BMeldDÜV) vom 18.7.1983 (BGBl. I S. 943) in Kraft getreten.

Dagegen ist die „Verordnung zur Durchführung von regelmäßigen Datenübermittlungen der Meldebehörden an Behörden oder sonstige öffentliche Stellen des Bundes" (2. BMeldDÜV) noch nicht erlassen. Ein Entwurf des Bundesinnenministeriums liegt vor, ist jedoch mit den Ländern und den Datenschutzbeauftragten noch nicht abschließend abgestimmt worden. Vorgesehen sind im Entwurf Datenübermittlungen an die Wehrersatzbehörden, an die Bundesanstalt für Arbeit (Kindergeldabgleich) sowie an den Rentendienst der Deutschen Bundespost.

3.8.1.2 Probleme bei der Umsetzung des Meldegesetzes in die Praxis

In mehreren Fällen bin ich durch Eingaben auf Probleme aufmerksam gemacht worden, die sich bei der Anwendung des neuen Melderechts in der Praxis ergaben.

3.8.1.2.1 Löschung von Haftmitteilungen

Vor Inkrafttreten des neuen HmbMG am 23.8.1982 sind im Melderegister auch Eintragungen über Haftzeiten auf der Grundlage von Haftmitteilungen der Polizei gespeichert worden. Diese Speicherungen sind jedenfalls nach dem neuen Melderecht nicht mehr

zulässig; Haftnotierungen kommen nur noch unter den engen Voraussetzungen des § 25 HmbMG in Betracht. Sie sind daher zu löschen. Dabei entstehen jedoch z. Z. kaum überwindbare Probleme:

Alle vor dem 23.8.1982 angelegten Karteikarten des Personenregisters können Eintragungen über Haftzeiten enthalten. Das Einwohner-Zentralamt hat zunächst durch Dienstanweisung angeordnet, daß bei jeder Bearbeitung einer Karteikarte infolge eines Meldevorgangs
- mit Blei eingetragene Vermerke zu löschen (radieren) und
- bleibend eingetragene Vermerke zu schwärzen sind.

Bei allen anderen Karteikarten, nämlich
- den aktuellen, aber nicht bearbeiteten,
- den ausgesonderten (Verstorbener und Weggezogener), seien sie schon mikroverfilmt (bis einschl. 1973) oder aber für die Mikroverfilmung bereitgestellt (bis 1979),

bleiben die Eintragungen unbehandelt.

Auf den mikroverfilmten Karteikarten können die Eintragungen weder geschwärzt noch sonst gelöscht werden. Auf den noch nicht mikroverfilmten Karteikarten könnten die Eintragungen geschwärzt werden. Das ist jedoch wegen des damit verbundenen Aufwands (die jetzt zur Verfilmung anstehenden Jahrgänge umfassen ca. 560.000 – 600.000 Karteikarten; wenn je Karteikarte nur 2 Minuten angesetzt werden, sind zu ihrer Bereinigung rd. 12 Mannjahre erforderlich) und der Unmöglichkeit, entsprechend qualifiziertes Personal zu bekommen, nicht machbar.

Eintragungen über Haft könnten auch dadurch gelöscht werden, daß die Karteikarten ohne die Haftvermerke neu geschrieben und die alten Karteikarten vernichtet werden. Der Aufwand für dieses Verfahren der Löschung ist noch höher, insbesondere weil in solchen Fällen eine Person in der Regel mehrere Karteikarten hat; es kann daher nur in Einzelfällen in Betracht gezogen werden (z. B. bei Transsexuellen).
Außerdem muß dabei bedacht werden, daß eine neu angefertigte Karteikarte zumindest die Information trägt, daß auf der alten (vernichteten) Karte diskriminierende Vermerke gestanden haben. Dem könnte nur dadurch begegnet werden, daß auch für einige normale Fälle neue Karteikarten angelegt werden.

Um die Lösung dieses Problems praktisch in Angriff nehmen zu können, habe ich dem Einwohner-Zentralamt – in Anlehung an § 10 Abs. 4 HmbMG – die folgenden Maßnahmen vorgeschlagen, die dieses auch akzeptiert hat:
- Die Eintragungen auf mikroverfilmten Karteikarten, die aus technischen Gründen nicht gelöscht werden können, sind zu sperren.
- Die Eintragungen auf den nicht mehr in laufender Bearbeitung befindlichen Karteikarten (sie stehen jetzt oder bald zur Mikroverfilmung an) können wegen des damit verbundenen Aufwands nicht gelöscht werden; auch hier sind die entsprechenden Daten zu sperren.
- Die Eintragungen auf den in laufender Berarbeitung befindlichen Karteikarten werden bei jedem Berarbeitungsvorgang durch Schwärzen gelöscht.
- Die Beachtung der Sperrung und der Löschung durch Schwärzen wird durch Dienstanweisung und eine strikte Dienstaufsicht abgesichert; jeder Verstoß gegen die Geheimhaltung muß unnachsichtig verfolgt und streng geahndet werden.
- Falls ein Betroffener von den Eintragungen (z. B. durch eine Einsichtnahme aufgrund eines Auskunftsantrages) erfährt, und die physische Löschung verlangt, werden neue Karteikarten geschrieben und die alten vernichtet.

Bei dem seit dem 23.8.1982 erfolgenden Mitteilungen über Haft bei Personen ohne festen Wohnsitz (§ 25 HmbMG) wird wie folgt verfahren:
- die Haft wird, wenn über die gemeldete Person eine (frühere) Karteikarte vorliegt, auf dieser mit Blei eingetragen und nach Beendigung gelöscht (radiert),
- sonst wird eine neue (vorübergehende) Karteikarte mit der Eintragung „Haft" angelegt, die nach Beendigung der Haft vernichtet wird.

3.8.1.2.2 Auskunft an den Betroffenen

Durch eine Eingabe – kurz vor Abschluß dieses Berichts – wurde ich darauf aufmerksam, daß das Einwohner-Zentralamt die Auskunfterteilung an den Betroffenen nicht den Anforderungen des § 8 Abs. 1 HmbMG entsprechend handhabt. Dem Petenten wurde auf sein Auskunftsersuchen mitgeteilt, er habe Gelegenheit, die beim Einwohner-Zentralamt über ihn gespeicherten Meldeunterlagen einzusehen. Ich habe diese Meldebehörde darauf hingewiesen, daß sie dem Betroffenen nach § 8 Abs. 1 HmbMG auf Antrag schriftlich Auskunft über die zu seiner Person gespeicherten Daten zu erteilen hat. Die Erteilung einer schriftlichen Auskunft setzt keinen besonderen Antrag auf schriftliche Auskunftserteilung voraus; vielmehr heißt es in der amtlichen Begründung zum HmbMG (Bürgerschafts-Drucksache 9/3994) ausdrücklich, daß eine beantragte Auskunft in Abweichung von § 8 MRRG „schriftlich ergeht".

Ich verkenne nicht, daß das Einwohner-Zentralamt mit seinem Angebot auf direkte Einsichtnahme in die Akten bürgerfreundliche Absichten verfolgte – vermutlich sogar unter Inkaufnahme eines höheren Verwaltungsaufwandes. Dennoch hat es das Verfahren so umzugestalten, daß eine Auskunft schriftlich erteilt wird, es sei denn, daß der Betroffene ausdrücklich darauf verzichtet.

Eine abschließende Stellungnahme des Einwohner-Zentralamtes lag bei Berichtsschluß noch nicht vor.

3.8.1.2.3 Melderegisterauskunft an Dritte

Gem. § 34 Abs. 1, 2 HmbMG dürfen dritten Personen oder Stellen einfache oder – unter engeren Voraussetzungen – erweiterte Melderegisterauskünfte über bestimmte einzelne Einwohner übermittelt werden. Das bedeutet, daß die gesuchte Person als Voraussetzung für eine Melderegisterauskunft mit den vom Anfragenden vorgegebenen Daten im Melderegister zweifelsfrei zu identifizieren sein muß. Andernfalls kann es zu Personenverwechslungen mit möglicherweise für die Betroffenen recht unangenehmen Folgen kommen (z. B. nicht begründete Pfändungsversuche). Diese Problematik ist den Anfragenden leider häufig nicht bekannt und entsprechend Anlaß zu Beschwerden. Das Einwohner-Zentralamt besteht also völlig zu Recht darauf, daß die Anfragenden neben dem Namen zumindest eine frühere Wohnanschrift, möglichst aber das Geburtsdatum angeben. Wenn eine einwandfreie Indentifizierung – ggf. auch mit weiteren Angaben – nicht möglich ist, darf die Meldebehörde nach § 34 HmbMG keine Einzelauskunft erteilen.

3.8.1.3 Automation im Meldewesen

In meinem 1. TB habe ich unter Nr. 6.6.2 auf S. 37 über den gegenwärtigen Stand der Automation im Einwohnerwesen berichtet und darauf hingewiesen, daß ein neues Verfahren erforderlich ist. Die Planungen für ein neues Verfahren sind noch nicht abgeschlossen; die Umrisse sind jedoch schon erkennbar. Ich halte eine Darstellung der wesentlichen Punkte für notwendig, auch um übertriebene Befürchtungen nicht entstehen zu lassen bzw. vorhandene abzubauen.

Gegenstand der Automation sind nur die regionalen Einwohnerkarteien in den Einwohnerdienststellen. Das gegenwärtige manuelle Verfahren im Einwohner-Zentralamt wird beibehalten; ein Anschluß des Einwohner-Zentralamtes an das künftige automatisierte Verfahren ist gegenwärtig nicht vorgesehen.

Das automatisierte Verfahren wird aus Kostengründen in Teilen von Schleswig-Holstein übernommen. Es sieht eine zentrale Einwohnerdatenbank vor, die die Teilbestände aller Einwohnerdienststellen zusammenfaßt; jede Einwohnerdienststelle darf grundsätzlich nur auf Daten ihres Teilbestandes (Datensätze aller Einwohner, die in ihrem Zuständigkeitsbereich gemeldet sind) zugreifen. An die Datenbank sind Benutzerstationen ange-

schlossen, über die aufgrund von Meldevorgängen die Daten in der Datenbank geändert werden. Die Benutzerstationen dienen der Datenerfassung und -eingabe; sie sind – abgesehen von Ausnahmefällen (insbesondere innerstädtischer Umzug) – keine Auskunftsstationen.

Auskunftsgrundlage für die in den Einwohnerdienststellen tätigen Sachbearbeiter sind Mikroverfilmungen (sog. COM-Fiches) des Teilbestandes ihrer Einwohnerdienststelle. Die COM-Fiches werden alle 2 Tage hergestellt und an die Einwohnerdienststellen verteilt (ggf. erhalten Bezirksämter für die Wahrnehmung zentraler Aufgaben die COM-Fiches aller Einwohnerdienststellen ihres Zuständigkeitsbereichs). Für das Lesen der COM-Fiches stehen COM-Lesegeräte zur Verfügung. Die COM-Fiches sind passive Auskunftsmittel; sie können nicht verändert werden. Der Sachbearbeiter entnimmt ihnen die zu erfassenden oder zu ändernden Daten und trägt sie in einen Erfassungsbeleg ein, der nach Abschluß des Bearbeitungsvorganges über die Benutzerstation eingegeben wird.

3.8.2 Personalausweis-/Paßwesen

Schwerpunktmäßig hatte ich mich mit den Problemen zu beschäftigen, die mit der geplanten Einführung neuer fälschungssicherer und computerlesbarer Personalausweise und Pässe im Zusammenhang stehen.

Bereits im Jahre 1980 wurden wesentliche Bestimmungen des Bundespersonalausweisgesetzes (BPAG) neu gefaßt. Meine Kollegen im Bund und in den anderen Ländern haben sich schon damals intensiv mit dem vorgesehenen neuen Ausweis befaßt, eine Reihe von Forderungen zum BPAG erhoben und auch weitgehend durchgesetzt sowie einige Rahmenbedingungen formuliert, die vor der Einführung der neuen Ausweiskarte erfüllt sein müßten.
Nach der Verabschiedung des Änderungsgesetzes von 1980 ist die Einführung des neuen Personalausweissystems – insbesondere wegen der Kosten – nochmals grundsätzlich zwischen Bund und Ländern erörtert worden; gleichzeitig wurde beschlossen, das Inkrafttreten des neuen BPAG auszusetzen.

Erst im Februar 1983 passierte das 4. Gesetz zur Änderung des BPAG abschließend den Bundesrat. Hamburg stimmte diesem Gesetz nach Abwägung der Vor- und Nachteile des neuen Systems – insbesondere des Verhältnisses zwischen dem angestrebten Sicherheitsgewinn einerseits und der Kostenbelastung für den Bürger und die öffentliche Hand andererseits – nicht zu. An der Vorbereitung dieser Entscheidung bin ich nicht beteiligt worden.

Erst in der Folgezeit – insbesondere veranlaßt durch das Erfordernis, bis zum Inkrafttreten des Bundesgesetzes auch ein Landespersonalausweisgesetz zu erlassen – hatte ich Gelegenheit, mich mit dem neuen System zu befassen.
Im August habe ich dem Präses der Behörde für Inneres eine detaillierte Auflistung von Forderungen zum Bundes-PAG, zum Landes-PAG und zu flankierenden Maßnahmen (bereichsspezifischen Datenschutzregelungen) im Sicherheitsbereich übermittelt. Der Präses der Behörde für Inneres hat mir zwischenzeitlich mitgeteilt, daß er meine Anforderungen an die Personalausweisgesetze voll akzeptiert. Offen ist noch, wieweit auch meine Forderungen zu bereichsspezifischen Regelungen im Polizeirecht berücksichtigt werden.

Im September 1983 haben die Datenschutzbeauftragten des Bundes und der Länder eine Entschließung mit datenschutzrechtlichen Anforderungen an den fälschungssicheren und maschinenlesbaren Personalausweis bzw. Paß verabschiedet. Sie kommen zu dem Ergebnis: Ihre – frühere – Aussage, daß ein maschinenlesbarer Personalausweis unter Datenschutzgesichtspunkten hinnehmbar sei, könne nur dann aufrechterhalten werden, wenn die bereits 1979 erhobenen Forderungen in ausreichendem Maße erfüllt würden und auch im übrigen bei der Ausführung des BPAG den Datenschutzbelangen Rechnung getragen werde.

Im folgenden werde ich zunächst noch einmal deutlich machen, worin ich das zusätzliche Gefährdungspotential der neuen Ausweiskarte sehe (Nr. 3.8.2.1) und sodann im einzelnen auf Unklarheiten des BPAG (Nr. 3.8.2.2) und Anforderungen an das Landespersonalausweisgesetz eingehen.

3.8.2.1 Gefahren des neuen Ausweises

Die geplante Ausweiskarte unterscheidet sich von dem bisherigen Ausweisbuch nicht nur durch eine erhöhte Fälschungssicherheit, sondern auch – was aus Sicht des Datenschutzes allein relevant ist – durch seine automatische Lesbarkeit. Das bedeutet zum einen, daß vorhandene Dateien mit Hilfe des Personalausweises automatisch danach abgefragt werden können, ob über den Ausweisinhaber eine Information vorliegt (Erschließung von Dateien). Weiter wird es ermöglicht, die Ausweisdaten z. B. zusammen mit Ort, Zeit und Anlaß des Lesens automatisch in einer Datei zu speichern (Einrichtung einer Datei). Es ist somit technisch nicht ausgeschlossen, daß vom Betroffenen unbemerkt und mit minimalem Aufwand unzulässige Datensammlungen entstehen, die über den jeweiligen Aufenthalt und die Zusammenhänge, in denen der Ausweis vorgezeigt und verwendet wird, Aufschluß geben.

Die Datenschutzbeauftragten haben diese Gefahren gesehen und bereits vor 1980 durchgesetzt, daß beide o. g. Nutzungsmöglichkeiten im behördlichen Bereich durch Gesetz grundsätzlich untersagt sind: Nach § 3 Abs. 5 S. 1 BPAG darf der Personalausweis nicht zur automatischen Einrichtung oder Erschließung von Dateien verwendet werden. Eine wichtige Ausnahme von diesem Verbot wird durch den folgenden Satz 2 zugelassen: Polizei und Grenzbehörden dürfen für Zwecke der Grenzkontrolle sowie für Zwecke der Fahndung aus Gründen der Gefahrenabwehr und Strafverfolgung von den neuen, beschriebenen Möglichkeiten Gebrauch machen. Unter welchen Voraussetzungen und in welchem Umfang solche Maßnahmen rechtlich zulässig sind, hängt von den jeweiligen Befugnissen ab, die der Polizei nach Polizei- und Strafverfahrensrecht zustehen. Diese Befugnisse sind bislang noch recht unklar geregelt und z. T. auch – insbesondere im Hinblick auf die neuen technischen Möglichkeiten – zu weitgehend.

Aus diesem Grunde haben die Datenschutzbeauftragten auf ihrer Konferenz vom 9.11.1979 im Zusammenhang mit dem BPAG den folgenden Vorbehalt beschlossen:
„Die Datenschutzbeauftragten betonen jedoch, daß damit über den zulässigen Umfang von Datenspeicherungen und -übermittlungen im Sicherheitsbereich noch nicht entschieden ist und fordern die baldige Verabschiedung eines datenschutzgerechten Melderechts sowie die zügige Erarbeitung spezieller Datenschutzvorschriften für die Sicherheitsbehörden. Nur unter dieser Bedingung ist die Verwendung der maschinenlesbaren Ausweiskarte für Zwecke des polizeilichen Informationssystems annehmbar."

Der Bundestag hat die Vorbehalte akzeptiert und in seine anläßlich der Verabschiedung des BPAG am 17.1.1980 einstimmig beschlossene Entschließung (vgl. BT-Drs. 8/3498, sowie Protokoll über die 196. Sitzung S. 15666) einfließen lassen. Diese hat folgenden Wortlaut:
„Der Deutsche Bundestag ist der Auffassung, daß angesichts der raschen Fortentwicklung der automatischen Datenverarbeitung und deren Einsatz in der öffentlichen Verwaltung über die Verabschiedung des Gesetzes zur Änderung des Gesetzes über Personalausweise hinaus weitere Maßnahmen erforderlich sind, um einen ausreichenden Schutz der Persönlichkeitsrechte der Bürger gegen mißbräuchliche Verwendung ihrer persönlichen Daten zu gewährleisten.
Die Bundesregierung wird deshalb ersucht,
1. den Entwurf eines datenschutzgerechten Melderechtsrahmengesetzes einzubringen und
2. die Arbeiten zur Entwicklung bereichsspezifischer Datenschutzregelungen für die Sicherheitsbehörden nachdrücklich fortzusetzen."

Diese Rahmenbedingungen sind bislang nicht hinreichend erfüllt. Zwar sind auf Bundesebene (MRRG) sowie in den meisten Ländern zwischenzeitlich Meldegesetze in Kraft getreten, die – soweit sie nicht die Speicherung der Serien-Nr. des Personalausweises vorsehen – im großen und ganzen als datenschutzgerecht bezeichnet werden können. Dagegen haben – mit Ausnahme von Bremen – Bund und Länder nur wenig unternommen, um die polizeiliche Datenverarbeitung auf die notwendigen gesetzlichen Grundlagen zu stellen. Der Bundesinnenminister hat kürzlich zu erkennen gegeben, daß er die in den Jahren 1980/81 für den Sicherheitsbereich geschaffenen Verwaltungsvorschriften (KpS-Richtlinien, Amtshilferichtlinien) für völlig ausreichend hält.

Ob andere Länder, die z. T. erst in jüngster Zeit ihre Polizeigesetze nach dem Vorbild des „Musterentwurfs für ein einheitliches Polizeigesetz" novelliert haben, bereit sind, ihre Vorschriften über Personenkontrollen noch einmal zu überprüfen und ihren Standpunkt aufzugeben, daß es bereichsspezifischer Regelungen der polizeilichen Datenerhebung und -verarbeitung nicht bedürfe, halte ich nach meinem derzeitigen Informationsstand für sehr zweifelhaft. Selbst wenn die im kommenden Jahr geplante Novellierung des Hamb. SOG Regelungen erbringt, die den Anforderungen eines bereichsspezifischen Datenschutzes gerecht werden, sind damit allein die notwendigen Rahmenbedingungen für die Einführung der neuen Ausweiskarte noch nicht erfüllt. Nach meiner derzeitigen Einschätzung werden am 1.1.1984 die einer Einführung des neuen Systems entgegenstehenden datenschutzrechtlichen Bedenken nicht ausgeräumt sein.

Abgesehen von dieser grundsätzlichen Kritik müßten bei einer Ausführung des Gesetzes im übrigen noch diverse Einzelpunkte berücksichtigt werden, die nachstehend ausgeführt werden.

3.8.2.2 Unklarheiten und Defizite im Bundespersonalausweis-Gesetz

Zu diesem Themenkomplex hat die DSB-Konferenz am 13.9.1983 eine Position erarbeitet, die folgende Punkte umfaßt:

3.8.2.2.1 Protokollierung von Anfragen in polizeilichen Informationssystemen

Soweit bei polizeilichen Personenkontrollen Anfragen in polizeilichen Informationssystemen vorgenommen werden, dürfen diese Anfragen nicht personenbezogen kontrolliert werden, damit insbesondere keine Bewegungsbilder entstehen können. Da solche Protokollierungen, die als „Einrichtung von Dateien" anzusehen sind, nicht Zwecken der Grenzkontrolle und der Fahndung i. S. des § 3 Abs. 5 S. 2 BPAG dienen, sind sie nach § 3 Abs. 5 S. 1 BPAG unzulässig.

Demgegenüber hat das Bundesinnenministerium bei der Beantwortung einer Kleinen Anfrage am 24.8.1983 die folgende Position vertreten (Drs. 10/341, Nr. 8):
„Die Regelung in § 3 Abs. 5 S. 2 des BPAG in der Fassung vom 15.3.1983 schließt eine automatische Protokollierung der Abfragen mit dem maschinell lesbaren Personalausweis an das polizeiliche Informationssystem INPOL für Zwecke der Grenzkontrolle und der Fahndung aus Gründen der Strafverfolgung und der Gefahrenabwehr nicht aus; eine solche ist aber im BPAG nicht vorgesehen und nach § 9 Abs. 1 des BDSG nur zulässig, wenn dies zur rechtmäßigen Erfüllung der Aufgaben der die Abfragen speichernden Stelle erforderlich ist."

3.8.2.2.2 Verwendung der Serien-Nr. durch die Polizei

Die Datenschutzbeauftragten gehen davon aus, daß die Nutzung des Personalausweises durch die Polizei nach § 3 Abs. 5 S. 2 BPAG nicht auch die Verwendung der Seriennummer einschließt; hierfür ist § 3 Abs. 4 BPAG die Spezialvorschrift. Die Behörde für Inneres hat mir mitgeteilt, daß sie diesen Standpunkt teilt.

3.8.2.2.3 Nutzung des Personalausweises im nicht-öffentlichen Bereich

Wie bereits oben ausgeführt (vgl. Nr. 3.8.2.1) darf der neue Personalausweis im behördlichen Bereich – vom Sicherheitsbereich abgesehen – weder zur automatischen Erschließung noch zur automatischen Einrichtung von Dateien verwendet werden (§ 3 Abs. 5 S. 1 BPAG). Für den privaten Bereich ist in § 4 BPAG lediglich die Verwendung zur automatischen Erschließung von Dateien verboten, die automatische Einrichtung ist jedoch erlaubt. Meines Wissens war es eine bloße Panne, daß beide Fälle unterschiedlich geregelt worden sind. Der Bundesinnenminister hat jedoch zwischenzeitlich erklärt, der Gesetzgeber habe die automatische Einrichtung von Dateien im Hinblick auf die Privatautonomie des Bürgers für zulässig erklären wollen. Der Ausweisinhaber sei gegenüber privaten Stellen nicht verpflichtet, seinen Ausweis vorzulegen. Daher könne die Verwendung des Ausweises ohnehin nur mit Einwilligung des Ausweisinhabers erfolgen. In diesem Rahmen sollten dem privaten Sektor vorhandene technische Rationalisierungsmöglichkeiten nicht vollständig verschlossen werden (BT-Drs. 10/436 Nr. 9).

Diese Erwägungen können die vom Gesetzgeber vorgenommene Differenzierung nach Auffassung der Datenschutzbeauftragten aber nicht rechtfertigen. Sie fordern, daß die Regelung in § 4 BPAG der in § 3 BPAG angeglichen wird, da die Risiken für den Betroffenen im privaten Bereich nicht geringer sind als im öffentlichen Bereich.

Auch in § 15 Abs. 6 des von der Bundesregierung beschlossenen Entwurfs eines Paßgesetzes (EPaßG) ist – im nicht-öffentlichen Bereich – ebenfalls nur die automatische Erschließung von Dateien mit Hilfe des neuen Passes verboten. In der Begründung hierzu heißt es eigenartigerweise, daß die Verbote des Abs. 6 mit den Beschränkungen korrespondieren, die der öffentlichen Verwaltung auferlegt sind. Bislang bleibt es das Geheimnis des Bundesinnenministers, warum er in der Verwendung des neuen Personalausweises/Passes zur automatischen Einrichtung – jedenfalls im nicht-öffentlichen Bereich – weniger Risiken für den Betroffenen sieht als in der automatischen Erschließung.

Der Präses der Behörde für Inneres hat mir mitgeteilt, daß Hamburg sich nach seiner Auffassung im Rahmen der Beratungen des Paßgesetzentwurfs im Bundesrat für eine Angleichung der Regelungen für den nicht-öffentlichen Bereich an die für den öffentlichen Bereich geltenden Bestimmungen sowohl im Paßgesetzentwurf als auch im Personalausweisgesetz einsetzen sollte.

3.8.2.2.4 Internationale Lesbarkeit

Die internationale Lesbarkeit des Personalausweises erfordert für deutsche Staatsangehörige die gleiche Schutzintensität auch im grenzüberschreitenden Reiseverkehr. Die DSB-Konferenz hat daher die Bundesregierung gebeten, sich dafür einzusetzen, daß die datenschutzrechtlichen Anforderungen an die innerstaatliche Verwendung des Ausweises auch im internationalen Bereich umgesetzt werden.

3.8.2.3 Anforderungen an ein Landespersonalausweisgesetz

Zur Umsetzung des BPAG sind noch Ausführungsgesetze der Länder erforderlich. Ein Formulierungsvorschlag für solche Ländergesetze ist von einem Arbeitskreis der Innenministerkonferenz erarbeitet und von einigen Ländern bereits ins Parlament eingebracht worden. Die Datenschutzbeauftragten haben diesen Formulierungsvorschlag kritisch überprüft und eine Reihe von zusätzlichen Anforderungen formuliert. Im einzelnen geht es um folgende Punkte, die auch in dem noch ausstehenden Hamburger Entwurf zu berücksichtigen sind:

1. Im Ausführungsgesetz oder in den Verwaltungsvorschriften muß festgelegt werden, daß ein Personenfeststellungsverfahren nur durchzuführen ist, wenn Zweifel an der Identität des Ausweisbewerbers nicht ausgeräumt werden können, und daß in diesem Verfahren erkennungsdienstliche Maßnahmen nur als letztes Mittel zulässig

sind. Eine Weiterleitung dieser Unterlagen an das Bundeskriminalamt darf nur für den Vergleich mit anderen Unterlagen zugelassen werden.

2. Im Ausführungsgesetz muß bestimmt werden, daß die erkennungsdienstlichen Unterlagen zu vernichten sind, sobald die Identität festgestellt ist.

3. In das Personalausweisregister dürfen nur die im Personalausweis enthaltenen personenbezogenen Daten (§ 1 Abs. 2 BPAG) sowie Vermerke über Anordnungen nach § 2 Abs. 2 BPAG aufgenommen werden. Von der Aufnahme der Angabe „unveränderliche Kennzeichen" (§ 11 Abs. 2 Nr. 6 des Formulierungsvorschlages) muß abgesehen werden.

4. Der Zweck des Personalausweisregisters ist im Ausführungsgesetz selbst festzulegen. Hierbei ist zu berücksichtigen, daß es nicht Aufgabe dieses Registers sein kann, eine weitere umfassende Identifizierungsdatei neben dem Melderegister zu eröffnen, zumal dadurch weitere Daten (Lichtbild und Unterschrift) mit den Meldedaten verknüpft werden können. Datenübermittlungen an andere öffentliche Stellen und an Private sind auszuschließen. Eine Ausnahme darf nur für Übermittlungen an die Polizei zugelassen werden, wenn es im Einzelfall für deren Aufgabenerfüllung erforderlich ist.

5. Spätestens 5 Jahre nach Ablauf der Gültigkeit des Personalausweises sind die Daten im Personalausweisregister ohne Einschränkung zu löschen.

   Für die Ausstellung eines vorläufigen Personalausweises reicht eine kürzere Aufbewahrungsdauer aus. Entspechend § 10 Abs. 4 des Entwurfs des Niedersächsischen Ausweisgesetzes sollten die Daten höchstens bis zu einem Jahr nach Ablauf des Jahres der Gültigkeitsdauer aufbewahrt werden.

6. Für Daten der Personen, die im Fall der Entmündigung wegen Geisteskrankheit oder im Fall dauernder Anstaltsunterbringung von der Ausweispflicht befreit worden sind, ist wegen der damit gegebenen Sonderstellung eine strenge Verwendungsbeschränkung vorzusehen.

7. In den Verwaltungsvorschriften zum Ausführungsgesetz der Länder müssen das Verfahren bei Mitteilungen über den Verlust des Personalausweises geregelt und das Formular festgelegt werden.

Die Beratungen über diesen Themenkomplex haben in Hamburg noch nicht begonnen. Der Präses der Behörde für Inneres hat mir jedoch mitgeteilt, daß er meine Vorstellungen in den von ihm vorzulegenden Entwurf eines Landespersonalausweisgesetzes in allen wesentlichen Punkten übernehmen will.

3.8.2.4 Entwurf eines neuen Paßgesetzes

Am 13. Juli 1983 hat die Bundesregierung den Entwurf eines neuen Paßgesetzes beschlossen, der die Einführung eines fälschungssicheren maschinenlesbaren Reisepasses vorsieht und inhaltlich dem PAG – mit seinen Mängeln – entspricht. Die Datenschutzbeauftragten haben klargestellt, daß für dieses Gesetz die gleichen Forderungen gelten wie für das Personalausweisgesetz. Sie haben das Gesetz jedoch noch nicht im einzelnen beraten und sich weitere Forderungen zum Paßgesetz vorbehalten.

3.8.3 Ausländerwesen

Mit der Tätigkeit der Hamburger Ausländerbehörde (also des Einwohner-Zentralamtes – Abt. Ausländerangelegenheiten –) habe ich mich bisher noch nicht befaßt. Zur Überprüfung von Einzelfällen bestand kein Anlaß, da mich noch keine einzige Eingabe eines ausländischen Mitbürgers erreichte. Dies liegt wohl daran, daß die Informationen über die

Rechte nach den Datenschutzgesetzen unter ausländischen Mitbürgern noch wesentlich weniger verbreitet sind als unter deutschen. Ich möchte deshalb betonen, daß die Betroffenenrechte nach den Datenschutzgesetzen ebenso wie das grundgesetzliche Persönlichkeitsrecht für Ausländer wie Deutsche gleichermaßen gelten. Auch das Recht, den Hamburgischen Datenschutzbeauftragten anzurufen, hat jedermann, also auch jeder Ausländer.

Ich habe keinen Grund zu der Annahme, daß das Ausbleiben von Eingaben, die die Ausländerbehörde betreffen, darauf zurückzuführen ist, daß diese Stelle wesentlich sorgfältiger mit personenbezogenen Daten umgeht als andere. Vor allem zur Erfüllung der ihr nach dem Ausländergesetz übertragenen ordnungsbehördlichen Aufgabe der Ausländerüberwachung sammelt und erfaßt sie in erheblichem Umfang Erkenntnisse über einzelne Ausländer.

Ich habe mir vorgenommen, mich im nächsten Jahr aus eigener Initiative näher mit der Tätigkeit der Ausländerbehörde zu befassen. Gegenstand meiner Prüfung werden auch die mir von der Behörde für Inneres übermittelte Neukonzeption des Ausländerzentralregisters in Köln und dessen informationelle Beziehungen zur Hamburger Ausländerbehörde sein.

3.8.4 Personenstandswesen

3.8.4.1 Neufassung der Dienstanweisung für die Standesbeamten

Auf eine Initiative des Bundesbeauftragten für den Datenschutz im Jahre 1981 hat eine Arbeitsgruppe der DSB-Konferenz die geltende „Dienstanweisung für die Standesbeamten und ihre Aufsichtsbehörden" (kurz: DA) überprüft. In dieser Verwaltungsvorschrift sind zahlreiche Mitteilungspflichten der Standesämter vorgesehen, die z. T. aus datenschutzrechtlicher Sicht bedenklich erscheinen. Parallel zu dieser Tätigkeit haben auch die Personenstandsreferenten von Bund und Ländern eine Überarbeitung der DA eingeleitet.

Die Arbeit der Datenschutzbeauftragten wurde im Juni mit einem Beschluß der DSB-Konferenz vorläufig abgeschlossen. Den Wortlaut dieses Beschlusses habe ich in der Anlage dokumentiert.
Diesen Beschluß habe ich der Behörde für Inneres übersandt und ergänzend zum wiederholten Mal auf die besondere Bedenklichkeit der in §§ 103, 201 DA vorgesehenen Datenübermittlungen über umherziehende Personen ohne festen Wohnsitz hingewiesen, von der in erster Linie die Gruppe der Sinti und Roma betroffen ist.
Die Behörde für Inneres hat mir daraufhin mitgeteilt, daß sie ihre Bedenken gegen einen Wegfall dieser Übermittlungen aufgegeben hat.

In dem zwischenzeitlich vorliegenden Entwurf des Bundesinnenministers sind die Forderungen der Datenschutzbeauftragten zum großen Teil berücksichtigt worden, soweit sie sich auf in der Verwaltungsvorschrift regelbare Sachverhalte beziehen. Noch offen ist die Schaffung präziser Rechtsgrundlagen.

3.8.4.2 Durchführung des Transsexuellengesetzes

Nach dem „Gesetz über die Änderung der Vornamen und die Feststellung der Geschlechtszugehörigkeit in besonderen Fällen (Transsexuellengesetz – TSG)" vom 10. September 1980 (BGBl. I, 1654) können Personen, die sich nicht mehr den in ihrem Geburtsantrag angegebenen, sondern dem anderen Geschlecht als zugehörig empfinden, unter bestimmten Voraussetzungen ihren Vornamen ändern oder eine andere Geschlechtszugehörigkeit feststellen lassen. Es liegt nahe, daß eine solche Entscheidung weit in den besonders schützenswerten Bereich privater Lebensgestaltung hineinreicht. Dementsprechend ist in § 5 TSG ein weitgehendes Offenbarungsverbot geregelt: Ist eine Entscheidung nach dem TSG rechtskräftig, so dürfen der frühere Vorname bzw. das frühere Geschlecht des Antragstellers nur noch in wenigen Ausnahmefällen offenbart und ausgeforscht werden.

Aufgrund einer Beschwerde habe ich im Berichtszeitraum eine Bestandsaufnahme über die verschiedenen bei der Ausführung des TSG in Betracht kommenden Datenübermittlungen (z. B. vom Vormundschaftsgericht an das Standesamt, vom Standesamt an die Meldebehörde, von der Meldebehörde an dritte Stellen) gemacht und überprüft, ob die Einhaltung des Offenbarungsverbots hinreichend sichergestellt ist. Diese Überprüfung ist noch nicht abgeschlossen. Es zeichnet sich jedoch bereits ab, daß einige Verwaltungsvorschriften den Grundgedanken des TSG noch besser angepaßt werden müssen.

3.9 Allgemeine Bemerkungen zum Sicherheitsbereich

In meinem 1. TB (Nr. 8.7.1, S. 38 ff) habe ich ausführlich die Sonderregelungen erläutert, die für den Datenschutz im Sicherheitsbereich (Polizei, Staatsanwaltschaft, Verfassungsschutz und Teile der Steuerverwaltung) gelten, und auch erwähnt, daß der Senat unter bestimmten Voraussetzungen die Möglichkeit hat, die Akteneinsicht des Datenschutzbeauftragten einzuschränken. Eingehendere praktische Erfahrungen und viele Diskussionen vor allem im Zusammenhang mit der Volkszählung und dem maschinenlesbaren Personalausweis mit datenschutzbewußten Bürgern veranlassen mich, die Ausführungen zu meinen gesetzlichen Prüfungsbefugnissen zu verdeutlichen und einige Wünsche zum Auskunftsverhalten der Sicherheitsbehörden gegenüber dem Bürger anzumelden.

3.9.1 Zur Prüfkompetenz des Datenschutzbeauftragten

Bei vielen interessierten Bürgern ist – insbesondere durch Presseberichte über Behinderungen des Bundesbeauftragten – der irrige Eindruck entstanden, daß dem Datenschutzbeauftragten im Sicherheitsbereich eine effektive Kontrolle schon rechtlich nicht möglich sei. Ich nehme diese Gelegenheit zum Anlaß, noch einmal auf die folgenden, immer wiederkehrenden Fragen einzugehen:

- Wie weit reicht das Akteneinsichtsrecht des Datenschutzbeauftragten?
- Welche Bedeutung hat der sog. Sicherheitsvorbehalt (Staatswohlklausel) nach § 20 Abs. 4 Satz 4?
- Können dem Datenschutzbeauftragten besondere Berufs- und Amtsgeheimnisse (wie das Steuergeheimnis) entgegengehalten werden?

3.9.1.1 Der Umfang der Kontrollaufgabe

Gem. § 20 Abs. 1 Satz 1 hat der Datenschutzbeauftragte die Aufgabe, bei den in § 2 Abs. 1 genannten Stellen zum einen die Einhaltung der Vorschriften des Datenschutzgesetzes, zum anderen die Einhaltung weiterer Vorschriften über den Datenschutz zu überwachen. Der Begriff „weitere Vorschriften" erstreckt sich außer auf Gesetze und Verordnungen auch auf Verwaltungsvorschriften.

3.9.1.2 Allgemeine Befugnisse des HmbDSB

Um die o. g. weitgespannten Kontrollaufgaben verwirklichen zu können, steht dem DSB gem. § 20 Abs. 4 eine Reihe von Befugnissen zu, ohne die § 20 Abs. 1 bedeutungslos wäre.
Grundlage der Befugnisse ist die in § 20 Abs. 4 S. 1 normierte Grundpflicht aller öffentlichen Stellen, die der Kontrolle unterliegen, den Datenschutzbeauftragten und seine Mitarbeiter bei der Erfüllung ihrer Aufgaben zu unterstützen. Diese allgemeine Unterstützungspflicht – die von einer in der Praxis bislang nicht relevanten Ausnahme abgesehen (§ 20 Abs. 4 S. 4; s. u.) auch im Sicherheitsbereich gilt – wird im § 20 Abs. 4 Satz 2 HmbDSG durch eine Reihe von beispielhaft aufgezählten Einzelbefugnissen konkretisiert. Dem Datenschutzbeauftragten und seinen Mitarbeitern ist danach insbesondere

„1. Auskunft zu ihren Fragen und Einsicht in **alle** Unterlagen und Akten zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen, namentlich in die gespeicherten Daten und Datenverarbeitungsprogramme,

2. jederzeit Zutritt in **alle** Diensträume zu gewähren."

Die Hervorhebungen stammen von mir, um deutlich zu machen, wie weit die Pflichten reichen, die lediglich beispielhaft als Ausprägungen der allgemeinen Unterstützungspflicht genannt sind.

3.9.1.3 Zum Umfang des Akteneinsichtsrechts

Von der Verwaltung wird gelegentlich versucht, die Kontrolltätigkeit des Datenschutzbeauftragten auf solche Daten zu beschränken, die in Dateien verarbeitet werden. Diese Auffassung erscheint mir jedoch rechtlich nicht haltbar. Zwar sind vom HmbDSG (wie von den anderen Datenschutzgesetzen auch) nur personenbezogene Daten geschützt, die in Dateien verarbeitet werden (§ 1 Abs. 2). Doch sieht § 20 Abs. 1 Satz 1 ausdrücklich vor, daß ich die Einhaltung anderer Vorschriften über den Datenschutz zu überwachen habe; diese Vorschriften schützen aber in aller Regel personenbezogene Daten ohne Beschränkung darauf, daß sie in Dateien verarbeitet werden. Lediglich das baden-württembergische Landesdatenschutzgesetz begrenzt – nach einer 1982 erfolgten Änderung – die Kontrolltätigkeit der Landesdatenschutzbeauftragten auf die Datenverarbeitung mit Dateibezug.

Selbst wenn man jedoch der Auffassung beitreten würde, daß jegliche Kontrolltätigkeit des Datenschutzbeauftragten einen Dateibezug voraussetzt, so verschafft § 20 Abs. 4 S. 2 ihm doch die Befugnis, auch Akten oder sonstige Unterlagen einzusehen, wenn die hierin enthaltenen Daten nur in irgendeiner Form zugleich auch dateimäßig registriert sind. Auch die bei „Registratur-Dateien" weitgehend übliche Beschränkung des Inhalts auf Aktenfundstellen und Personen-Identifikations-Daten begründet bereits das Recht des Datenschutzbeauftragten festzustellen, ob die registrierte Akte unter Einhaltung der einschlägigen Gesetze und Verwaltungsvorschriften gespeichert wird. Es kommt also nicht auf den Umfang der in einer Datei im Zusammenhang mit einer Akte gespeicherten Daten an. Sowohl die Rechtmäßigkeit der Speicherung (in einer Registraturdatei) als auch die Rechtfertigung von Übermittlungen aus der – mit Hilfe der Registraturdatei aufgefundenen – Akte ergeben sich immer erst aus dem Zusammenhang von Akte und den registrierten Aktenfundstellen.

Schon aus Kapazitätsgründen wird allerdings nicht in jedem Fall die Akte mit überprüft werden können. Häufig werden Auskünfte der zuständigen Behörden ausreichen. Langjährige Prüferfahrungen insbesondere des Bundesbeauftragten haben jedoch gezeigt, daß – für die Bewertung einer Speicherung oder Übermittlung – entscheidende Hinweise bisweilen auf einem Aktenblatt stehen, auf dem man sie nicht vermutet hätte.

Allein dem Prüfer muß es somit überlassen bleiben zu entscheiden, an welchem Punkt er eine Prüfung beenden will. Dies gilt insbesondere auch für die Überprüfung der Behauptung, es finde überhaupt keine dateimäßige Verarbeitung – auch nicht in Registraturform – statt.

3.9.1.4 Die Bedeutung des Sicherheitsvorbehalts

Die oben skizzierten Prüfungsbefugnisse gelten im Sicherheitsbereich – ebenso wie in der sonstigen Verwaltung – mit einer Ausnahme, die allerdings noch nie Bedeutung erlangt hat und sicherlich auch nur selten erlangen wird:

Gem. § 20 Abs. 4 S. 4 gilt § 20 Abs. 4 S. 2 für die Sicherheitsbehörden nicht, soweit der Senat im Einzelfall feststellt, daß die Einsicht in Unterlagen und Akten die Sicherheit des Bundes oder eines Landes gefährdet. Diese Einschränkung – die aber nur das Akteneinsichtsrecht, nicht jedoch das allgemeine Zutrittsrecht zu allen Diensträumen betrifft – kann weiterhin nur auf einen konkreten einzelnen Vorgang („Einzelfall") bezogen, nicht jedoch für einen ganzen Sachkomplex (z. B. Terrorismus-/Spionagebekämpfung) geltend gemacht werden.

Tatbestandlich muß vom Senat im konkreten Einzelfall festgestellt werden, daß gerade durch die von mir begehrte Akteneinsicht die Sicherheit des Bundes oder eines Landes gefährdet ist.

3.9.1.5 Keine Einschränkung der Prüfkompetenz durch Berufs- oder Amtsgeheimnisse

Starke Zweifel an den rechtlichen Möglichkeiten des Datenschutzbeauftragten wurden in der Öffentlichkeit besonders aufgrund von Presseberichten laut, in denen berichtet wurde, wie dem Bundesbeauftragten im Sicherheitsbereich unter Berufung auf die ärztliche Schweigepflicht (Amt für Wehrmedizinalstatistik) bzw. das Steuergeheimnis (Zollkriminal-Institut) Prüfungen nicht gestattet wurden.

Diese Prüfungsverweigerungen sind aus zwei Gründen rechtlich nicht haltbar:

- Die Datenschutzbeauftragten überwachen die Einhaltung des Datenschutzes bei allen öffentlichen Stellen, also auch bei denen, die Patienten- oder Steuerdaten verarbeiten. Einzig und allein für Gerichte, soweit sie nicht in Verwaltungsangelegenheiten tätig werden, gilt ihre Kontrollkompetenz nicht. Abgesehen vom oben erwähnten Sicherheitsvorbehalt haben die Behörden in allen weiteren Fällen ihrer allgemeinen Unterstützungspflicht nachzukommen. Eine pauschale Ausgrenzung ganzer Bereiche z. B. der Finanzverwaltung wäre mit den Datenschutzgesetzen nicht vereinbar.

- Zu den anderen Vorschriften über den Datenschutz, die die Datenschutzbeauftragten zu kontrollieren haben, zählen insbesondere die klassischen Datenschutzregelungen wie die Berufs- und Amtsgeheimnisse. Wie sollte die Einhaltung dieser Vorschriften überprüft werden können, wenn dem Kontrolleur die entsprechenden Unterlagen nicht zugänglich gemacht werden.

3.9.1.6 Resümee

Die vorstehenden Erläuterungen zeigen aus meiner Sicht deutlich, daß der Datenschutzbeauftragte – entgegen häufig geäußerten Bedenken – vom Gesetzgeber mit den zur Erfüllung seiner Kontrollaufgaben erforderlichen Befugnissen – auch im Sicherheitsbereich – ausgestattet worden ist.

Von Verwaltungsstellen vorgebrachte Begründungen für Einschränkungen seiner Prüfbefugnisse sind nicht überzeugend. Wie ich aber einleitend (Nr. 1.1) ausgeführt habe, ist es im Interesse der betroffenen Bürger nicht hinnehmbar, daß die Befugnisse der Kontrollinstanz von der Verwaltung in Frage gestellt werden. Um das Vertrauen der Öffentlichkeit in die Stellung des Datenschutzbeauftragten als Bürgeranwalt zu stärken, muß Klarheit über die Kontrollbefugnisse geschaffen werden. Geeignet wäre eine Ergänzung der Datenschutzgesetze in die Richtung, daß gesetzliche Geheimhaltungsvorschriften einem Auskunfts- oder Einsichtsverlangen nicht entgegengehalten werden können und daß die Kontrolle anderer datenschutzrechtlicher Vorschriften nicht beschränkt ist auf Daten, die in Dateien verarbeitet werden. Der BDSG-Novellierungs-Entwurf ist leider auch diesen Forderungen der Datenschutzbeauftragten nicht nachgekommen.

3.9.2 Zum Auskunftsverhalten der Sicherheitsbehörden gegenüber dem Bürger

Nach meinen Erfahrungen rührt das Unbehagen vieler Bürger an der polizeilichen Informationsverarbeitung daher, daß sie nicht wissen, welche Daten in welchen Zusammenhängen über sie gespeichert und verarbeitet werden, und daß sie wegen der durch die Datenschutzgesetze eingeschränkten Auskunftspflichten der Sicherheitsbehörden fürchten, auf Nachfrage keine Auskünfte zu erhalten. Diese Befürchtungen sind – wie ich im folgenden zu zeigen beabsichtige – in aller Regel unbegründet. Gleichwohl sollten gesetzgeberische Konsequenzen erwogen werden, um die weit verbreitete Skepsis weiter abzubauen.

3.9.2.1 Auskünfte der Polizei

Die Hamburger Polizei hat nach meinen Feststellungen akzeptiert, daß manche Bedenken der Bürger am besten durch Offenheit überwunden werden können, und in großzügiger Weise Auskunft erteilt. In den – bundesweit geltenden – Richtlinien über kriminalpolizeiliche personenbezogene Sammlungen (KpS-Richtlinien) ist für die Polizei festgelegt worden, daß auf Antrag Auskunft darüber erteilt wird, ob und ggf. welche Unterlagen zur Person in diesen Sammlungen vorhanden sind,

> „es sei denn, daß die Belange des Bürgers hinter dem öffentlichen Interesse an der Nichtherausgabe der jeweiligen Daten zurücktreten müssen."

Es findet also eine Güterabwägung statt. Dazu heißt es in den KpS-Richtlinien weiter:

> „Die Erteilung der Auskunft kommt insbesondere in Betracht, wenn es sich um Unterlagen handelt, an deren Zustandekommen der Betroffene selbst beteiligt war und von denen er nach den Umständen annehmen kann, daß sie bei der Polizei aufbewahrt werden."

Auch für eine Auskunftsverweigerung geben die KpS-Richtlinien nähere Erläuterungen. Es heißt:
Die Auskunftserteilung hat zu unterbleiben, soweit

1. die Auskunft die öffentliche Sicherheit oder Ordnung gefährdet oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde;
2. die personenbezogenen Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen der überwiegenden berechtigten Interessen einer dritten Person, geheimgehalten werden müssen;
3. die Auskunft sich auf die Übermittlung personenbezogener Daten an die in § 12 Abs. 2 Nr. 1 BDSG genannten Behörden bezieht, falls diese nicht zustimmen;
4. die Stelle, die die Daten angeliefert hat, die Auskunftserteilung ausgeschlossen hat.

In Anwendung der Abwägungsgrundsätze hat jedenfalls die Hamburger Polizei in der weitaus überwiegenden Anzahl der Fälle die erbetene Auskunft erteilt, ohne sich auf ihr Verweigerungsrecht zu berufen. Nachteilige Folgen für ihre Aufgabenerfüllung sind dadurch, soweit mir bekannt ist, nicht aufgetreten. In allen mir bekannt gewordenen Fällen, in denen die Polizei eine Auskunft verweigert hat, war dies auch aus meiner Sicht akzeptabel: etwa wenn offensichtlich versucht wurde, den genauen Kenntnisstand der Polizei in laufenden Ermittlungsverfahren zu erforschen.

3.9.2.2 Auskünfte des Verfassungschutzes

Gegenüber dem Verfassungschutz ist das Auskunftsinteresse der Betroffenen nach meinen Erfahrungen erheblich schwieriger zur Geltung zu bringen als gegenüber der Polizei, wenngleich die Auskunftspraxis nicht ganz so restriktiv ist, wie ich es in meinem 1. TB dargestellt habe.

Auch der Verfassungsschutz hat in jedem Einzelfall zu prüfen, ob er eine beantragte Auskunft erteilt oder nicht. Wie verschiedene Verwaltungsgerichte in der letzten Zeit festgestellt haben (vgl. VG Köln, Urt. v. 5.5.1982, NVwZ 1983, 112; OVG Hamburg, Urt. v. 26.8.1982 – OVG Bf III 19/81 –; OVG Bremen, Urt. v. 26.10.1982, NVwZ 1983, 358) hat der Betroffene einen Anspruch darauf, daß ermessensfehlerfrei darüber entschieden wird, ob ihm eine Auskunft erteilt wird. Aufgabe dieser Ermessensbetätigung ist es, den Konflikt zwischen den Datenschutzrechten des Betroffenen einerseits und den Geheimhaltungsinteressen des Verfassungsschutzes andererseits unter Beachtung des Verhältnismäßigkeitsprinzips und des Verfassungsgebots eines effektiven Rechtsschutzes zu einem möglichst schonenden Ausgleich zu bringen.

Konkrete Richtlinien, an denen sich die Entscheidung im Einzelfall orientieren könnte, gibt es für den Verfassungschutz noch nicht. Die zitierten Entscheidungen enthalten jedoch Hinweise auf eine Reihe von Kriterien, die in der Regel zu beachten sind. Einstweilen habe ich mich mit dem Verfassungsschutzamt darauf verständigt, daß die maßgebenden Gründe für eine Auskunftsverweigerung – auch soweit diese dem Antragsteller nicht mitgeteilt werden – vom Sachbearbeiter in einem Vermerk festgehalten werden. Eine spätere Nachprüfung dieser Vermerke soll dann zeigen,ob und in welcher Form konkretisierbare Regelungen für die Auskunftspraxis möglich sind.

3.9.2.3 Auskünfte der Staatsanwaltschaft

Nach meinen Erfahrungen erteilt die Staatsanwaltschaft großzügig Auskünfte aus der Zentralkartei. Die StA hat auch am wenigsten Anlaß zur Geheimhaltung von Daten, da das Vorhandensein von Vorgängen den Betroffenen in aller Regel bekannt ist, soweit es sich nicht um frühe Stadien von laufenden Ermittlungsverfahren handelt. Nach der Beendigung eines Ermittlungsverfahrens ist überhaupt kein Grund mehr ersichtlich, warum die beantragte Auskunft nicht erteilt werden sollte. Der mit der Auskunftserteilung verbundene Aufwand rechtfertigt eine Verweigerung jedenfalls nicht, denn auch für die StA gilt die o. g. Pflicht zur fehlerfreien Ermessensausübung.

3.9.2.4 Resümee

Die bisherigen Erfahrungen mit der Auskunftspraxis der Sicherheitsbehörden geben Anlaß, nochmals zu prüfen, ob es überhaupt einer gesetzlichen Sonderregelung für die Auskunftserteilung im Sicherheitsbereich bedarf, ob nicht vielmehr die Regelung des § 14 Abs. 2 Nr. 1 einfach aufgehoben werden kann. Bisher ist mir kein Fall bekannt geworden, in dem die für alle Behörden geltende Auskunftsbeschränkung des § 14 Abs. 3 nicht auch für die Sicherheitsbehörden ausreicht. Ein Wegfall bzw. eine Einschränkung dieser Sonderregelungen könnte wesentlich dazu beitragen, die besondere Skepsis von Teilen der Bevölkerung gegenüber der Datenverarbeitung der Sicherheitsbehörden abzubauen.

Das Land Bremen hat bereits Konsequenzen gezogen und jedenfalls den Auskunftsanspruch gegenüber der Polizei weitgehend dem allgemein geltenden Auskunftsanspruch angepaßt. § 34 BremPolG vom 16.3.1983 lautet:

„Auskunft an den Betroffenen

(1) Dem Betroffenen ist auf Antrag Auskunft über die zu seiner Person gespeicherten Informationen zu erteilen. In dem Antrag soll die Art der personenbezogenen Informationen, über die Auskunft erteilt werden soll, näher bezeichnet werden. Die speichernde Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen.

(2) Ein Anspruch auf Auskunft besteht nicht, wenn

1. a) die Mitteilung der zur Person des Antragstellers gespeicherten Informationen oder
   b) die Mitteilung, daß zur Person des Antragstellers Informationen gespeichert sind,

   die Erfüllung der polizeilichen Aufgaben erschweren oder gefährden würde,
2. die personenbezogenen Informationen oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder wegen der überwiegenden berechtigten Interessen einer dritten Person geheimgehalten werden müssen.

(3) Statt einer Auskunft über Informationen in Akten kann die Polizei unbeschadet des Absatzes 2 Akteneinsicht gewähren."

Ebenso unbedenklich wäre es, wenn auch das Auskunftsrecht gegenüber der Staatsanwaltschaft entsprechend ausgestaltet würde.
Eine Sonderregelung käme – wegen seiner besonderen Aufgabenstellung – allenfalls für das Landesamt für Verfassungsschutz in Betracht.

In die entgegengesetzte Richtung scheint der Bundesminister des Innern marschieren zu wollen. Mit der im BDSG-Novellierungs-Entwurf enthaltenen Regelung soll den Sicherheitsbehörden die Handhabung ihres Auskunftsverweigerungsrechts gar noch erleichtert werden. Während der frühere Referentenentwurf (Stand 31.3.1982) wenigstens klargestellt hatte, daß – wie es in den KpS-Richtlinien bereits vorgesehen ist – über die Erteilung einer Auskunft nach fehlerfreiem Ermessen unter Abwägung der verschiedenen Belange zu entscheiden ist, wird durch den neuen Entwurf die Rechtsposition des Betroffenen noch dadurch verschlechtert, daß die Auskunftsverweigerung nicht mehr begründet zu werden braucht. Diese Regelung beeinträchtigt das Verfassungsgebot eines effektiven Rechtsschutzes: ablehnende Bescheide müssen einer gerichtlichen Überprüfung zugänglich sein und erkennen lassen, daß die Behörde eine einzelfallbezogene Prüfung vorgenommen hat und welche Gründe sie zur Zurückweisung des Auskunftsbegehrens bewogen haben.

3.10 Polizei

3.10.1 Überblick

Bei der Polizei lag im Berichtszeitraum – von Sonderbelastungen wie der Volkszählung abgesehen – der Schwerpunkt meiner Tätigkeit. Ich habe zahlreiche Dienststellen besucht, mich vor Ort gründlich über die Handhabung verschiedener manueller Dateien sowie über neue ADV-Anwendungen unterrichten lassen und habe zu diversen von der Polizei beabsichtigten Maßnahmen Stellung genommen. Ich meine, daß ich durch diese vielfältigen Kontakte mit den entscheidenden Problemen in Berührung gekommen bin, die sich für den Datenschutz bei der Polizei stellen. Ich habe versucht, die verschiedenen mir relevant erscheinenden Problembereiche in diesem Bericht etwas systematischer zusammenzustellen, auch wenn die Lösung an einigen Punkten noch offen ist. Nützliche Klärungen verspeche ich mir vor allem von den Beratungen über die gesetzliche Regelung der polizeilichen Informationsverarbeitung in einem novellierten HmbSOG, die 1984 anstehen werden.

3.10.2 Informationsverarbeitung außerhalb von Dateien

In der Öffentlichkeit wird kaum beachtet, daß kriminalpolizeiliche personenbezogene Sammlungen sowie andere Berichte und Meldungen von der Polizei nicht nur in manuell oder automatisiert geführten Dateien, sondern auch in Akten und anderem Schriftgut gespeichert werden. Auch bei der Verarbeitung dieser Unterlagen gibt es noch eine Reihe von Problemen und Ungereimtheiten, ohne deren Beseitigung der Datenschutz im polizeilichen Bereich unvollständig bliebe.

3.10.2.1 Akten zur Bearbeitung von Kriminalfällen

Bei der Bearbeitung von Kriminalfällen werden Informationen von der Polizei regelmäßig in drei verschiedenen Akten verarbeitet, die ein ganz unterschiedliches Schicksal haben können:

- Die gesamten Ergebnisse eines konkreten Ermittlungsverfahrens (Vernehmungsprotokolle etc.) werden zunächst in einer **Ermittlungsakte** aufbewahrt. Diese wird nach dem polizeilichen Ermittlungsverfahren der Staatsanwaltschaft zugeleitet und wird dort Bestandteil der staatsanwaltschaftlichen Ermittlungsakte. Diese Akte wird erschlossen über die Zentralkartei der Staatsanwaltschaft (vgl. Nr. 3.12.1). Ihre Aufbewahrungsfrist richtet sich nach Aufbewahrungsbestimmungen für Schriftgut der Justizverwaltungen (z. Z. mindestens fünf Jahre bei eingestellten Straftaten).

- Eine komplette Durchschrift der polizeilichen Ermittlungsakte verbleibt auch nach Abschluß des Ermittlungsverfahrens als **Handakte** bei den zuständigen Polizeikommissariaten. Sie wird dort gem. den „Aufbewahrungsfristen für Schriftgut" der Polizei generell fünf Jahre aufbewahrt. Eine unbegrenzte Aufbewahrung ist für Handakten bei Tötungsdelikten im Hamburger Zuständigkeitsbereich vorgesehen.

- Bestimmte Grundinformationen aus den sog. Ermittlungsakten (Anzeige, Ermittlungsergebnis etc.) werden schließlich in den zu bestimmten Personen geführten **Kriminalakten** bei der Fachdirektion 67 gespeichert. Diese Kriminalakte (also die Personalakte eines Verdächtigen) wird über einen Index im POLAS erschlossen (demnächst bei Akten von überregionaler Bedeutung auch über den KAN). Die Aufbewahrungsfristen für diese Akten sind in den KpS-Richtlinien (abhängig von der Schwere des zuletzt gespeicherten Delikts) geregelt.

Diese völlig unterschiedlichen Regelungen können zu dem unbefriedigenden Ergebnis führen, daß Unterlagen, die nach den KpS-Richtlinien im POLAS und in der Kriminalakte gelöscht werden müssen, an anderen Stellen – in der Handakte und in der Staatsanwaltschaftsakte – noch jahrelang gespeichert bleiben. Wie dies Problem, auf das ich die Polizei aufmerksam gemacht habe, am besten gelöst werden kann, ist z. Z. noch offen. Bei der noch nicht abgeschlossenen Neuregelung der Aufbewahrungsfristen für die Zentralkartei der Staatsanwaltschaft ist darauf zu achten, daß diese möglichst auf die polizeilichen Aufbewahrungsfristen abgestimmt werden. Auch für die polizeilichen Handakten muß noch sichergestellt werden, daß diese nicht mehr verwendet werden, wenn ein Vorgang im POLAS z. B. wegen erwiesener Unschuld kurzfristig gelöscht worden ist.

3.10.2.2 Anhaltemeldungen

In meinem 1. TB (S. 43) hatte ich bereits auf das Problem der sog. „Anhaltemeldungen" hingewiesen, die die Polizei bei präventiv-polizeilichen Personenkontrollen fertigt. Bei diesen Anhaltemeldungen werden auf einem Formular neben den Personalien der betroffenen Person Ort, Zeit, Anlaß und Ergebnis der Überprüfung notiert.

Diese von mir als bedenklich angesehene Praxis konnte im Berichtszeitraum befriedigend neu geregelt werden. Nach der Neufassung der polizeilichen Dienstvorschrift sind Anhaltemeldungen zu fertigen, wenn Personen kontrolliert werden, deren auffälliges Verhalten vermuten läßt, sie könnten als Täter oder Teilnehmer mit einer Straftat in Verbindung stehen. Diese Anhaltemeldungen werden zur Ermittlungsakte genommen, wenn sie einer anhängigen Strafsache zugeordnet werden können. Ist eine solche Zuordnung nicht sofort möglich, werden sie noch für maximal drei Monate bei der zuständigen Polizeidirektion vorgehalten. Ist auch während dieser Frist keine Zuordnung zu einem anhängigen Ermittlungsverfahren möglich, werden sie vernichtet bzw. unter bestimmten Voraussetzungen nach Einzelfallprüfung in eine evtl. über den Betroffenen schon vorhandene Kriminalakte aufgenommen.

Die zentrale Sammlung der Anhaltemeldungen im Polizeipräsidium ist aufgelöst worden.

3.10.2.3 Sonstige Kurzberichte

Auch in Fällen von Personenkontrollen, in denen keine Veranlassung zu einer „Anhaltemeldung" besteht, fertigt die Polizei häufig kurze Berichte an. So werden z. B. regelmäßig die Personalien und das Kfz-Kennzeichen von Bürgern festgehalten, die im Rahmen von Verkehrskontrollen überprüft worden sind, und zwar auch dann, wenn die Überprüfung keinen Anlaß zu Beanstandungen ergab. Die Anfertigung dieser Meldungen erfolgt in erster Linie zu Dokumentationszwecken. Die Polizei will jederzeit aussagefähig sein und einen Nachweis über vorgenommene Tätigkeiten im Fall von Nachfragen, Eingaben oder Beschwerden erbringen können. Im Hinblick auf diesen begrenzten Zweck hat sie die Aufbewahrungsfristen für derartige Unterlagen von drei Jahren auf ein Jahr verkürzt. Die Behörde für Inneres steht jedoch auf dem Standpunkt, daß ein Rückgriff auf die für

die polizeiliche Aufgabenerfüllung zunächst bedeutungslos gewesenen Unterlagen keineswegs ausgeschlossen ist, wenn sich im Laufe des Jahres zeigt, daß die Unterlagen z. B. Bedeutung für ein Strafermittlungsverfahren erlangen.

Ob die einjährige Speicherung der Unterlagen auch für diesen Zweck zulässig ist, wird im Rahmen der Diskussion über die Regelung der Personenkontrolle und der polizeilichen Informationsverarbeitung in der geplanten SOG-Novellierung zu klären sein.

3.10.3 Entwicklung der automatisierten Datenverarbeitung bei der Polizei

Die Entwicklung der automatisierten Datenverarbeitung bei der Polizei wird dadurch gekennzeichnet, daß sie in drei Richtungen ständig ausgeweitet wird.

3.10.3.1 Quantitative Ausweitung automatisierter Dateien

Zum einen nimmt rein quantitativ die Anzahl der automatisierten Dateien auch in Hamburg ständig zu. Es ist beabsichtigt, alle bislang manuell geführten Karteien (wie z. B. die Kartei jugendlicher Gewalttäter) in den automatisierten Bestand zu übernehmen. Zusätzlich werden neue Dateien (insbesondere Spurendokumentationssysteme) eingerichtet.

3.10.3.2 Bundesweite Zentralisierung der ADV

Zum anderen findet entsprechend dem INPOL-Fortentwicklungskonzept in zunehmendem Maße eine Zentralisierung polizeilicher Informationen auf Bundesebene statt (zu nennen ist hier als aktuelle Maßnahme insbesondere die Einrichtung des bundesweiten Kriminalaktennachweises, vgl. dazu Nr. 3.10.5.4). Diese kann sowohl im Hinblick auf die begrenzten gesetzlichen Aufgaben des Bundeskriminalamtes („als Zentralstelle, soweit eine Koordinierung der Verbrechensbekämpfung erforderlich ist") als auch im Hinblick auf das Gebot der Verhältnismäßigkeit von Grundrechtseingriffen problematisch sein. In diesem Zusammenhang ist allerdings positiv hervorzuheben, daß manche Zentralisierungsbestrebungen auch von der Behörde für Inneres kritisch gesehen werden. Dementsprechend hat sie sich an einer Reihe von Zentralisierungsmaßnahmen (wie z. B. an dem aus datenschutzrechtlicher Sicht problematischen kriminalpolizeilichen Meldedienst „Landfriedensbruch und verwandte Straftaten") nicht beteiligt.

3.10.3.3 Ausweitung des Anwendungsbereichs

Der entscheidende Gesichtspunkt liegt jedoch darin, daß der Anwendungsbereich der ADV ständig ausgeweitet wird.

3.10.3.3.1 Fahndungs- und Aktennachweissysteme

Ursprünglich diente die Automatisierung lediglich Fahndungszwecken. Mit der INPOL-Personen- und Sachfahndung wurde das Fahndungsbuch herkömmlicher Art ersetzt. Hinzu kamen noch regional begrenzte Akten- und Personennachweis-Systeme, mit denen die Polizei in relativ kurzer Zeit feststellen kann, ob eine Person „bekannt" ist.

3.10.3.3.2 PIOS-Dateien

Diese Systeme sind in der Folgezeit durch die verschiedenen PIOS-Dateien ausgebaut worden, die – vom BKA entwickelt – auch von der Hamburger Polizei benutzt werden. Die PIOS-Anwendungen haben über die Funktion eines reinen Personen- und Aktennachweissystems hinaus den Zweck, die Daten von Personen, Institutionen, Objekten und Sachen zu erfassen, zwischen ihnen Verknüpfungen herzustellen und systematische Auswertungen zu ermöglichen. Es soll – wie der Bundesbeauftragte in seinem 5. Tätigkeitsbericht S. 85 ausführlicher erläutert hat – mehr erfaßt und ausgewertet werden als bloß der Name der Hauptperson, gegen die sich ein Verfahren richtet. Die spezifische Ar-

beitsweise von PIOS besteht vielmehr darin, daß möglichst auch die Randpersonen, gegen die sich noch kein konkreter Verdacht richtet, erfaßt werden. (Zu dieser Problematik vgl. Nr. 3.10.5.1). Der Anwendungsbereich von PIOS-Systemen, die ursprünglich nur der Bekämpfung der terroristischen Gewaltkriminalität dienten, ist zwischenzeitlich auf diverse andere Arten von Kriminalität ausgedehnt worden. Derzeit aktuellste Hamburger Anwendung ist die „Arbeitsdatei PIOS Organisierte Kriminalität".

3.10.3.3.3 Spurendokumentationssysteme

Ähnliche Verknüpfungs- und Auswertungsmöglichkeiten wie die PIOS-Anwendungen eröffnen auch die seit Beginn dieses Jahres in Hamburg zur Anwendung kommenden Spurendokumentationssysteme (SPUDOK). Der Zweck dieser Verfahren besteht in erster Linie darin, das Spurenaufkommen bei umfangreichen Ermittlungsverfahren (z.B. im Bereich der organisierten Kriminalität) zu dokumentieren, damit bei einer Vielzahl eingehender Hinweise kein Informationsverlust eintritt. Auch bei SPUDOK stellt sich die besondere Problematik, daß – im Rahmen einzelner Ermittlungsverfahren – umfangreiche Datenbestände nicht nur über Verdächtige, sondern auch über „andere" Personen aufgebaut werden. Ein besonderes Problem entsteht durch die außerordentlich vielseitige Verwendbarkeit von SPUDOK. Da SPUDOK's in relativ großem Umfang Freitext verarbeiten und nahezu alle erfaßten Textteile miteinander abgleichen können, besteht jedenfalls objektiv-technisch die Möglichkeit, mit Hilfe der Verfahrenshülle SPUDOK schwer kontrollierbare Sonderdateien einzurichten, die nicht dem eigentlichen Zweck der SPUDOK-Anwendung entsprechen.

Die Behörde für Inneres hat mir die Errichtungs- bzw. Feststellungsanordnungen für die bisher von der Polizei betriebenen SPUDOK-Anwendungen übersandt. Ich habe mir den Betrieb dieser Systeme angesehen, bereits einige Einzelfälle überprüft und eine Reihe von Bedenken formuliert. Die Verhandlungen sind noch nicht abgeschlossen. Probleme ergeben sich insbesondere daraus, daß SPUDOK's z. Z. nicht einzelfallbezogen (beschränkt auf bestimmte einzelne Ermittlungsverfahren), sondern deliktsgruppenbezogen zur Anwendung kommen. In einem SPUDOK-Verfahren werden nebeneinander Spurenhinweise zu verschiedenen Strafermittlungsverfahren des gleichen Deliktsbereichs eingespeichert und zwar jeweils in einer gemeinsamen Datei. Dies führt zu erheblichen Schwierigkeiten bei der Definition der von der Speicherung betroffenen Personengruppen und kann eine unnötige Verlängerung der Aufbewahrungsfristen nach sich ziehen. Auch die Möglichkeiten einer Kontrolle werden bei solchen breit angelegten SPUDOK-Anwendungen wegen der wesentlich schwerer überschaubaren Anzahl der Daten verschlechtert.

Im Arbeitskreis „Sicherheit" der Datenschutzbeauftragten des Bundes und der Länder steht das Thema SPUDOK z. Z. ebenfalls im Vordergrund. Auch diese Beratungen haben noch nicht zu einem abschließenden Ergebnis geführt.

3.10.3.3.4 Falldateien

Falldateien sollen die Möglichkeiten der Polizei zur unmittelbaren Recherche mit dem Computer weiter verstärken. Mit ihnen soll erreicht werden, daß bekannte Straftaten vom Computer unbekannten Tätern zugeordnet werden. Inwieweit der Polizei auf diese Art und Weise erfolgversprechende Ermittlungsansätze für ihre Arbeit geliefert werden, läßt sich noch nicht absehen. Zur Zeit ist die Hamburger Polizei nur an die beim BKA betriebene Falldatei Rauschgift angeschlossen. Geplant ist die Errichtung einer einige weitere Delikte umfassenden POLAS-Falldatei. Nach der Verwirklichung dieser Falldatei wird das herkömmliche Tagebuch nicht mehr benötigt.
Die Planung für diese neue Datei steht noch am Anfang. Es hat bisher lediglich eine Arbeitsgruppe der Polizei gegeben, die den Datenbedarf näher definiert und die erwünschte Struktur der Datei beschrieben hat. Die Ergebnisse dieser Arbeitsgruppe liegen mir vor. Ich habe mich – aus Kapazitätsgründen – jedoch noch nicht detaillierter damit befassen können und kann daher auch noch nicht beurteilen, ob und inwieweit sich aus dieser

ADV-Anwendung besondere datenschutzrechtliche Probleme ergeben. Ich beabsichtige, eine gründliche datenschutzrechtliche Prüfung vorzunehmen, wenn die Realisierung dieser Datei konkretere Formen annimmt.

3.10.3.4 Ausblick

Aus der vorstehend dargestellten Entwicklung wird deutlich, daß der Einsatz der automatisierten Datenverarbeitung nicht mehr allein der Unterstützung und Beschleunigung traditioneller polizeilicher Arbeitstechniken dient, sondern zunehmend an Eigengewicht gewinnt. Das Bild des Kriposachbearbeiters, der seine Fälle quasi am Computer löst, nimmt deutlichere Konturen an. An dieser Stelle soll allerdings nicht unerwähnt bleiben, daß die Hamburger Polizei – auch im Vergleich mit den Polizeibehörden anderer Bundesländer – noch am Anfang der skizzierten Entwicklung steht: Hamburg hat bisher weder ein echtes Verbundsystem mit dem BKA-Computer hergestellt noch verfügt es über eigene Rechnerkapazitäten für PIOS- und SPUDOK-Anwendungen. Diese Anwendungen werden im Auftrage beim BKA ausgeführt. Auch die Frage, wann die POLAS-Falldatei realisiert wird, ist noch offen.

Unter diesen Bedingungen ist es dem Hamburgischen Datenschutzbeauftragten noch gerade gelungen, mit der Entwicklung Schritt zu halten. Dies wird jedoch bei den sich abzeichnenden neuen schnelleren Entwicklungen mit den Arbeitskapazitäten meiner Dienststelle immer schwerer werden. Im übrigen wird aus den geschilderten Entwicklungen nachhaltig deutlich, wie wichtig präzise Rechtsgrundlagen für die polizeiliche Informationsverarbeitung sind.

3.10.4 Stand des Datenschutzes bei der Polizei

In keinem Bereich gibt es so viele konkrete Richtlinien zur Ausführung der Datenschutzgesetze wie bei der Polizei, und in keiner anderen Behörde werden die Bediensteten besser auf datenschutzrechtliche Anforderungen in ihrer Praxis vorbereitet. Dies soll allerdings nicht über das Defizit an gesetzlichen Regelungen im Sicherheitsbereich sowie über das Fortbestehen einiger Grundsatzprobleme hinwegtäuschen.

3.10.4.1 KpS-Richtlinien

Wie ich bereits in meinem 1. TB erläutert habe, sind die datenschutzrechtlichen Anforderungen für weite Bereiche der polizeilichen Informationsverarbeitung in den „Richtlinien über kriminalpolizeiliche personenbezogene Sammlungen" (KpS-Richtlinien) präzisiert worden.
Diese bundeseinheitlich geltenden Richtlinien, die in Hamburg durch ergänzende Erläuterungen des Polizeipräsidenten noch weiter konkretisiert worden sind, haben sich im großen und ganzen bewährt. Wieweit noch Schwachstellen vorhanden sind, soll eine grundsätzliche Überprüfung zeigen, die im nächsten Jahr von Polizei und Datenschutzbeauftragtem vollzogen werden soll.

3.10.4.2 Datei-Richtlinien

In meinem letzten TB (S. 41) hatte ich kritisiert, daß es in Hamburg keine präzisen Richtlinien für die Einrichtung der polizeilichen Dateien gibt. In solchen Richtlinien soll festgelegt werden, daß jede Datei-Errichtung einer besonderen Anordnung bedarf, in der u. a. Rechtsgrundlage, Datei-Zweck, betroffener Personenkreis, Art der zu speichernden Daten sowie die Stellen, an die Auskunft erteilt wird, festgelegt werden (Feststellungs-bzw. Errichtungsanordnungen). Die Behörde für Inneres hat diese Forderungen akzeptiert und die Erarbeitung von Datei-Richtlinien eingeleitet.

Darüber hinaus hat sie – im Vorgriff auf die Datei-Richtlinien – bereits eine Reihe von Feststellungs- bzw. Errichtungsanordnungen für einzelne Dateien erlassen und diese mit mir abgestimmt. Diese Anordnungen sind sowohl geeignet, die Polizei zu veranlas-

sen, intensiver darüber nachzudenken, welche Informationen zu welchem Zweck eigentlich gespeichert werden müssen, als auch die Kontrolle durch den Datenschutzbeauftragten zu erleichtern.

Die mir vorgelegten Errichtungsanordnungen wurden ihrer Funktion zumeist gerecht. Wenn problematische Festlegungen auftauchten, bezogen sich diese fast ausschließlich auf zu speichernde „andere Personen" (vgl. dazu Nr. 3.10.5.1). Meine Bedenken richten sich regelmäßig gegen eine zu ungenaue Eingrenzung des insofern betroffenen Personenkreises und zu lange Aufbewahrungsfristen.

3.10.4.3 Zugriffsregelungen

Im Sommer 1983 hat die Polizei eine Regelung über die Zugriffsberechtigung für POLAS/INPOL erlassen, in der im einzelnen festgelegt ist, welcher Polizeibeamte zur Erfüllung seiner Aufgaben Zugriff auf welche Datengruppen im POLAS/INPOL nehmen darf. Zur Umsetzung dieses Programms in die Praxis sind allerdings noch zusätzliche technische Maßnahmen erforderlich (Einführung von Magnetkarten). Einstweilen ist eine Übergangsregelung getroffen worden, die bestimmten Dienststellen per Dienstanweisung bestimmte Abfragen verbietet.

Ich hatte ursprünglich gefordert, daß nach Vorliegen der technischen Voraussetzungen eine generelle Protokollierung aller Abfragen erfolgt, um genau überprüfen zu können, wer wann welche Person abgefragt hat. Diese Forderung habe ich jedoch im Verlaufe der Diskussionen um die Einführung des maschinenlesbaren Personalausweises aufgegeben, da das zusätzliche Gefährdungspotential, das mit der allgemeinen Protokollierung angesammelt würde, in keinem angemessenen Verhältnis zu der erreichbaren Kontrolldichte stände: Bei einer Auswertung der neuen Dateien ließe sich theoretisch feststellen, wann (Zeitpunkt der Abfrage) einzelne Personen sich an welchem Ort (Ort der Abfrage) aufgehalten haben. Demgegenüber könnte ein Kontrolleur angesichts der riesigen Anzahl täglicher Anfragen kaum jemals unzulässige Zugriffe aufdecken. Es muß jedoch noch geklärt werden, auf welche andere Weise eine wirksame Zugriffskontrolle gewährleistet werden kann.

3.10.4.4 Rückmeldungen von der Staatsanwaltschaft an die Polizei

In meinem 1. TB (Nr. 8.2, S. 61) hatte ich darauf hingewiesen, daß die Rückmeldung von Verfahrensergebnissen von der Staatsanwaltschaft an die Polizei häufig sehr lange dauerte, zu ungenau war oder ganz ausblieb. Dies hatte zur Folge, daß die Polizei nicht entscheiden konnte, ob bestimmte Speicherungen weiterhin erforderlich waren.
Um dieses Problem zu lösen, hat die Polizei gemeinsam mit der Staatsanwaltschaft einen neuen Akten-Laufzettel entwickelt, mit dem die Polizei schneller und differenzierter über das Verfahrensergebnis unterrichtet wird. Auf diesem Laufzettel wird konkret vermerkt, durch welche Art der Entscheidung (Einstellung, Einstellung mit Auflagen, Urteil etc. jeweils mit Angabe der einschlägigen StPO-Vorschrift) von der Staatsanwaltschaft oder vom Gericht ein Verfahren beendet wurde. Aufgrund dieser Information hat die Polizei die Möglichkeit, umgehend über die Frage einer Löschung oder weiteren Speicherung zu entscheiden. Welcher Verfahrensausgang zu welcher Entscheidung führt, ist in einer Dienstvorschrift näher konkretisiert worden:
Ist z. B. ein Freispruch erfolgt bzw. ein Verfahren eingestellt worden, weil die Tat unter keinen Straftatbestand fällt bzw. weil der Beschuldigte/Angeklagte nicht der Täter ist, sind die gespeicherten Daten und die dazugehörigen Unterlagen umgehend zu vernichten.
Erfolgt eine Verurteilung bzw. wird das Verfahren z. B. gem. § 153a StPO wegen Geringfügigkeit eingestellt, bleibt es bei der nach den KpS-Richtlinien festgelegten Aufbewahrungsdauer.
Erfolgt – um noch ein drittes Beispiel zu nennen – eine Einstellung gem. § 170 Abs. 2 StPO, weil Täterschaft, Tat oder Tatumstände nicht nachweisbar sind, so wird im Einzelfall anhand bestimmter Prognosekriterien (wie Art und Schwere des Falles, Intensität des Verdachts etc.) geprüft, ob eine weitere Speicherung erforderlich ist.

3.10.5 Problemfälle bei Speicherungen

Wenn auch meine Nachprüfungen, die sich auf bestimmte einzelne Personen bezogen, keine Veranlassung zu Beanstandungen ergeben haben, so gibt es doch gegen die Speicherung bestimmter Personengruppen sowie gegen bestimmte im Datensatz enthaltene Merkmale grundsätzliche Bedenken.

3.10.5.1 Speicherung „anderer Personen"

Entsprechend den KpS-Richtlinien speichert die Polizei z. Z. nicht nur Daten von (im strafrechtlichen Sinne) Verdächtigen und Beschuldigten sowie von (im polizeirechtlichen Sinne) Störern, sondern auch Daten sog. „anderer Personen". Die Speicherung solcher „anderen Personen" ist nach den KpS-Richtlinien zulässig, „wenn zureichende tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß dies zur Aufklärung oder vorbeugenden Bekämpfung schwerwiegender Straftaten, zur Ergreifung von zur Festnahme gesuchter Personen oder zur Abwehr einer im Einzelfall bestehenden erheblichen Gefahr erforderlich ist". Eine solche Registrierung von Personen, bei denen noch nicht bekannt ist, ob sie einmal zu Verdächtigen oder Beschuldigten werden oder als Zeugen in Betracht kommen, ist im Strafverfahrensrecht nicht vorgesehen. Auch nach dem SOG kann eine Registrierung grundsätzlich nur unter engen Voraussetzungen in Betracht kommen.

Die Datenschutzbeauftragten haben bereits vor dem IMK-Beschluß über die KpS-Richtlinien (sowie die – insoweit gleichlautenden – Dateienrichtlinien des BKA) auf die Problematik einer Speicherung dieses Personenkreises hingewiesen. Ihre Bedenken sind seinerzeit nicht berücksichtigt worden. Zwischenzeitlich drängt sich das Problem jedoch immer stärker in den Vordergrund. Ich bin fast geneigt, es als das Schlüsselproblem der polizeilichen Speicherungsbefugnis einzustufen.

Dieses ergibt sich zunächst daraus, daß der Umfang der Speicherung anderer Personen nach meinem Eindruck zunimmt. Ich habe im Zusammenhang mit der Entwicklung der PIOS- und SPUDOK-Systeme bereits darauf hingewiesen. Auch in anderen – z. T. noch manuellen – Dateien ist häufig die Speicherung „anderer Personen" vorgesehen, wie sich aus den mir in letzter Zeit vorgelegten Errichtungsanordnungen ergibt.

Das Problem wird dadurch verschärft, daß die Polizei sich in den erwähnten Errichtungsanordnungen regelmäßig nur unter großen Schwierigkeiten in der Lage sieht, den Kreis „anderer Personen" im Hinblick auf den konkreten Zweck der Daten näher einzugrenzen. In den Errichtungsanordnungen wurde zumeist bei der Beschreibung des von der Datei betroffenen Personenkreises schlicht der Wortlaut der KpS-Richtlinien wiedergegeben.

Schließlich hat sich gezeigt, daß auch zusätzliche Sicherungen, die in die KpS-Richtlinien eingebaut worden sind, in der Praxis nicht funktionieren. So ist die Löschungsfrist für „andere Personen" in den Hamburger Kps-Richtlinien auf generell ein Jahr festgelegt worden. Gleichwohl ist in allen Entwürfen von Errichtungsanordnungen, die mir vorgelegt wurden, durchgängig eine Löschungsfrist von drei Jahren für „andere Personen" vorgesehen. Die gleiche Tendenz ist, wie meine Kollegen beobachten, auf Bundesebene und in anderen Ländern festzustellen, wenngleich eine generelle Verlängerung von Lösch- und Prüffristen zunächst noch gestoppt werden konnte.

Auch dieser Punkt wird bei der Beratung der SOG-Novelle von besonderer Bedeutung sein. Wenn auch nicht gesagt werden kann, daß die Polizei mit der Speicherung „anderer Personen" die Verfolgung Unschuldiger beabsichtigt, so dürfen gleichwohl die Gefahren einer solchen Speicherung nicht übersehen werden: wenn es bei genauer Betrachtungsweise an zureichenden Anhaltspunkten für einen Anfangsverdacht fehlt oder festgestellte Anhaltspunkte sich als nicht stichhaltig erwiesen haben, so kann eine dennoch vorgenommene oder aufrechterhaltene Speicherung bewirken, daß die Betroffenen

ungerechtfertigten Verdächtigungen, belastenden Ermittlungen und im ungünstigsten Fall sogar Diskriminierungen aufgrund von Übermittlungen an andere Stellen ausgesetzt werden.

3.10.5.2 Suizidversuche

Bereits in meinem letzten TB hatte ich darauf hingewiesen, daß die Polizei generell Daten ihr bekannt werdender Personen speichert, die einen Suizidversuch begangen haben. Zu einer solchen Speicherung ist die Polizei nach meiner derzeitigen Beurteilung nicht befugt. Obgleich ich der Behörde für Inneres bereits im September 1982 erstmalig meine Bedenken vorgetragen habe, liegt mir eine endgültige Stellungnahme noch nicht vor. Die Behörde für Inneres wartet noch eine Stellungnahme der Gesundheitsbehörde ab, die sie im Oktober 1983 erbeten hat, um sich eine abschließende Meinung zu bilden. Gleichwohl halte ich es wegen des bereits sehr lange andauernden Klärungsprozesses für geboten, einmal den Sachstand (a), wie ich ihn bisher ermitteln konnte, und eine zumindest vorläufige Beurteilung (b) des Problems darzulegen.

a) Wenn die Polizei z. Z. Kenntnis von einem Freitodversuch erhält, sucht sie den Tatort auf und fertigt nach Durchführung der erforderlichen Maßnahmen einen formularmäßigen Bericht. Das Formular enthält Angaben zur Person, zur Ausführung der Tat, zum Verbleib des Freitodsuchenden sowie Feststellungen im Krankenhaus. Es wird in mehreren Ausfertigungen hergestellt, von denen ein Exemplar zu Dokumentationszwecken in dem Polizeirevier bleibt, das den Freitodversuch aufgenommen hat. Eine weitere Ausfertigung geht an die Kriminalpolizei, wo zunächst untersucht wird, ob Anhaltspunkte für eine Straftat (Fremdverschulden) vorliegen. Falls nicht, wird mit dem Formular eine Akte angelegt, die zur Kriminalaktensammlung genommen wird. In POLAS wird dann auf einem für diese Zwecke bereitgehaltenen Datenfeld ein Hinweis auf das Aktenzeichen dieses Vorgangs nebst den Identifikationsdaten des Betroffenen eingestellt. Dieses Datum ist allerdings kein Suchbegriff. Ob das Aktenzeichen eines Freitodversuchs gespeichert ist, kann nur unter Angabe der Personalien abgefragt werden.

b) Die Polizei stützt ihre Befugnis zur Speicherung des Hinweises auf einen Freitodversuch bislang auf § 3 Abs. 1 HmbSOG. Sie hält die Speicherung dieser Daten für geeignet und erforderlich, eine Gefahr für Leib oder Leben des Betroffenen abzuwehren. Aufgrund dieses Hinweises könne sie im Falle polizeilicher Maßnahmen gegen den Betroffenen (z. B. vorläufige Festnahme) eine situationsgerechte Behandlung vornehmen (z. B. Hinzuziehen von Angehörigen, Ärzten; besondere vorübergehende Unterbringung in geeigneten Räumen – nicht in Zellen; Abnahme bestimmter Gegenstände).

Ich bezweifle nicht, daß bei einer Person, die einen Freitodversuch unternommen hat, die Gefahr eines erneuten Freitodversuchs größer sein dürfte, wenn sie von der Polizei in Gewahrsam genommen wird. Eine solche **latente** Gefahr, die nicht für sich allein, sondern erst durch den Hinzutritt neuer Umstände – also den relativ unwahrscheinlichen Fall, daß polizeiliche Maßnahmen gegen den Betroffenen ergriffen werden – den Eintritt eines Schadens ernsthaft befürchten läßt, rechtfertigt jedoch keine polizeilichen Eingriffsmaßnahmen nach § 3 HmbSOG. Voraussetzung wäre vielmehr das Vorliegen einer **konkreten** Gefahr, die sich allenfalls in wenigen Ausnahmefällen begründen ließe.

An dieser Stelle möchte ich auch der gelegentlich heute noch vertretenen Meinung entgegentreten, die das Speichern von Informationen durch die Polizei für polizei-interne Zwecke nicht als einen Eingriff in die Grundrechtssphäre ansieht, der eine gesetzliche Grundlage erfordert, sondern als eine schlicht hoheitliche Maßnahme. Gerade das hier erörterte Beispiel veranschaulicht m. E. sehr plastisch, daß eine erhebliche Beeinträchtigung der Persönlichkeitsrechte auch in einer solchen nach außen kaum sichtbar werdenden Maßnahme liegen kann.

Ärzte haben mich darauf aufmerksam gemacht, daß Suizidversuche häufig Ausdruck einer Selbstwertkrise bzw. -kränkung sind. Sie werden von Menschen unternommen, die übermäßig empfindlich reagieren auf subjektiv erlebte oder tatsächlich erfahrene Zweifel am eigenen Wert oder am Idealbild der eigenen Person. Sehr oft werden Gefühle der Ohnmacht, der beschämenden Kränkung oder der eigenen Wertlosigkeit als Motiv für den Freitodversuch angegeben. Unter Berücksichtigung dieser Zusammenhänge muß man davon ausgehen, daß die polizeiliche Datenspeicherung von solchen Patienten im Anschluß an den Freitodversuch als zusätzliche Beschämung und Selbstwertkränkung verarbeitet wird.

Weiterhin zeichnen sich suizidgefährdete Menschen durch ein überstrenges Gewissen aus. Dies wird daraus erkennbar, daß Patienten – so die Erfahrung von Therapeuten – nach einem Suizidversuch häufig über Schuldgefühle klagen, sich subjektiv nicht als Patienten, sondern als Delinquenten erleben und den Freitodversuch selbst als unmoralisch-verwerflichen, ja „verbrecherischen" Akt bewerten. Unter diesen Umständen kann man sich leicht vorstellen, daß die Speicherung persönlicher Daten gerade durch die Polizei – als Repräsentanten der Verbrechensbekämpfung – die beim Suizidenten ohnehin unangemessen stark ausgeprägten Schuldgefühle und Gewissensängste in verhängnisvoller Weise verstärken oder reaktivieren könnte.

Fazit: Schon durch eine schlichte polizeiliche Speicherung kann die therapeutisch gebotene Entlastung und Stabilisierung von Patienten nach Freitodversuchen erheblich gefährdet werden.

3.10.5.3 Hinweise auf Sinti und Roma

Besondere Hinweise auf die Volksgruppe der Sinti und Roma im INPOL sind in den vergangenen Jahren bereits mehrfach von den Datenschutzbeauftragten kritisiert worden. So wurden Angehörige dieser Gruppe mit einem Hinweis als „fahrendes Volk" gekennzeichnet. Von ihnen geführte Ruf- bzw. Spitznamen wurden nicht – wie bei anderen gespeicherten Personen – als „sonstiger Name", sondern ausdrücklich als „Zigeunername" gespeichert.

Die Hamburger Polizei hat die genannten Datenfelder erfreulicherweise schon seit Jahren nicht mehr genutzt. Anders war die Haltung anderer Länder. Trotz gegenläufiger Bemühungen hatte der Arbeitskreis II der Innenminister-Konferenz im Juni 1982 mehrheitlich beschlossen, die Benutzung eines Datenfeldes „Zigeunername" weiter zuzulassen.

Im Mai 1983 hat sich der Arbeitskreis II darauf verständigt, dieses Datenfeld doch zu streichen. Damit wurde nun auch bundesweit ein **wichtiger** Schritt zum Abbau von Diskriminierungen der Sinti und Roma getan. Diesem Ziel ist der Arbeitskreis II gleichwohl nicht viel näher gekommen, weil er gleichzeitig beschlossen hat, ein neues Datenfeld für einen personengebundenen Hinweis auf Beschuldigte/Tatverdächtige ohne festen Wohnsitz bzw. mit häufig wechselndem Aufenthaltsort (HWAO) einzuführen. Dieser Hinweis bezieht sich zwar nicht mehr ausdrücklich auf ethnische Merkmale, ich sehe jedoch – worauf ich die Behörde für Inneres bereits vor Beschlußfassung in dieser Sache hingewiesen hatte – die große Gefahr, daß „Zigeuner" künftig lediglich ein anderes Etikett erhalten. Die Begründung, die der Arbeitskreis II für die Einrichtung des neuen personengebundenen Hinweises gegeben hat, halte ich nicht für schlüssig und überzeugend.

Zunächst wurde angeführt, daß unter kriminalistisch/kriminologischen Gesichtspunkten ein Bedürfnis für die Einführung eines weiteren personengebundenen Hinweises bestehe, der an den fehlenden Lebensmittelpunkt oder die hohe Mobilität anknüpfe. Dieses Ziel werde mit der Kennzeichnung zusätzlicher Namen nicht erreicht. Es bedürfe vielmehr der Einführung eines entsprechenden Merkmals, das ergänzend zu anderen Selektionsmerkmalen (z. B. Alter, Geschlecht) die Möglichkeit biete, aus einer Anzahl namensgleicher Datensätze den wahrscheinlich relevanten auszuwählen.

Worin die erwähnten kriminalistisch/kriminologischen Gesichtspunkte bestehen, ist mir nicht ersichtlich geworden. Auch das Argument, den sachbearbeitenden Dienststellen müsse wegen der hohen Mobilität der betroffenen Personen deutlich gemacht werden, daß Ermittlungsarbeiten unverzüglich aufzunehmen seien, halte ich nicht für schlüssig. Bei Personen, die bereits mehrfach Straftaten begangen haben und keinen festen Wohnsitz nachweisen können, bedarf es keines besonderen Hinweises, um eine intensivere Ermittlungstätigkeit auszulösen.

Schließlich soll neben dem Hinweis „HWAO" der personengebundene Hinweis „LAST" für Land-und Stadtstreicher beibehalten werden. Auch für diese Personen trifft erfahrungsgemäß zu, daß sie entweder ohne festen Wohnsitz sind oder häufig ihren Aufenthaltsort wechseln, so daß es zwei Arten von Hinweisen auf Täter ohne festen Lebensmittelpunkt bzw. mit hoher Mobilität gibt, die verschieden kombinierbar sind. Unter diesen Umständen liegt die Vermutung nahe, daß es sich bei denjenigen Betroffenen, die zwar den Hinweis „HWAO", nicht jedoch den Hinweis „LAST" aufweisen, um Zigeuner handelt.

Die Behörde für Inneres hat mir mitgeteilt, daß die Hamburger Polizei kaum Anlaß zu einer Eingabe von Daten für den neuen personengebundenen Hinweis in INPOL haben würde. Sollte ich im Einzelfall gleichwohl eine von Hamburg veranlaßte Speicherung feststellen, müßte ich diese gem. § 20 HmbDSG beanstanden.

Weitere diskriminierende Erfassungen von Sinti und Roma sind zwischenzeitlich abgestellt worden:

- In der polizeilichen Kriminalstatistik der Freien und Hansestadt Hamburg wurden bis zum Jahr 1982 (wie in derjenigen des Bundes) Straftaten von „Landfahrern" besonders ausgewiesen. Diese besondere Erfassung von Landfahrern ist in Hamburg mit Wirkung vom 1.1.1983 entfallen. Die „Anleitung für die Erfassung von Daten zur Kriminalstatistik" sowie die Statistik-Erhebungs-Bögen sind entsprechend geändert worden.

- Die Polizei verzichtet auf die Erfassung von Standesamtsdaten über „umherziehende Personen ohne festen Wohnsitz" (vgl. Nr. 3.8.4.1).

- Zur Archivierung von polizeilichen Unterlagen über Zigeuner beim Staatsarchiv vgl. Nr. 3.2.2.

3.10.5.4 Straftaten von überregionaler Bedeutung im bundesweiten Kriminalaktennachweis (KAN)

Durch die Einführung des KAN wird es im Aktennachweissystem aller Polizeibehörden grundlegende Veränderungen geben. Während bislang die Polizeibehörden in ihren Auskunftssystemen nur Hinweise auf ihre eigenen Akten verzeichnet hatten, sollen im KAN nunmehr Akten über überregional bedeutsame und schwere Straftaten auch überregional registriert und damit entsprechend verfügbar gemacht werden. Dies bedeutet, daß eine Stuttgarter Polizeibehörde z. B. einen Hinweis auf eine in Hamburg existierende Kriminalakte erhalten kann. Will die Stuttgarter Polizei sodann den Inhalt der Hamburger Akte näher kennenlernen, so kann sie sich mit einem konventionellen Übermittlungsersuchen an die zuständige Hamburger Dienststelle wenden. Dies bedeutet zwar aus polizeilicher Sicht eine erhebliche Verbesserung des Informationsflusses bei der Verbrechensbekämpfung, begründet aber aus datenschutzrechtlicher Sicht zusätzliche Gefährdungen für schutzwürdige Belange der betroffenen Bürger.

In meinem 1. TB (S. 40 f) hatte ich bereits ausgeführt, welche groben Bewertungskriterien für die überregionale Bedeutung von Straftaten unter Beteiligung der Datenschutzbeauftragten festgelegt worden sind. Im Oktober 1983 hat mir die Behörde für Inneres den Entwurf von „Richtlinien für die Führung des Kriminalaktennachweises im INPOL

/POLAS" (KAN-Richtlinien) vorgelegt. Mit Hilfe dieser Richtlinien soll sichergestellt werden, daß die von der Innenminister-Konferenz formulierten relativ groben Aufnahmekriterien für den KAN von den Sachbearbeitern, die die in den KAN aufzunehmenden Akten auswählen, einheitlich gehandhabt werden. Die von der Polizei vorgesehene Prüfung der Akten auf KAN-Relevanz soll zweigleisig erfolgen: Zum einen wurde ein Katalog von Straftaten ausgearbeitet, bei dem eine KAN-Relevanz immer angenommen werden soll. Darüber hinaus wurde eine Reihe von Kriterien näher definiert, bei deren Vorliegen im Einzelfall auch über die Katalog-Straftaten hinaus eine KAN-Relevanz bejaht werden kann.

Der Entwurf bietet dem Kripo-Sachbearbeiter im großen und ganzen eine zweckgerechte Entscheidungshilfe. Ich habe sowohl den Straftaten-Katalog als auch die ergänzenden Einzelfallkriterien überprüft und der Behörde für Inneres noch einige Präzisierungen und Ergänzungen vorgeschlagen. Die Erörterung dieser Angelegenheit war bei Redaktionsschluß noch nicht abgeschlossen. Die folgenden Punkte sind aus meiner Sicht von besonderer Bedeutung:

- In den Katalog dürfen nur Verbrechen sowie die in § 100a StPO genannten besonders gefährlichen Straftaten aufgenommen werden.

- Die Auswahl der Strafakten muß sich immer an dem obersten Grundsatz orientieren, daß nur Straftaten von überregionaler Bedeutung auszufiltern sind. Diese Bedeutung ist bei Straftaten mit einem geringeren Unrechtsgehalt generell nicht gegeben.

- Bei der Definition des Straftatenkatalogs ist klarzustellen, daß die darin genannten Vorschriften aus dem StGB nicht immer, sondern nur im Regelfall überregional bedeutsam sind. Im Einzelfall kann auch eine Katalogstraftat nur von regionaler Bedeutung sein (z. B. der regelmäßige Wirtshausschläger).

- Es ist festzulegen, daß eine Eintragung im KAN wieder zu löschen ist, wenn die Ermittlungen bzw. staatsanwaltschaftliche oder gerichtliche Entscheidungen ergeben haben, daß keine KAN-relevante Straftat vorlag.

3.10.6 Problemfälle bei Übermittlungen an die Polizei

Während bei den Datenübermittlungen von der Polizei an andere Stellen (mit Ausnahme des Verfassungsschutzes, vgl. Nr. 3.11) keine Probleme auftraten, erwiesen sich die Übermittlungen anderer Stellen an die Polizei bisweilen als problematisch. Im Ergebnis konnten jedoch weitgehend befriedigende Lösungen erzielt werden.

3.10.6.1 Sozialdaten

Das Problem ob, in welchem Umfang und unter welchen Voraussetzungen die Polizei Sozialdaten von Sozialleistungsträgern im Wege der Amtshilfe erhalten kann – das ich in meinem 1. TB bereits kurz skizziert hatte – konnte zwischenzeitlich geklärt werden. Die Datenschutzbeauftragten haben sich weitgehend der vom Bundesbeauftragten für den Datenschutz in seinem 5. TB (Nr. 2.11.2, S. 53) begründeten Position angeschlossen. Danach dürfen die Sozialleistungsträger der Polizei unter den Voraussetzungen des § 68 SGB X Amtshilfe, beschränkt auf die dort genannten Stammdaten, gewähren.

3.10.6.2 Feuerwehr-Einsatz-Daten

Durch Pressemeldungen sowie verschiedene parlamentarische Anfragen (Bürgerschafts-Drucksachen 10/542 und 10/621) wurde ich auf die Problematik der Datenübermittlungen von der Feuerwehr an die Polizei aufmerksam gemacht. Ich habe den Sachverhalt in eingehenden Gesprächen mit Feuerwehr und Polizei geklärt und im großen und ganzen befriedigende Lösungen erzielen können.

Bis zum 1. Mai 1983 gab es eine Reihe von Datenübermittlungen, die für die Aufgabenerfüllung der Polizei nicht erforderlich waren. Im einzelnen ergaben sich folgende Feststellungen:
Die Feuerwehr übermittelte an die Polizei
- laufend die Einsatzprotokolle der Feuerwehr (Fernschreiberausdrucke) sowie
- täglich eine vom Rechner ausgedruckte Liste mit den Namen der am Vortag von der Feuerwehr transportierten Personen.

Im einzelnen ging es um folgende Daten:
Auf den Einsatzprotokollen ist zunächst enthalten die sog. Ausmeldung, die ausgedruckt wird, wenn ein Rettungs- oder Notarztwagen der Feuerwehr zum Einsatz ausrückt. Darauf enthalten sind der Grund der Alarmierung sowie der Einsatzort. Diese Informationen dienen der Polizei dazu zu beurteilen, ob ein polizeilicher Einsatz angezeigt ist.

Weiter enthalten sind auf den Einsatzprotokollen die sog. Einmeldungen, die die Besatzungen der Rettungswagen nach Abschluß des Einsatzes von der Feuerwache aus an die Feuerwehreinsatzzentrale durchgeben. Darauf enthalten sind im wesentlichen der Name der transportierten Person sowie der Zielort des Einsatzes. Diese Informationen dienen der Polizei dazu, bereits während des laufenden Tages Auskünfte nach dem Verbleib der transportierten Personen beantworten zu können.

In der Tagesliste sind die Personen, die am vorangegangenen Tage von der Feuerwehr transportiert worden sind, alphabetisch geordnet enthalten. Diese Liste dient ebenfalls dazu, der Polizei die Beantwortung von Auskunftsersuchen nach vermißten Personen zu ermöglichen.

Die Daten, die die Feuerwehr an die Polizei übermittelt, beziehen sich auf Rettungswageneinsätze im Zusammenhang mit verschiedenen Notfällen, die wie folgt klassifiziert werden: Straßenunfall, Hausunfall, Verkehrsunfall, Betriebsunfall, Schiffsunfall, Sportunfall, Notfall-Erkrankung, Notfall-Blutkonserve und Notfall-Verlegung. Einsätze zum Zwecke der Krankenbeförderung von Haus zu Haus oder von Krankenhaus zu Krankenhaus, werden der Polizei nicht übermittelt. Einsätze im Zusammenhang mit Demonstrationen werden lediglich als Straßenunfall gekennzeichnet.

Eine Datenübermittlung in dem vorstehend genannten Umfang erwies sich für die Aufgabenerfüllung der Polizei nicht als erforderlich. Während die Polizei früher in allen genannten Notfällen ebenfalls zum Einsatz ausrückte, sind es heute nur noch ca. 10% der Feuerwehreinsätze, in denen auch die Polizei tätig wird.

Zu nennen sind in diesem Zusammenhang alle Verkehrsunfälle und alle Schiffsunfälle. Bei den übrigen Unfällen wird die Polizei nur tätig, wenn entweder ein Rettungshubschrauber oder ein Notarztwagen eingesetzt wird oder die Feuerwehr zusätzliche Hinweise auf strafrechtlich relevante Vorgänge gibt. Nur Meldungen über Einsätze, in denen die Polizei selbst auch zum Einsatz ausrücken muß, können für die Polizei notwendig sein.

Künftig werden nur noch alle Ausmeldungen per Fernschreiben übermittelt, die in der Regel kaum personenbezogene Daten enthalten. Anhand dieser Ausmeldungen veranlaßt die Polizei ggf. eigene Einsätze. Darüber hinaus erhält sie Rückmeldungen der Feuerwehr, aus denen sich die Erforderlichkeit eines Einsatzes ergeben kann.

Nicht mehr übermittelt werden in Zukunft die Einmeldungen mit dem Zielort und dem Namen der transportierten Person. Diese Regelung ist noch nicht vollständig befriedigend, weil die Polizei nach wie vor – wenn auch in erheblich eingeschränktem Maße – Informationen erhält, die sie zur Aufgabenerfüllung nicht zwingend benötigt. Eine weitergehende Einschränkung ließe sich jedoch mit einem vertretbareren technischen Aufwand nicht realisieren. Insofern wird erst die Neuorganisation der Polizei-Einsatz-Zentrale optimale Lösungen ermöglichen.

Diese Neuorganisation ist für 1987 geplant. Ich habe mich bisher lediglich über den derzeitigen Planungsstand unterrichten lassen. Die Bewertung dieses Vorhabens bleibt einem späteren Tätigkeitsbericht vorbehalten.

Auch die Übermittlung von Daten der transportierten Personen (sowohl aus den Einmeldungen als auch aus den Tageslisten) erwies sich nicht als notwendig. Nach Auffassung der Feuerwehr benötigte die Polizei diese Angaben, um Anfragen nach vermißten Personen beantworten zu können. Die Aufklärung des Schicksals von vermißten Personen sei eine Aufgabe der Polizei. Demgegenüber habe ich darauf hingewiesen, daß zur Erfüllung der genannten polizeilichen Aufgaben keine Vorratshaltung von Listen aller transportierten Personen erforderlich ist. Vielmehr ist es ebensogut möglich, daß die Polizei im Einzelfall, wenn nach einer vermißten Person gesucht wird, bei der Feuerwehr nachfragt, ob die Person irgendwohin transportiert worden ist.

Dementsprechend ist die Bereitstellung von Listen mit den Namen beförderter Personen eingestellt worden.

3.10.6.3 Kraftfahrzeug-Register-Daten

Seit Mitte der 70er Jahre ist das Kraftfahrt-Bundesamt (KBA) in Flensburg damit befaßt, die Führung der zentralen Kraftfahrzeugbestände und des Verkehrszentralregisters auf der Grundlage eines Datenbank-Konzepts neu zu organisieren. Unter Beteiligung des Bundeskriminalamtes wurde ein sog. „Zentrales Verkehrsinformationssystem (ZEVIS)" entwickelt, das folgende Daten aufnehmen und für den on-line-Abruf bereithalten soll:
- alle Daten des zentral geführten Kfz-Bestandes,
- alle Daten des Bestandes der Fahrzeuge mit Versicherungskennzeichen,
- die Personalien der im Verkehrszentralregister Eingetragenen und
- Angaben über entzogene oder versagte bzw. zurückgegebene Fahrerlaubnisse.

Zur Zeit sind noch nicht alle Kfz-Bestände der Länder in ZEVIS aufgenommen. Die Überspielung der Hamburger Bestände soll Ende 1983 erfolgen. Gesamt-ZEVIS soll in der 2. Hälfte des Jahres 1984 realisiert sein.

Im Mai 1983 hat der Bundesverkehrsminister die generelle Zustimmung für den unmittelbaren Zugriff von Polizeidienststellen des Bundes und der Länder auf Daten von ZEVIS gegeben. Auch der Hamburger Polizei ist von der Behörde für Inneres die Genehmigung erteilt worden, sich mit insgesamt neun vorhandenen Datenstationen am Dialog mit ZEVIS zu beteiligen.

Die Einrichtung solcher on-line-Verbindungen halten die Datenschutzbeauftragten nach dem Übergang vom Test- zum Dauerbetrieb für bedenklich, solange noch die – von allen Seiten als notwendig erkannten – Rechtsgrundlagen fehlen. Die für ZEVIS erforderlichen Rechtsgrundlagen sollen nach der Vorstellung des Bundesverkehrsministers durch einen bereits vorliegenden Entwurf eines Fahrzeugregistergesetzes geschaffen werden. Zur Zeit ist jedoch nicht absehbar, wann das Gesetzgebungsverfahren eingeleitet wird. Es ist aus meiner Sicht nicht akzeptabel, daß der Ausbau des gesamten Systems vollzogen wird, bevor der Gesetzgeber mit der Angelegenheit befaßt war. Er wird damit vor vollendete Tatsachen gestellt.

Neben den grundsätzlichen Bedenken gegen den on-line-Anschluß ohne tragfähige gesetzliche Grundlage habe ich ferner Zweifel, ob der Polizei in Zukunft bestimmte Abfragemöglichkeiten eingeräumt werden dürfen. Zur Zeit sind nur folgende Abfragearten zugelassen:
- Halterermittlung (KBA-H),
- Halterermittlung mit Fahrzeugbeschreibung (KBA-K),
- Halterermittlung mit unvollständigem Kennzeichen (KBA-A) und
- Fragen zur Fahrerlaubnis (KBA-F).

Die Polizei wünscht jedoch auch – die bislang noch nicht zugelassene – Einführung der sog. „P-Anfrage", mit der unter dem Namen einer Person nach ihrer aktuellen Anschrift sowie nach allen auf sie zugelassenen Kraftfahrzeugen gefragt werden kann. Ohne die Problematik wegen der fehlenden Aktualität an dieser Stelle vertiefen zu wollen, möchte ich vorsorglich darauf hinweisen, daß die Einführung der P-Anfrage aus datenschutzrechtlicher Sicht höchst bedenklich wäre; denn mit der Bereitstellung einer solchen Anfrage wäre technisch die Möglichkeit eröffnet, den Halterbestand mit seinen rund 30 Mio. betroffenen Bürgern wie ein Bundesadreßregister zu verwenden.

3.10.6.4 Sonstige Problemfälle

Auf einige andere Fälle, in denen Übermittlungen an die Polizei als problematisch angesehen werden, die jedoch zwischenzeitlich befriedigend geregelt werden konnten, bin ich an anderen Stellen des Berichts eingegangen. Hinzuweisen ist auf
- Übermittlungen der Standesämter (vgl. Nr. 3.8.4.1),
- der Schufa (vgl. Nr. 4.9.1) und
- der Hamburger Wasserwerke (vgl. Nr. 4.9.2).

3.11 Landesamt für Verfassungsschutz

Beim Verfassungsschutz habe ich im Jahre 1983 aufgrund von Eingaben nur einige Einzelfälle genauer geprüft. Verglichen mit der Polizei war die Anzahl der Eingaben allerdings sehr gering. Anlaß zu Beanstandungen war in keinem Fall gegeben, in einem Fall konnte eine Löschung erreicht werden.

Neben diesen Einzelfallprüfungen habe ich mich darüber informiert, bei welchen Arten von Personenüberprüfungen im öffentlichen Dienst sowie in sicherheitsempfindlichen Bereichen privater Stellen der Verfassungsschutz beteiligt ist und wie das Verfahren im einzelnen aussieht. Bedenken aus datenschutzrechtlicher Sicht haben sich nicht ergeben. Ich habe mich davon überzeugt, daß bei der Einstellung von Bewerbern in den öffentlichen Dienst – entsprechend einem Senatsbeschluß vom 13.2.1979 – keine Regelanfrage beim Verfassungsschutz erfolgt. Ich werde noch zu prüfen haben, ob die Sicherheitsüberprüfungsrichtlinien (für Bedienstete, die eine sicherheitsempfindliche Tätigkeit ausüben) im Einzelfall eingehalten werden, insbesondere ob diejenigen zu überprüfenden Personen, die lediglich einer Karteiüberprüfung – und nicht weitergehenden Sicherheitsübermittlungen – zu unterziehen sind, hiervon auch unterrichtet werden.

Schließlich habe ich mich bemüht, in einem Gespräch mit dem Leiter des Landesamts einige allgemeine Fragen zu klären. Dabei ging es vornehmlich um die Prüfungskompetenzen des Datenschutzbeauftragten (s. o. Nr. 3.9.1), das Auskunftsverhalten des Landesamts gegenüber Bürgern (vgl. Nr. 3.9.2) sowie die Zusammenarbeit zwischen dem Verfassungsschutz und der Polizei.

Das zuletzt genannte Thema, dessen rechtliche Problematik ich in meinem 1. Tätigkeitsbericht (Nr. 6.7.3, S. 44) bereits skizziert hatte, wurde anhand einiger Fallgruppen erörtert. Dabei konnte z. T. Einigkeit erzielt werden, z. T. blieben Fälle noch streitig.

Einig bin ich mit dem Landesamt insbesondere in folgendem:

- der Verfassungsschutz darf von der Polizei keine Informationen erhalten und speichern, die diese aus Telefonüberwachungsmaßnahmen gem. §§ 100a, 100b StPO gewonnen hat. Die Übermittlung solcher Erkenntnisse wäre von den Verwertungsvorschriften des § 100b StPO nicht gedeckt und im übrigen auch geeignet, die Bestimmungen des Gesetzes zu Artikel 10 GG (G-10-Gesetz), das die Telefonüberwachung durch Nachrichtendienste regelt, zu unterlaufen,

- der Verfassungsschutz darf nicht die Polizei im Amtshilfeweg ersuchen, bestimmte – der Polizei vorbehaltene – Eingriffsmaßnahmen durchzuführen (wie z. B. eine Haus-

suchung), um auf diese Weise zu Informationen zu kommen, die der Verfassungsschutz mit eigenen Mitteln nicht erlangen kann.

Keine Einigkeit besteht in der Frage, ob es mit den §§ 108, 110 StPO sowie mit dem Gebot der prinzipiellen Trennung von Verfassungsschutz und Polizei vereinbar ist, daß die Polizei bei Haussuchungen gewonnene „Zufalls-Informationen" – wie etwa Karteien, Adreßverzeichnisse, die sie für das von ihr betriebene Ermittlungsverfahren nicht braucht – an den Verfassungsschutz weitergibt, wenn die Daten für diesen relevant sein könnten. Im Gegensatz zum Verfassungsschutz bin ich – mit dem Bundesbeauftragten für den Datenschutz (vgl. dessen 5. Tätigkeitsbericht, S. 94) – der Meinung, daß dies unzulässig ist: die genannte Übermittlung durch die Polizei dient nicht mehr dem Zweck des Strafverfahrens und läßt den Verfassungsschutz mittelbar an polizeilichen Befugnissen teilhaben, die ihm selbst nicht zustehen. Das Problem bedarf noch weiterer Klärung.

Ich werde aufmerksam beaobachten, ob sich für die Zusammenarbeit zusätzliche Probleme daraus ergeben, daß die Polizei – künftig in stärkerem Maße – Vorfelderkundungen betreibt (durch Einsatz von V-Leuten und under-cover-agents).

3.12 Staatsanwaltschaft

Meine Aktivitäten im Bereich der Staatsanwaltschaft konzentrierten sich weiterhin auf die Zentralkartei, über die ich bereits im letzten Jahr berichtete. Daneben habe ich mich auf Grund von Eingaben mit mehreren Problemen beschäftigt, die mit der Verarbeitung personenbezogener Daten in Akten zusammenhängen.

3.12.1 Zentralkartei

Nachdem die Justizbehörde zu den von mir übersandten „Mindestanforderungen für den Datenschutz bei den Zentralen Namenskarteien der Staatsanwaltschaft" (Beschluß der Konferenz der Datenschutzbeauftragten) Stellung genommen hatte, habe ich die Probleme gesprächsweise mit der Justizbehörde sowie dem Leiter der Staatsanwaltschaft bei dem Landgericht weiter erörtert. Mit Schreiben vom 7.3.1983 habe ich festgestellt, daß die derzeitige Führung der Zentralkartei gegen die Bestimmungen des § 15 Abs. 3 und 4 verstößt. Ich habe jedoch einstweilen hinnehmbare Zwischenlösungen erzielen können, die eine Beeinträchtigung schutzwürdiger Belange Betroffener weitestgehend ausschließen.

Im einzelnen habe ich folgende Feststellungen treffen müssen: § 15 Abs. 4 verlangt von den speichernden Stellen, daß alle gespeicherten Daten regelmäßig alle vier Jahre auf ihre Erforderlichkeit hin zu überprüfen und ggf. zu bereinigen sind. Eine solche Prüfung wird derzeit bei der Zentralkartei von der Staatsanwaltschaft nicht vorgenommen.

Nach § 15 Abs. 3 sind personenbezogene Daten zu löschen, wenn ihre Kenntnis für die speichernde Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist und kein Grund zu der Annahme besteht, daß durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden. Das derzeit praktizierte Verfahren bei der Zentralkartei, möglichst alle Karteikarten, deren letzte Eintragung 10 Jahre und länger zurückliegt, aus dieser Kartei zu entfernen, entspricht diesen Anforderungen nicht:

Es kann nicht davon ausgegangen werden, daß alle Karteikarten der Zentralkartei nach der letzten Eintragung noch 10 Jahre lang aufbewahrt werden müssen. Dies ergibt sich u. a. schon aus der Tatsache, daß nach den geltenden Aufbewahrungsbestimmungen Schriftgut der Staatsanwaltschaft bei eingestellten Verfahren nur 5 Jahre aufbewahrt werden muß.

Im übrigen scheint mir der Stellenwert, den die Löschungsarbeiten bei der Zentralkartei haben, zu gering zu sein. Es reicht nicht aus, Löschungsmaßnahmen erst vorzunehmen, wenn nach Erledigung aller anderen Aufgaben noch Arbeitskapazitäten frei sind.

Im 1. TB hatte ich ausgeführt, daß ich wegen der bevorstehenden Automation der Zentralkartei, die die o. g. Probleme mit geringem Aufwand lösen wird, einstweilen von einer formalen Beanstandung gem. § 21 abgesehen habe. Es hat sich jedoch herausgestellt, daß das Automationsvorhaben nicht bis 1983 - wie ursprünglich angekündigt – zu realisieren war. Nach neuesten Informationen wird es sogar für möglich gehalten, daß sich die Inbetriebnahme noch bis 1985 verzögern wird, weil zwischen der Justizbehörde und dem Senatsamt noch keine Einigkeit über die Frage erzielt werden konnte, ob das Verfahren auf zentraler oder dezentraler Hardware implementiert werden soll.

Aus diesem Grunde habe ich von der Staatsanwaltschaft als **Zwischenlösung** einschränkende Regelungen für Auskünfte aus der Zentralkartei verlangt. Ich bin dabei davon ausgegangen, daß die entscheidenden Gefährdungen von Belangen der Betroffenen darin liegen, daß möglicherweise personenbezogene Daten über Ermittlungsverfahren, die die Staatsanwaltschaft nicht mehr zur Erfüllung ihrer Aufgaben benötigt und infolgedessen nicht mehr speichern dürfte, an Dritte weitergegeben werden. Um diese Gefahr einzuschränken, habe ich gefordert, daß bis zur Einführung des automatisierten Verfahrens nur noch solche Daten an Dritte (auch an Gerichte, Kriminalpolizei, Justizbehörde) weitergegeben werden, deren Speicherung mit einiger Wahrscheinlichkeit auch ohne Einzelfallprüfung noch zulässig ist. Das sind – in Anlehnung an § 15 Abs. 4 – Daten aus den letzten 4 Jahren.

Dementsprechend dürfen Karteikarten, deren letzte Eintragungen aus dem Jahre 1978 oder früher stammen, grundsätzlich nicht mehr genutzt oder verarbeitet werden. Daten solcher Karteikarten dürfen nur noch im Einzelfall übermittelt werden, nachdem der zuständige Dezernent sorgfältig geprüft hat, ob eine Speicherung noch erforderlich ist. Als **vorläufige** Richtschnur für solche Entscheidungen der Dezernenten habe ich – bis zur Einführung der Automation – die geltenden „Aufbewahrungsbestimmungen für Schriftgut" akzeptiert. Danach ist vor allem darauf zu achten, daß Daten über eingestellte Verfahren nach Ablauf von 5 Jahren nicht mehr übermittelt werden.

Die Staatsanwaltschaft hat die Forderungen voll akzeptiert und durch Rundverfügung vom 3.5.1983 die Auskunftspraxis einschränkend geregelt.

Ich betone jedoch, daß diese Zwischenlösung nur für eine Übergangszeit bis zur Automation akzeptabel ist. Es sind noch erhebliche Anstrengungen nötig, um in jeder Hinsicht den datenschutzrechtlichen Anforderungen entsprechende Zustände herzustellen. Insbesondere sind noch keine differenzierten Löschungs- und Aufbewahrungsfristen für die (automatisierte) Zentralkartei entwickelt worden. Die bislang geltende pauschale Zehn-Jahres-Frist wird den gesetzlichen Anforderungen nicht gerecht. Zu klären wird sein, ob die Aufbewahrungszeit der in der Zentralkartei gespeicherten Daten strikt an die Aufbewahrungsvorschriften für Akten zu koppeln ist oder ob kürzere Fristen für die Zentralkartei möglich sind. Eine im Mai 1983 von der Justizbehörde angekündigte Stellungnahme der Staatsanwaltschaft zu diesem Problem lag bei Abschluß dieses Berichts noch nicht vor.

Im Rahmen der Vorbereitung der Automation der Zentralkartei hat die Justizbehörde mir den die Detailplanung enthaltenden Hauptbericht zur Stellungnahme übersandt. Ich habe einige Bedenken vorgetragen, die sich auf die Speicherbefugnis hinsichtlich einzelner Felder des geplanten Datensatzes sowie auf erforderliche Maßnahmen zur Datensicherung beziehen. Eine Klärung dieser Fragen steht ebenfalls noch aus.

3.12.2 Persönlichkeitsschutz bei der Datenverarbeitung in Akten

Der weitaus überwiegende Teil der bei der Staatsanwaltschaft anfallenden Daten wird nicht in Dateien, sondern in Akten verarbeitet. Aus diesem Grunde liegt es nahe, daß mich Bürger häufig wegen eines Problems anrufen, das sich beim Umgang mit Akten ergibt. Dies gibt mir Veranlassung, einige grundsätzliche Anmerkungen zum Persönlichkeitsschutz bei der Aktenverarbeitung zu machen. Auch wenn das HmbDSG gem. § 1

Abs. 2 S. 1 i. V. m. § 4 Abs. 4 Nr. 3 für die Verarbeitung von Daten in Akten nicht unmittelbar gilt, besteht insoweit kein datenschutzfreier Raum. Soweit die Speicherung und Übermittlung von Daten nicht spezialgesetzlich geregelt sind, ist vielmehr auf die tragenden Bestimmungen der Verfassung zum Schutze der Persönlichkeit (Art. 2 Abs. 1, Art. 1 Abs. 1) zurückzugreifen.

Als gemeinschaftsbezogener und gemeinschaftsgebundener Bürger hat jedermann nur diejenigen Maßnahmen hinzunehmen, die im überwiegenden Interesse der Allgemeinheit unter strikter Wahrung des Verhältnismäßigkeitsgebotes erfolgen (vgl. insbesondere das „Scheidungsakten-Urteil", BVerfGE 27, 344, 351).

Der Grundsatz der Verhältnismäßigkeit verlangt – neben der generellen Abwägung zwischen dem Schutz und der Privatsphäre und dem öffentlichen Interesse –, daß die Maßnahme zur Erreichung des angestrebten Zwecks geeignet und erforderlich ist und daß der mit ihr verbundene Eingriff seiner Intensität nach nicht außer Verhältnis zur Bedeutung der Sache steht (BVerfG a. a. O.).

Die somit erforderliche Güter- und Interessenabwägung ist durch die Datenschutzgesetze näher konkretisiert. Es bietet sich daher an, die entsprechenden Bestimmungen des Hamburgischen Datenschutzgesetzes als Entscheidungshilfe mit heranzuziehen, wenn es gilt, die Zulässigkeit der Speicherung und Übermittlung personenbezogener Daten sowie Angemessenheit von Maßnahmen der Datensicherung zu beurteilen. Auch für die Aktenbearbeitung ist also grundsätzlich davon auszugehen, daß eine Speicherung und Übermittlung personenbezogener Daten nur zulässig ist, wenn sie zur rechtmäßigen Erfüllung der Aufgaben einer öffentlichen Stelle erforderlich ist bzw. – bei einer Übermittlung – der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden. Ferner ist durch technisch-organisatorische Maßnahmen sicherzustellen, daß Unbefugte den Inhalt von Akten weder einsehen noch verändern oder beseitigen können.

Verschiedene Eingaben von Bürgern betrafen gerade den zuletzt genannten Komplex der Datensicherungsmaßnahmen, z. B. Probleme beim Rücktransport von Akten und Unterlagen an die Polizei. Alle festgestellten Probleme konnten jedoch zügig bereinigt werden, da die Staatsanwaltschaft von mir empfohlene Sicherungsmaßnahmen umgehend akzeptierte und in die Tat umsetzte.

Andere Eingaben wiesen auf Probleme bei der Übermittlung von Daten im Rahmen von Akteneinsicht durch andere Behörden bzw. durch Rechtsanwälte hin. In einem Fall hatte die Polizei einem Sozialleistungsträger Akteneinsicht gewährt. In voller Übereinstimmung mit der Staatsanwaltschaft habe ich klargestellt, daß allein die Staatsanwaltschaft in Ermittlungsverfahren über die Gewährung von Akteneinsicht zu entscheiden hat.

In einem weiteren Fall ging es um die Gewährung von Akteneinsicht an bevollmächtigte Rechtsanwälte. Diesem Personenkreis wird gem. Nr. 185 Abs. 4 der Richtlinien für das Straf- und Bußgeldverfahren (RiStBV) Akteneinsicht gewährt, wenn er ein berechtigtes Interesse darlegt und wenn sonst Bedenken nicht bestehen. Ich habe der Justizbehörde in diesem Zusammenhang mitgeteilt, daß ich generell Bedenken sehe, wenn die betroffenen Rechtsanwälte – insbesondere Anwälte von Gläubigern in JGG-Sachen – auch Einsicht in solche Aktenteile erhalten, die besonders sensible persönliche Daten der Beschuldigten enthalten. Ich habe empfohlen, bei einer Akteneinsicht nicht nur die Registerauskunft (vgl. 16 RiStBV), sondern auch den Jugendgerichtshilfebericht und die Vernehmungsprotokolle der Polizei, soweit sie sich auf die persönlichen Verhältnisse beziehen, zurückzuhalten.

3.13 Justizverwaltung und Strafvollzug

Meine Beratungs- und Prüftätigkeit bei Justiz und Strafvollzug konzentrierte sich im Berichtszeitraum auf die Mitarbeit bei der Neufassung einiger Verwaltungsvorschriften sowie auf die Bearbeitung vereinzelter Eingaben.

3.13.1 Überarbeitung von Justizverwaltungsvorschriften

Bei der laufenden Überarbeitung diverser Verwaltungsvorschriften, über die ich z. T. bereits in meinem 1. TB (S. 46 ff) berichtete, ist folgender Sachstand festzuhalten:

3.13.1.1 Anordnung über Mitteilungen in Strafsachen (MiStrA)

Die Justizverwaltungen der Länder haben im Berichtszeitraum den Entwurf für eine Neufassung der MiStrA erarbeitet, den die Justizbehörde mir im September zur Stellungnahme zugeleitet hat. Einige Mitteilungspflichten sollen entfallen; einige weitere Streichungen und Präzisierungen sind jedoch aus datenschutzrechtlicher Sicht noch erforderlich.

Die Datenschutzbeauftragten haben im November 1983 eine gemeinsame Stellungnahme zu Problemen der MiStrA erarbeitet, die ich im Anhang auszugsweise zur Information beifüge.

3.13.1.2 Anordnung über Mitteilungen in Zivilsachen (MiZi)

Die Eingaben, die die Justiz betrafen, richteten sich zumeist gegen Übermittlungen, die auf der Grundlage der MiZi erfolgten, insbesondere gegen die in Pflegschafts-, Vormundschafts- und Entmündigungssachen angeordneten Mitteilungen an das Einwohner-Zentralamt, die Gesundheitsämter, das Polizeiverkehrsamt sowie die Kriminalpolizei. Ich habe inzwischen Stellungnahmen zu diesen Komplexen von der Justizbehörde, der Gesundheitsbehörde und der Behörde für Inneres eingeholt, zur abschließenden Beurteilung des Sachverhalts sind jedoch noch weitere Aufklärungen notwendig. Die abschließende Bewertung dieses wie auch anderer Probleme werde ich gemeinsam mit den anderen Datenschutzbeauftragten in einer Arbeitsgruppe „MiZi" vornehmen. Folgender Einzelfall sollte jedoch nicht unerwähnt bleiben, um die Problematik dieser Übermittlungen zu verdeutlichen:

Eine Bürgerin schilderte mir, daß für sie im Jahre 1976 wegen Krankheit eine Pflegschaft angeordnet worden war, die jedoch im Jahre darauf wieder aufgehoben wurde. Die Bürgerin wunderte sich darüber, daß sie jahrelang keine Wahlbenachrichtigungen erhielt. Als sie sich vor der letzten Bürgerschaftswahl einmal bei der Wahldienststelle erkundigte, erhielt sie die Auskunft, sie dürfe nicht wählen, es bestände eine Pflegschaft. Das Vormundschaftsgericht hatte die in der MiZi genannten Stellen zwar von der Anordnung, nicht jedoch von der Beendigung der Pflegschaft unterrichtet. Die Bürgerin war dadurch u. a. in der Ausübung ihres Wahlrechts behindert. Nach dieser aus meiner Sicht schwerwiegenden Beschwerde habe ich die Justizbehörde u. a. gebeten, mir mitzuteilen, wie es dazu kommen konnte, daß dem Einwohner-Zentralamt (und dem Polizeiverkehrsamt) die Aufhebung der Pflegschaft nicht mitgeteilt wurde. Ich erhielt folgende Antwort: „. . . Von der Aufhebung der Pflegschaft durch den Beschluß vom 19.7.1977 sind diese Dienststellen nicht unterrichtet worden. Dies beruht offensichtlich auf einem Versehen. Nachdem sich Frau xxxxx im April 1983 an das Vormundschaftsgericht gewandt hatte, ist die Mitteilung über die Aufhebung der Pflegschaft unverzüglich nachgeholt worden." Ein derart lockerer und unsensibler Umgang mit den wichtigen Berichtigungsmitteilungen – wie er aus dem zitierten Antwortschreiben spricht – erscheint mir unangemessen. Ich habe die Justizbehörde nachdrücklich darum gebeten, dafür Sorge zu tragen, daß solche Pannen sich nicht wiederholen können.

3.13.1.3 Schuldnerverzeichnis

In meinem 1. TB (Nr. 6.8.3, S. 47 f) hatte ich bereits erläutert, welche Probleme im Zusammenhang mit den listenmäßigen Abschriften aus dem beim Amtsgericht geführten Schuldnerverzeichnis nach § 915 ZPO verbunden sind. Ich hatte berichtet, daß der Bundesjustizminister zur Lösung der aufgetretenen Probleme und zur Eingrenzung der Informationsflüsse bereits im Dezember 1980 den Entwurf einer „Verordnung über Abschriften aus dem Schuldnerverzeichnis" vorgelegt hatte. Einen Fortgang dieser Diskussion

hat es meines Wissens im Jahre 1983 nicht gegeben. Es sieht z. Z. so aus, als wenn diese Angelegenheit von den Landesjustizverwaltungen nicht mehr mit großem Interesse betrieben wird.

3.13.2 Strafvollzug

Die Zusammenarbeit mit dem Strafvollzugsamt erwies sich im Berichtszeitraum als besonders positiv. Zum einen hat es mich von sich aus an der Überprüfung von Dateien sowie bei der Neugestaltung von Vordrucken beteiligt. Meinen Vorschlägen wurde dabei weitgehend Rechnung getragen, einige Datensätze wurden reduziert.

Auch zwei Beschwerden, die den Strafvollzug betrafen, wurde in meinem Sinne abgeholfen:

- in einer Justizvollzugsanstalt konnte durch einfache organisatorische Maßnahmen erreicht werden, daß Besucher während einer Besichtigung der Anstalt nicht mehr die Namen von Insassen, die bislang auf Türschildern sichtbar angebracht waren, zur Kenntnis nehmen können,

- in einer anderen Justizvollzugsanstalt wurde veranlaßt, daß eine im Hinblick auf das Datengeheimnis problematische Verarbeitung personenbezogener Daten im Auftrag externer Stellen nicht mehr erfolgt. Wegen der besonderen Problematik von Patientendaten vgl. auch Nr. 3.14.1.

3.14 Gesundheitswesen

Im Gesundheitswesen habe ich erste umfangreichere Prüfungen durchgeführt und – veranlaßt durch die Prüfergebnisse – intensive Beratungen mit allen Krankenhausträgern begonnen, um die in diesem Bereich weit verbreiteten Unklarheiten und Unsicherheiten beim Umgang mit datenschutzrechtlichen Bestimmungen abzubauen.

3.14.1 Prüfung von Kliniken des Universitäts-Krankenhauses Eppendorf (UKE)

Veranlaßt durch den „Aktenfund im UKE-Gelände" (vgl. Bürgerschaftsdrucksache 11/95) habe ich stichprobenweise vier Kliniken sowie das Krankengeschichtenarchiv der Verwaltung des UKE überprüft und eine Reihe von schwerwiegenden Mängeln festgestellt, die ich gem. § 21 gegenüber dem Direktorium des UKE beanstandet habe. Folgendes war zu bemängeln:

1. Es gab keine klaren schriftlich fixierten Regelungen für die Ausführung der Datenschutzgesetze bzw. zur Verhinderung von Schweigepflichtsverletzungen. Es fehlen für die Bediensteten eindeutige Festlegungen darüber

   - wer Zugang zu den jeweiligen Patientendaten hat

   - an wen Auskünfte über Patienten erteilt werden

   - an wen Patientendaten übermittelt werden dürfen

   - in welcher Art und Weise die Patientenunterlagen aufzubewahren sind

   - wann spätestens und wie Patientendaten zu vernichten sind.

2. In der Neurologischen Poliklinik sowie in der Augenklinik sind nicht die technisch-organisatorischen Vorkehrungen getroffen worden, die erforderlich sind, um eine Offenbarung der Patientendaten an Unbefugte zu verhindern. Da diese Feststellungen einer Stichproben-Überprüfung entstammen, ist nicht ausgeschlossen, daß auch in weiteren Kliniken insoweit Mängel bestehen.

Das UKE hat meine Feststellungen akzeptiert und Sofortmaßnahmen getroffen, um die dringlichsten technisch-organisatorischen Vorkehrungen zur Datensicherung zu organisieren. Der Wachdienst und die Betriebs-Abteilung wurden zu verstärkten Kontrollen von Datensicherungsmaßnahmen angewiesen und eine Bestandsaufnahme zu den angesprochenen Problemen in allen Kliniken des UKE wurde veranlaßt. Die Lösung der Probleme ist jedoch noch nicht abgeschlossen. Insbesondere die vorhandene, z. T. sehr alte Bausubstanz der UKE-Kliniken und -Pavillons erwies sich bei vielen Datensicherheitsmaßnahmen als besonderes Problem.

Durch die Eingabe eines Strafgefangenen wurde ich ferner darauf aufmerksam, daß das UKE Unterlagen mit medizinischen Patientendaten in der Buchbinderei einer Justizvollzugsanstalt binden ließ. Diese gem. § 203 StGB unzulässige Datenoffenbarung wurde jedoch – nachdem sie dem Direktorium des UKE bekannt geworden war – ebenso wie alle anderen Arten einer Datenverarbeitung (incl. Löschung) bei externen Stellen umgehend gestoppt.

Ferner hat das UKE die Erarbeitung von Datenschutzrichtlinien in Angriff genommen, wobei ich beratend hinzugezogen wurde. Bei dieser Arbeit wurde jedoch sehr schnell deutlich, daß es nicht allein um die Lösung UKE-spezifischer Probleme ging, sondern daß die meisten Fragestellungen für alle Krankenhäuser gleichermaßen von Bedeutung waren. Das UKE wird mithin die Beratungsergebnisse des von mir initiierten Gesprächskreises zum „Datenschutz im Krankenhaus" mit einbeziehen.

3.14.2 Beratungen zum „Datenschutz in Krankenhäusern"

Da nicht nur beim UKE, sondern auch bei den sonstigen meiner Kontrolle unterliegenden staatlichen und nicht-staatlichen Krankenhäusern noch eine Reihe von Defiziten und Unsicherheiten bei der Umsetzung des Datenschutzes vorliegen, habe ich im Frühjahr alle Krankenhausträger zu einer Gesprächsrunde eingeladen.

Dieses Angebot ist von allen eingeladenen Stellen (Gesundheitsbehörde einschl. allgemeiner Krankenhäuser, Behörde für Wissenschaft und Forschung einschl. UKE sowie Hamb. Krankenhausgesellschaft als Dachorganisation der privaten und freigemeinnützigen Krankenhäuser) angenommen worden.

In dem Gespräch mußte ich feststellen, daß es unter den Teilnehmern große Unsicherheiten insbesondere wegen des Verhältnisses zwischen der ärztlichen Schweigepflicht und den Datenschutzgesetzen gab.

Diese Frage konnte zunächst abstrakt geklärt werden. Es wurde herausgearbeitet, daß die Anwendung der Vorschriften des BDSG auf der einen sowie des § 203 StGB auf der anderen Seite in aller Regel zu gleichen Ergebnissen führt (vgl. dazu Nr. 3.14.3). Ich habe deshalb empfohlen, bei der geplanten Erarbeitung von Richtlinien den Umgang mit Daten in den Krankenhäusern die Differenzierung nach der Form der Datenverarbeitung nicht zu sehr in den Vordergrund zu rücken.

Nach der von mir initiierten Gesprächsrunde sind die Diskussionen in zwei – vom Landesbetrieb Krankenhäuser bzw. vom UKE federführend betreuten – Arbeitskreisen weitergeführt worden. Abschließende Ergebnisse wurden noch nicht erzielt. Besondere Probleme zeigten sich vor allem bei den folgenden Fragen:

Zum einen ging es darum, wie die Aufbewahrung von Akten und anderen Unterlagen so organisiert werden kann, daß nur zugriffsberechtigte Personen auch Zugang erhalten; zum weiteren ging es vor allem um das Problem, ob und unter welchen Voraussetzungen Patientendaten zu Forschungszwecken verwendet bzw. übermittelt werden dürfen.

3.14.3 Zum Verhältnis zwischen dem Schutz des Patientengeheimnisses nach § 203 StGB und den Datenschutzgesetzen

Nach der übereinstimmenden Auffassung der im „Düsseldorfer Kreis" vertretenen Aufsichtsbehörden sind die Vorschriften der Datenschutzgesetze und des § 203 StGB auf die Verarbeitung medizinischer Daten von Krankenhauspatienten gleichrangig nebeneinander anwendbar („Zwei-Schranken-Prinzip"). Soweit also

1. personenbezogene „medizinische" Daten, in welcher Form auch immer, verarbeitet werden, gilt immer § 203 StGB,

2. personenbezogene „medizinische" Daten in **Dateien** verarbeitet werden, gilt neben § 203 StGB das BDSG,

3. das Krankenhaus nicht-medizinische Daten, also Informationen, die nicht dem Arzt in seiner beruflichen Eigenschaft gegeben wurden, in Dateien verarbeitet, gilt allein das BDSG.

Die im konkreten Einzelfall bisweilen schwierige Abgrenzung der verschiedenen Anwendungsbereiche verliert **praktisch** erheblich an Bedeutung, weil die Anwendung der verschiedenen Vorschriften in aller Regel zu gleichen Ergebnissen führt. Dies läßt sich anhand von zwei praktisch besonders wichtigen Beispielen (Zulässigkeit von Übermittlungen [1.]; Notwendigkeit von Datensicherungsmaßnahmen [2.]) zeigen.

1. Ein Fall, in welchem eine Übermittlung nach § 203 StGB unbefugt aber nach § 24 BDSG zulässig ist oder umgekehrt, kann praktisch nicht vorkommen: Zu § 203 StGB haben Rechtsprechung und Literatur folgende Rechtfertigungsgründe herausgearbeitet, bei deren Vorliegen eine Offenbarung i. S. d. § 203 StGB befugt ist. Soweit die Offenbarungsbefugnis nicht ausdrücklich geregelt ist, ist die Offenbarung erlaubt, wenn sie zur Wahrung entgegenstehender berechtigter eigener oder fremder Interessen unter Berücksichtigung der widerstreitenden Interessen ein angemessenes Mittel dazu ist. Ferner ist die Offenbarung befugt, wenn sie mit Einwilligung des Betroffenen erfolgt. Die Einwilligung kann auch durch schlüssiges Verhalten ausgedrückt werden.

   Als Rechtfertigungsgrund kommt schließlich die mutmaßliche Einwilligung in Betracht, die vorliegt, wenn der Offenbarende im vermeintlichen Interesse und Einverständnis des Geheimnisgeschützten zu handeln glaubt, insbesondere, wenn dessen Einverständnis nicht eingeholt werden kann oder er offensichtlich keine Einwendungen hat.

   Nach § 24 BDSG dürfen personenbezogene Daten übermittelt werden zur Wahrung berechtigter Interessen der übermittelnden Stelle oder eines Dritten oder der Allgemeinheit, wenn dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden. Es findet also ebenfalls eine Interessenabwägung statt. Das bedeutet, daß nach § 203 StGB und nach dem BDSG in gleicher Weise geprüft werden muß, ob eine Datenübermittlung zur Wahrung berechtigter Interessen erforderlich ist und ob sie unter Berücksichtigung der widerstreitenden Interessen ein angemessenes Mittel dazu ist. Die Ergebnisse der jeweiligen Beurteilung können sich folglich nicht unterscheiden.

   Zu übereinstimmenden Ergebnissen gelangt man auch bei der Einwilligung oder mutmaßlichen Einwilligung. Die wirksame Entbindung von der Schweigepflicht gem. § 203 StGB läßt zugleich den Schluß zu, daß schutzwürdige Belange des Betroffenen i. S. des § 24 Abs. 1 BDSG nicht beeinträchtigt sind. Das Verhalten und der Wille des Betroffenen können bei der Auslegung des Begriffs „schutzwürdige Belange" nicht unberücksichtigt bleiben. Dasselbe gilt für die mutmaßliche Einwilligung, die nur ein Ersatz für die wirklich erteilte Einwilligung ist. Sie richtet sich nach dem hypothetischen Willen des Betroffenen, wie ihn der Offenbarende aufgrund einer objektiven sorgfältigen Prüfung aller Umstände vermuten dürfte.
   Die Tatsache, daß nach § 203 StGB eine Einwilligung des Betroffenen formlos erteilt

werden kann, nach § 3 BDSG aber schriftlich erfolgen muß, ist daher ohne praktische Bedeutung. Wenn damit auch eine formlose Einwilligung nach § 203 StGB für die datenschutzrechtliche Zulässigkeit ausreicht, sollte schon der Rechtsklarheit wegen nicht auf eine schriftliche Einwilligung verzichtet werden.

2. Auch im Bereich der Datensicherungsmaßnahmen führt die Anwendung des BDSG nicht zu anderen Ergebnissen als die des § 203 StGB.

   Für die in Dateien geführten Unterlagen gilt § 6 BDSG. Danach sind die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des BDSG zu gewährleisten. Zwar gelten die in der Anlage zu § 6 Abs. 1 BDSG (die wörtlich übereinstimmt mit der Anlage zu § 8 Abs. 1 HmbDSG) genannten Anforderungen nur für automatisierte Verfahren; auch in nicht automatisierten Dateien sind jedoch Sicherheitsregelungen notwendig, um der Beeinträchtigung schutzwürdiger Belange der Betroffenen entgegenzuwirken. Es ist zu gewährleisten, daß Unbefugte den Inhalt der Dateien weder einsehen, verändern oder löschen noch deren Datenträger entwenden oder zerstören können.

   Auch bei **Krankenakten**, auf die nur der § 203 StGB Anwendung findet, gilt im Ergebnis nichts anderes: Jeder Arzt und jeder seiner Gehilfen hat danach die Pflicht, das Bekanntwerden der ihm anvertrauten Geheimnisse über Patienten zu verhindern. Auch ein Unterlassen kann den Tatbestand der Schweigepflichtverletzung erfüllen. Daraus folgt, daß die verpflichteten Personen die technischen, organisatorischen, baulichen und personellen Vorkehrungen zu treffen haben, die erforderlich sind, um eine Offenbarung der Patientendaten an Unbefugte zu verhindern.

3.14.4 Übermittlungen von Patientendaten an die Kirchen

Besondere Probleme entstanden im Berichtszeitraum im Zusammenhang mit der Übermittlung von Patientendaten an die Krankenhausseelsorge der Kirchen. Der Landesbetrieb Krankenhäuser hatte die Erhebung der Religionszugehörigkeit von stationär behandelten Krankenhauspatienten sowie die Übermittlung von Patientennamen an die jeweils zuständigen Kirchen eingestellt und wurde deswegen von den Kirchen kritisiert. Die Gesundheitsbehörde hat mich in diesem Konflikt beratend hinzugezogen und es konnte eine – auch den Belangen der Kirchen Rechnung tragende – datenschutzgerechte Lösung gefunden werden: in die Erhebungsbögen der allgemeinen Krankenhäuser wird in Zukunft folgende Klausel aufgenommen, nach deren Maßgabe eine Übermittlung an die Kirchen zulässig sein wird:

> „Falls sie auch in der Zeit ihres Krankenhausaufenthalts eine seelsorgerische Betreuung wünschen, geben sie bitte Ihre Religionszugehörigkeit an. Das Krankenhaus hält ihre Angabe fest und setzt aufgrund dessen den für sie zuständigen Krankenhausseelsorger von ihrem Wunsch in Kenntnis. Die Beantwortung dieser Frage ist freiwillig."

3.15 Sozialwesen

Ein überdurchschnittlich großer Anteil der Beratungsersuchen, die ich im Berichtszeitraum zu erledigen hatte, entfiel auf Datenschutzprobleme im Sozialwesen (insbesondere bei Bezirksgesundheits- und -sozialämtern, der BAJS und LVA). Nach wie vor gibt es dort große Schwierigkeiten bei der Umsetzung der bereichsspezifischen Regelungen zum Schutz der Sozialdaten im 10. Buch des Sozialgesetzbuches (SGB X). Die BAJS hat ihre „Hinweise zum Schutz der Sozialdaten" zwar zwischenzeitlich vereinheitlicht, so daß nunmehr dieselben Verwaltungsvorschriften für das Amt für Jugend und die übrigen Ämter der BAJS gelten, gleichwohl sind die Unsicherheiten unter den Bediensteten nach wie vor groß. Immerhin habe ich bei vielen Mitarbeitern ein relativ hohes Problembewußtsein beim Umgang mit personenbezogenen Daten feststellen können, was auch zu den vielen Anfragen geführt hat, die an meine Dienststelle gerichtet waren.

3.15.1 Problemfälle bei der Anwendung der Übermittlungsvorschriften des SGB X

Leider bin ich an der Vereinheitlichung der Verwaltungsvorschriften der BAJS zum Schutze der Sozialdaten nicht beteiligt worden. Ich beabsichtige, dies im nächsten Jahr im Lichte der bisher gemachten praktischen Erfahrungen zu überprüfen und ggf. Vorschläge zu unterbreiten, wie sie konkreter und anschaulicher formuliert werden können.

In diesem Bericht möchte ich lediglich kurz auf zwei Vorschriften des SGB X eingehen, deren Anwendung sich in der Praxis als besonders schwierig herausstellte: es handelt sich dabei um die §§ 69 und 76 SGB X. Auf die §§ 68 und 75 SGB X bin ich in anderem Zusammenhang eingegangen (vgl. Nr. 3.10.6.1 und Nr. 3.16.3).

3.15.1.1 § 69 Abs. 1 Nr. 1 SGB X

§ 69 Abs. 1 Nr. 1 SGB X ist in der Praxis die wichtigste Vorschrift für den Datenaustausch unter den Sozialleistungsträgern. Hiernach ist eine Offenbarung von Sozialdaten zulässig, soweit sie erforderlich ist für die Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch durch einen Sozialleistungsträger. Diese weitgehende Regelung trägt dem Umstand Rechnung, daß die genannten Aufgaben nicht von einer einheitlichen Sozialverwaltung, sondern von einer Vielzahl verschiedener Stellen durchgeführt werden.

In der Praxis wird leider häufig nicht berücksichtigt, daß diese Vorschrift die Offenbarung auf die erforderlichen Daten beschränkt: Es genügt also nicht, daß der Übermittlung lediglich eine entsprechende Aufgabe zugrundeliegt oder daß die Daten zur Aufgabenerfüllung geeignet sind und ihre Nutzung zweckmäßig ist. Vielmehr muß es der jeweiligen Behörde unmöglich sein, ihre Aufgabe ohne Kenntnis der zu übermittelnden personenbezogenen Daten rechtmäßig zu erfüllen.

Beispielsweise war es unzulässig, daß das Versorgungsamt Durchschriften von allen Feststellungsbescheiden nach dem Schwerbehindertengesetz an die Bezirksgesundheitsämter übermittelte. Ich habe erreicht, daß solche Übermittlungen künftig nur noch mit Einwilligung der Betroffenen erfolgen.

3.15.1.2 § 76 SGB X

In der Verwaltung wird häufig übersehen, daß diese Vorschrift eine nach den §§ 68 bis 75 SGB X zulässige Offenbarung noch weiter einschränkt, wenn es sich um Daten handelt, die einem Sozialleistungsträger von einem Arzt oder einer anderen in § 203 Abs. 1 und 3 StGB genannten Person zugänglich gemacht worden sind. Sie soll vor allem gewährleisten, daß die ärztliche Schweigepflicht und die sonstigen in § 203 Abs. 1 und 3 StGB genannten Berufsgeheimnisse auch dann gewahrt werden, wenn z. B. der Arzt personenbezogene Daten an einen Sozialleistungsträger (z. B. gesetzliche Krankenversicherung) weiterleitet. Solche Daten darf der Sozialleistungsträger gem. § 76 Abs. 1 StGB nur (weiter) übermitteln, wenn auch der Arzt selber insoweit offenbarungsbefugt wäre. Dementsprechend dürfen z. B. Sozialdaten mit ärztlichen Unterlagen, wie sie etwa bei OEG-Akten anfallen (vgl. Nr. 3.16.3) zu Forschungszwecken nur unter den Voraussetzungen übermittelt werden, unter denen sie auch der Arzt selbst zu Forschungszwecken hätte weitergeben dürfen – d. h. in der Regel nur mit Einwilligung des betroffenen Patienten.

Zusätzliche Schwierigkeiten entstehen dadurch, daß es von der Ausnahmevorschrift des § 76 Abs. 1 SGB X wiederum eine Rück-Ausnahme gibt, nämlich § 76 Abs. 2 SGB X.

Danach gilt der eben dargestellte Abs. 1 vor allem im Rahmen der Zusammenarbeit der Sozialleistungsträger untereinander(§ 69 Abs. 1 Nr. 1 SGB X) nicht für eine bestimmte Gruppe von Arztdaten. Es handelt sich dabei um die Patientendaten, die im Zusammenhang mit einer vom Betroffenen oder vom Sozialleistungsträger veranlaßten Begutach-

tung wegen der Erbringung von Sozialleistungen oder der Ausstellung einer Bescheinigung erhoben werden. Nicht erfaßt von der Rück-Ausnahme sind somit die üblichen, ohnehin beim behandelnden Arzt vorhandenen Anamnese-, Befund- und Diagnosedaten. Für diese gilt vielmehr in vollem Umfang § 76 Abs. 1 SGB X.

3.15.2 Bestellung von betrieblichen Datenschutzbeauftragten gem. § 79 SGB X

3.15.2.1 Sachstand

In meinem 1. TB (Nr. 6.10.1, S. 49) hatte ich darauf hingewiesen, daß die Behörden und sonstigen öffentlichen Stellen der Freien und Hansestadt Hamburg ihrer Pflicht, betriebliche Datenschutzbeauftragte gem. § 79 SGB X i. V. m. §§ 28, 29 BDSG zu bestellen – soweit sie Sozialleistungsträger sind –, nicht nachgekommen waren. Ich äußerte damals die Erwartung, daß die Verwaltung dies bald nachholen werde; doch hat sich diese Erwartung bis heute nicht erfüllt. Erst Ende November hat der Senat eine Zuständigkeitsanordnung für die Wahrnehmung der Datenschutzaufgaben nach dem SGB X beschlossen. Bis zur Entscheidung des Senats sind die beteiligten Behörden untätig geblieben.

Bei diesem Sachstand muß ich feststellen, daß die hamburgischen Behörden, die Aufgaben von Sozialleistungsträgern wahrzunehmen haben (BSB, BWF, BAJS, Gesundheitsbehörde, Bezirksämter) sowie – jedenfalls nach meiner Auffassung – alle Behörden mit eigener Personalverwaltung ihre Verpflichtungen nach § 16 Satz 1 HmbDSG verletzt haben: Sie haben es unterlassen, die Ausführung des § 79 SGB X – als anderer Rechtsvorschrift über den Datenschutz i. S. des § 16 – für ihren Geschäftsbereich sicherzustellen. Ich bedaure das besonders deshalb, weil im Sozialbereich nach meinen oben geschilderten Erfahrungen noch besondere Defizite bei der Umsetzung der bereichsspezifischen Datenschutzregelungen bestehen, für deren Abbau die Tätigkeit eines zusätzlichen verwaltungsinternen Kontrollorgans sehr nützlich hätte sein können.

3.15.2.2 Vorschläge zur Organisation des betrieblichen Datenschutzbeauftragten

Ich habe dem Senatsamt für den Verwaltungsdienst im Berichtszeitraum meine Vorschläge für eine sinnvolle, den stadtstaatlichen Verhältnissen angepaßte Organisation der Aufgaben der betrieblichen Datenschutzbeauftragten mitgeteilt und habe dabei in fast allen Fragen Einigkeit erzielen können. Im einzelnen erscheinen mir folgende Punkte erwähnenswert:

- Die Übertragung eines Teils der Zuständigkeiten des betrieblichen Datenschutzbeauftragten von den originär zuständigen Behörden auf externe Stellen wie das Senatsamt für den Verwaltungsdienst (Organisationsamt) ist aus meiner Sicht unbedenklich.

  Die bei der Durchführung des HmbDSG vorgenommene Differenzierung der Zuständigkeiten zwischen der Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungs-Programme (gem. § 16 S. 2 Nr. 2) einerseits und der Aufgabe nach § 16 Satz 2 Nr. 1 andererseits hat sich nach meinem Eindruck bewährt und sollte daher auch bei der Durchführung des Datenschutzes im Bereich der Sozialleistungsträger beibehalten werden.

  Die Konzentration aller Aufgaben des bDSB beim Senatsamt für den Verwaltungsdienst würde hingegen dazu führen, daß bei den eigentlich zuständigen Behörden nicht genügend Verantwortung für die Durchführung der Datenschutzgesetze verbleiben würde und sie für die Kontroll- und Beratungstätigkeit des Hamburgischen Datenschutzbeauftragten keine geeigneten Gesprächspartner zur Verfügung stellen könnten.

- Bedenken habe ich auch nicht dagegen, daß die Aufgaben des „betrieblichen Datenschutzbeauftragten" den Stellen übertragen werden, die bereits mit der Aufgabe der

Sicherstellung des Datenschutzes in der jeweiligen Behörde (nach § 15 BDSG bzw. § 16 HmbDSG) betraut sind. Mögliche Einwände gegen ihre Zuverlässigkeit wegen etwaiger Loyalitätskonflikte, die solche Doppelfunktionen im nicht-öffentlichen Bereich unzulässig erscheinen lassen, treten wegen der zusätzlichen Kontrolltätigkeit durch den Hamburgischen Datenschutzbeauftragten zurück.

- An die Stelle der Bestimmung bestimmter Personen zum bDSB kann auch die Verankerung der Aufgaben eines bDSB in Arbeitsplatzbeschreibungen an einer oder mehreren Stellen einer Behörde, die Leistungsträger ist, treten. In diesem Falle müssen

  - die Aufgaben gem. §§ 16, 29 BDSG,

  - die persönlichen Anforderungen an den Stelleninhaber gem. § 28 Abs. 2 BDSG sowie

  - die organisatorische Eingliederung (§ 28 Abs. 3 BDSG)

  in der Arbeitsplatzbeschreibung geregelt sein. Betrieblicher Datenschutzbeauftragter ist dann derjenige, der diesen Arbeitsplatz einnimmt.

Auch meine Vorstellungen über Einzelheiten der in einer solchen Arbeitsplatzbeschreibung zu definierenden Aufgaben und persönlichen Anforderungen und zur organisatorischen Eingliederung (im Assistenzbereich) habe ich dem Senatsamt vorgetragen und grundsätzliche Zustimmung feststellen können.

3.15.2.3 Betriebliche DSB auch bei den Personalverwaltungen?

Keine Einigkeit konnte bis zum Schluß in der Frage erzielt werden, ob die Behörden mit eigener Personalverwaltung, soweit sie das Bundeskindergeldgesetz ausführen, ebenfalls als Sozialleistungsträger – mit der Folge, bDSB bestellen zu müssen – anzusehen sind.

Das Organisationsamt vertrat den Standpunkt, daß die Aufzählung der Leistungsträger in den §§ 15 – 29 SGB X, die die Personalverwaltung nicht nenne, abschließend sei. Ich habe dem widersprochen. Zwar erweckt der Wortlaut der §§ 12 Satz 1, 18 bis 29 SGB X den Anschein, als handele es sich um eine für das Sozialgesetzbuch abschließende Aufzählung der Leistungsträger. Tatsächlich handelt es sich bei den §§ 18 – 29 aber um spezifische Einweisungsvorschriften, die keine Anspruchs-, sondern Informationsnormen mit dem Zwecke sind, „jedem Bürger eine möglichst genaue Kenntnis des Sozialleistungssystems und der ihm zustehenden Leistungsansprüche zu verschaffen" (Begründung der Bundesregierung in BT – Drs. 7/868 S. 26). „Die Einweisung kann und will nicht abschließend sein" (ebenda). Deswegen kann auch die „zuständige" Stelle oder der Leistungsträger endgültig erst dort klargestellt werden, wo die einschlägige Anspruchsgrundlage für den Anspruch auf eine bestimmte Sozialleistung zu finden ist. Da das Bundeskindergeldgesetz (BKGG) bis zu seiner Einordnung gem. Art. II § 1 Nr. 13 des Sozialgesetzbuches – Allgemeiner Teil – vom 11.12.1975 (BGBl. I S. 3015) als besonderer Teil des Sozialgesetzbuches gilt, ist § 45 BKGG eine Vorschrift des Sozialgesetzbuches mit der Folge, daß die dort genannten Stellen Leistungsträger sind.

Um eine zügige Bestellung betrieblicher Datenschutzbeauftragter jedenfalls bei den unstreitig als Leistungsträger angesehenen Behörden zu fördern, habe ich meine rechtlichen Bedenken gegen die Auffassung des Organisationsamtes zurückgestellt, falls bestimmte Bedingungen akzeptiert werden. Dabei kommt es mir vor allem darauf an, daß die strenge Zweckbindung und besondere Vertraulichkeit der Daten gewährleistet sind, die den Personalverwaltungen bei der Ausführung des Bundeskindergeldgesetzes über die Daten, die sie ohnehin bei der Erfüllung ihrer Aufgaben erfahren, hinaus zur Kenntnis gelangen (z. B. Einkommensverhältnisse des Ehegatten). Nach meiner Auffassung entspricht die Vertraulichkeit der Personalakte in dem materiellen Gehalt der Normen und in der geübten Praxis weitgehend dem Sozialgeheimnis; darüber hinaus muß sichergestellt werden, daß

- die zusätzlichen Daten aus der Ausführung des BKGG nicht für andere Aufgaben der Personalverwaltung genutzt und

- in einem besonderen Teil der Personalakte aufbewahrt werden, der bei der vorübergehenden Überlassung der Personalakte an andere Stellen (z. B. Nr. 31 der zitierten Anordnung) zurückbehalten wird.

3.15.3 Ausführung des Bundeskindergeldgesetzes

Die Ausführung des durch das Haushaltsbegleitgesetzes vom 20.12.1982 geänderten Bundeskindergeldgesetzes wirft eine Reihe datenschutzrechtlicher Probleme auf und war mehrfach Gegenstand von Eingaben. Nach der Neuregelung erhalten bekanntlich Eltern mit 2 oder mehr Kindern, deren Einkommen bestimmte Grenzen übersteigt, nur noch ein gekürztes Kindergeld. Die Folge ist, daß die Eltern gegenüber den Kindergeldstellen (also den Arbeitsämtern bzw. – für den öffentlichen Dienst – den Personalverwaltungen) Angaben über ihre Einkünfte machen müssen.

Die zur Erhebung dieser Angaben zunächst benutzten einheitlichen Vordrucke sahen mehr Einzelangaben vor, als für die Ausführung des BKGG erforderlich waren. Hier konnten die Datenschutzbeauftragten in einer gemeinsamen Aktion gegenüber den zuständigen Verwaltungen Änderungen erwirken.

Im Gegensatz zu den zunächst eingesetzten Vordrucken wird in einem neu entwickelten Vordruck nun die detaillierte Darlegung der Einkommensverhältnisse sowie die Angabe der Steuernummer nicht mehr verlangt. Die entsprechenden Beträge entnimmt die Kindergeldstelle selbst dem vom Antragsteller vorzulegenden Einkommensteuerbescheid /Bescheid über den Lohnsteuerjahresausgleich bzw. einer Jahreslohnbescheinigung. Die Vorlage dieser Nachweise wird zwar in allen Fällen verlangt; es genügt jedoch die Einreichung einer Fotokopie, auf der die für das Kindergeld nicht erforderlichen Angaben unkenntlich gemacht sind. Ablesbar müssen lediglich sein: Alle Einkünfte (bis zur Summe der Einkünfte), die Vorsorgeaufwendungen, die Unterhaltsleistungen nach § 10 Abs. 1 Nr. 1 oder § 33a Abs. 1 EStG sowie die festgesetzten Steuerbeträge.

Damit sind einige wesentliche Forderungen der Datenschutzbeauftragten erfüllt worden. In einigen anderen Punkten konnten sie sich dagegen nicht durchsetzen.

Die Datenschutzbeauftragten hatten gefordert, nur die maßgebliche Summe der positiven Einkünfte, nicht aber deren Aufschlüsselung in einzelnen Einkunftsarten zu erheben (bzw. festzustellen) sowie ferner die Überprüfung der angegebenen Einkommensverhältnisse durch Vorlage des Einkommensteuerbescheides oder durch Einholung von Auskünften bei den Finanzämtern auf solche Einzelfälle oder Fallgruppen zu beschränken, bei denen konkrete Anhaltspunkte für Mißbrauch gegeben sind oder Unstimmigkeiten vorliegen, die mit dem Antragsteller nicht geklärt werden können.

Diesen Forderungen haben die zuständigen Behörden mit folgender Begründung widersprochen:

- Die Berechtigten wären mit der Meldung der Summe häufig überfordert, da sie hierzu Rechenoperationen anstellen müßten, die nicht ganz einfach sind; das Risiko unbewußt falscher Angaben wäre sehr groß.

- Der förmliche Nachweis der Einkünfte sei für den Regelfall geboten, um das Risiko von Überzahlungen auf das vertretbare Maß zu mindern. Der Nachweis ließe sich häufig auch nicht durch die Vorlage einer Fotokopie des Einkommensteuerbescheides führen, auf der die einzelnen Summanden unkenntiich gemacht sind und nur die Summe der Einkünfte ablesbar ist. Denn die im Einkommensteuerbescheid ausgewiesene Summe ergebe sich oft aus der kindergeldrechtlich unzulässigen Berücksichtigung negativer Einkünfte.

Die Finanzämter müßten in allen Fällen um entsprechende Auskunft gebeten werden, womit sie allzu stark belastet würden. Die Kindergeldstellen wären nicht in der Lage, den Berechtigten zu erklären, wie die vom Finanzamt genannte Zahl (Summe der positiven Einkünfte) errechnet worden ist, und damit würde das Risiko von Rechtsstreitigkeiten unangemessen vergrößert.

Auch andere Verfahrensvorschläge wurden von den zuständigen Behörden als – angeblich – unpraktikabel verworfen. Alternativ vorgeschlagen war z. B. die Ausstellung einer besonderen Bescheinigung durch die Finanzämter, die nur die für das Kindergeld relevanten Daten enthält, eine direkte Datenübermittlung durch die Finanzämter an die Kindergeldstellen ohne Beteiligung des Berechtigten und die Übertragung der Kindergeldzahlung auch für Angehörige des öffentlichen Dienstes auf die Arbeitsämter.

Der letztgenannte Vorschlag ist aus der Befürchtung heraus gemacht worden, die durch die Angabe- und Nachweispflicht dem Dienstherrn/Arbeitgeber bekanntgewordenen Einkommensverhältnisse könnten zutreffende Personalentscheidungen in unzulässigerweise zum Nachteil des Bediensteten beeinflussen. Diese aus der Sicht der Betroffenen sicherlich ernst zu nehmenden Befürchtungen haben die Datenschutzbeauftragten veranlaßt, nachdrücklich auf die strenge Zweckbindung hinzuweisen, der die Kindergelddaten unterliegen, und ferner darauf aufmerksam zu machen, daß bei der Erfüllung von Aufgaben nach dem BKGG das Sozialgeheimnis nach dem Sozialgesetzbuch zu wahren ist. Ob die Durchführung des Bundeskindergeldgesetzes dem Sozialgesetzbuch oder aber dem jeweiligen Datenschutzgesetz unterliegt, ist auf Bundesebene wie auch in Hamburg streitig. Ich habe jedoch in Hamburg zumindest durchsetzen können, daß die Zweckbindung der Daten akzeptiert und durch getrennte Aktenführung organisatorisch abgesichert wird (s. a. Nr. 3.15.2.3).

3.16 Wissenschaft und Forschung

3.16.1 Modelle zur Lösung des Konflikts zwischen Forschung und Datenschutz

Gegenstand häufiger und z. T. auch heftiger Diskussionen ist der Zielkonflikt zwischen Datenschutz und wissenschaftlicher Forschung. Die Wissenschaft ist bemüht, ihre Erkenntnismöglichkeiten ständig zu erweitern und sie durch die – von der modernen Informationstechnik ermöglichten neuen Formen der Datenbeschaffung, -speicherung und -auswertung – voll auszunutzen. Demgegenüber ist es Aufgabe des Datenschutzes, die Interessen des Einzelnen, über den Daten verarbeitet werden, auch gegenüber der Wissenschaft zur Geltung zu bringen. Dies gilt insbesondere, soweit die Interessen des Einzelnen nicht nur durch die allgemeinen Datenschutzgesetze, sondern darüber hinaus noch durch spezielle Geheimhaltungsvorschriften (wie z. B. die ärztliche Schweigepflicht) geschützt sind.

Nach meinen Erfahrungen, die ich bei der Prüfung einiger Forschungsvorhaben gesammelt habe, bieten sich zur gesetzlichen Lösung des Konfliktes drei typische Regelungsmodelle an:

a) Soweit es um die auf Dauer angelegte Verarbeitung großer Mengen besonders sensibler Daten geht, die für einen klar überschaubaren, konkret definierten Informations-und Forschungsbedarf benötigt werden, bietet sich eine gesetzliche Regelung nach dem Vorbild des Krebsregistergesetz-Entwurfes an (vgl. dazu Nr. 3.16.2.2).

b) Soweit Forscher Zugang zu Datenbeständen wünschen, die wegen ihres Inhalts (z. B. die Grunddaten des Melderegisters) oder ihrer weitgehenden Anonymisierung (bei statistischen Einzelangaben) von vornherein nur eng begrenzte Risiken für die Betroffenen enthalten, kommt eine relativ breite Öffnung von Datenbeständen für wissenschaftliche Interessen in Betracht. Ein Beispiel für solche Regelungen – die übrigens weiter gefaßt sein können und nicht auf Forschungszwecke beschränkt sein müssen – enthält § 34 Abs. 3 HmbMG für die Gruppenauskunft aus dem Melderegister.

c) Wenn persönliche Daten von hoher Sensibilität zu verarbeiten sind, ohne daß sich eine langfristige Forschungsaufgabe so präzise definieren und eingrenzen läßt wie beim Krebsregister, kann eine Abwägung zwischen den beiderseitigen Interessen nur im Einzelfall vorgenommen werden. Auf die Notwendigkeit einer solchen einzelfallbezogenen Abwägung stellen etwa die Forschungsklauseln einiger Landesdatenschutzgesetze sowie die Regelung des § 75 SGB X (vgl. dazu Nr. 3.16.3) ab; auch § 3a des Referenten-Entwurfs des Bundesinnenministeriums für die Novellierung des BDSG orientiert sich an diesem Modell. Solche Forschungsklauseln sollen Komplikationen vermeiden, die sich bei der Anwendung der Datenschutzgesetze auf Forschungsvorhaben bisweilen ergeben, und Kriterien bereitstellen, die es erlauben, die Besonderheiten der wissenschaftlichen Datenverwertung im Rahmen der Abwägung angemessen, d. h. ohne Einräumung von Freibriefen für die Forschung in Rechnung zu stellen.

Diesen Forderungen wird der vorliegende Entwurf für eine BDSG-Novelle nicht gerecht: zum einen knüpft er bei der Beurteilung der Zulässigkeit bestimmter Datenverarbeitungsmaßnahmen nicht an ein bestimmtes, klar zu definierendes Forschungsvorhaben (wie etwa § 75 SGB X und auch noch der BDSG-Novellierungsentwurf, Stand 31.3.1982), sondern nur an einen bestimmten Forschungszweck an, der von der forschenden Stelle sehr weit gefaßt werden kann. Desweiteren enthält die Vorschrift eine Reihe von zu allgemein gehaltener Formulierungen, so daß auch in Zukunft Auslegungsstreitigkeiten bestehen würden (z. B. fehlen gesetzliche Maßstäbe für die Auslegung von unbestimmten Rechtsbegriffen wie „zumutbar" und „schutzwürdige Belange"). Unklar ist, ob und in welchem Umfang besondere Amts- und Berufsgeheimnisse zu Forschungszwecken durchbrochen werden dürfen. Schließlich fehlen in dem Entwurf einige Regelungen über den weiteren Umgang mit den Daten durch die Forscher (z. B. Zweckbindung).

Ob und in welcher Form in das Hamburgische Datenschutzgesetz eine Forschungsklausel übernommen werden sollte, wird im kommenden Jahr unter Berücksichtigung der Ergebnisse zu prüfen sein, die die Diskussion über die BDSG-Novelle erbringen wird.

3.16.2 Forschung im Gesundheitswesen

Als besonders problematisch erweisen sich in der Praxis immer wieder die Fragen, die bei der Forschung mit Patientendaten auftauchen. Gerade in diesem Bereich wird der Datenschutz häufig als großes Hindernis für die Forschung hingestellt, obwohl die Hindernisse hier kaum in den Datenschutzgesetzen, sondern in den althergebrachten besonderen Berufsgeheimnissen (§ 203 StGB) zu sehen sind.

Bevor ich auf konkrete Forschungsvorhaben eingehe, die ich geprüft habe, erlaube ich mir daher einige allgemeine Vorbemerkungen zu diesem Komplex.

3.16.2.1 Allgemeine Probleme bei der Forschung mit Patientendaten

Nach meinen Feststellungen war es bisher im UKE und – in eingeschränktem Maße – auch in den allgemeinen Krankenhäusern üblich, z. B. Doktoranden mit den im Krankenhaus anfallenden Daten (aus Krankengeschichten u. ä.) forschen zu lassen bzw. Meldungen an externe Stellen wie das Hamburgische Krebsregister vorzunehmen, ohne den Patienten darüber zu unterrichten, geschweige denn, ihn um seine Einwilligung zu bitten.

Als Petenten sich bei mir beschwerten und ich bei meinen Gesprächen mit Vertretern der Krankenhäuser diese Offenbarungen in Frage gestellt habe, breitete sich große Unsicherheit aus. Es zeigte sich, daß viele forschende Ärzte nur schwer zu überzeugen sind, daß lange geübte Praktiken im Hinblick auf das in neuerer Zeit gewandelte Verständnis der ärztlichen Schweigepflicht aufgegeben werden müssen.Dem steht allerdings der klare Standpunkt des deutschen Ärztetages gegenüber, der erst im letzten Jahr be-

schlossen hat, die ärztliche Schweigepflicht nach der Berufsordnung dahingehend zu präzisieren, daß die geschützten Daten für wissenschaftliche Zwecke nur in anonymisierter Form weitergegeben werden dürfen.

Ich habe immer die Auffassung vertreten, daß eine Offenbarung von (nicht anonymisierten) Patientendaten grundsätzlich – sowohl nach § 203 StGB als auch nach den Datenschutzgesetzen – nur mit Einwilligung des betroffenen Patienten zulässig ist. Der Betroffene muß die Gewißheit haben, daß seine persönlichen Angaben in bestimmten Bereichen streng vertraulich behandelt werden. Sonst kann die notwendige Vertrauensbeziehung zwischen Arzt und Patient schweren Schaden erleiden.

Aus diesen Gründen kommt eine Durchbrechung dieser Geheimnisse (sei es durch Regelung gesetzlicher Offenbarungsbefugnisse wie im Krebsregister – vgl. Nr. 3.16.2.2 – sei es durch Anwendung allgemeiner Rechtfertigungsgründe z. B. mutmaßliche Einwilligung) nur in Einzelfällen in Betracht, die für den Betroffenen in ihren konkreten Auswirkungen überschaubar bleiben. Denkbar ist eine Durchbrechung demnach etwa unter folgenden Voraussetzungen:

- die Durchbrechung dient einem Forschungszweck von überragender Bedeutung,

- dieser Zweck kann mit anonymisierten Daten nicht erreicht werden, und die Erhebung einer Einwilligung beim Betroffenen ist unmöglich bzw. würde den Zweck der Forschung erheblich gefährden.

Diese Grundsätze sind bei der Fassung des Krebsregistergesetz-Entwurfes berücksichtigt worden. Sie sind auch von maßgebender Bedeutung für die Regelungen des Umgangs mit Patientendaten zu Forschungszwecken, die der Arbeitskreis „Datenschutz im Krankenhaus" (s. dazu Nr. 3.14.2) z. Z. erarbeitet.

3.16.2.2 Hamburgisches Krebsregister

Nach langer Vorlaufzeit ist es der Gesundheitsbehörde nun gelungen, einen Entwurf für ein Hamburgisches Krebsregistergesetz vorzulegen, der die Arbeit des – bereits seit 1929 tätigen – Hamburgischen Krebsregisters auf eine – nach heute einhelliger Auffassung unabdingbare – gesetzliche Grundlage stellen soll. An der Ausarbeitung dieses Entwurfs, der zu Beginn des Jahres 1984 der Bürgerschaft zugeleitet werden soll, habe ich von Anfang an mitarbeiten können. Bis auf einige Punkte von untergeordneter Bedeutung, die noch verbessert werden können, meine ich, daß der Konflikt zwischen Forschung und Datenschutz in diesem Entwurf in vernünftiger Weise aufgelöst worden ist. Ich verzichte an dieser Stelle darauf, das Gesetz im einzelnen darzustellen – Einzelheiten können der demnächst allgemein zugänglichen Bürgerschaftsdrucksache entnommen werden.

Ich möchte lediglich die drei Punkte hervorheben, deren Regelung aus datenschutzrechtlicher Sicht besonders bedeutsam ist und die in der politischen Diskussion vermutlich besonders umstritten sein werden.

a) Eine entscheidende Regelung des Entwurfs, die auch aus datenschutzrechtlicher Sicht unabdingbar ist, besagt, daß Meldungen an das Krebsregister – im Gegensatz zum Musterentwurf des BMJFG – grundsätzlich nur mit Einwilligung der Patienten zulässig sind. Eine bestimmte Form für die Einwilligung ist – wie für die Einwilligung zur Offenbarung nach § 203 StGB – nicht vorgesehen. Aus Gründen der Rechtsklarheit hielte ich es für sinnvoll, in Anlehnung an § 5 Abs. 2 grundsätzlich eine schriftliche Erklärung zu verlangen.

b) § 2 Abs. 2 HmbKrebsRG-E läßt ausnahmsweise Meldungen auch ohne Einwilligung des Patienten zu und schafft damit einen gesetzlichen Offenbarungstatbestand, der die ärztliche Schweigepflicht überwindet. Die Ausnahmeregelung lautet:

„Die Meldung kann ausnahmsweise ohne Einwilligung des Patienten erfolgen, wenn der Patient nicht um seine Einwilligung gebeten werden kann, weil er wegen der sonst eintretenden Gefahr einer ernsthaften und nicht behebbaren Gesundheitsverschlechterung über das Vorliegen einer Krebserkrankung nicht unterrichtet worden ist, und wenn außerdem kein Grund zu der Annahme besteht, daß der Patient die Einwilligung verweigert hätte. Der Meldende hat die Gründe dafür, daß er die Einwilligung nicht eingeholt hat, aufzuzeichnen". (§ 2 Abs. 2)

Diese Ausnahmeregelung lehnt sich eng an die höchstrichterliche Rechtsprechung (BGHZ 29.17b 185, 85, 327, 333) an, wonach es Situationen geben kann, in denen ein Arzt von einer Aufklärung des Patienten absehen darf, weil die mit der Aufklärung verbundene Eröffnung der Natur des Leidens zu einer ernsthaften nicht behebbaren Gesundheitsschädigung des Patienten führen würde. Gerade die in der Bevölkerung weit verbreitete Furcht vor einer Krebserkrankung bringt es mit sich, daß einzelne Patienten bei Offenbarung der wahren Diagnose in Hoffnungslosigkeit verfallen und sich selbst aufgeben würden. Bei Krebserkrankungen ist aber der Wille des Patienten, die Krankheit zu meistern, von entscheidender Bedeutung für die Therapie.

Wenn ein Arzt es in einem konkreten Fall für geboten hält, seinem Patienten die Tatsache, daß er an Krebs erkrankt ist, zu verheimlichen, dann kann er naturgemäß den Patienten auch nicht um seine Einwilligung für die Meldung an das Hamburgische Krebsregister bitten.

Ich habe mich von den Krebsforschern überzeugen lassen, daß eine solche Ausnahmeregelung für Zwecke der Forschung unverzichtbar ist. Ein genereller Verzicht auf die Meldung in den Ausnahmefällen würde nach ihren Erfahrungen dazu führen, daß ein Krebsregister die Situation nur verzerrt wiedergibt, da sich die Ausnahmefälle nicht gleichmäßig auf alle Formen und Stadien von Krebskrankheiten verteilen, sondern bei bestimmten Formen und Stadien häufiger sind.

Es wird jedoch streng zu überprüfen sein, ob in der Praxis Meldungen ohne Einwilligung tatsächlich die Ausnahme sind und bleiben werden. Erwägenswert erscheint mir auch die Möglichkeit, zunächst auf die Ausnahme zu verzichten, um zu testen, wie sich dies auf die Anlieferung der Daten auswirkt. Dies würde m. E. auch die Akzeptanz des Krebsregisters in der Hamburger Ärzteschaft erhöhen.

c) Datenschutzrechtliche Belange sind ferner besonders tangiert, wenn es um die Übermittlung personenbezogener Daten aus dem Krebsregister geht. Der Rahmen für solche Übermittlungen ist in § 9 in Anlehnung an die Regelung des § 75 SGB X bewußt sehr eng gezogen worden. Übermittlungen dürfen nur erfolgen an öffentlichrechtliche Forschungseinrichtungen für ein genau beschriebenes Forschungsvorhaben und nur auf besonderen Antrag, über den nicht das Hamburgische Krebsregister, sondern der Präses (oder Staatsrat) der Gesundheitsbehörde entscheidet. Zuvor sind der Hamburgische Datenschutzbeauftragte und die Ethik-Kommission der Ärztekammer zu hören.

   Die Übermittlung darf nur zugelassen werden, wenn das Forschungsvorhaben ohne die personenbezogenen Daten nicht durchgeführt werden kann und schutzwürdige Belange des Patienten nicht beeinträchtigt werden.

3.16.2.3 Basisdokumentation Psychiatrie

An allen staatlichen psychiatrischen Kliniken Hamburgs – AK Eilbek, AK Ochsenzoll und Psychiatrische Klinik des UKE – werden z. Z. Psychiatrische Basisdokumentationen erstellt. Sinn dieser Vorhaben ist es, Daten über das Auftreten von psychischen Erkrankungen sowie deren Behandlung zu gewinnen. Alle Basisdokumentationen arbeiten einheitlich auf der Grundlage eines Erhebungsbogens, der von der PROGNOS AG zur Begleitforschung beim Modellprogramm Psychiatrie der Bundesregierung entwickelt worden ist.

Dieser Erhebungsbogen wird von den behandelnden Ärzten ausgefüllt und an eine Dokumentationsassistentin im jeweiligen Krankenhaus übersandt. Diese überprüft die abgelieferten Bögen und trennt deren Kopfteile mit den Identifikationsdaten der Patienten von den Rumpfbögen mit Angaben zu Diagnose und Behandlung ab, nachdem sie beide mit einer Fall-Nr. gekennzeichnet hat. Identifikationsdaten und statistische Daten werden sodann getrennt aufbewahrt, nur die statistischen Daten werden auf einer ADV-Anlage verarbeitet.

Ich habe mir bislang die Verfahren im AK Ochsenzoll und im UKE angesehen und insbesondere Datensicherungsmaßnahmen geprüft. Bestimmte Probleme, die mit der Anonymisierung der Daten zusammenhängen, sind noch zu lösen.

Nicht abschließend geklärt ist bislang auch die Frage der Speicherbefugnis. Soweit hier medizinische Forschung mit Patientendaten betrieben wird, bedarf die Speicherung grundsätzlich der Einwilligung; soweit die Auswertung lediglich einer Art innerbetrieblicher Erfolgskontrolle dient, kann möglicherweise auf die Einwilligung verzichtet werden. Eine derart zweckgebundene Speicherung könnte sich noch im Rahmen des Vertragsverhältnisses nach § 23 BDSG (Behandlungszusammenhang) bewegen; offen ist jedoch, ob eine derartige Verwendung in der Klinik bereits die ärztliche Schweigepflicht verletzt.

Die abschließende Klärung der Frage der Speicherbefugnis wurde vertagt, bis der mit den Fragen befaßte Arbeitskreis mit den Krankenhäusern Ergebnisse erzielt hat.

3.16.3 Forschung und Sozialdaten

Ein Bürger beschwerte sich darüber, daß das Landesversorgungsamt seine Sozialdaten, die im Zusammenhang mit einem Anspruch nach dem Opferentschädigungsgesetz erhoben worden waren, zu Forschungszwecken einer Stelle der Universität Hamburg offenbart hatte. Meine Nachprüfungen haben ergeben, daß die BAJS – Amt für Arbeit und Sozialordnung – im Februar 1981 die Offenbarung von Sozialdaten für ein Forschungsprojekt „Praxis des OEG" im Frühjahr 1981 gem. § 75 SGB X genehmigt hatte. Ich habe den Genehmigungsvorgang geprüft und festgestellt, daß er in formeller Hinsicht den Anforderungen des § 75 Abs. 2 SGB X entsprechend abgelaufen ist.

Die Prüfung der Rechtmäßigkeit in materieller Hinsicht konnte noch nicht abgeschlossen werden. Zu diesem Komplex habe ich der BAJS mit Schreiben vom 28.6.1983 Fragen vorgelegt, die bis zum Abschluß dieses Berichts noch nicht beantwortet waren. Ich kann mir daher noch kein Urteil bilden, ob die Nutzung der Akten des Versorgungsamtes zu Forschungszwecken schutzwürdige Belange der Betroffenen beeinträchtigt bzw. ob ggf. das öffentliche Interesse an der Forschung das Geheimhaltungsinteresse des Betroffenen erheblich überwiegt. Ein weiteres noch offenes Bewertungsproblem hängt schließlich damit zusammen, daß die OEG-Akten regelmäßig auch Daten enthalten, die dem Versorgungsamt vom behandelnden Arzt bzw. Krankenhaus des Betroffenen mitgeteilt worden sind und deren Offenbarung daher nur unter den, den § 75 SGB X weiter einschränkenden Voraussetzungen des § 76 SGB X zulässig ist.

3.16.4 Forschung im Justizwesen

Auf Bitten der beteiligten Forscher habe ich eine Stellungnahme zum Forschungsprojekt „Strafvollstreckungskammern" beim Landgericht Hamburg abgegeben. Die Durchführung dieses Vorhabens ist aus datenschutzrechtlicher Sicht nicht zu beanstanden. Zum einen entspricht es voll den Anforderungen des im Jahr 1982 neu geregelten § 185a der Richtlinien für das Straf- und Bußgeldverfahren (RiStBV), das die Akteneinsicht für wissenschaftliche Zwecke regelt. In dieser in der Öffentlichkeit wie auch unter Forschern wenig bekannten Verwaltungsvorschrift heißt es:

„§ 185a Akteneinsicht für wissenschaftliche Vorhaben

1. Für wissenschaftliche Vorhaben wird Akteneinsicht gewährt, wenn und soweit deren Bedeutung dies rechtfertigt, der Verwaltungsaufwand vertretbar ist, und die Gewähr besteht, daß ein Mißbrauch der erlangten Kenntnisse nicht zu befürchten ist.

   Die Gewährung von Akteneinsicht kann mit Auflagen verbunden werden: in der Regel ist die Auflage zu erteilen, daß die Akten nicht an Dritte weitergegeben werden dürfen und daß Hinweise auf Verfahrensbeteiligte oder auf Tatsachen, die zu ihrer Identifizierung führen können, zu vermeiden sind.

2. Im vorbereitenden Verfahren und in Verfahren mit sicherheitsrelevanten Bezügen wird Akteneinsicht grundsätzlich nicht gewährt.

3. Über die Akteneinsicht für wissenschaftliche Vorhaben entscheidet in den Fällen der Nr. 183 Buchstabe a der Behördenleiter; dies gilt auch in den Fällen der Nr. 183 Buchstabe c, soweit die Akten bei der Staatsanwaltschaft verwahrt werden. Nr. 184 findet keine Anwendung. Betrifft das Vorhaben mehrere Staatsanwaltschaften, so entscheidet die gemeinschaftliche übergeordnete Behörde."

Über diese Anordnungen hinaus sind den Forschern mehrere zusätzliche Auflagen aufgegeben worden, die sie bei der Durchführung des Projekts einzuhalten haben:

- Die Akteneinsicht erfolgt nur in den Räumen des Landgerichts, die Akten dürfen das Haus nicht verlassen.

- Die aus den Akten erhobenen Daten werden nur anonymisiert auf Datenträger übertragen.

- Laufzettel, die die Zuordnung verschiedener Erhebungsunterlagen zu einzelnen Probanden gewährleisten sollen, werden im Landgericht getrennt aufbewahrt und nach Ablauf eines halben Jahres vernichtet.

Die zusätzlichen Beschränkungen entsprechen den Regelauflagen, die die Datenschutzbeauftragten zur weiteren Konkretisierung des § 185a RiStBV für erforderlich halten, bislang aber nicht durchgesetzt haben.

Bei Einhaltung dieser Auflagen ist eine Beeinträchtigung schutzwürdiger Belange der Betroffenen nicht zu befürchten.

4. Einzelne Probleme des Datenschutzes im nicht-öffentlichen Bereich

4.1 Handel

4.1.1 Umtauschzettel bei Kaufhäusern

Zu Beginn des Jahres machte mich eine Petentin darauf aufmerksam, daß bei einem großen Hamburger Kaufhaus personenbezogene Daten derjenigen Kunden gespeichert würden, die Ware im Wert von über DM 100,– umtauschen.
Ich bin der Sache nachgegangen und habe festgestellt, daß die Rückzahlung bei Beträgen über DM 100,– nur gegen Vorlage eines Ausweises (Personalausweis, Paß) erfolgt. Der Organisationsleiter dieses Kaufhauses hat mir zur Begründung mitgeteilt, daß in einer Vielzahl von Fällen gestohlene Ware zurückgegeben und mit der Behauptung, der Kassenzettel sei verlorengegangen, eine Rückzahlung des Kaufpreises begehrt werde. Ihm gehe es darum, die Zahl dieser Serien- und Trickbetrügereien dadurch einzuschränken, daß durch die Vorlage eines Ausweises eine „psychologische Barriere" aufgebaut werde.

Ich habe gegen dieses Verfahren keine grundsätzlichen Bedenken: Die Umtauschzettel, denen einige Grunddaten (Name, Adresse und Nr. des Personalausweises) zu entnehmen sind, werden weder in eine manuelle noch in eine EDV-gestützte Kartei übertragen. Sie werden in keiner Weise systematisiert, sondern in der Reihenfolge des Umtausches abgelegt. Die Daten werden nicht ausgewertet und auch nicht an andere Stellen – weder innerhalb der speichernden Stelle noch an Dritte – übermittelt. Eine regelmäßige Durchsicht, Prüfung oder anderweitige Kontrolle der Umtauschzettel erfolgt nicht. Nur dann, wenn der Kunde den an der Umtauschkasse tätigen Mitarbeitern bereits durch häufiges Umtauschen bekannt ist oder er sich auffällig benimmt, werden die unsortierten Umtauschzettel durchgesehen. Die Zettel werden 1 Jahr aufbewahrt und dann vernichtet.

4.1.2 Versandhandel

Mehrfach haben mich Fragen erreicht, die sich auf den Erstbestellschein des Versandhandels beziehen. Hierin wird eine relativ große Menge personenbezogener Daten vom künftigen Kunden abgefordert. Wie in meinem 1. TB (vgl. Nr. 4.2.2, Beispiel 5, Seite 21) bereits erwähnt, will sich das Versandhaus über die Bonität des Vertragspartners ein Bild machen, bevor es ihm ein Dauer- oder Sammelbesteller-Konto einrichtet. Dazu wird bei der Schufa angefragt, die zur eindeutigen Identifizierung eine Reihe von personenbezogenen Merkmalen benötigt (z. B. auch die Voranschrift). Andere Angaben werden direkt zur Bonitätsprüfung verwendet. So kann es für ein Kreditangebot durchaus von Belang sein, ob ein neuer Kunde ein eigenes Einkommen bezieht, nur im Rahmen der Schlüsselgewalt oder nur eines Taschengeldes über eigene Mittel verfügen kann.

Wie ein Handelsunternehmen vorgeht, um im Einzelfall ein mögliches Risiko vor Vertragsabschluß zu prüfen, ist nirgends vorgeschrieben. Wenn die internen Kreditvergaberegeln einer Firma vorsehen, daß auch bei einem Einzelkauf gegen Rechnung und bei kürzester Zahlungsfrist eine Bonitätsprüfung vorzunehmen ist, dann spielt sich dieser Vorgang innerhalb der vertraglichen Beziehungen ab, die von beiden Seiten frei ausgestaltet werden können. Ich bin allerdings der Meinung, daß es eine Grenze des Erforderlichen gibt. Wenn allzu kleinlich viele Daten erhoben werden, um das kaufmännische Risiko nahezu völlig auszuschalten, ist diese Grenze sicher überschritten.

Letztlich bleibt es aber jedem selbst überlassen, welche Angaben er seinem möglichen Vertragspartner liefern will. Wenn er von der Beantwortung derjenigen Fragen absieht, von denen er meint, daß sie für eine Bonitätsprüfung nicht erforderlich sind, sind negative Folgen nicht zu erwarten. Das Versandhaus kann allenfalls zurückfragen oder das Vertragsangebot ablehnen. Dann hat der Kunde erneut Gelegenheit, nach dem konkreten Zweck der gewünschten Angaben zu fragen. Wenn er seine personenbezogenen Daten nicht hergeben will, bleibt in der Regel nur der Weg über den Kauf per Nachnahme.

In meinem 1. TB hatte ich eine Beschwerde erwähnt, die sich dagegen richtete, daß ein Versandhaus auf dem vollständigen Ausfüllen des Erstbestellscheins bestanden hatte, obwohl der Petent die bestellte Ware bei Lieferung zahlen wollte. Nach einem Gespräch mit dem Kundenberater des Versandhauses hatte er den Eindruck gewonnen, daß auch bei einer Lieferung gegen Nachnahme vorher die Schufa befragt würde. Ich habe festgestellt, daß dies ein Mißverständnis war. Gerade weil sich der Petent für den Kauf per Nachnahme entschieden hatte, erfolgte eine Anfrage bei der Schufa nicht.Beim Nachnahme-Verfahren entsteht kein kreditorisches Risiko, das durch eine Schufa-Anfrage bzw. -auskunft abzudecken wäre. Deshalb wird die Schufa bei dieser Art der Lieferung niemals eingeschaltet.

Wohl aber holen Versandhäuser regelmäßig auch dann eine Auskunft der Schufa ein, wenn sie gegen offene Rechnung liefern sollen, weil der Kunde die Möglichkeit erhält, ein paar Tage später zu zahlen. Auch wenn sofort nach Lieferung gezahlt wird, erfolgt bis zum Eingang des Rechnungsbetrages eine Waren-Kreditierung.

Hierbei wird jedoch eine mit den Aufsichtsbehörden abgestimmte Bagatell-Grenze (DM 100,–) berücksichtigt. Die Schufa erteilt bei Anfragen wegen kleinerer Beträge keine Auskunft.

4.1.3 Direktwerbung

4.1.3.1 „Robinsonliste"

Wer nicht umworben werden will, kann sich in die beim **Allgemeinen Direktwerbe- und Direktmarketing-Verband e. V. (ADV)** geführte „Robinsonliste" eintragen lassen. In meinem vorigen TB hatte ich die Adresse dieses Verbandes und die der Deutschen Postreklame GmbH und vom Kraftfahrtbundesamt mitgeteilt, die ähnliche Karteien eingerichtet haben.

Dazu ist anzumerken, daß es sich hierbei um freiwillige – am eigenen Interesse orientierte – Angebote handelt, die mir allerdings verbesserungsfähig erscheinen. Die „Robinsonliste" z. B. wird nur jeweils im Herbst und im Frühjahr auf ihren aktuellen Stand gebracht und den Verbandsmitgliedern zur Verfügung gestellt. Es kann also vorkommen, daß der Aufnahmewunsch eines Betroffenen bis zu 6 Monaten unberücksichtigt bleibt. Ich halte einen häufigeren Änderungsdienst für erforderlich.

Ich möchte im übrigen daran erinnern, daß der ADV nur ein Drittel des Werbemarktes vertritt.

4.1.3.2 Übermittlung listenmäßiger oder sonst zusammengefaßter Daten

Wünschenswert wäre es, daß die Rechtsposition des Betroffenen durch eine Novellierung des § 24 BDSG gestärkt wird.

Der Referentenentwurf vom März 1982 hatte dem Betroffenen das Recht einräumen wollen, einer Übermittlung seiner Daten zu Zwecken der Werbung oder der Markt- und Meinungsforschung weitgehend zu widersprechen (und damit klarzustellen, daß er durch die Verwendung seiner Daten zu Werbezwecken seine schutzwürdigen Belange beeinträchtigt sieht). Diesen Lösungsansatz hat der neue Referentenentwurf (Stand Juni 1983) leider fallengelassen. Im übrigen soll es dabei bleiben (§ 24 Abs. 3 des Referentenentwurfs), daß die listenmäßige Datenübermittlung für Werbezwecke erleichtert werden soll. Durch die Neufassung der Vorschrift werden die Bedenken nicht ausgeräumt, die schon gegen den Referentenentwurf 1982 vorgebracht wurden. Es bleibt problematisch, daß die Übermittlung von Daten einer Personenmehrheit – einschließlich der möglicherweise sehr sensiblen Angabe über die Zugehörigkeit zu der Personengruppe – privilegiert werden soll, während die Übermittlung der gleichen Datenarten für einen einzelnen Betroffenen den strengeren Zulässigkeitsvoraussetzungen des § 24 Abs. 1 BDSG unterliegt.

4.2 Kreditwirtschaft

4.2.1 Erteilung von Bankauskünften

Während der Datenaustausch zwischen Banken und Schufa zufriedenstellend geregelt ist, gibt das Verhalten der Kreditinstitute bei sog. Bankauskünften zu Bedenken Anlaß. Eine Bankauskunft ist die Mitteilung eines Kreditinstituts an ein anderes oder auch an einen Kunden über die wirtschaftlichen Verhältnisse, das geschäftliche Gebaren und die Geschäftsmoral eines ihrer Kunden. Es wird z. B. angegeben, für welchen Kreditbetrag der Kunde „gut" ist, ob er ein pünktlicher Zahler ist, wie die geschäftlichen Verhältnisse bewertet werden; eine Rolle können aber auch persönliche Verhältnisse des Kunden im engeren Sinne spielen, etwa bei Angaben über Familienangehörige.
Die Bankauskunft wird in der Regel ohne das Einverständnis des Kunden erteilt; er erfährt meist gar nicht, daß sein Kreditinstitut Auskünfte über ihn erteilt hat.

Diese Praxis ist nach meiner Auffassung mit der Regelung der §§ 3, 24 BDSG nicht vereinbar. Die Anwendbarkeit dieser Normen ergibt sich daraus, daß die in der Bankauskunft enthaltenen Daten i. d. R. Dateien entstammen.

In § 3 BDSG hat der Gesetzgeber die Datenverarbeitung unter ein generelles Verbot mit Erlaubnisvorbehalt gestellt. Erlaubt ist die Datenverarbeitung – dazu gehören auch Übermittlungen – nur dann, wenn entweder der Betroffene i. d. R. schriftlich eingewilligt hat (§ 3 Nr. 2 BDSG) oder das BDSG oder eine andere Rechtsvorschrift sie erlaubt (§ 3 Nr. 1 BDSG).

Eine ausdrückliche Einwilligung des Betroffenen liegt meist nicht vor. Sie kann auch nicht aus den allgemeinen Geschäftsbedingungen der Banken (§ 10 AGBB) oder Sparkassen (§ 7 AGBSp) abgeleitet werden. Diese Bedingungen besagen lediglich, daß die Bank (Sparkasse) dem Kunden nach bestem Wissen zu allen bankmäßigen Auskünften zur Verfügung steht. Daraus kann der Kunde jedoch nicht ersehen, daß das Kreditinstitut über ihn auch an andere Auskünfte erteilen will.

Der Bankvertrag kann auch nicht unter Berücksichtigung einer etwaigen Verkehrssitte gem. § 157 BGB dahingehend ergänzend ausgelegt werden, daß der Betroffene mit Abschluß des Bankvertrages – mutmaßlich – in die Erteilung von Bankauskünften einwilligt. Zum einen wird eine solche Verkehrssitte auch im bankfachlichen Schrifttum meist abgelehnt, zum anderen würde die Verkehrssitte sich am vorrangigen Grundsatz von Treu und Glauben messen lassen müssen. Der Regelungszweck der Datenschutzgesetze widerspricht aber einer Berücksichtigung der Verkehrssitte.

Kerngedanke der Datenschutzgesetzgebung ist es, die Datenverarbeitung für den Bürger transparent zu machen: Um dieses Ziel zu erreichen, ist es zumindest nötig, daß der Betroffene weiß oder sich denken kann, wer über ihn welche Daten verarbeitet. Diese Zielvorstellung des Gesetzgebers ist aber mit Zulassung einer mutmaßlichen Einwilligung nicht zu erreichen.Hier weiß der Betroffene ja gerade nichts von der Datenübermittlung. Die Einwilligung muß deshalb ausdrücklich erfolgen. Das Gesetz schreibt sogar die Schriftform vor, damit der Betroffene sorgfältig überlegen kann, ob er einwilligen will.Die Einwilligung kann das Kreditinstitut auch ohne weiteres einholen. Im Falle der Weigerung unterbleibt die Bankauskunft auch heute schon. Das Verbot mit Erlaubnisvorbehalt des § 3 BDSG kann nicht durch die Annahme einer Verkehrssitte dahin umgekehrt werden, daß die Übermittlung von Daten mit Vorbehaltsverbot erlaubt wird.Spätestens seit Inkrafttreten des BDSG widerspräche eine solche Verkehrssitte damit dem Grundsatz von Treu und Glauben und wäre deshalb nicht zu berücksichtigen. Dies gilt mangels Differenzierung durch das BDSG auch für den Handelsbrauch der Kaufleute.

Auch der Erlaubnistatbestand des § 24 Abs. 1 Satz 1, 1. Alternative BDSG liegt nicht vor. Die Erteilung einer Bankauskunft kann nicht als Erfüllung vertraglicher Pflichten aus dem Bankvertrag mit dem Betroffenen angesehen werden. Ebensowenig nimmt das Kreditin-

stitut mit der Bankauskunft seine Rechte aus dem Bankvertrag mit dem Betroffenen wahr. Die Beauskunftung eines Dritten steht mit dem Bankvertrag in keinem direkten Zusammenhang.

Auch die Annahme einer Verkehrssitte kann die Bankauskunft nicht zum Vertragszweck erheben. Durch sie würde die mutmaßliche Einwilligung des Betroffenen im Wege der ergänzenden Vertragsauslegung zum Vertragsinhalt gemacht. Wie oben ausgeführt, ist aber die mutmaßliche Einwilligung dem Datenschutzrecht wesensfremd.

Auch § 24 Abs. 1 Satz 1, 2. Alternative BDSG gibt dem Kreditinstitut in der Regel kein Recht zur Datenübermittlung im Rahmen der Bankauskunft.

Zwar ist ein berechtigtes Interesse des auskunfterteilenden Kreditinstituts oder der anfragenden Stelle meist zu bejahen, die Beeinträchtigung schutzwürdiger Belange des Betroffenen kann aber grundsätzlich nicht ausgeschlossen werden. Durch die Übermittlung von Daten ohne Einwilligung des Betroffenen entsteht für diesen ein Verlust an Kontrolle über seine Daten. Er kann nicht mehr nachvollziehen, wer alles über seine Daten verfügt. Da im Rahmen der Bankauskunft übermittelte Daten dem engeren Bereich der Persönlichkeitssphäre zuzuordnen sind, werden durch die Bankauskunft i. d. R. also schutzwürdige Belange des Betroffenen tangiert. Das ergibt sich außerdem aus dem Institut des Bankgeheimnisses, das gerade gewährleisten soll, daß das Verhältnis des Kunden zu seinem Kreditinstitut, dem er zwangsläufig seine wirtschaftlichen Verhältnisse offenlegen muß, unter besonderem Schutz steht.

Diese schutzwürdigen Belange des Betroffenen werden i. d. R. die berechtigten Interessen des Kreditinstituts und des Anfragenden an einer Auskunft ohne Einwilligung überwiegen.Lediglich in Einzelfällen ist denkbar, daß das berechtigte Interesse an der Übermittlung überwiegt, das gilt vor allem dann, wenn die Auskunft sich für den Betroffenen positiv auswirkt. Dabei ist allerdings zweifelhaft, inwieweit das Kreditinstitut das Verhältnis zwischen Betroffenem und Anfragendem einschätzen kann, um die sichere positive Wirkung der Auskunft prognostizieren zu können. Ohne daß der Kunde eine der Schufa-Klausel ähnliche Ermächtigungsklausel unterzeichnet hat und zuvor über deren Bedeutung aufgeklärt worden ist, halte ich die Erteilung einer Bankauskunft über ihn in der Regel also für unzulässig.

4.2.2 Girokontenführung auf Guthabenbasis

Einige Bürger haben sich bei mir darüber beschwert, daß die Kreditinstitute bei Eröffnung eines Girokontos in allen Fällen die Unterzeichnung der sog. Schufa-Klausel fordern. Bei Streichung dieser Klausel haben einige Kreditinstitute die Girokonteneröffnung abgelehnt, auch wenn der Kunde erklärt hat, daß er Überziehungskredite nicht in Anspruch nehmen wolle. Gegen diese Verfahrensweise habe ich Bedenken angemeldet.

Ich bin der Auffassung, daß die Unterrichtung der Schufa über die Eröffnung eines Girokontos, das nur auf Guthabenbasis geführt werden soll, gem. § 24 BDSG nicht zulässig ist, und daß in diesen Fällen das Verlangen, die Schufa-Klausel zu unterzeichnen, gegen § 9 AGBG sowie gegen § 242 BGB verstößt.

Eine Datenübermittlung an die Schufa setzt voraus, daß ein Geschäft mit kreditorischem Risiko abgeschlossen wird. Deshalb kann die Unterzeichnung der Schufa-Klausel dann nicht verlangt werden, wenn eine Kontoüberziehung durch besondere Vereinbarungen und Beschränkungen ausgeschlossen werden kann.

Ich habe den in Hamburg ansässigen Verbänden der Kreditwirtschaft empfohlen, zur Vermeidung von Überziehungen organisatorische Maßnahmen (tägliche Überwachung durch Überziehungslisten, Eingabe des EDV-Merkmals „keine Überziehung", keine Aushändigung von Euroschecks) zu veranlassen, die Eröffnung eines Girokontos, das nur auf Guthabenbasis geführt werden soll, zu ermöglichen. Ich sehe hierin eine Lösung, die

zugleich kreditorische Risiken ausschließt und dem erklärten Willen des Kunden und seinen darin zum Ausdruck gebrachten schutzwürdigen Belangen Rechnung trägt.

Bislang haben erst zwei von sechs Verbänden auf mein Schreiben vom 8.8.1983 geantwortet.

4.2.3 Ermittlung der Anschriften von Kindergeldempfängern für Werbezwecke

Von einer Gewerkschaft hatte ich erfahren, daß ein Kreditinstitut zur Unterstützung einer Marketing-Aktion die Adressen der Kunden, die Kindergeldzahlungen erhalten, zusammenstellen wollte.

Das Kindergeld wird von den Arbeitsämtern berechnet und mit entsprechendem Hinweis in der Rubrik „Verwendungszweck" an das Kreditinstitut des Empfängers weitergeleitet. Aus den von den Landeszentralbanken übersandten Gutschriftsbändern wollte das Kreditinstitut eine Datei mit Kontonummern der Kindergeldempfänger erstellen, um dann ein bestimmtes Werbeprogramm anzubieten. Der Verwendungszweck „Kindergeld" muß dem Kontoinhaber mitgeteilt werden, da er wissen muß, wofür die Überweisung bestimmt ist. Das Kreditinstitut des Empfängers erhält ein Exemplar des Überweisungsformulars ausschließlich zu dem Zweck, dem Kontoinhaber das Kindergeld gutzuschreiben. Die Angabe des Verwendungszweckes ist ausschließlich als Mitteilung für den Kontoinhaber gedacht.

Die beabsichtigte Marketing-Aktion hätte mithin gegen § 78 SGB X verstoßen, da diese Daten zu einem anderen Zweck als zur Information des Kontoinhabers genutzt worden wären.

Insbesondere aufgrund meiner frühzeitig in der Presse geäußerten Bedenken hat das betreffende Kreditinstitut die Auswertung der Kindergeldempfänger gestoppt und ihre EDV-Zentralen angewiesen, die zur Vorbereitung der Aktion bereits erstellten Selektionsbänder zu löschen.

4.3 Versicherungswirtschaft

4.3.1 Zentrale Dateien der Versicherungsverbände

Beim Abschluß einer privaten Versicherung sind der Versicherungsgesellschaft verschiedene Angaben mitzuteilen, die dem Unternehmen die Bearbeitung des Antrags – insbesondere das Abschätzen des zu übernehmenden Risikos – sowie die Durchführung des Versicherungsvertrages ermöglichen.Die Zustimmung zu einer entsprechenden Datenverarbeitung gibt der Versicherte durch Unterzeichnung der sog. Ermächtigungsklausel. Entsprechend einer Vereinbarung zwischen den Versicherungen, dem Bundesaufsichtsamt für das Versicherungswesen (BAV) und den Datenschutzaufsichtsbehörden der Länder hat diese Klausel folgenden Wortlaut:

> „Ich willige ein, daß der Versicherer im erforderlichen Umfang Daten, die sich aus den Antragsunterlagen oder der Vertragsdurchführung (Beiträge, Versicherungsfälle, Risiko-/Vertragsänderungen) ergeben, an Rückversicherer zur Beurteilung des Risikos sowie an den . . . . .verband und andere Versicherer zur Beurteilung des Risikos und der Ansprüche übermittelt.
> Ich willige ferner ein, daß die Versicherer der . . . . .gruppe, soweit dies der ordnungsgemäßen Durchführung meiner Versicherungsangelegenheiten dient, allgemeine Vertrags-, Abrechnungs- und Leistungsdaten in gemeinsamen Datensammlungen führen und an ihre Vertreter weitergeben. Gesundheitsdaten dürfen nur an Personen- und Rückversicherer übermittelt werden; an Vertreter dürfen sie nur weitergegeben werden, soweit es zur Vertragsgestaltung erforderlich ist."

Zwischen der Versicherungswirtschaft und den Aufsichtsbehörden ist streitig, welche Datenübermittlungen der Versicherungen an den jeweiligen Verband und welche Datenübermittlungen des Verbandes an die ihm angeschlossenen Mitgliedsunternehmen von dieser Ermächtigungsklausel gedeckt sind.

4.3.1.1 Zentrale Registrierstelle Rechtsschutz

Die Rechtsschutzversicherer und der HUK-Verband haben ein Auskunftssystem eingerichtet, das den Versicherern in der Hauptsache dazu dient, vor Annahme eines Versicherungsvertrages das einzugehende Risiko besser einschätzen zu können.

Gem. § 19 Abs. 2 der Allgemeinen Bedingungen über die Rechtsschutzversicherungen (ARB) ist einem Rechtsschutzversicherer die Kündigung eines Versicherungsvertrages möglich, wenn ein Versicherungsnehmer seine Versicherung häufiger in Anspruch nimmt und damit kein „normales Risiko" mehr darstellt.

Um beurteilen zu können, ob in einem Antragsfall von normalen Risikobedingungen ausgegangen werden kann, hat der Versicherer zunächst nur die Angaben des Antragstellers. Nach § 16 des Versicherungsvertragsgesetzes (VVG) hat dieser alles anzugeben, was der Risikobeurteilung dient; dazu zählt auch der Verlauf von Vorversicherungen. Das Problem liegt in der Vielzahl der Anträge, denen ein mögliches höheres Risikó (durch Nicht-Beantwortung der Frage nach dem Vorversicherer) nicht sofort zu entnehmen ist.

Da es häufig vorkommt, daß die erforderlichen Angaben nicht gemacht werden, sind die Rechtsschutzversicherer (z. Z. sind 25 Gesellschaften im HUK-Verband organisiert) dazu übergegangen, alle Kündigungen nach § 19 Abs. 2 ARB dem HUK-Verband zu melden. Dessen zentrale Registrierstelle Rechtsschutz hat z. Z. einen Bestand von ca. 15.000 – 20.000 Datensätzen, jährlich gibt es 2.500 – 3.000 Neuzugänge. Der HUK-Verband informiert alle anderen Rechtsschutzversicherer über die Kündigungen durch die regelmäßige Übersendung einer vollständigen Kopie der Datei. Auf diese Weise ist relativ leicht festzustellen, ob ein Antragsteller die Angaben über eine Vorversicherung „vergessen" hat.

Ich habe dem HUK-Verband mitgeteilt, daß ich gegen die Datenübermittlungen der einzelnen Versicherungsunternehmen an den Verband keine Bedenken habe. Die Datenübermittlungen vom Verband an alle Versicherer dieser Sparte im ganzen Bundesgebiet halte ich allerdings nicht für zulässig, weil weder eine wirksame Einwilligung des Betroffenen nach § 3 BDSG vorliegt noch die Voraussetzungen für eine Datenübermittlung nach § 32 Abs. 2 BDSG erfüllt sind.

M. E. liegt in der von den Rechtsschutzversicherern verwendeten Ermächtigungsklausel eine klare Begrenzung auf die Datenübermittlungen, die für eine konkrete Risikobeurteilung erforderlich sind. Mit der derzeitigen Ermächtigungsklausel wird mithin nicht die für die breite Streuung der Kündigungsdaten erforderliche Einwilligung erreicht, zumal dem Betroffenen praktisch keine Information über das bundesweite Meldeverfahren gegeben wird, so daß er nicht erkennen kann, welcher zusätzlichen Nutzung seiner Daten er zustimmt, wenn er seinen Versicherungsantrag unterschreibt.

M. E. läßt sich die Zulässigkeit der Übermittlungen auch nicht aus § 32 Abs. 2 BDSG herleiten.§ 32 Abs. 2 BDSG verlangt, daß der Empfänger sein berechtigtes Interesse glaubhaft darlegt. Ein berechtigtes Interesse kann vor allem gegeben sein, wenn die Kenntnis der Daten im Zusammenhang mit Rechtsverhältnissen erforderlich ist. Ein berechtigtes Interesse liegt allerdings nur dann vor, wenn die Kenntnis der Daten für die angegebenen Ziele oder Geschäftszwecke erforderlich ist. Erforderlich wird eine Datenübermittlung im Rahmen einer Risikoprüfung, wie sie von einem Rechtsschutzversicherer vorgenommen wird, allerdings erst dann, wenn in einem konkreten Einzelfall ein Versicherungsantrag vorliegt.Darüber hinaus ist auch im Rahmen des § 32 Abs. 2 BDSG in die Betrachtung mit einzubeziehen, ob die Beeinträchtigung schutzwürdiger Belange des Betroffenen die Übermittlung ausschließt.

In der Abwägung zwischen dem angestrebten Zweck (Risikobeurteilung), der Art und dem Umfang der übermittelten Daten (vollständige Datei) und dem Gebot der größtmöglichen Schonung des Betroffenen komme ich zu dem Ergebnis, daß die Datenübermittlung auf die Fälle zu beschränken ist, in denen ein Empfänger ein konkretes berechtigtes Interesse an der Kenntnis der Daten glaubhaft darlegt.

Das vom HUK-Verband praktizierte Verfahren – die Übermittlung von vollständigen Dateien an alle Versicherer der Sparte – ist unzulässig, weil

- die Empfänger – die einzelnen Rechtsschutzversicherer – ihr konkretes berechtigtes Interesse nicht darlegen,
- der HUK-Verband nicht in der Lage ist, die Zulässigkeitsvoraussetzungen im Einzelfall zu prüfen und
- die Gründe für das Vorliegen eines berechtigten Interesses und die Mittel für die glaubhafte Darlegung nicht aufgezeichnet werden können.

Ich habe dem HUK-Verband vorgeschlagen, auf ein Anfrageverfahren umzustellen, das auf die Erforderlichkeit im konkreten Einzelfall ausgerichtet ist. Denkbar wäre es auch, die Ermächtigungsklausel entsprechend den strengen Anforderungen der Rechtsprechung zu konkretisieren und so zu erweitern, daß die Voraussetzungen für eine wirksame Einwilligung erfüllt werden.

Der HUK-Verband hält meinen Vorschlägen insbesondere wirtschaftliche Erwägungen entgegen.

In Verhandlungen mit dem HUK-Verband versuche ich – wie auch mit den anderen Verbänden der Versicherungswirtschaft – ein praktikables Verfahren zu finden, das meinen rechtlichen Bedenken ebenso Rechnung trägt wie den wirtschaftlichen Argumenten der Versicherungswirtschaft. Die Gespräche werden Anfang nächsten Jahres fortgesetzt.

4.3.1.2 Sonderwagnisdatei der Lebensversicherer

In der beim Verband der Lebensversicherungsunternehmen e. V. eingerichteten Sonderwagnisstelle wird eine „Wagnisdatei" der Lebensversicherungsgesellschaften geführt. In dieser Datei sind die zur Identifikation einer Person erforderlichen Daten sowie ein Hinweis darauf gespeichert, daß beim Abschluß eines Lebensversicherungsvertrages ein überdurchschnittliches Risiko besteht. Nähere Angaben über die Art und die Qualität des Sonderwagnisses können diesem Datensatz nicht entnommen werden. Gesundheitsdaten werden in keinem Fall übermittelt.

Der Zweck der Datei besteht darin, den Versicherern die Möglichkeit zu verschaffen, die Angaben der Antragsteller zu überprüfen, die diese dem Versicherer zu machen haben (§ 16 VVG), damit diese die versicherten Risiken besser einschätzen und tariflich richtig einordnen können.

Die Auskunftserteilung geschieht in der Weise, daß einmal monatlich je ein Magnetband mit dem gesamten Bestand an alle Lebensversicherungsgesellschaften übermittelt wird. Die einzelnen Gesellschaften gleichen zunächst alle bestehenden eigenen Verträge mit dem übermittelten Magnetband ab, um zu prüfen, ob das jeweilige Risiko korrekt tarifiert ist. Darüber hinaus wird jeder eingehende Versicherungsantrag auf „vergessene Angaben" über Risiko und Vorversicherer überprüft, zu deren Mitteilung der neue Kunde nach § 16 VVG verpflichtet ist.

Die Lebensversicherungsunternehmen erreichen 5 Mio. Anträge p. a. Die Summe der Neuzugänge zur Wagnisdatei beträgt 150.000 p. a. Innerhalb von 5 Jahren werden also 750.000 Datensätze von jedem der ca. 70 Lebensversicherungsunternehmen gespeichert, die dem Verband angeschlossen sind.

Ich habe den Verband der Lebensversicherer darauf hingewiesen, daß ich die Übermittlung sämtlicher Datensätze aus der Wagnisdatei an alle Lebensversicherungsunterneh-

men des Verbandes datenschutzrechtlich für bedenklich halte. Zur Begründung verweise ich auf die Ausführungen zur Zentralen Registrierstelle Rechtsschutz (Nr. 4.3.1.1).

4.3.1.3 Meldeverfahren des Deutschen Transportversicherungsverbandes (DTV)

Der DTV betreibt einen Informationsaustausch, der den ihm angeschlossenen Reisegepäckversicherern hauptsächlich zur Überprüfung auffälliger Schadensereignisse dient. Nur ausnahmsweise wird auch zur Risikoprüfung vor Vertragsschluß beim Verband angefragt.

Die Reisegepäckversicherer melden in Form von „Vertraulichen Rundschreiben" dem Verband jeden auffälligen Schadensfall. Der Grund für die Auffälligkeit liegt darin, daß entweder gegen strafrechtliche Vorschriften oder zumindest gegen versicherungsvertragliche Obliegenheiten verstoßen wurde.Gewollt ist, daß zwei Reisegepäckversicherer ihre Informationen dann austauschen, wenn ähnliche Fallgestaltungen bekanntgeworden sind, um unredlichen Versicherungsnehmern die Leistung in einem konkreten Schadensfall verweigern bzw. sogar einen Strafantrag stellen zu können.

Die Meldung an den Verband hat allerdings nicht nur den Zweck, bei begründetem Betrugsverdacht zusätzliche Informationen zu erhalten, die bei einem anderen Versicherer vorhanden sein könnten. Sie bietet gleichzeitig allen anderen Versicherern die Möglichkeit, in ihrem eigenen Versicherungsbestand zu prüfen, ob für diesen Versicherungsnehmer bereits ein Schaden reguliert worden ist, der ggf. erst aufgrund der Anfrage als auffälliger Schaden oder gar als Betrug erkannt werden kann.
Der DTV kopiert die eingehenden Meldungen und verteilt sie an alle anderen Reisegepäckversicherer im Bundesgebiet. Die Originale bleiben zu Beweiszwecken beim Verband. Auskünfte aus dieser Datensammlung werden nur in wenigen Einzelfällen erteilt.

Nach Auffassung der Reisegepäckversicherer ist zur Beurteilung des Verfahrens nicht von einem Auskunftverfahren des Verbandes, sondern der Reisegepäckversicherer untereinander auszugehen. Dieser Informationsaustausch unter den Versicherern sei auf der Basis des § 24 Abs. 1 BDSG zu rechtfertigen. Diese Auffassung teile ich nicht.

Hinsichtlich der rechtlichen Würdigung verweise ich auf die Darstellung unter Nr. 4.3.1.1, die in den Grundzügen auch für das Datenübermittlungsverfahren der Reisegepäckversicherer gilt, wenngleich ich nicht verkenne, daß es Unterschiede zum Meldeverfahren der Rechtsschutzversicherer gibt, die eine differenziertere Beurteilung erfordern. Ich habe den DTV aber darauf hingewiesen, daß insbesondere die detaillierte Beschreibung des Schadensverlaufs mit Angabe von Datum, Uhrzeit, Ort, Gegenstand und Wert des Diebstahls (z. T. in Verbindung mit Flug-Nr., Reiseweg) bei der breiten Streuung an alle Reisegepäckversicherer per Rundschreiben die schutzwürdigen Belange des Betroffenen beeinträchtigen kann. Ich habe dem DTV empfohlen, das Anfrageverfahren an der Erforderlichkeit im konkreten Einzelfall auszurichten und die Datei mit stark eingeschränktem Datenkatalog als reine Hinweisdatei auszugestalten oder aber die Ermächtigungsklausel entsprechend zu konkretisieren und zu erweitern, wobei aber – auch bei einer Einwilligungslösung – die Übermittlung auf die Daten zu beschränken wäre, die zur Herstellung von Kontakten erforderlich sind, um eine Überprüfung von auffälligen Schadensmeldungen zu ermöglichen.

4.3.1.4 Malus-Datei des HUK-Verbandes für die Kfz-Haftpflicht-Versicherer

Der HUK-Verband steht für die Kfz-Haftpflicht-Sparte kurz vor der Einführung einer neuen zentralen Datei, die der Kontrolle der richtigen Tarifierung vor Vertragsabschluß dienen soll.

Bekanntlich richtet sich der Beitragssatz bei der Kfz-Haftpflicht-Versicherung nach der Dauer von Schadensfreiheiten. Autofahrer, die erstmalig einen Versicherungsvertrag abschließen, haben grundsätzlich einen Beitragssatz von 175% zu zahlen. Tritt bei einem

Anfänger ein Schadensfall ein, so gerät er entsprechend dem vom BAV genehmigten Tarif in eine Schadensklasse und muß einen höheren Beitrag leisten. Wer einen neuen Versicherungsvertrag abschließen will, legt im Normalfall eine „Versicherer-Wechsel-Bescheinigung" vor, um seinen Bonus zu erhalten. Fehlt eine solche Bescheinigung, so verlangt die vom Bundesministerium für Wirtschaft gegebene Tarifverordnung die Vorversicherer-Anfrage. In den Fällen, in denen ein Versicherungsvertrag gekündigt worden ist und der Neuabschluß eines Vertrages wegen schuldhaft verursachter Schäden die Eingliederung in eine der Malus-Klassen zur Folge hätte, sollen bestimmte Daten von Versicherungsnehmern beim HUK-Verband gespeichert werden. Für die Meldung sind die Daten vorgesehen, die ein Versicherungsnehmer auch in seinem Versicherungsvertrag zur Risikobewertung anzugeben hat:

1. Name und Anschrift
2. Stornodatum des Vertrages
3. Schadensfreiheits- bzw. Schadensklasse
4. Zahl der Schäden im Meldejahr
5. Kennzeichen des versicherten Kfz
6. Name des Versicherers
7. Versicherungs-Nr.

In der Vergangenheit haben Versicherungsnehmer in zunehmendem Maße versucht, die Einstufung ihres Versicherungsvertrages in eine Schadensklasse dadurch zu verhindern, daß sie den Versicherer wechselten und beim neuen Versicherer den schadensbehafteten Vorvertrag verschwiegen, um die für sie günstigere Eingangsstufe zu erreichen. Der HUK-Verband schätzt die Zahl derer, die in Malus-Klassen eingestuft werden müßten, auf rd. 500.000, während tatsächlich im Jahre 1980 nur ca. 156.000 Risiken hier eingestuft waren. Das BAV hat die Kfz-Versicherer und den HUK-Verband gedrängt, hier Abhilfe zu schaffen.

Um die Umgehung der Schadensklassen künftig verhindern zu können, will der HUK-Verband ab 1.1.1984 in seiner Verbandsgeschäftsstelle eine Malus-Datei einrichten. Anträge auf Abschluß eines Versicherungsvertrages, die keine Angaben über einen Vorversicherer enthalten, sollen zu einer Anfrage beim HUK-Verband führen. Das Meldeverfahren soll so ausgestaltet werden, daß die Unternehmen nur Daten über stornierte Verträge, die in eine Schadensklasse eingestuft sind oder aufgrund des Schadensverlaufs im Folgejahr in eine Schadensklasse eingestuft werden müssen, an die Verbandsgeschäftsstelle übermitteln (sog. „Meldepflichtige Verträge").

Der entscheidende Unterschied zu den anderen zentralen Dateien der Versicherungswirtschaft (vgl. Nr. 4.3.1.1 – 4.3.1.3 dieses TB) liegt darin, daß der HUK-Verband nicht vollständige Kopien des Gesamtbestandes dieser Datei an alle Kfz-Haftpflicht-Versicherer weitergibt; nur dann, wenn Anträge auf Abschluß eines Versicherungsvertrages keine Angaben über einen Vorversicherer enthalten, sollen auf Einzelanfrage aus der Malus-Datei Auskünfte gegeben werden. Es ist vorgesehen, bei der Anfrage den Namen und die Anschrift des Versicherungsnehmers, das Kennzeichen des versicherten Kfz, die Nr. des Versicherungsunternehmens und die Versicherungsschein-Nr. zu übermitteln. Die Anfragedaten werden in der Verbandsgeschäftsstelle – und nicht bei allen angeschlossenen Unternehmen – mit den Daten über die stornierten Verträge verglichen. Zeigt sich dabei, daß für das betreffende Kfz bzw. für den Versicherungsnehmer ein Vorversicherer vorhanden ist, wird das anfragende Unternehmen auf den Vorversicherer hingewiesen.

Ich habe weder gegen die Übermittlung an den HUK-Verband noch gegen die beabsichtigte Datenspeicherung beim HUK-Verband Bendenken, da m. E. kein Grund zur Annahme besteht, daß dadurch schutzwürdige Belange des betroffenen Versicherungsnehmers beeinträchtigt werden (§ 32 Abs. 1 BDSG).Einerseits sind unter dem Aspekt der Sensitivität und des Bedeutungsgehaltes lediglich diejenigen personenbezogenen Daten zur Speicherung vorgesehen, die ein Versicherungsnehmer auch in seinem Versicherungsvertrag zur Risikobewertung anzugeben hat, andererseits ist aus dem zukünfti-

gen Verwendungskontext – reine Hinweisdatei – keine Beeinträchtigung schutzwürdiger Belange ersichtlich. Wichtig ist auch, daß eine in Listen zusammengefaßte Weitergabe des Gesamtbestandes nicht vorgesehen ist.

Auch die Prüfung der Zulässigkeit der Datenübermittlungen vom Verband an die einzelnen Versicherungsunternehmen führt zu dem Ergebnis, daß das beschriebene Verfahren den Anforderungen des § 32 Abs. 2 BDSG genügt. Ein berechtigtes Interesse liegt vor, wenn die Kenntnis der Daten im Zusammenhang mit Rechtsverhältnissen erforderlich ist. Bei der Anbahnung geschäftlicher Beziehungen muß durch das beabsichtigte Verfahren gewährleistet sein, daß ein Versicherungsunternehmen sein berechtigtes Interesse an der Kenntnis des Vertragsverhältnisses Versicherungsnehmer/Vorversicherer, das regelmäßig im Abschluß eines neuen Versicherungsvertrages unter Verhinderung der Umgehung von Schadensklassen liegt, in der Einzelanfrage darlegt. Die Kenntnis der Daten aus der Hinweisdatei ist für den angegebenen Zweck – den dem tatsächlichen Risiko entsprechenden „tarifgerechten" Abschluß eines neuen Versicherungsvertrages – erforderlich, weil nur so das Ziel, den Versicherungsgesellschaften eine Überprüfung der nach § 16 VVG gemachten Angaben der Versicherungsnehmer zu ermöglichen, erreicht werden kann.

Im Hinblick auf die Relation von angestrebtem Zweck, der Verhinderung der Umgehung von Schadensklassen durch Verschweigen von Vorverträgen, und der Art der hierzu zu übermittelnden Daten (Hinweisdatei) halte ich die geplante Datenübermittlung unter Einbeziehung des Gebots der größtmöglichen Schonung des Betroffenen nach dem Maßstab der Interessenabwägung im Einzelfall datenschutzrechtlich für zulässig.

Ich habe den HUK-Verband jedoch darauf hingewiesen, daß der Empfänger verpflichtet ist, sein berechtigtes Interesse an der Kenntnis der Daten glaubhaft darzulegen. Nach § 32 Abs. 2 Satz 2 BDSG sind die Gründe für das Vorliegen eines berechtigten Interesses und die Mittel für ihre glaubhafte Darlegung aufzuzeichnen. Hierzu gehören alle Tatsachen, die von der übermittelnden Stelle bei der Prüfung des berechtigten Interesses zu berücksichtigen sind.

Für den vorliegenden Fall käme in Betracht, daß der Versicherungsantrag des Betroffenen, aus dem auch die Art des Vertrages entnommen werden kann, vorgelegt wird oder daß der HUK-Verband die Mittel für die glaubhafte Darlegung zur Prüfung des Vorliegens eines berechtigten Interesses auf andere Weise erhält und beim angeschlossenen Versicherungsunternehmen regelmäßig Stichproben nimmt. Da eine Rekonstruktion der Übermittlung und die Prüfung des berechtigten Interesses durch die Aufsichtsbehörde möglich sein muß, sind die dementsprechenden Aufzeichnungen aufzubewahren.

4.3.2 Herkunft von Werbeadressen

Eine Reihe von Eingaben bezieht sich auf die Zulässigkeit der Datenbeschaffung zu Werbezwecken durch Versicherungen. Versicherungen sammeln Adressen aus allen Lebensbereichen, um gezielt werben zu können. Als Quellen der personenbezogenen Daten potentieller Interessenten kommen in Betracht:
Empfehlungen sog. „stiller Mittler" (Personen, die der Versicherung Namen von Freunden, Bekannten und Kollegen angeben, aber zu Bedingung machen, bei den Beratungsgesprächen nicht genannt zu werden) oder Veröffentlichungen der Anschriften von Konfirmanden, Abiturienten, Studenten, Hochzeitspaaren etc.

Gegen die Inanspruchnahme der „stillen Mittler" ist datenschutzrechtlich genauso wenig einzuwenden wie gegen die Nutzung öffentlich zugänglicher Quellen.

Nicht zulässig ist hingegen, daß Personen, die im öffentlichen Dienst tätig sind, Daten, die ihnen dienstlich zugänglich geworden sind, für private Zwecke nutzen und an Versicherungsgesellschaften weitergeben. Ebenso wenig ist es zulässig, daß öffentliche Stellen, z. B. Standesämter oder Krankenhäuser, die für die Erfüllung ihrer Aufgaben ge-

speicherten Daten verkaufen, ohne daß die Einwilligung des Betroffenen vorliegt. Adreßmaterial, daß eine Versicherung auf diese Weise beschafft hat, darf sie auch nicht speichern.

Die Speicherung von Daten ist nämlich nur dann zulässig, wenn diese ordnungsgemäß erlangt sind. Es ist davon auszugehen, daß der Empfänger der Daten nur an einer ordnungsgemäßen Datenübermittlung ein berechtigtes Interesse haben dürfte. Auf jeden Fall wird jedoch eine Beeinträchtigung schutzwürdiger Belange des Betroffenen anzunehmen sein, wenn eine Datenübermittlung mit einem Verstoß gegen die §§ 5 oder 11 BDSG verbunden ist. Daten, deren Speicherung unzulässig ist, sind nach § 27 Abs. 3 Satz 2 BDSG zu löschen.

Der Aufsichtsbehörde muß es möglich sein, im Einzelfall zu prüfen, ob eine Versicherungsgesellschaft die personenbezogenen Daten potentieller Interessenten speichern durfte oder ob der Speicherung eine unzulässige Datenübermittlung oder Datenerhebung zugrunde lag. In der Praxis gibt es Schwierigkeiten, weil sich die Außendienstmitarbeiter häufig nicht mehr erinnern können, von wem sie ihr Adressenmaterial erhalten haben, in aller Regel die Herkunft der Adresse auch nicht dokumentiert wird.

Hierüber werden z. Z. Gespräche geführt.

4.3.3 Datenübermittlungen im Rahmen von fakultativen Gruppenversicherungsverträgen

Durch mehrere Eingaben bin ich darauf aufmerksam gemacht worden, daß eine Hamburger Versicherung sich im Rahmen fakultativer Gruppenversicherungsverträge von verschiedenen Verbänden und Vereinen personenbezogene Daten ihrer Mitglieder übermitteln läßt, ohne daß deren Einwilligung vorliegt.

Anders als bei sog. obligatorischen Gruppenversicherungsverträgen, bei denen der Versicherungsvertrag zwischen dem Versicherungsunternehmen und dem Arbeitgeber/Verein/Verband geschlossen wird und dieser als Versicherungsnehmer auch die Beiträge zu zahlen hat, stellt durch einen fakultativen Gruppenversicherungsvertrag ein Verband für seine Mitglieder (oder ein Unternehmen für seine Mitarbeiter) lediglich den rechtlichen Rahmen für Einzelverträge (in der Regel zu günstigeren Konditionen) zur Verfügung. Es bleibt dem Mitglied überlassen, ob es von der Möglichkeit, einen Einzelversicherungsvertrag abzuschließen, Gebrauch machen will; die Versicherungsbeiträge sind von ihm zu leisten. Damit die Versicherung bei den Mitgliedern des Verbandes für den Gruppenversicherungsvertrag werben kann, übermittelt der Verband der Versicherung regelmäßig personenbezogene Daten seiner Mitglieder.

Der „Düsseldorfer Kreis" hat sich bereits 1979 eingehend mit der Zulässigkeit solcher Datenübermittlungen beschäftigt und sich in seiner Sitzung am 28./29.11.1979 mit dem Vorschlag des BAV einverstanden erklärt, daß im Rahmen von fakultativen Gruppenversicherungsverträgen entweder der Arbeitgeber/Verein/Verband die Werbung für den Abschluß einer Versicherung selbst vornimmt oder daß er nur Daten der Mitglieder übermittelt, die sich schriftlich damit einverstanden erklärt haben.

Die Praxis sieht anders aus. Die neuen Arbeitnehmer/Vereins-/Verbandsmitglieder erfahren lediglich, daß sie dem fakultativen Gruppenversicherungsvertrag, der ihnen im Rahmen einer Sterbegeld-und Unfallvorsorge-Versicherung besondere Vergünstigungen bietet, beitreten können. Sie werden hingegen nicht darüber unterrichtet, daß der Versicherung ihre Namen, ihre Anschriften und z. T. Geburtsdaten für Werbezwecke zur Verfügung gestellt werden.

M. E. besteht keine Veranlassung, von dem Beschluß des „Düsseldorfer Kreises" abzuweichen. Die Datenübermittlung hält sich nicht im Rahmen der Zweckbestimmung des Arbeits- bzw. Mitgliedschaftsverhältnisses, denn die Weitergabe von Arbeitnehmer-/Mitgliederdaten dient nicht den durch den Arbeitsvertrag bzw. die Satzung vorgegebe-

benen Zielen. Auch kann – wie die Eingaben zeigen – nicht von vornherein ausgeschlossen werden, daß die schutzwürdigen Belange einzelner Gruppenmitglieder beeinträchtigt werden.

Ich habe mit der betreffenden Versicherung ein Gespräch vereinbart, in dem eine für beide Seiten befriedigende Lösung erzielt werden soll, die nicht unbedingt auf die Einwilligung der Umworbenen abstellen muß.

4.4 Auskunfteien

4.4.1 Handels- und Wirtschaftsauskunfteien

4.4.1.1 Regeln zur Umsetzung des Datenschutzes

Aufgrund der Gespräche, die die Aufsichtsbehörden mit dem Verband der Handels- und Wirtschaftsauskunfteien geführt haben (s. Nr. 7.1.1 meines 1. TB) haben die Spitzen der jeweiligen Organisationen Regeln zur Umsetzung des Datenschutzes zusammengestellt und den Aufsichtsbehörden zur Kenntnis gegeben.

Diese haben inzwischen
- das Datenschutzkompendium der Auskunftei Bürgel Centrale GmbH,
- die „Inspektionsanweisung betreffend Datenschutz" der Firma Schimmelpfeng GmbH und
- die „Grundsätze des Datenschutzes nach den Verhandlungen mit den Aufsichtsbehörden" des Verbandes der Vereine Creditreform e. V.

auf Vollständigkeit und inhaltliche Übereinstimmung mit den Ergebnissen der Gespräche überprüft. Einige Regelungen wiesen offensichtliche Abweichungen auf; und an anderen Stellen mußten Ungenauigkeiten oder auch das Fehlen von Hinweisen auf die Absprache festgestellt werden; hauptsächlich die beiden folgenden Punkte wurden beanstandet:

- Nachmeldungen

  Die Handels- und Wirtschaftsauskunfteien arbeiten für einen festen Kundenkreis, der ein grundsätzliches wirtschaftliches Interesse an Auskünften dargelegt haben muß. Die Auskünfte werden vor Abschluß eines Vertrages, der ein wirtschaftliches Risiko bedeutet, über die potentiellen Geschäftspartner abgefordert. In der Regel werden Auskünfte von Firmen und Geschäftsleuten über andere Firmen oder im Wirtschaftsleben stehende Personen erbeten. Auch über Privatpersonen wird angefragt, am häufigsten im Zusammenhang mit der Gewährung einer Hypothek oder dem Eröffnen eines Dauerkontos beim Versandhandel. Der Anteil der über Privatpersonen erteilten Auskünfte liegt weit unter einem Drittel.

  Werden der Auskunftei nach Erteilung einer Wirtschaftsauskunft Tatsachen bekannt, die für den Anfragenden von Bedeutung sind, so werden diese Informationen innerhalb eines bestimmten Zeitraumes nachgemeldet – bei einer Auskunftei innerhalb eines halben, bei einer anderen innerhalb eines Jahres.

  Der Nachtrag von positiven Aussagen ist unproblematisch.Werden jedoch Negativdaten nachgereicht, so ist nach Ansicht der Aufsichtsbehörden jedesmal erneut zu prüfen, ob das ursprünglich angegebene berechtigte Interesse im Zeitpunkt des Nachtrags noch besteht oder ob durch die Übermittlung nunmehr schutzwürdige Belange des Betroffenen beeinträchtigt werden.

- Berechtigtes Interesse

  Übereinstimmend stellten Aufsichtsbehörden und Auskunfteien fest, daß die Vermeidung wirtschaftlicher Nachteile ein berechtigtes Interesse im datenschutzrechtlichen

Sinne darstellt. Die Aufsichtsbehörden meinten jedoch, daß nicht jede erbetene Auskunft erteilt werden dürfe. Beschränkungen ergeben sich sowohl aus dem Geschäftszweck der Auskunfteien als auch aus der Art der gespeicherten Daten. Sie wiesen z. B. darauf hin, daß nicht jede Personaleinstellung von wirtschaftlicher Bedeutung sei und deshalb mit Rücksicht auf die spezielle Verwendung des Bewerbers in jedem Einzelfall das berechtigte Interesse glaubhaft dargelegt werden müsse.

Auf dem Antragsformular gibt der Kunde der Auskunftei an, worauf sein Interesse an der Wirtschaftsauskunft sich gründet. Ihm sind zur Erleichterung verschiedene Begründungsmöglichkeiten mit Kennziffer vorgedruckt, die er durch Ankreuzen kenntlich machen kann. Zusätzlich ist Raum für die Angabe von sonstigen Gründen, die der Anfragende mit frei gewählten Worten beschreiben soll.

Das Original dieses Anfragescheins wird hauptsächlich zu Abrechnungszwecken verwendet und deshalb nicht im regionalen Auskunftsarchiv verwahrt, sondern der jeweiligen Zentrale zugeleitet. Die Kennziffern der Begründung für das berechtigte Interesse werden auf die Durchschrift der erteilten Auskunft übertragen, nicht aber die sonstigen Gründe. Die Aufsichtsbehörden können deshalb nur eine beschränkte Prüfung vornehmen. Die Auskunfteien wollen prüfen, ob und wie sich die Dokumentation des berechtigten Interesses verbessern läßt.

4.4.1.2 Eingaben

Die mir im Zusammenhang mit Handels- und Wirtschaftsauskunfteien zugegangenen Eingaben bezogen sich durchweg auf die im 1. TB geschilderten grundsätzlichen Probleme. Oft werde ich auch gebeten, das berechtigte Interesse dessen zu prüfen, der eine Auskunft abgefordert hat, weil sich der Betroffene niemanden in seinem perönlichen Umfeld vorstellen kann, der über ihn eine Auskunft eingeholt haben könnte. Ich bin allerdings nicht ohne weiteres in der Lage, den Empfänger der Auskunft zu nennen.

Die Auskunfteien wollen dem Betroffenen die Auskunftsempfänger nicht nennen, weil dies ihre Beziehungen zu ihren Geschäftspartnern erheblich beeinträchtigen könnte. Sie sind darüber hinaus der Meinung, zu solchen Angaben nicht verpflichtet zu sein, und stützen sich dabei auf ein BGH-Urteil vom 19.5.1981 (NJW 1981, 1738), in dem der BGH den Anspruch auf Auskunft über die Quelle einer Information verneint hatte.

Die Aufsichtsbehörden der Länder haben sich darauf verständigt, dem Betroffenen den Auskunftsempfänger nicht zu nennen, es sei denn, es läßt sich positiv feststellen, daß gegen Bestimmungen des BDSG verstoßen wurde, und der Betroffene benötigt diese Kenntnis, um eigene Rechtsansprüche durchsetzen zu können.

In einem Fall hatte ich den dringenden Verdacht, daß ein berechtigtes Interesse an einer Wirtschaftsauskunft nicht vorlag, daß es sich vielmehr um eine fingierte Anfrage handelte. Deshalb habe ich die Auskunftei gebeten, entsprechend ihren Geschäftsbedingungen das Vorliegen des berechtigten Interesses nachzuprüfen. Leider war mit der Antwort des Auskunftsempfängers nichts anzufangen: Er habe keine Unterlagen mehr und zu der angefragten Person bestünden keine Geschäftsbeziehungen. Bei dieser Sachlage habe ich dem Betroffenen den Auskunftsempfänger genannt, um ihm die Möglichkeit zu geben, einen Strafantrag wegen Verstoßes gegen § 41 Abs. 1 Nr. 1 oder Nr. 2 BDSG zu stellen.

4.4.1.3 Prüfungen

Im Berichtszeitraum habe ich eine große Handels- und Wirtschaftsauskunftei überprüft und dabei – über die bereits angesprochenen Problemfelder hinaus – folgende Sachverhalte festgestellt:

- Über Privatpersonen liegt nur in seltenen Fällen Archivmaterial vor. Daher befragt die Auskunftei die Privatpersonen selbst, indem sie ihnen ihren Fragebogen zusendet, wenn nicht der Empfänger eine derartige Selbstbefragung ausgeschlossen hat. Wenn die auf diese Weise gewonnenen Angaben nicht ausreichen oder wenn die Fragebögen nicht beantwortet werden, recherchiert die Auskunftei weiter und versucht, durch Befragen von Nachbarn weitere Informationen zu erhalten. Ich habe festgestellt, daß die überprüfte Auskunftei sich nicht immer an die mit dem „Düsseldorfer Kreis" abgesprochenen Fragestellungen hält. Sie fragt mitunter auch nach Ehegatten und Kindern. Fragen nach den persönlichen Lebensverhältnissen sind aber nicht von der Vereinbarung zwischen dem „Düsseldorfer Kreis" und den Vertretern der Handels- und Wirtschaftsauskunfteien umfaßt. Eine persönliche Beurteilung wird allerdings nicht mehr abgefragt.

- Wenn über den Betroffenen vom Rechercheur eine Auskunft gefertigt ist, wird sie nicht sofort an die anfragende Stelle übermittelt, sondern es erfolgt noch eine Endkontrolle durch einen erfahrenen Innendienst-Mitarbeiter. Hierbei wird der Inhalt der Recherche ebenso wie das vom anfragenden Unternehmen nachzuweisende berechtigte Interesse nochmals überprüft.

- Bereits in meinem 1. TB (Nr. 7.1.1.1, S. 51) hatte ich darauf hingewiesen, daß die Auskunfteien gegen § 915 ZPO verstoßen, da sie die für die regelmäßig aus den öffentlichen Schuldnerregistern übernommenen Informationen vorgeschriebenen Löschungsfristen nicht einhalten. Ich hatte ein systematisches Löschen dieser Daten gefordert. Auch wenn die Unterlagen nicht jeweils am Jahresende vernichtet werden, so ist bei der überprüften Auskunftei inzwischen doch eine kleine Gruppe von Mitarbeitern damit beschäftigt, das Archiv systematisch „auszudünnen". Bei der derzeitigen Vorgehensweise wird für eine Durchsicht des gesamten Archivbestandes allerdings ein Zeitraum von 2 1/2 bis 3 Jahren angesetzt. Darüber hinaus entfernt der einzelne Sachbearbeiter bei jedem Zugriff auf eine Archiv-Tasche die – nach Jahrgängen farblich gekennzeichneten – Karteikarten mit Angaben aus dem Schuldnerregister, die älter als 3 Jahre sind.

- Bei der Beurteilung der Datenspeicherung ist mir aufgefallen, daß im Rechercheboger, der die Grundlage für die spätere Auskunft darstellt, die Datenquelle – insbesondere bei Nachbarschaftsbefragungen – z. T. nicht dokumentiert wird. Damit bin ich, wenn ich einen Beschwerdefall zu beurteilen habe, mangels Quellennachweis häufig nicht in der Lage, die Zulässigkeit der Speicherung zu prüfen. Eine Spezifizierung der Quelle halte ich für dringend geboten, da bei unzulässiger Beschaffung von Informationen die anschließende Speicherung ebenfalls unzulässig wäre.

- Die überprüfte Auskunftei erteilt auch telefonisch Auskünfte über den Betroffenen. Hierbei werden Kurzauskünfte über die Rechtsform, Negativinformationen, Bankverbindung, Bestätigung der Identität und das Datum der letzten Recherche erteilt. Welche Einzeldaten im Einzelfall übermittelt wurden, ist allerdings nicht rekonstruierbar. Dies hat zur Folge, daß ich nicht prüfen kann, ob der Empfänger im Rahmen von telefonischen Anfragen sein berechtigtes Interesse glaubhaft dargelegt hat. Ich halte es daher für erforderlich, daß entweder der Inhalt der Datenübermittlung dokumentiert wird oder daß die Empfänger veranlaßt werden, im Nachhinein Nachweise vorzulegen, aus denen die für die Anfrage relevanten wirtschaftlichen Vorgänge erkennbar sind.

- Zwischen Vertretern der Handels- und Wirtschaftsauskunfteien und Vertretern der Aufsichtsbehörden der Länder ist 1981 vereinbart worden, daß die Auskunfteien bei einem Teil der Empfänger das berechtigte Interesse später noch einmal stichprobenartig überprüfen. Dieser Beschluß ist bei der überprüften Auskunftei noch im Jahre 1981 umgesetzt worden. Die Häufigkeit der Stichproben liegt über dem vereinbarten Satz von 1 ‰. Inhaltlich gingen die vom Empfänger erbetenen

Angaben z. T. allerdings nicht über die Bezeichnung des berechtigten Interesses im Anfrageschein hinaus. Auch hier sollte die Auskunftei darauf hinwirken, daß der Empfänger sein berechtigtes Interesse für Stichproben detailliert begründet, wenn sie Stichproben durchführt.

4.4.2 Auskunftsstelle über den Versicherungsaußendienst e. V. Hamburg (AVAD)

Viele Eingaben bezogen sich auf die Tätigkeit der AVAD. Die AVAD ist eine Institution, die von Verbänden der Versicherungswirtschaft und der Bausparkassen mit dem Ziel eingerichtet wurde, die Auflage des Bundesaufsichtsamtes für das Versicherungswesen (BAV) zu erfüllen, nur vertrauenswürdige Personen zum Außendienst zuzulassen. Über alle ausgeschiedenen Außendienstmitarbeiter werden von den jeweiligen Gesellschaften formularmäßige Auskünfte gefertigt, an die AVAD gesandt und bei späteren Bewerbungen auf Anfrage an andere Unternehmen der Versicherungsbranche im gesamten Bundesgebiet weitergegeben. Diese Auskünfte enthalten außer den Personalien Angaben über Dauer und Art der Beschäftigung, Kündigungsgrund, Beanstandungen bei der Werbung, beim Inkasso oder Abrechnungsverkehr, zivil- und strafrechtliche Tatbestände und ähnliches.
Im Rahmen des AVAD-Auskunftsverfahrens haben 1983 200000 Datenübermittlungen stattgefunden. Die AVAD hat 764 Auskunftsgesuche von Außendienstmitarbeitern gem. § 34 Abs. 2 BDSG beantwortet.
Die personenbezogenen Daten werden bei der AVAD in einer Datei geführt. Denn hinsichtlich der Bedeutung für den Benutzer, der Funktion und des Informationsgehaltes liegt der Schwerpunkt bei den formatisierten Unterlagen, mit denen auch in der Hauptsache gearbeitet wird. Die Akten enthalten im übrigen – als Hintergrundmaterial wie auch zu Beweiszwecken – lediglich die Informationen, die zur Erstellung der formatisierten Unterlagen benutzt werden. Da inzwischen mehrere Gerichtsurteile von der Anwendung des BDSG ausgegangen sind und die AVAD sich auch bemüht, den Bestimmungen des BDSG Rechnung zu tragen, habe ich kein Verständnis dafür, daß die AVAD Dritten gegenüber weiterhin ihren überkommenen Rechtsstandpunkt aufrechterhält, sie falle nicht unter die Vorschriften des BDSG.

Schon vor Jahren hat die AVAD ihre frühere Praxis aufgegeben, Listen „schwarzer Schafe" in Form eines sog. „B-Rundschreibens" an die Versicherungen und Bausparkassen zu versenden. Die Streuung eines derartigen „Schwarzbuches" von Außendienstmitarbeitern im gesamten Bundesgebiet hatte bereits die damalige Aufsichtsbehörde für unzulässig erklärt.

Bereits in meinem 1. TB (vgl. Nr. 7.1.2, S. 52) habe ich über die Tätigkeit der AVAD berichtet und erklärt, daß mich die Rechtssprechung einiger Arbeitsgerichte veranlaßt hat zu überprüfen, ob das Speichern auf der Grundlage des § 32 BDSG ohne Einwilligung des Betroffenen zulässig ist.

Ich bin nicht der Meinung, daß eine reine Einwilligungslösung zu sachgerechten Ergebnissen führt. Einerseits könnte die Einwilligung von Mitarbeitern durch unangemessenen Druck bei Vertragsabschluß herbeigeführt werden (vgl. auch Nr. 4.5.1 dieses TB). Andererseits könnte die AVAD ihre Tätigkeit nicht mehr sinnvoll weiterführen, weil sie über diejenigen, die nicht einwilligen, keine Auskünfte erhielte und mithin nicht mehr alle Außendienstmitarbeiter erfaßt hätte. Die AVAD könnte also – mangels Einwilligung – die ihr angeschlossenen Unternehmen gerade vor solchen Personen nicht warnen, deren Vertrauenswürdigkeit Zweifeln begegnet.

Ich habe der AVAD daher folgende Lösung der bestehenden datenschutzrechtlichen Probleme vorgeschlagen:

Um das Auskunftsverfahren von Anfang an transparent zu gestalten und unnötige Nachfragen bzw. Beschwerden zu vermeiden, wird jeder Bewerber für den Außendienst, der bisher nicht in der Versicherungs- oder Bausparbranche tätig gewesen ist, erstmals

durch den Personalfragebogen auf die Existenz der AVAD hingewiesen. Er wird darüber unterrichtet, daß über alle ausgeschiedenen Außendienstmitarbeiter formularmäßige Auskünfte gefertigt, an die AVAD gesandt und bei späteren Bewerbungen auf Anfrage an Unternehmen der Versicherungs-/Bausparbranche im gesamten Bundesgebiet weitergegeben werden. Er wird belehrt, daß er der Übersendung des Auskunftsfragebogens widersprechen kann. Damit kann er erreichen, daß die Gesellschaft in der Regel nur die Identifizierungsmerkmale, Tätigkeitsnachweise und Daten zur Form der Vertragsbeendigung an die AVAD übermitteln wird. Für den Fall aber, daß erhebliche Bedenken an der Vertrauenswürdigkeit des Mitarbeiters bestehen, darf ausnahmsweise auch ein Hinweis hierauf übermittelt werden.

Der aus einem Unternehmen ausscheidende Mitarbeiter erhält zeitgleich mit der Übermittlung an die AVAD eine Durchschrift des ausgefüllten Auskunftsfragebogens. Er wird darauf hingewiesen, daß er, da die AVAD den Vorschriften des BDSG unterliegt, die Möglichkeit hat, unrichtige Daten berichtigen und streitige sperren zu lassen, und daß er sich, wenn er einen solchen Anspruch geltend machen will, auch unmittelbar an die AVAD wenden kann. Der AVAD habe ich empfohlen, aus Gründen der Praktikabilität den Auskunftsfragebogen nicht unverzüglich, sondern mit einer Verzögerung von ca. 3 Tagen nach seinem Eingang an ein anfragendes Unternehmen weiterzugeben.

Einen Tag vor Redaktionsschluß erreichte mich eine Nachricht der AVAD. Sie habe meine Vorschläge in ihren Gremien diskutiert und sei zu dem Ergebnis gelangt, daß sie durch eine Widerspruchslösung nachhaltig in ihrer Arbeit behindert würde. Ein wirkungsvoller Schutz der Versicherungsunternehmen und der Verbraucher erscheine ihr nicht mehr hinreichend gewährleistet, sie könne meine Vorschläge deshalb nicht akzeptieren.

Meinen datenschutzrechtlichen Bedenken scheint die AVAD nur wenig Beachtung geschenkt zu haben. Auf meine Empfehlung, ihr Auskunftsverfahren transparenter zu gestalten, ist sie überhaupt nicht eingegangen. Deshalb wiederhole ich: Nur wenn die Datenflüsse zwischen der AVAD und den Versicherungsunternehmen den Betroffenen offengelegt und diese in die Lage versetzt werden, eine mögliche Beeinträchtigung ihrer schutzwürdigen Belange geltend zu machen, kann die Tätigkeit der AVAD unter datenschutzrechtlichen Aspekten akzeptiert werden.
Das derzeit praktizierte Meldeverfahren wird diesen Anforderungen nicht gerecht.
Das Schreiben der AVAD schließt mit einem Gesprächsangebot, auf das ich selbstverständlich eingehen werde. Ich hoffe, daß es in den weiteren Verhandlungen doch noch gelingen wird, eine datenschutzgerechte, aber auch praktikable Lösung zu finden.

4.4.3 Schufa

Die Beschwerden und Fragen, deren Gegenstand die Tätigkeit der Schufa war, betrafen bis auf wenige Ausnahmen Probleme, mit denen sich die Aufsichtsbehörden schon in den vergangenen Jahren befaßt hatten und die zum großen Teil auch von der „Arbeitsgruppe Schufa" des „Düsseldorfer Kreises" mit Vertretern der Bundes-Schufa und regionalen Schufa-Gesellschaften erörtert worden sind.

4.4.3.1 Interner Datenverkehr zwischen den Schufa-Gesellschaften

Folgendes neues Problem ist an mich herangetragen worden: Alle Schufa-Gesellschaften verstehen sich – obwohl es sich um 13 eigenständige juristische Personen handelt – praktisch als Einheit. Das kommt u. a. im Schufa-Anschluß-Vertrag zum Ausdruck:

„Sofern der Vertragspartner am überörtlichen Auskunfts-, Beobachtungs- und Meldeverfahren teilnimmt, gelten diese Vertragsbedingungen auch im Verhältnis zu der jeweiligen Schufa-GmbH. Insoweit handelt die vertragschließende Schufa in Vollmacht aller anderen Schufa-Gesellschaften."

In einem Einzelfall beklagte sich ein Petent aus Nordrhein-Westfalen darüber, daß eine Erledigungsmeldung zu einem gespeicherten Negativmerkmal nicht rechtzeitig bei der für seinen Wohnort tätigen Schufa gespeichert worden ist. Diesem Fall lag ein Vertrag zwischen einer hamburgischen Hypothekenbank und dem Betroffenen zugrunde, den die Hypothekenbank nach unregelmäßigen Zahlungen gekündigt hatte.

Die Hypothekenbank hatte einen Schufa-Anschlußvertrag und meldete pflichtgemäß diese Vertragskündigung, die ein Negativmerkmal darstellt. Nachdem sich jedoch der Kunde und die Hypothekenbank verglichen hatten, wurde die Vertragskündigung aufgehoben.
Diese Information verarbeitete die Schufa in Nordrhein-Westfalen jedoch erst etwa 6 Wochen später. In der Zwischenzeit konnte sie kein korrektes Bild über den Betroffenen vermitteln.
Der Petent fühlte sich beschwert, weil zunächst wegen „schlechter Auskunft" eine günstige Geschäftsverbindung nicht zustande gekommen war. Später wurde ein ihm ausgehändigter Scheck für einen bereits vereinbarten Vorschuß gesperrt. Im Glauben, sein Konto führe ein ausreichendes Guthaben, stellte er selbst mehrere Schecks aus. Weil die Gutschrift ausgeblieben war, wurden diese Schecks nicht eingelöst; und schließlich kündigte das Kreditinstitut sein Konto.
Als sich auf diese Weise zahlreiche zusätzliche Negativ-Daten bei der Schufa angesammelt hatten, wurde dem Betroffenen auch die Ursache bekannt.

Die Hypothekenbank behauptete, die Erledigungs-Meldung entsprechend den Vereinbarungen unverzüglich an die Schufa Hamburg abgeschickt zu haben. Ich konnte indes nicht feststellen, wann oder ob diese überhaupt eingegangen war und wann und ggf. wohin sie weitergeleitet wurde. Die Schufa sendet die Meldungen, die nicht für den eigenen Geschäftsstellenbereich bestimmt sind, i. d. R. im Original noch am Tage des Eingangs an die regional zuständige Geschäftsstelle weiter. Da keine Durchschreibesätze verwendet und keine Aufzeichnungen geführt werden, ist nicht nachvollziehbar, wer in diesem Fall nicht korrekt gehandelt hatte.

Darin, daß die interne Weitergabe von einer Schufa-Gesellschaft an eine andere nicht nachvollziehbar ist, sehe ich einen schweren Organisationsmangel. Eine Änderung des Verfahrens scheint mir dringend erforderlich, auch wenn die Schufa den zusätzlichen Aufwand für nicht vertretbar hält.

Dem Betroffenen, der mich zur Durchsetzung etwaiger Schadensersatzansprüche um Hilfe gebeten hatte, konnte ich lediglich mitteilen, daß ich seinen Fall in die Verhandlungen mit der Schufa einbringen werde, um für die Zukunft eine bessere Regelung zu erreichen. Im übrigen mußte ich ihn auf die Beweisschwierigkeiten hinweisen, die sich in einem Rechtsstreit für ihn ergeben würden.

4.4.3.2 Identitätsprüfung bei fehlendem Geburtsdatum

Nach Meinung der Aufsichtsbehörden ist ein Speichern nur zulässig, wenn die Identität des Betroffenen zweifelsfrei festzustellen ist. Deshalb muß immer das Geburtsdatum als Identifikationsmerkmal mitgeliefert werden.

Nach Darstellung der Schufa wird jetzt schon so verfahren. So würden häufig Meldungen von B-Vertragsfirmen zurückgewiesen, die kein Geburtsdatum enthielten. Problematisch blieben nur die Angaben aus dem Schuldnerregister (HB = Haftbefehl zur Erzwingung der Eidesstattlichen Versicherung, EV = Leistung der Eidesstattlichen Versicherung), bei denen das Geburtsdatum fehlt. Sie werden bei der Schufa in einer gesonderten Datei gespeichert. Bei einer Übermittlung dieser Daten wird ein deutlicher warnender Hinweis auf die unsichere Identifizierung und die Notwendigkeit einer Prüfung durch den Empfänger hinzugefügt.

Darüber hinaus haben die Aufsichtsbehörden zur Absicherung der korrekten Zuordnung von Informationen ohne Geburtsdatum folgende Vorschläge gemacht:

- Telefonisch erteilte Auskünfte sollten von allen Schufa-Gesellschaften regelmäßig schriftlich wiederholt werden, um Verwechslungen zu vermeiden. Dies ist bei der Schufa Mannheim schon üblich und bedeutet zugleich eine zusätzliche Hemmschwelle gegen unbefugte Abrufe.

- Bei Meldungen der Schufa, die die empfangende Anschlußfirma keiner Person zuordnen kann, hat sie bisher nur das in der Technischen Anleitung festgeschriebene Nutzungsverbot zu beachten. Darüber hinaus sollte eine Pflicht zur Löschung begründet werden.

- Jede Anschlußfirma, die eine Meldung ohne Geburtsdatum empfangen hat, muß zurückmelden, ob und wie sie die Zuordnung vorgenommen hat.

Über diese Lösungsansätze wollen die Schufa-Vertreter nachdenken und die Durchsetzbarkeit bei den Anschlußfirmen prüfen.

4.4.3.3 Aussagekraft von Negativdaten

Oft werde ich auch gefragt, wie groß der Kreis derer ist, die am Schufa-Verfahren teilnehmen, und in welchem Umfang Daten ausgetauscht werden. Die wesentlichen Nutzer der Schufa sind die Kreditinstitute, die einen sog. A-Vertrag geschlossen haben. Daneben sind aber auch Unternehmen anderer Wirtschaftszweige angeschlossen, vor allem Versand- und Kaufhäuser; sie haben den sog. B-Vertrag geschlossen, der lediglich zu einer Auskunft über negatives Verhalten im Zusammenhang mit Krediten oder anderweitigen Verpflichtungen (sog. „Negativmerkmale") berechtigt. Diese Merkmale können aus dem Schuldnerregister stammen oder der Schufa durch eine andere Anschlußfirma als vertragswidriges Verhalten gemeldet werden.

Die A-Vertragspartner lassen ihre Kunden die sog. Schufa-Klausel unterschreiben, die von den Aufsichtsbehörden als Einwilligung in die Datenverarbeitung angesehen wird. Die B-Vertragsfirmen verwenden eine solche Klausel nicht. Sie können den Informationsaustausch mit der Schufa also nicht auf die Einwilligung des Betroffenen stützen. Die Aufsichtsbehörden haben Zweifel, ob die Übermittlung einiger Negativmerkmale, die über die Kreditwürdigkeit praktisch nichts aussagen, noch mit den schutzwürdigen Belangen des Betroffenen vereinbar ist.

In diese Richtung geht auch ein Urteil des OLG Celle vom 14.11.1979 (3 U 92/79), das die ohne Einwilligung des Betroffenen erfolgte Übermittlung personenbezogener Daten an die Schufa dann nicht für gerechtfertigt hält, wenn es sich um solche „Negativmerkmale" handelt, die keinen sicheren Schluß auf die Zahlungsfähigkeit oder Zahlungswilligkeit des Betroffenen zulassen.

Diese Entscheidung, die die Übermittlung des Negativmerkmals „LZ" (Inanspruchnahme einer Lohnabtretung) betraf, wird von zwei jüngeren Urteilen des OLG Hamm (3 U 300/81 vom 8.3.1982 und 11 U 200/82 vom 25.3.1983) gestützt, nach dessen Auffassung der Erlaß eines Mahnbescheides (Negativmerkmal „MB") nichts über die Berechtigung der geltend gemachten Forderung und über einen etwaigen Verzug des Schuldners besagt. Bei der Speicherung des Mahnbescheides werde besonders deutlich, daß diese Angabe praktisch keine Aussagekraft über die Bonität des Betroffenen habe. Mahnbescheide würden ohne jede Schlüssigkeitsprüfung allein auf die Behauptung des „Gläubigers" erlassen. Die Aussagekraft der bloßen Mitteilung des Erlasses eines Mahnbescheides erschöpfe sich darin, daß sich jemand einer Forderung gegen den Betroffenen berühme. Demgegenüber sieht das OLG München (Urteil vom 13.10.1981, 5 U 2200/81) die schutzwürdigen Belange des Betroffenen nicht einmal dadurch verletzt, daß erledigte Negativmerkmale (z. B. durch Forderungsausgleich) bis zum Ablauf der bei der Schufa üblichen Aufbewahrungsfrist von 3 Jahren gespeichert bleiben.

Ich teile die Bedenken des OLG Celle und des OLG Hamm und meine, daß jedenfalls dann schutzwürdige Belange des Betroffenen beeinträchtigt sein können, wenn Negativ-Merkmale wie z. B. LZ oder MB nur vereinzelt oder einmalig auftreten.

Es bietet sich an, den Umfang der auszutauschenden Negativdaten einzuschränken oder die Einwilligung des Betroffenen auch für den Auskunftsverkehr mit B-Anschlußfirmen herbeizuführen. Hierüber muß weiter mit der Schufa verhandelt werden.

Über weitere Schufa-Probleme habe ich berichtet unter

Nr. 4.1.2 (Erstbestellschein im Versandhandel)
Nr. 4.5.2.2 (Auskünfte an Wohnungsvermieter)
Nr. 4.9.1 (Kontakte zwischen Schufa und Polizei)

4.5 Datenschutz auf dem Wohnungsmarkt

Aufgrund weiterer Eingaben und Anfragen der Presse sowie aus der Bürgerschaft war ich auch in diesem Jahr mit den datenschutzrechtlichen Problemen befaßt, die mit der Vermietung von Wohnungen zusammenhängen (vgl. 1. TB Nr. 7.4., S. 57). Die Fragen und Beschwerden bezogen sich in erster Linie auf Fragebögen zur Wohnungsvermietung und auf die Zusammenarbeit von Vermietern mit Auskunfteien.

4.5.1 Fragebögen zur Wohnungsbewerbung

Wer sich um eine Wohnung bewirbt, hat in der Regel auf Wunsch des Vermieters – insbesondere wenn es sich um eine der großen Wohnungsbaugesellschaften handelt – einen Fragebogen auszufüllen. Viele Vermieter verlangen nicht nur detaillierte Auskünfte über die persönlichen Verhältnisse des Mietinteressenten, sondern darüber hinaus eine Erklärung, mit der er in die Einholung von Auskünften bei früheren Vermietern, Arbeitgebern, Auskunfteien bzw. Banken einwilligt.

In den meisten Fällen beziehen sich die einzelnen Fragen sowohl auf Angaben zur gesuchten Wohnung als auch auf die Einkommens- und Vermögensverhältnisse des Bewerbers. Einige Fragebögen beziehen auch Angaben über die familiären Verhältnisse mit ein und dringen z. T. tief in die Privatsphäre der Betroffenen ein. Ein berechtigtes Interesse der Vermieter ist häufig nicht zu erkennen.

Wie ich im 1. TB a. a. O. ausgeführt habe, liegt das Problem darin, daß die Mietinteressenten den Datenwünschen der Vermieter praktisch hilflos ausgeliefert sind; denn sie müssen damit rechnen, daß sie von vornherein aus der Liste der Bewerber gestrichen werden, wenn sie auch nur einzelne der geforderten Angaben oder Einwilligungen nicht erteilen. Das BDSG kann den notwendigen Schutz nicht bieten, weil die Angaben von den Mietinteressenten auf „freiwilliger" Basis erhoben werden.

Das BDSG fragt nicht danach, ob die Datenverarbeitung, in die eingewilligt worden ist, zu dem angestrebten wirtschaftlichen Zweck erforderlich oder auch nur geeignet und angemessen ist. Die Problematik der geltenden Einwilligungsregelung ist schon mehrfach betont worden. Die eine fast uneingeschränkte Datenverarbeitung ermöglichende Einwilligung beruht wegen vielfältiger sozialer oder wirtschaftlicher Zwänge oft auf einer Schein-Freiwilligkeit. Der Verzicht auf Strom-, Gas- und Wasserlieferungen, auf ein Bankkonto, auf Versicherungsschutz oder Krankenhausversorgung ist keine reale Alternative. Wenn das BDSG der Einwilligung eine Schlüsselrolle einräumt, dann muß es auch dafür sorgen, daß der Betroffene vor Benachteiligungen bei Verweigerung des Einverständnisses geschützt und die Widerruflichkeit der Einwilligung garantiert wird, da es andernfalls seinem Schutzzweck nicht genügt.

Es kann keine die Zulässigkeit begründende „freiwillige" Einwilligung angenommen werden, wenn sie durch unangemessenen Druck bewirkt wurde.

Ich bin mir klar darüber, daß es nicht einfach ist, mit Hilfe einer – notwendigerweise allgemein bleibenden – gesetzlichen Regelung eine Grenzlinie zwischen zulässigen und unzulässigen Fragen zu ziehen. Doch darf deshalb nicht abgewartet werden, daß zunächst

die Rechtsprechung anhand von Einzelfällen die Grenzen des Zumutbaren und Zulässigen herausarbeitet, wie es der Bundesregierung richtig erscheint. Das Warten auf einschlägige Rechtsprechung bedeutet, daß für längere Zeit soziale Ungerechtigkeiten und Verletzungen des Persönlichkeitsrechts in Kauf genommen werden (so auch der BfD in seinem 5. TB, Nr. 4.3.1).

Deshalb unterstütze ich den Vorschlag der Justizbehörde (in ihrer Stellungnahme zu dem Referentenentwurf des Bundesministers des Innern zur Novellierung des BDSG), § 3 BDSG um folgende Regelungen zu ergänzen:

- Die Einwilligung ist unwirksam, wenn sie durch unangemessenen Druck, fehlende Aufklärung oder in sonstiger gegen die Gebote von Treu und Glauben verstoßender Weise bewirkt wurde.
- Wegen Verweigerung der Einwilligung dürfen dem Betroffenen keine unbilligen Nachteile zugefügt werden.
- Der Widerruf der Einwilligung kann nicht durch Rechtsgeschäft ausgeschlossen werden.

4.5.2 Zusammenarbeit von Vermietern mit Auskunfteien

Von mehreren Petenten bin ich gefragt worden, ob sich Wohnungseigentümer von der Schufa oder einer Handels- und Wirtschaftsauskunftei aus deren Datenbeständen personenbezogene Daten von Mietern übermitteln lassen dürfen, um deren Zahlungsfähigkeit überprüfen zu können.

4.5.2.1 Zusammenarbeit mit der Schufa

Im Rahmen sog. B-Verträge erteilt die Schufa auf Anfrage Wohnungseigentümern eingeschränkte Auskünfte, d. h. Auskünfte nur über negatives Verhalten im Zusammenhang mit Krediten oder anderweitigen Verpflichtungen (sog. „Negativ-Merkmale").

Die Angaben der Schufa können aus allen Bereichen der Wirtschaft stammen. Sie sind allerdings auf Geschäfte mit kreditorischem Risiko beschränkt. Beispiele dafür sind Verkauf gegen Rechnung, Ratengeschäfte, Dauerkonten des Versandhandels oder auch Hypothekengewährungen. Aus der Anleitung „Technische Abwicklung des Auskunfts- und Meldeverfahrens" (TA) der Schufa ist zu ersehen, daß diese Daten auch für die Beurteilung kreditorischer Risiken übermittelt werden. Die Schufa selbst stellt sich in ihren Veröffentlichungen stets als Einrichtung der kreditgebenden Wirtschaft dar, die diese vor Verlusten im Kreditgeschäft schützen will.

Ich habe deshalb gegen die Erteilung von Schufa-Auskünften an Wohnungsvermieter vor Abschluß eines Mietvertrages erhebliche Bedenken. Der Abschluß eines Mietvertrages ist kein Geschäft mit kreditorischem Risiko; es handelt sich vielmehr um ein Dauerschuldverhältnis, bei dem die einzelnen Zahlungsverpflichtungen – im Gegensatz zu Kreditgeschäften – periodisch durch Zeitablauf entstehen, so daß Auskünfte an Wohnungsvermieter aus der Zwecksetzung der Schufa herausfallen.

Demgegenüber hat die Schufa darauf hingewiesen, daß Wohnungsunternehmen seit eh und je der Schufa angeschlossen seien; sie zählten sogar zu den Gründungsmitgliedern. Im übrigen hält die Schufa Auskünfte an Wohnungsvermieter aufgrund von B-Verträgen für zulässig, weil die Vermietung von Wohnungen für die Anschlußfirma mit einem „geschäftlichen Risiko" verbunden sei.

Ich halte das Merkmal „AV" (= Anfrage wegen Vorleistung oder Lieferung mit kreditorischem oder geschäftlichem Risiko) der TA der Schufa, das zur Glaubhaftmachung eines berechtigten Interesses verwendet wird, für zu unbestimmt, als daß es Grundlage für die Datenübermittlung an Vermieter sein könnte.

Darüber hinaus habe ich Zweifel, ob es mit dem Zweckbindungsprinzip vereinbar ist, einen so umfassenden Datenpool, wie ihn die Schufa unterhält, einem nahezu unbegrenzten Kreis von Auskunftsempfängern zur Nutzung zu überlassen. Der Betroffene, der die Schufa-Klausel der Kreditwirtschaft unterschrieben hat, weiß nicht, wer alles in welchem Umfang von der Schufa bedient wird; im Vertrauen auf das Bankgeheimnis geht er davon aus, daß seine Angaben im Bereich der Kreditwirtschaft verbleiben.

4.5.2.2 Zusammenarbeit mit Handels- und Wirtschaftsauskunfteien

Auch bei Handels- und Wirtschaftsauskunfteien holen Wohnungsvermieter Auskünfte über Mietbewerber ein. Die großen Wohnungsbaugesellschaften in Hamburg machen von dieser Möglichkeit bei der Vermietung von Wohnraum allerdings nur selten Gebrauch. Lediglich bei der Anmietung von Gewerberäumen werden in Ausnahmefällen Auskünfte von Wirtschaftsauskunfteien zur Bonitätsprüfung eingeholt.

Da der Abschluß eines Mietvertrages regelmäßig mit einem nicht unerheblichen wirtschaftlichen Risiko verbunden ist, ist es bisher nicht beanstandet worden, daß Vermieter vor Abschluß eines Mietvertrages über künftige Mieter Auskünfte bei Wirtschaftsauskunfteien einholen. Wie die Schufa haben aber auch die Handels- und Wirtschaftsauskunfteien ihre Geschäftszwecke auf Geschäfte mit kreditorischem bzw. handelsmäßigen Einschlag beschränkt. Der Geschäftszweck des Vereins Creditreform wird z. B. in § 2 der Satzung des Vereins Creditreform wie folgt umschrieben: „Der VC hat den Zweck, Kreditmißbrauch zu verhindern und die Wirtschaftskriminalität zu bekämpfen sowie Kreditschäden zu beseitigen." In den Geschäftsbedingungen der Vereinigten Auskunfteien Bürgel heißt es u. a., daß die Mitglieder sich verpflichtet haben, ihren Kunden „Handels- und Kreditauskünfte über Dritte" zu erteilen.

Ebenso wie bei der Schufa muß auch bei den anderen Auskunfteien geprüft werden, ob die Speicherung für andere Zwecke, z. B. zur Risikoabschätzung im Zusammenhang mit dem Abschluß eines Mietvertrages, vom satzungsmäßig umschriebenen Geschäftszweck gedeckt ist.

4.6 Datenschutz bei Verkehrsbetrieben

4.6.1 Sog. „Schwarzfahrer-Datei" der HHA

Mehrere Eingaben bezogen sich auf die Speicherung personenbezogener Daten bei der HHA wegen Verstoßes gegen die Allgemeinen Beförderungsbedingungen. Den Eingaben liegt folgender Sachverhalt zugrunde:

Wenn ein Fahrkartenprüfer feststellte, daß jemand ohne gültigen Fahrausweis ein Verkehrsmittel benutzt, hält er handschriftlich auf einer sog. FP-Meldung Daten des Fahrgastes (Name, Vorname, Geburtsdatum und Anschrift sowie ggf. Personalausweis- oder Paßnummer) zusammen mit Angaben über Datum, Zeit und Ort des Vorfalls handschriftlich fest. Diese FP-Meldungen werden – bevor sie an die Abteilung Verkehrsrechnung gehen – der Abteilung Datenverarbeitung zugeleitet, die Name, Vorname, eine Bearbeitungsnummer sowie das Datum der Feststellung für die EDV erfaßt.

Die Abteilung Datenverarbeitung erstellt für die Abteilung Verkehrsrechnung Monatslisten der erfaßten personenbezogenen Daten, mit denen ausschließlich die Zahlung des erhöhten Beförderungsentgeltes überwacht werden soll. Die Befürchtung eines besorgten Bürgers, daß die HHA die FP-Meldungen oder auch nur die Monatslisten an die Polizei weitergibt, hat sich nicht bestätigt; ebenso gibt es keinen regelmäßigen Datenaustausch zwischen der HHA und der Deutschen Bundesbahn.

Die HHA hat ein berechtigtes Interesse daran, diejenigen personenbezogenen Daten aufzubewahren, die sie benötigt, um das vom „Schwarzfahrer" verwirkte erhöhte Beför-

derungsentgelt durchsetzen zu können. Darüber hinaus muß ihr zugestanden werden, wiederholte Verstöße gegen die Beförderungsbedingungen zum Zwecke der Strafverfolgung nachweisen zu können.

Eine Beeinträchtigung schutzwürdiger Belange der Betroffenen ist regelmäßig auszuschließen, weil grob vertragswidriges oder gar strafrechtlich relevantes Verhalten nicht verdient, davor geschützt zu werden, daß ein erhöhtes Entgelt verlangt wird oder – im Wiederholungsfall – Strafanzeige erstattet wird.

Wegen einiger Einzelheiten des derzeitigen Verfahrens habe ich allerdings Bedenken angemeldet.
Meinem Vorschlag, die Aufbewahrungsdauer der FP-Meldungen und Monatslisten generell auf 2 Jahre zu beschränken, ist die HHA gefolgt.

Darüber hinaus habe ich Zweifel geäußert, ob die Erhebung und Speicherung der Personalausweis-Nr. erforderlich ist. Jedenfalls kann ich der Auffassung der HHA, daß eine festgestellte und nachprüfbare Ausweisnummer im Rahmen der gerichtlichen Verfolgung ein notwendiges Beweismittel zum Schutz unbeteiligter Personen und auch zur Überprüfung des wahren Täters dienlich sei, in dieser Allgemeinheit nicht folgen. Nur in einigen Einzelfällen mag ein berechtigtes Interesse nach § 23 BDSG begründet sein. Vorsorglich habe ich auf § 4 Satz 2 des Gesetzes über Personalausweise in der Fassung vom 15.3.1983 verwiesen, wonach die Seriennummer des neuen maschinenlesbaren Personalausweises nicht zur Einrichtung und Erschließung von Dateien verwendet werden darf.

4.6.2 Speicherung personenbezogener Daten im Rahmen von Fahrgeldbeanstandungen

Wenn jemand bei dem Versuch, eine Fahrkarte des HVV am Automaten zu kaufen, den Fahrschein oder das Wechselgeld nicht erhält, muß er beim Aufsichtsbeamten der Haltestelle einen Antrag auf Erstattung des Geldes stellen.

Ein besorgter Bürger teilte mir mit, daß auf dem Antragsformular neben Angaben über Ort und Nr. des Fahrkartenautomaten auch Vorname und Zuname, Anschrift, Geburtstag, Geburtsort und die Nr. des Personalausweises einzutragen seien. Das Personal des HVV nehme den Antrag nicht an, wenn nicht auch die Personalausweis-Nr. angegeben werde.

Ich halte die Speicherung der reinen Identifizierungsdaten (Name, Vorname, Geburtsdatum und Anschrift) gem. § 23 BDSG für zulässig, da die HHA sie sowohl zu Abrechnungszwecken als auch zum Nachweis wiederholter Verstöße gegen die Beförderungsbestimmungen benötigt. Sofern es um „betrügerische Rückerstattungsforderungen" geht, ist eine Beeinträchtigung schutzwürdiger Belange des Betroffenen regelmäßig auszuschließen.

Die Speicherung der Personalausweis-Nr. scheint mir allerdings nicht zulässig. Ich habe der zugrungeliegenden Dienstbestimmung entnommen, daß die Mitarbeiter der HHA generell angewiesen sind, die Personalausweis-Nr. zu erheben.
Es scheint mir nicht notwendig zu sein, daß neben den o. b. Identifizierungsdaten auch die Personalausweis-Nr. gespeichert wird. Um „betrügerische Erstattungsforderungen noch mehr zu reduzieren", reicht eine Speicherung der reinen Identifizierungsmerkmale aus, die über einen Ausweis verifiziert werden können, ohne daß deshalb auch die Personalausweis-Nr. gespeichert werden muß.
Da die Erhebung und Speicherung der Personalausweis-Nr. weder zu Abrechnungs- noch zu Beweiszwecken in möglichen späteren gerichtlichen Auseinandersetzungen erforderlich ist, habe ich der HHA nahegelegt, künftig von einer Speicherung der Serien-Nr. abzusehen und lediglich die Tatsache, daß ein qualifiziertes Legitimationspapier vorlag, auf dem Formular „Automaten-Fahrgeld-Beanstandung" zu notieren.

4.7 Öffentliche Bekanntgabe von Lotteriegewinnern

In einer zu Beginn des Jahres an mich gerichteten Eingabe sind Bedenken dagegen vorgebracht worden, daß Namen und Anschriften der Hauptgewinner der ARD-Fernsehlotterie „Ein Platz an der Sonne" öffentlich bekanntgegeben werden.

Ich habe der Deutschen Fernsehlotterie GmbH empfohlen, sie möge die Teilnehmer darauf hinweisen, daß sie einer öffentlichen Bekanntgabe dieser Daten widersprechen können. Die Geschäftsführung der Deutschen Fernsehlotterie GmbH will meinen Anregungen folgen und ihr seit 1956 bestehendes Bekanntgabe-Verfahren (durch Ergänzung der Teilnahmebedingungen, Veränderung des Textes auf der Rückseite sowie mit einem Hinweis im Mittelfeld des Bankeinzahlungsscheines bzw. auf der Rückseite des Posteinzahlungsscheines) beginnend mit der Fernsehlotterie 1984 ändern.

4.8 Arbeitnehmer-Datenschutz

Ein erheblicher Anstieg der Beratungstätigkeit ist im Problembereich „Arbeitnehmer-Datenschutz" zu verzeichnen gewesen.

Wie ich bereits in meinem letzten TB hervorgehoben habe, ist das Unternehmen Kulminationspunkt privater und staatlicher Informationsansprüche. Da die im Unternehmen vorhandenen Informationen aus EDV-technischer Sicht mühelos multifunktional verknüpft werden können, besteht für den betroffenen Arbeitnehmer die Gefahr, zum vollständig erfaßten, beliebig manipulierbaren Objekt unternehmerischer Entscheidung zu werden. Um dieses Gefährdungspotential zu beschränken, ist die frühzeitige Einbeziehung des Betriebsrates (BR) und des betrieblichen Datenschutzbeauftragten (bDSB) bei der Lösung aller die Arbeitnehmer betreffenden Datenschutzprobleme Grundvoraussetzung. Bedauerlicherweise mußte ich jedoch feststellen, daß eher das Gegenteil unternehmerische Praxis ist, so daß ein emotionalisierter Konfliktherd geschaffen, statt daß ein sachlicher Dialog geführt wird.

4.8.1 Zum Verhältnis von BDSG und BetrVG

Eingaben von Betriebsräten berührten häufig Sachprobleme, die an der Schnittstelle von Betriebsverfassungs- und Datenschutzrecht liegen. Deshalb soll als Vorfrage das Verhältnis von Betriebsverfassungs- und Datenschutzrecht geklärt werden. Ausgangspunkt ist dabei § 45 BDSG, der die Subsidiarität der BDSG-Normen gegenüber besonderen Rechtsvorschriften des Bundes, soweit diese auf in Dateien gespeicherte personenbezogene Daten anzuwenden sind, bestimmt.

Aus dieser Formulierung folgt nicht, daß dem BDSG von vornherein die Geltung bei der Verarbeitung von Arbeitnehmerdaten abzusprechen ist. Vielmehr ist die Subsidiarität der BDSG-Normen nur dann anzunehmen, wenn die konkurrierende Norm genau den Sachverhalt zum Gegenstand hat, den auch die entsprechende BDSG-Norm anvisiert.

Daraus folgt, daß die kollektiv-rechtlichen Befugnisse des BR individualrechtliche Positionen des Betroffenen aus dem BDSG keineswegs verdrängen. Soweit aber das BetrVG dem einzelnen Arbeitnehmer Rechte gewährt, gehen diese den BDSG-Ansprüchen vor, wenn sie deckungsgleich sind. So verdrängt das Einsichtsrecht in die Personalakte gem. § 83 Abs. 1 BetrVG ein Auskunftsrecht nach § 26 Abs. 2 Satz 1 BDSG, soweit es sich um Informationen handelt, die in der Personalakte enthalten sind. Verlangt der Betroffene darüber hinaus Informationen, die nicht Gegenstand von Personalakten sind, so verbleibt ihm der Anspruch aus § 26 Abs. 2 BDSG. Das Verhältnis von Datenschutz- und Betriebsverfassungsgesetz ist also im Einzelfall durch konkreten Normenvergleich zu ermitteln.

4.8.2 Die Position des betrieblichen Datenschutzbeauftragten

Im Berichtszeitraum wurde ich mehrfach von Betriebsräten gebeten, mich in Konflikte zwischen BR und bDSB einzuschalten.

4.8.2.1 Kann der bDSB zugleich Mitglied der Geschäftsleitung oder Leiter der EDV-Abteilung sein?

Mir wurde u. a. die Frage vorgelegt, ob ein bDSB, welcher Mitglied der Geschäftsleitung und Leiter der Datenverarbeitungsabteilung ist, seiner gesetzlichen Kontrollaufgabe noch gerecht werden kann.

Ich habe folgende Bedenken geäußert: Nach § 29 Satz 1 BDSG hat der bDSB die Ausführung des BDSG sowie anderer Vorschriften über den Datenschutz sicherzustellen. Ein Mitglied der Geschäftsleitung ist mit Rücksicht auf seine Position und seine unternehmerischen Aufgaben primär daran interessiert, alle Informationen zu bekommen, die es der speichernden Stelle ermöglichen, ihre Ziele optimal zu verwirklichen. Unter diesen Umständen ist ein Interessenkonflikt wegen der vom BDSG geforderten Restriktionen bei der Verarbeitung personenbezogener Daten vorprogrammiert. Der bDSB hat auf der strikten Einhaltung der gesetzlichen Verarbeitungsgrenzen zu bestehen. Deshalb dürfen in aller Regel beide Funktionen nicht in einer Person vereinigt werden.

Ein ähnlicher Interessenkonflikt entsteht, wenn der Leiter einer EDV-Abteilung zum Datenschutzbeauftragten bestellt wird. Zwar sind gerade in einem solchen Fall keinerlei Zweifel an der nach § 28 Abs. 2 BDSG erforderlichen Fachkunde berechtigt. Jedoch begründet der Gesichtspunkt, daß der EDV-Leiter letztlich sich selbst zu kontrollieren hat, Zweifel an seiner Zuverlässigkeit gem. § 28 Abs. 2 BDSG.

4.8.2.2 Zur Kompetenzüberlagerung zwischen betrieblichem Datenschutzbeauftragten und Betriebsrat

In diesem Zusammenhang war auch auf das Problem der Kompetenzüberlagerung zwischen BR und bDSB einzugehen. Gem. § 80 Abs. 1 Nr. 1 BetrVG hat der BR darüber zu wachen, daß die zugunsten der Arbeitnehmer geltenden Gesetze durchgeführt werden. Hierzu zählen auch die Vorschriften des BDSG, die bei der Verarbeitung von Arbeitnehmerdaten einzuhalten sind. Daraus ergibt sich, daß hinsichtlich des Arbeitnehmerdatenschutzes neben dem bDSB nach § 29 Abs. 1 BDSG auch der BR nach § 80 Abs. 1 Nr. 1 BetrVG zuständig ist.

Die Lösung dieses positiven Kompetenzkonfliktes ist nicht in der vorrangigen Zuständigkeit des einen oder des anderen Organs, sondern in der Pflicht beider Seiten zur engen und vertrauensvollen Zusammenarbeit zu suchen. Der bDSB muß mithin dem BR für Einzelauskünfte ebenso zur Verfügung stehen wie für eine langfristig angelegte Kooperation im Hinblick auf die Überprüfung bestehender und die Entwicklung neuer Datenverarbeitung. Umgekehrt hat der BR den bDSB über die aus Arbeitnehmersicht bestehenden Risiken und Bedenken zu informieren und sie mit ihm zu beraten. Um den Kooperationsgedanken in die betriebliche Praxis umzusetzen, kommt es darauf an, daß die Unternehmensleitung eine Persönlichkeit zum bDSB bestellt, die der BR nicht von vornherein der Arbeitgeberseite zurechnet, und ihr auch bei der Erfüllung ihrer Aufgaben genügend Spielraum beläßt, um zwischen beiden Seiten vermitteln zu können.

4.8.2.3 Mitwirkung des Betriebsrates bei der Bestellung des betrieblichen Datenschutzbeauftragten

Im Zusammenhang mit den hier vorgestellten Eingaben, aber auch auf Seminaren, Betriebsversammlungen und Betriebsrätetreffen bin ich wiederholt gefragt worden, welche Mitwirkungsmöglichkeiten der BR bei der Bestellung des bDSB hat. Das BDSG sieht eine Mitwirkung des BRs bei der Bestellung des bDSB nicht vor. Deshalb ist der Akt der Bestellung ein mitbestimmungsfreier Vorgang. Daraus kann jedoch nicht geschlossen werden, daß der BR keinerlei Einflußmöglichkeit besitzt. Denn die Bestellung zum bDSB kann zugleich eine Einstellung oder Versetzung i. S. von § 99 Abs. 1 Satz 1 BetrVG sein.

Dies ist der Fall, wenn ein nicht-leitender Angestellter, der also nicht unter § 5 Abs. 3 BetrVG einzuordnen ist, zum internen bDSB bestellt wird. In einem solchen Fall ist das

Zustimmungsrecht des BRs nach § 99 Abs. 1 Satz 1 BetrVG begründet. Wenn hingegen ein leitender Angestellter i. S. von § 5 Abs. 3 BetrVG zum bDSB bestellt wird, ist zu differenzieren: Verbleiben ihm neben seiner Tätigkeit als bDSB auch unternehmerische Aufgaben, so ist der BR auf ein Informationsrecht gem. § 105 BetrVG beschränkt. Ist der leitende Angestellte hingegen von sonstigen Aufgaben freigestellt, um sich allein der Kontrolltätigkeit als bDSB widmen zu können, ist der BR nach § 99 Abs. 1 Satz 1 BetrVG zustimmungsberechtigt, weil die (Kontroll-) Aufgabe des bDSB nicht zu den Funktionen eines leitenden Angestellten gehört.

An der Bestellung eines externen bDSB ist der BR nach geltendem Recht nicht zu beteiligen.

Ich meine, daß der neue § 28 Abs. 3 des seit Juni 1983 vorliegenden Referentenentwurfs zur Novellierung des BDSG den Erfordernissen der betrieblichen Praxis nicht gerecht wird. Um die Stellung des bDSB zu stärken, sollten seine Bestellung und Abberufung an die Zustimmung des BR geknüpft werden.

Im übrigen halte ich es für sachgerecht, sowohl die Kündigung des Arbeitsverhältnisses des bDSB wie auch seine Abberufung aus dieser Funktion in Anlehnung an § 626 BGB vom Vorliegen eines wichtigen Grundes abhängig zu machen.

4.8.3 Personalfragebögen

Aufgrund mehrerer Eingaben habe ich mich mit der Problematik der Erhebung von Personaldaten im nicht-öffentlichen Bereich befaßt.

Das BDSG unterwirft nicht die Erhebung, sondern erst die Speicherung personenbezogener Daten einer gesetzlichen Grenze, § 1 Abs. 1 BDSG. Da die Speicherung personenbezogener Daten in einer Datei gem. § 23 BDSG nur dann zulässig ist, wenn auch der vorausgegangene Vorgang der Erhebung rechtmäßig war, ist die datenschutzrechtliche Regelungslücke durch die in der arbeitsrechtlichen Literatur und Rechtsprechung entwickelten Grundsätze zur Begrenzung des Fragerechts des Arbeitgebers zu schließen.

Entsprechend den unterschiedlichen Funktionen eines Personalfragebogens ist auch eine Differenzierung bei ihrer rechtlichen Beurteilung sachgerecht. Personalfragebögen dienen einerseits der Vorbereitung der Entscheidung über die Einstellung oder Nichteinstellung eines Bewerbers. Andererseits sind sie vom Zeitpunkt der Einstellung an Grundlage der Personalführung und -bewirtschaftung.

In Personalfragebögen, die anläßlich einer Bewerbung auszufüllen sind, sollen nur die für die Einstellungsentscheidung erforderlichen Informationen erhoben werden. Demgemäß sind Fragen, die ausschließlich persönliche Dinge betreffen, ohne daß ein erkennbarer Zusammenhang mit dem Arbeitsverhältnis besteht, unzulässig. Daraus folgt, daß beispielsweise Angaben über Größe, Haar- und Augenfarbe oder Gewicht, wie sie in einem mir vorgelegten Fragebogen gefordert wurden, nur in Ausnahmefällen als zulässig erachtet werden können.
Ebenso sind Fragen, die sich auf Wohnverhältnisse (bei den Eltern, zur Miete oder im eigenen Haus) beziehen, offensichtlich ohne Bezug zum angestrebten Arbeitsverhältnis und daher rechtswidrig. Der Befragte kann sanktionslos die Antwort verweigern oder – praktisch wichtiger – eine falsche Angabe machen.

Eine sog. Auflösungsklausel, mit welcher der Bewerber bestätigt, daß bei unwahren Angaben das Arbeitsverhältnis aufgelöst werden kann, ist rechtlich ohne Bedeutung. Eine solche Klausel hat nämlich entweder nur deklaratorischen Charakter, indem sie nur auf **gesetzliche** Befugnisse des Arbeitgebers verweist. Soll ihr dagegen konstitutive Wirkung zukommen, so ist eine solche Klausel wegen Verstoßes gegen zwingendes Kündigungsschutzrecht nach § 134 BGB unwirksam.

Erfreulicherweise hat das Unternehmen den Fragebogen, der diese Elemente enthielt, aufgrund meiner Bedenken korrigiert und verwendet nunmehr eine einwandfreie Fassung.

Personalfragebögen, welche als Einstellungsunterlagen dienen, dürfen im Gegensatz zu Bewerbungsbögen weitergehende Informationen enthalten, die z. B. für die Berechnung der Vergütung erforderlich sind.

Meines Erachtens machen die weitgefächerten Möglichkeiten automatisierter Personaldatenverwaltung, etwa zum Zwecke der Personalsteuerung und -planung mit Hilfe von Personalinformationssystemen es erforderlich, diese Dimension schon bei der Datenerhebung zu berücksichtigen. Nach meiner Ansicht umschließt daher das Mitbestimmungsrecht des BR bei der Erstellung von Personalfragebögen gem. § 94 BetrVG die Befugnis, jedenfalls bei sensiblen Daten zu verlangen, daß schon im Fragebogen eine Umschreibung oder Beschränkung des zulässigen Verwendungszwecks festgelegt wird.

4.8.4 Personalinformationssysteme

Mehrfach haben BRe, in deren Unternehmen ein Personalinformationssystem eingeführt werden soll, mich gebeten, sie zu beraten.

Personalinformationssysteme sind – nach einer Definition von Kilian – „intelligente" Dokumentationen von Personalangaben. Sie werden unter den Bezeichnungen PAISY, PERSIS, ISA, INTERPERS u. a. auf dem Softwaremarkt angeboten und decken in unterschiedlichem Umfang Personalverwaltungsfunktionen ab. So können einige Systeme für die Lohn- und Gehaltsabrechnung verwendet, aber auch zum Zwecke der Personalplanung und -steuerung erweitert werden (PAISY). Andere dagegen, z. B. INTERPERS, sind zur Lohn- und Gehaltsabrechnung nicht geeignet, sondern erfüllen ausschließlich weitergehende Funktionen wie etwa Personalsteuerung, -förderung und -planung.
Nach den Erfahrungen aus den mir vorliegenden Eingaben äußern BRe in erster Linie Ängste und Befürchtungen, weniger dagegen gezielte Kritik an einer bestimmten Anwendungsplanung. Dies beruht häufig auf einem Informationsdefizit der BRe, denen mit dem Hinweis, ihnen stünden Mitbestimmungsrechte nicht zu, bereits die Kenntnisnahme detaillierter Systembeschreibung verweigert wird. Hier ist es dann Aufgabe der Aufsichtsbehörde, den Anfragenden die nötigen Informationen zu geben, damit sie in ihren Betrieben ihre eigenen Rechte wahrnehmen oder für die Rechte der von ihnen vertretenen Arbeitnehmer tätig werden können.

4.8.4.1 Das Mitbestimmungsrecht des Betriebsrates nach § 87 Abs. 1 Nr. 6 BetrVG

Die „schärfste Waffe" der BRe sind die zwingenden Mitbestimmungsrechte nach § 87 Abs. 1 BetrVG. Nach herrschender Meinung sind in diesem Regelungsbereich einseitige Maßnahmen des Arbeitgebers, die nicht durch Betriebsvereinbarung oder den Spruch der Einigungsstelle abgedeckt sind, rechtsunwirksam. Die rechtliche Unwirksamkeit kann freilich nichts an der faktischen Existenz derartiger rechtswidriger Maßnahmen ändern. Deshalb sind in solchen Fällen BRe in erster Linie auf den vorläufigen Rechtsschutz nach § 85 Abs. 2 ArbGG zu verweisen.

Gem. § 87 Abs. 1 Nr. 6 BetrVG hat der BR ein Mitbestimmungsrecht bei der Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten und die Leistung der Arbeitnehmer zu überwachen. Ein computergestütztes Personalinformationssystem stellt unzweifelhaft eine technische Einrichtung i. S. dieser Vorschrift dar.

Dementsprechend entzünden sich Kontroversen vornehmlich an der Frage, wann eine technische Einrichtung zur Verhaltens- oder Leistungskontrolle bestimmt ist. Seit der Produktographen-Entscheidung des Bundesarbeitsgerichts (BAG AP Nr. 2 zu § 87 BetrVG) besteht insoweit Klarheit, als es nicht auf die subjektive Absicht des Arbeitgebers, sondern auf die unmittelbare und objektive Eignung der Einrichtung zur Überwachung ankommt.

M. E. ist eine objektive und unmittelbare Eignung zur Leistungs- und Verhaltenskontrolle i. S. der Rechtsprechung des BAG regelmäßig zu bejahen. Es ist offensichtlich, daß beispielsweise die automatische Fortschreibung von Krankheits-, Überstunden- oder Leistungsbewertungsstatistiken Elemente der Leistungs- und Verhaltenskontrolle enthält. Im übrigen meine ich, daß an das Unmittelbarkeitskriterium keine allzu strengen Anforderungen gestellt werden dürfen, weil sonst die Gefahr von Zufallsergebnissen besteht, je nachdem welche technische Variante eines Personalinformationssystems zu beurteilen ist.

Statt des Unmittelbarkeitskriteriums sollten die unterschiedlichen Rechtsgüter und Gefährdungspotentiale, welche dem Arbeitnehmer- und Arbeitgeberinteresse jeweils zugrundeliegen, im Mittelpunkt der Argumentation stehen. Es gilt, die auftretenden Wertungsfragen offenzulegen und dem Schutzzweck der Norm entsprechende Lösungen zu suchen. Der Schutzgedanke des § 87 Abs. 1 Nr. 6 BetrVG liegt darin, Eingriffe in den Persönlichkeitsbereich der Arbeitnehmer durch Verwendung anonymer technischer Kontrolleinrichtungen nur bei gleichberechtigter Mitbestimmung des BR zuzulassen.

Personalinformationssysteme, welche zur Personalsteuerung, -förderung und -planung eingesetzt werden, setzen die Speicherung und Verknüpfung von z. T. hochsensiblen personenbezogenen Daten voraus. Anders als bei der früher üblichen Aktenführung sind diese Daten aktuell verfügbar und können variabel miteinander kombiniert und verknüpft werden. Die Gefahr, daß die Arbeitnehmer zum vollständig erfaßten – gläsernen – Menschen degradiert werden, wird noch gesteigert, wenn die Verknüpfung mit weiteren computergestützten Systemen, etwa Betriebsdatenerfassungssystemen, in die unternehmerische Planung einbezogen wird. Im Unternehmen kontrastiert also das Interesse des Arbeitgebers an einer möglichst effektiven Personaleinsatzplanung mit dem Persönlichkeitsrecht des Arbeitnehmers aus § 75 Abs. 2 BetrVG, welches eine vollständige Registrierung und Katalogisierung der Person verbietet.

Ich meine daher, daß der Schutzgedanke des § 87 Abs. 1 Nr. 6 BetrVG es gebietet, jedenfalls solche Personalinformationssysteme, die Planungs- und Steuerungsfunktionen erfüllen, dem Mitbestimmungsrecht des BR zu unterstellen.

Wenn ein Personalinformationssystem (untypischerweise) ausschließlich zur Lohn- und Gehaltsabrechnung verwendet werden soll, so ist die unmittelbare Eignung zur Überwachung nicht ersichtlich. Ich meine allerdings, daß mit dieser rechtlichen Feststellung die Problematik nicht erschöpfend behandelt ist. Es darf nämlich nicht außer acht gelassen werden, daß alle auf dem Markt vorhandenen Personalinformationssysteme, die zur Lohn- und Gehaltsabrechnung verwendbar sind, durch Ergänzung zusätzlicher Software zum Zweck der Personalsteuerung und -planung erweitert werden können. Die sonst bei Verfahrenserweiterungen üblichen kosten- und zeitintensiven Kompatibilitätsprobleme zwischen alten und neuen Programmteilen treten hier nicht auf, weil diese Ergänzungsmöglichkeiten „baukastenartig" vorgesehen sind. Die Erfahrung zeigt, daß in vielen Unternehmen sämtliche Möglichkeiten der vom Hersteller angebotenen Systeme sukzessiv ausgeschöpft werden. Wenn man aufgrund mangelnder „Unmittelbarkeit" die Anschaffung der EDV-Grundausstattung für Lohn- und Gehaltsabrechnung für mitbestimmungsfrei hält, so besteht die Gefahr, daß Mitbestimmungsrechte, die erst bei Folgeinvestitionen einsetzen, materiell entwertet sind. Bei der Ergänzung von „nicht unmittelbar geeigneten" Einrichtungen zu solchen, die nunmehr dieses Kriterium erfüllen, könnte nämlich die „richtige" Entscheidung weitgehend von ökonomischen Sachzwängen diktiert sein.

Diese Überlegungen zeigen die Schwierigkeiten auf, welche der Einsatz hochentwickelter Informationstechnologie allein auf dem Gebiet der Personalverwaltung für die Praxis der Mitbestimmung erzeugt hat.
Zwar ist der BR nicht auf § 87 Abs. 1 Nr. 6 BetrVG beschränkt, sondern er kann etwa mit Hilfe der §§ 94 Abs. 1, 111 Nr. 4, 5 BetrVG versuchen, im Einzelfall Einfluß zu nehmen. Aber diese Vorschriften sind nur partiell geeignet, die Problemsituation zu erfassen und eine befriedigende Lösung zu bieten.

Ich halte es für eine wichtige Aufgabe des Gesetzgebers, durch eine klare Regelung die Mitbestimmung der BRe bei automatischer Personal- und Betriebsdatenerfassung und -verwaltung sicherzustellen. Die jetzige Rechtsunsicherheit führt zu einer Fülle von Einigungsstellenverfahren und Prozessen mit wechselndem Ausgang.
In dieser Situation möchte ich auch an die Arbeitgeberseite appellieren, die BRe frühzeitig in ihre Planungen einzubeziehen und an den Entscheidungen zu beteiligen. An die Gewerkschaften möchte ich die Aufforderung richten, die pauschale Ablehnung von Personalinformationssystemen aufzugeben und sich um den Dialog mit der Arbeitgeberseite zu bemühen.

4.8.4.2 Dem Mitbestimmungsrecht vorgelagerte Informationsrechte des Betriebsrats

Mitbestimmung ist nur möglich, wenn das zur Mitbestimmung berufene Organ den gleichen Informationsstand wie sein Gesprächspartner hat. Die §§ 87 Abs. 1 Nr. 6, 80 Abs. 2 BetrVG begründen einen Anspruch des BR auf rechtzeitige und umfassende Information bereits in der Planungsphase. Im folgenden möchte ich die im 1. TB erhobene Forderung nach mehr Transparenz spezifieren.

1. Unverzichtbar ist es, dem BR eine Beschreibung des Systems incl. Benutzerhandbuch sowie Nutzungs- und Wartungsverträge zur Verfügung zu stellen. Die Einsicht in die Verträge ist erforderlich, da sie die anwenderspezifischen System-Konfigurationen anzeigen und die Systempflege einschließlich nachträglicher Systemberatung und Systemerweiterung regeln.

2. Der BR benötigt ferner einen Katalog aller personenbezogenen Daten einschl. ihrer Formatierung sowie der Lokalisierung im Datensatz und der verwendeten Schutzcodes, um die einzuspeichernde Informationsmenge kontrollieren zu können. Aus diesem Grund ist ihm auch das vollständige Schlüsselverzeichnis für alle nicht im Klartext abgelegten Daten offenzulegen.

3. Unabdingbar ist auch die Kenntnis sämtlicher beabsichtigter Datenverknüpfungen, um die zulässigen Verwendungen positiv und abschließend in einer späteren Betriebsvereinbarung regeln zu können. Insbesondere sind also die zur Erstellung von Statistiken benutzten Sortierprogramme einschl. der zugehörigen Bildschirmmasken bzw. Listenköpfe dem BR zu übergeben.

4. Zum Schutz vor beliebiger Einsichtnahme in personenbezogene Daten muß eine Regelung darüber erfolgen, wer wann auf welche Daten zugriffsberechtigt ist. Deshalb ist der BR über die beabsichtigte Zugriffshierarchie zu informieren.

5. Außer der Software ist auch die geplante Gerätekonfiguration und -ausstattung (Hardware) in die Informationspflicht einzubeziehen, um beliebige Systemerweiterungen, die auch eine Veränderung der Softwarekonfiguration indizieren, auszuschließen.

6. Wenn das Unternehmen sein Personalinformationssystem im Datenverbund mit externen EDV-Anlagen betreibt (etwa über das öffentliche Fernmeldenetz), so ist der BR über Schnittstellendefinitionen und Input-/Output-Beschreibungen zu informieren.

4.8.4.3 Elemente einer Betriebsvereinbarung

In einer Betriebsvereinbarung sollten zum Zweck ihrer Handhabbarkeit detaillierte und nicht generalklauselartige Regelungen über zulässige Speicherungen und Verknüpfungen getroffen werden. Ziel sollte es sein, die totale Erfassung zu verhindern.

Es scheint mir selbstverständlich zu sein, daß die zulässige Speicherung auf den Zweck des Arbeitsverhältnisses zu begrenzen ist. Ich meine zwar, daß eine solche Festlegung

in der Betriebsvereinbarung nur klarstellenden Charakter hat, da nach meiner Ansicht § 23 BDSG nur die Speicherung im Rahmen der Zweckbestimmung des Arbeitsvertrages erlaubt. Nach gegenteiliger – wohl herrschender – Auffassung kommt allerdings der zweite Erlaubnistatbestand des § 23 – Wahrung berechtigter Interessen ohne Beeinträchtigung schutzwürdiger Belange – neben dem ersten Erlaubnistatbestand – Speicherung im Rahmen der Zweckbestimmung eines Vetrages – zur Anwendung. Im Rahmen der Novellierung des BDSG ist eine Klarstellung des Gesetzgebers wünschenswert, daß die Erlaubnistatbestände der §§ 23 und 24 BDSG nur alternativ zu verstehen sind. Eine andere – denkbare – Lösung könnte darin bestehen, daß in das BDSG eine Vorschrift eingefügt wird, die die Datenverarbeitung im Rahmen eines Arbeitsverhältnisses in der Weise regelt, daß der Speicherungs- und Übermittlungsgrund „berechtigtes Interesse" ausgeschlossen wird.

Zwei Gesichtspunkte, welche mir für den Abschluß einer Betriebsvereinbarung wichtig erscheinen, möchte ich hervorheben:

Bei der Speicherung subjektiver Qualifikationsmerkmale wie z. B. Kontaktfreude, Einsatzbereitschaft usw. sollte Zurückhaltung geübt werden. Hier besteht die Gefahr, daß subjektive Eindrücke des Beurteilenden durch die für die Verarbeitung erforderliche Standardisierung „scheinobjektiviert" und dadurch verfestigt werden.

Die Verknüpfung mit anderen Systemen, etwa mit Betriebsdatenerfassungssystemen, sollte ausgeschlossen werden. Die Arbeitnehmer werden dadurch letztlich als Informationsobjekte behandelt, die der „Inventarisierung" unbegrenzt zugänglich sind. Die Zergliederung eines Mitarbeiters in einzelne standardisierte Parameter, die beliebig kombinierbar sind, ist mit seinem Anspruch, auch im Betrieb als Persönlichkeit respektiert zu werden, unvereinbar.

4.8.4.4 Systembenutzungskontrolle

Nach meiner Erfahrung sind die Probleme der Systembenutzungskontrolle, die sich regelmäßig erst nach dem Abschluß einer Betriebsvereinbarung stellen, ebenso wichtig wie diejenigen, welche dem Abschluß einer Betriebsvereinbarung vorgelagert sind. Jedoch gibt es in diesem Bereich kaum befriedigende Lösungen.

Die Durchsicht von Sytembenutzungsprotokollen ermöglicht zwar eine Kontrolle der tatsächlichen Systembenutzung. Aber einerseits sind die derzeit üblichen Protokolle für den EDV-Laien kaum verständlich, andererseits dürfte jeder BR bei vollständiger Protokolldurchsicht in einer Papierflut versinken. Hier muß in Zusammenarbeit mit dem bDSB eine praktikable Lösung erarbeitet werden, die ohne gegenseitiges Vertrauen der beiden innerbetrieblichen Kontrollinstanzen kaum erreichbar sein dürfte.

4.8.5 Probleme der Konzerndatenverarbeitung

Im Berichtszeitraum bin ich auch mit Problemen konfrontiert worden, die daraus resultieren, daß Arbeitnehmer in einem konzernabhängigen Unternehmen beschäftigt sind. Aus datenschutzrechtlicher Sicht verbinden sich damit spezifische Probleme. So wurde in dem mir vorliegenden Fall die Personaldatenverarbeitung für alle Mitarbeiter eines Konzerns zentral in einer der Konzerngesellschaften zusammengefaßt. Für die davon betroffenen Arbeitnehmer stellt sich dann die Frage, wer Adressat des Auskunfts-, Berichtigungs-, Sperrungs- oder Löschungsanspruchs nach dem BDSG ist. Der BR möchte wissen, gegen wen seine Informations- und Kontrollansprüche zu richten sind. Ich habe festgestellt, daß der Hinweis auf die „Fremdverarbeitung der Personaldaten" als Schranke gegen individual- und kollektivrechtliche Ansprüche nach dem BDSG und BetrVG eingesetzt wird. Auch in diesem Problembereich hat die Aufsichtsbehörde primär die Aufgabe, dem Anfragenden die datenschutzrechtliche Situation zu erläutern.

Nach dem BDSG ist Pflichtadressat die „speichernde Stelle" i. S. von § 2 Abs. 3 Nr. 1 BDSG. Dies kann nach § 1 Abs. 2 Nr. 2 BDSG nur eine natürliche oder juristische Person sein. Mangels eigener Rechtspersönlichkeit ist der Konzern als Unternehmensverbund dafür ungeeignet. Das BDSG berücksichtigt somit nicht die wirtschaftliche und organisatorische Verknüpfung der Konzernunternehmen. Mithin ist der gesamte Datentransfer zwischen den einzelnen Konzerngesellschaften dem BDSG unterworfen.

„Speichernde Stelle" i. S. des BDSG kann also nur ein einzelnes Konzernunternehmen sein. Bei Verarbeitung von Arbeitnehmerdaten außerhalb des Unternehmens, bei dem der Arbeitnehmer beschäftigt ist, kommt als speichernde Stelle dieser Daten entweder das eigene Unternehmen oder das tatsächlich verarbeitende in Betracht, je nachdem ob dieses die Datenverarbeitung für eigene Zwecke i. S. des 3. Abschnitts des BDSG betreibt, oder ob es die Daten geschäftsmäßig im Auftrag als Dienstleistungsunternehmen gem. § 31 Abs. 1 Nr. 3 BDSG verarbeitet.

Wenn in einem Konzern eine der Gesellschaften die Datenverarbeitung für den Konzern und gleichzeitig auch für die eigene juristische Person betreibt, dann liegt für den „Eigenanteil" Datenverarbeitung für eigene Zwecke vor. Bei dem Teil der Datenverarbeitung, der für die anderen Konzernunternehmen durchgeführt wird, handelt es sich im Grundsatz um Auftragsdatenverarbeitung.

Eine Ausnahme gilt für den Fall, daß eine gesamte Aufgabe (z. B. die Personalverwaltung) einschl. der Datenverarbeitung auf eine Gesellschaft übertragen wird. Bei einer solchen Funktionsübertragung ist nicht die Verarbeitung personenbezogener Daten Hauptzweck des Auftrages, sondern die Erfüllung einer darüber hinausgehenden Gesamtaufgabe; zum Zwecke der Erfüllung dieser Gesamtaufgabe wird die Datenverarbeitung betrieben. Es handelt sich also um Datenverarbeitung für eigene Zwecke i. S. des 3. Abschnitts des BDSG.

Eine Funktionsübertragung hat somit zur Folge, daß derjenige, dem die Funktion übertragen wurde, alle datenschutzrechtlichen Pflichten übernimmt. Die Auskunfts-, Berichtigungs-, Sperrungs- oder Löschungsansprüche der betroffenen Arbeitnehmer sind an ihn zu richten.

Hinsichtlich des Adressaten der Beteiligungsrechte des BR sollte m. E. analog differenziert werden.

Bei Auftragsdatenverarbeitung i. S. des § 31 Abs. 1 Nr. 3 BDSG bleibt die Leitung desjenigen Unternehmens, bei der der BR installiert ist, sein Ansprechpartner.

Im anderen Fall – z. B. bei einer Funktionsübertragung – liegen die Dinge für diejenigen BRe, die in einem anderen als dem datenverarbeitenden Unternehmen beschäftigt sind, komplizierter. Das BetrVG sieht als Ansprechpartner des BR grundsätzlich den Arbeitgeber vor, vgl. § 77 Abs. 2 BetrVG. Unternehmensübergreifend hat an sich nur ein Konzern-BR i. S. von § 54 Abs. 1 BetrVG einen Handlungsspielraum gem. § 58 Abs. 1 BetrVG. Ich meine aber, daß eine „Fremdverarbeitung" von Arbeitnehmerdaten nicht zu einer Verkürzung von Rechten des BR führen sollte.

Dem BR sollte die Erfüllung seiner Aufgabe, nach § 80 Abs. 1 Nr. 1 BetrVG darüber zu wachen, daß die zugunsten der Arbeitnehmer geltenden Gesetze (also auch das BDSG) durchgeführt werden, nicht durch den Hinweis auf „Fremdverarbeitung" unmöglich gemacht werden. Es ist abzuwarten, wie die arbeitsrechtliche Literatur und Rechtsprechung angesichts der zunehmenden rechtlichen Verselbständigung von einzelnen Unternehmensfunktionen und den damit verbundenen betriebsverfassungsrechtlichen Implikationen Stellung beziehen wird.

4.9 Datenübermittlungen zwischen nicht-öffentlichem und öffentlichem Bereich

4.9.1 Erteilung von Auskünften durch die Schufa an die Strafverfolgungsbehörden

Die Polizei hat zunehmend Schwierigkeiten bei der Beweisführung in Wirtschaftsstrafsachen, insbesondere bei Ermittlungsverfahren wegen Kreditbetruges. Sie ist z. T. auf Informationen angewiesen, die ihr die Schufa geben kann. So können in begründeten Einzelfällen insbesondere Angaben zu Bankverbindung, Art und Umfang eines aufgenommenen Kredits, Abzahlungsmodalitäten und Abwicklung des Kredits Lücken in Kausalitäts- und Beweisketten schließen.

Die Problematik dieses Auskunftsverfahrens liegt darin, daß die Polizei, um von der Schufa bestimmte Informationen zu erhalten, ihrerseits der Schufa einige Fakten über den Betroffenen, z. B. den Grund des Ermittlungsverfahrens, mitteilen müßte, um ihr berechtigtes Interesse an der Auskunft glaubhaft zu machen (§ 32 Abs. 2 BDSG). Damit erführe die Schufa Tatsachen, die geeignet sind, den Betroffenen zu diskriminieren, die die Schufa für ihre Auskunftszwecke aber nicht benötigt und deshalb auch nicht speichern darf.

Unter besonderer Berücksichtigung der Belange des Betroffenen habe ich mit den Beteiligten das bereits bestehende Auskunftsverfahren diskutiert und z. T. weiterentwickelt:

Die Polizei darf bei der Schufa nur anfragen, wenn es sich um einen Beschuldigten handelt. Nur einige leitende Kontaktbeamte einzelner Fachdienststellen sind anfrageberechtigt. Sie dürfen bei der Archivleiterin der Schufa nachfragen, ob Informationen über den Beschuldigten vorliegen. Sie nennen der Schufa anstelle des genau bezeichneten Strafvorwurfs lediglich ein neutrales Verknüpfungsmerkmal, das die Verbindung von der Schufa-Eintragung zum Ermittlungsvorgang herstellt. Die Schufa erhält keinerlei Hinweise auf den Grund des Ermittlungsverfahrens.

Die Schufa protokolliert jede erteilte Auskunft nach Datum und Tagebuch-Nr., ohne allerdings zu vermerken, welche Daten weitergegeben worden sind. Hierauf habe ich besonderen Wert gelegt, damit die Schufa nicht – z. B. für bestimmte Zeiträume – negative Rückschlüsse auf das Verhalten des Betroffenen ziehen und diese an ihre Vertragspartner übermitteln kann. Darüber hinaus bin ich mit den Beteiligten übereingekommen, daß auch die Polizei alle Auskunftsersuchen protokolliert und dazu Dienststelle, Aktenzeichen, Datum der Anfrage und Namen des Sachbearbeiters in eine Monatsliste einträgt. Die Aufbewahrungsfristen der Listen betragen sowohl bei der Schufa als auch bei der Polizei ein Jahr.

Ich meine, daß dieses Verfahren den Anforderungen des § 32 Abs. 2 BDSG genügt und zugleich am ehesten geeignet ist, eine Beeinträchtigung schutzwürdiger Belange der Betroffenen zu vermeiden. Mit der Doppel-Protokollierung ist überdies eine lückenlose Überprüfung des berechtigten Interesses – bis hin zum zugrundeliegenden Ermittlungsverfahren – gesichert.

4.9.2 Datenübermittlung Hamburger Wasserwerke (HWW) – Polizei

Die Ermittlungsgruppe Umwelt der Polizei (PD 455) benötigt häufiger zur Ermittlung von Umweltstraftätern, insbesondere im Bereich der Gewässerverunreinigungen, Angaben über den Trinkwasserverbrauch einzelner Unternehmen oder Privatpersonen.

Bei der Ermittlung einzelner Umweltstraftäter, die ohne wasserrechtliche Einleitungserlaubnis Abwässer abpumpen, ableiten oder versickern lassen, ist der Vergleich der Menge des abgefahrenen Wassers mit der Wasserrechnung ein hilfreiches Indiz. Gemeinsam mit den Beteiligten habe ich ein Verfahren über die Abwicklung von Anfragen von Polizeidienststellen über Wasserverbräuche einzelner Kunden bei Ermittlungen wegen Gewässerverunreinigungen entwickelt, das den berechtigten Interessen der PD 455 Rechnung trägt, ohne schutzwürdige Belange der betroffenen Kunden zu beeinträchtigen.

Eine Datenübermittlung durch die HWW an die Polizei erfolgt nur in Einzelfällen. Voraussetzung ist, daß die Polizei schriftlich anfragt, den Zweck der Anfrage begründet und das Ziel der Ermittlungen darlegt. Sie muß genaue Angaben über Art und Umfang der zu übermittelnden Daten machen und darlegen, daß die Daten auf andere Weise nicht beschafft werden können. Sie sichert zu, daß sie die Angaben ausschließlich für den angegebenen Zweck verwendet. Soweit im Einzelfall der Kunde einer Datenübermittlung an die Polizei zugestimmt hat, ist die Zustimmung in der Anfrage zu bestätigen. Wenn all diese Voraussetzungen gegeben sind, werden der Polizei Angaben zu Zählerstand und Abnahmemenge übermittelt.

Unter datenschutzrechtlichen Aspekten habe ich keine Bedenken gegen dieses Verfahren, zumal durch die Dokumentation des mitgeteilten Aktenzeichens und weiterer Einzelheiten bei der auskunftserteilenden Stelle der HWW eine jederzeitige Kontrolle sichergestellt ist. Zur Ermittlung von Umweltstraftätern muß die Polizei auch auf Angaben der HWW zum Stadtwasserverbrauch von Industrieunternehmen zurückgreifen. Da es dabei i. d. R. nicht um personenbezogene Daten geht, gehe ich hierauf nicht näher ein.

4.9.3 Errichtung von Fahrraddateien

Die Polizei hat mich gebeten, sie bei der Vorbereitung eines Projektes zu beraten, das sie gemeinsam mit den hamburgischen Sachversicherern durchführen will, um intensivere Vorbeugungsmaßnahmen gegen Fahrraddiebstahl sowie gegen Versicherungsbetrug im Zusammenhang mit angeblich gestohlenen Fahrrädern treffen zu können.

Ich bin dieser Bitte besonders gern nachgekommen, weil sich mir die Möglichkeit bot,ein Projekt von vornherein so mitzugestalten, daß es datenschutzrechtlichen Ansprüchen in hohem Maße gerecht wird.

Ausgangslage waren folgende Anforderungen:
Die Polizei möchte insbesondere

- die Anzahl der Fahrraddiebstähle insbesondere unter dem Gesichtspunkt des Einstiegsdelikts vermindern,
- die Aufklärungsmöglichkeiten nach einem Fahrraddiebstahl verbessern,
- die Anzahl der gefundenen Fahrräder erhöhen, die an ihre Eigentümer zurückgegeben werden.

Die Versicherungsunternehmen wollen versuchen, mehr gestohlene bzw. abhanden gekommene Fahrräder wieder aufzufinden und so Einsparungen bei ihren Versicherungsleistungen zu erzielen. Zur Erreichung dieser im öffentlichen Interesse liegenden Ziele sollen drei Dateien eingerichtet werden.

- Bestandsdaten

  Wie bisher bereits sollen in einem Modellversuch Fahrradpässe ausgegeben werden, mit denen Eigentümer – auf freiwilliger Basis – ihre Fahraddaten registrieren lassen können.
  Mit den durch den Fahrradpaß erhobenen Daten soll eine automatisierte „Bestandsdatei" aller registrierten Fahrräder aufgebaut werden.

- Datei „gestohlene Fahrräder"

  Aus den bei den Polizeirevierwachen (PRW) eingehenden Diebstahlsmeldungen über Fahrräder soll eine Datei „gestohlene Fahrräder" aufgebaut werden. Diese Datei soll nicht nur über alphanumerische Kennzeichen (Fahrradrahmennr.) erschlossen werden können (wie die Datei INPOL-Sachfahndung), sondern auch über sonstige Merk-

male wie Farbe, Marke des Rades etc. Diese Erweiterungen erleichtern es der Polizei, die gefundenen mit den gestohlenen Fahrrädern abzugleichen, da die Eigentümer, deren Fahrräder nicht registriert sind, häufig ihre Fahrradrahmennr. nicht kennen.

Bei als „gestohlen" gemeldeten Fahrrädern, die versichert sind, sollen die Versicherer zusätzlich ihre Schadensnr. einspeichern können. Diese zusätzliche Maßnahme soll es ermöglichen, den „zuständigen" Versicherern wöchentlich eine Liste derjenigen Fahrräder zu übermitteln, die nach Ablauf von sechs Wochen noch nicht wieder aufgefunden wurden.

- Datei „wiedergefundene Fahrräder"

  Aus den von den PRW eingehenden Fundmeldungen (gleiches Formular wie Diebstahlsmeldungen) soll eine Datei wiedergefundener Fahrräder aufgebaut werden, die in regelmäßigen Abständen mit der Datei „gestohlene Fahrräder" abgeglichen wird.

Die geplanten Maßnahmen einschl. der Datenverarbeitung sollen organisiert und vor allem finanziert werden von einem „Verein zur Verhütung von Fahrraddiebstahl (e. V.)". Mitglieder – und somit Finanzierende – dieses Vereins können Versicherungsunternehmen werden. Die Polizei ist in einem Beirat vertreten. Zweck des Vereins ist es, Fahrraddiebstähle zu verhüten und bei ihrer Aufklärung mitzuwirken. Zu diesem Zweck werden die von der Polizei gesammelten Daten zur Identifizierung von Fahrrädern in einer EDV-Anlage gespeichert und verarbeitet.

Ich habe die mit diesem Projekt verbundenen datenschutzrechtlichen Fragen gründlich prüfen können und Regelungen erreicht, die dem Bürger ein großes Maß an Sicherheit und Transparenz bei der Datenverarbeitung bieten. In einer Einwilligungserklärung, die von den Fahrradpaßbesitzern zu unterzeichnen ist, sind die Art der Daten, Adressaten der Übermittlung, der Verwendungszweck und die Dauer der Aufbewahrung für jedermann klar und verbindlich bezeichnet. Die zulässige Verwendung der gespeicherten Daten ist eindeutig und klar begrenzt.

4.9.4 Datenübermittlung des Amtes für Arbeitsschutz an Betriebsräte

Ein Unternehmen wurde einer Prüfung durch das Amt für Arbeitsschutz der Behörde für Arbeit, Jugend und Soziales unterzogen, bei der festgestellt werden sollte, inwieweit im Rahmen geleisteter Überstunden die Bestimmungen der Arbeitszeitordnung (AZO) und der Gewerbeordnung eingehalten worden sind. Das Amt für Arbeitsschutz hat den gesamten Schriftwechsel in dieser Sache an den BR der überprüften Firma weitergegeben.

Diese Firma vertritt die Auffassung, daß die Weitergabe des gesamten Schriftwechsels vom Amt für Arbeitsschutz an den BR jeglicher Rechtsgrundlage entbehre und gegen datenschutzrechtliche Bestimmungen verstoße. Eine Unterrichtung des BR über Ermittlungen wegen möglicher Ordnungswidrigkeiten sei vom BetrVG nicht erfaßt. Der BR habe lediglich ein Recht auf Einsichtnahme, jedoch kein Recht auf Aushändigung von Unterlagen im Rahmen des § 89 BetrVG.

Ich bin anderer Meinung: Nach § 89 Abs. 2 BetrVG sind Arbeitgeber und die für den Arbeitsschutz zuständigen Behörden verpflichtet, den BR oder die von ihm bestimmten Mitglieder des BR bei allen im Zusammenhang mit dem Arbeitsschutz oder der Unfallverhütung stehenden Besichtigungen und Fragen und bei Unfalluntersuchungen hinzuzuziehen. Der BR erhält gem. § 89 Abs. 4 BetrVG die Niederschriften über Untersuchungen, Besichtigungen und Besprechungen, zu denen er nach Abs. 2 und 3 hinzuzuziehen ist.

Das Amt für Arbeitsschutz hat danach also eine originäre Pflicht, bei betriebsbezogenen Maßnahmen des Arbeits- und Gesundheitsschutzes den BR von sich aus zu beteiligen;

es ist nicht gehalten, den Umweg über den Arbeitgeber zu benutzen, sondern kann den BR auch unmittelbar unterrichten. Das Verfahren der Unterrichtung ist gesetzlich nicht weiter ausgestaltet.

Der Auffassung der überprüften Firma, daß sich § 89 BetrVG ausschließlich auf Fragen der betrieblichen Gestaltung von Arbeitsabläufen bzw. im Rahmen der AZO auf Fragen der Genehmigungserteilung bzw. -versagung beziehe, konnte ich mich nicht anschließen. Das Arbeitszeitrecht ist Teil des Arbeitsschutzrechts und somit ist auch der BR im Rahmen der AZO in vollem Umfang mitwirkungsberechtigt.

Bei den übersandten Unterlagen handelt es sich ausschließlich um Niederschriften bzw. Ergänzungen zu Niederschriften i. S. des § 89 Abs. 4 BetrVG.

Abschließend habe ich das betroffene Unternehmen darüber aufgeklärt, daß es nicht Zweck der allgemeinen Datenschutzgesetze ist, die Rechte des BR einzuschränken. Das Recht des einzelnen auf Schutz seiner Individualsphäre muß gegenüber der dem BR obliegenden sozialen Schutzfunktion zugunsten der gesamten Arbeitnehmerschaft als dem vorrangigen Recht zurücktreten, und zwar auch dann,wenn dem BR dabei beiläufig persönliche Daten von Arbeitnehmern bekanntwerden.

5. Ausblick

5.1 Rechtsentwicklung in Hamburg

Das Jahr 1984 wird nach meiner derzeitigen Einschätzung in Hamburg einige wichtige Fortentwicklungen des Datenschutzrechts mit sich bringen.

5.1.1 Hamburgisches Datenschutzgesetz (HmbDSG)

Am 1. Mai 1984 werden (gem. § 29 Nr. 3) alle Vorschriften des Hamburgischen Datenschutzgesetzes in Kraft getreten sein. Auch das – allein in Hamburg vorgesehene – Recht des Betroffenen auf Sperrung von Übermittlungen zwischen verschiedenen Behörden nach § 6 Abs. 1 Nr. 4 wird dann gelten. Einzelheiten dieser Vorschrift und ihrer Problematik habe ich an einem Beispielfall unter Nr. 3.5.1.2 erörtert. Mir ist aufgefallen, daß nach wie vor nur sehr wenige Behörden einen konkreten Regelungsbedarf für Übermittlungen an andere Behörden geltend gemacht haben (insb. Polizei und Schulbehörde). Ich hoffe, daß keine Behörde mehr § 10 als ein Gesetz i. S. des § 6 Abs. 1 Nr. 4 ansieht mit der Folge, daß Übermittlungen, die zur Aufgabenerfüllung erforderlich sind, nicht gesperrt werden können. Dies wäre ein Irrtum (vgl. auch dazu Nr. 3.5.1.2).

5.1.2 Krebsregistergesetz und Archivgesetz

Ich erwarte, daß im Jahr 1984 das Krebsregistergesetz (vgl. Nr. 3.16.2.2) in der Bürgerschaft verhandelt wird. Diesen Beratungen messe ich große Bedeutung für die Entwicklung des Datenschutzes bei Wissenschaft und Forschung zu.

Ich gehe ferner davon aus, daß der Senat noch im Jahre 1984 einen Entwurf für ein Archivgesetz in die Bürgerschaft einbringen wird. Einen von den DSBen erarbeiteten Musterentwurf habe ich der Senatskanzlei und dem Staatsarchiv zugeleitet.

5.1.3 Novellierung des HmbSOG

In meinem 1. TB (Nr. 8.2, S. 60) hatte ich bereits darauf hingewiesen, daß es keine eindeutigen, hinreichend abgesicherten Befugnisnormen für die polizeiliche Informationsverarbeitung gibt. Dieses Regelungsdefizit hat sich bei meiner Kontrolltätigkeit im Berichtszeitraum an diversen Beispielen, auf die ich unter Nr. 3.10 eingegangen bin, bestätigt. Verschärft wird die Problematik durch die allem Anschein nach nicht mehr vermeidbare Einführung des neuen maschinenlesbaren Personalausweises ab 1.11.1984 (vgl. Nr. 3.8.2).

Die Behörde für Inneres hat erfreulicherweise die Notwendigkeit von gesetzlichen Regelungen für die polizeiliche Informationsverarbeitung akzeptiert und angekündigt, daß sie der Bürgerschaft Anfang 1984 einen Entwurf zur Novellierung des SOG zuleiten will, der entsprechende Vorschriften enthalten wird. Ich nehme das zum Anlaß, an dieser Stelle in aller Kürze den verfassungsrechtlichen Rahmen abzustecken, in den sich die Regelungen des SOG einpassen müssen, und die wichtigsten Punkte zu skizzieren, die aus datenschutzrechtlicher Sicht regelungsbedürftig sind.

Mit dem Anwachsen des polizeilichen Kontrollpotentials geht eine zunehmende Gefährdung des grundrechtlich geschützten Privatbereichs der Bürger einher. Auch wenn die hohe Mobilität vieler Straftäter und neue Formen organisierter Kriminalität zusätzliche personelle, organisatorische und technische Anstrengungen der Polizei erfordern, dürfen die Persönlichkeitsrechte der Bürger und der Schutz der demokratischen Freiheiten nicht vernachlässigt werden. Die einzelnen Maßnahmen polizeilicher Informationsbeschaffung und -verarbeitung müssen in diesem verfassungsrechtlichen Gesamtzusammenhang gesehen werden. Welche Maßnahmen nach Abwägung der Erfordernisse der inneren Sicherheit einerseits und des Persönlichkeitsschutzes andererseits zulässig

sind, kann nur vom Gesetzgeber entschieden werden. Der Umfang dieses parlamentarischen Gesetzesvorbehaltes bestimmt sich nach der Intensität, mit der die Grundrechtssphäre von polizeilichen Maßnahmen berührt ist. Es kann schon seit dem Mikrozensus-Beschluß (BVerfGE 27, 1) und dem Scheidungsaktenurteil (BVerfGE 27, 344) des BVerfG nicht mehr bezweifelt werden, daß es sich bei der polizeilichen Personenkontrolle sowie bei der Speicherung und Übermittlung von Informationen durch die Polizei um grundrechtsrelevante Eingriffe handelt. Deshalb erfordern diese Maßnahmen – wie die sonstigen polizeilichen Standardmaßnahmen (z. B. Durchsuchung von Personen oder Betreten von Wohnungen) auch – klar geregelte gesetzliche Befugnisnormen.

Der Rückgriff auf die polizeiliche Generalklausel (§ 3 SOG) kann solche nach Abwägung aller relevanten Gesichtspunkte konkretisierten Befugnisse nicht ersetzen. Zum einen enthält diese keine präzisen Begrenzungen polizeilicher Befugnisse. Zum anderen hat sich in der Vergangenheit deutlich gezeigt, daß die Generalklausel, die lediglich Maßnahmen gegen Störer im Falle einer konkreten Gefahr vorsieht, überstrapaziert wird, wenn alle von der Polizei für erforderlich gehaltenen Informationsverarbeitungsmaßnahmen unter sie subsumiert werden (vgl. „andere Personen", Suizidversuche etc., s. Nr. 3.10.5).

Auch ein Rückgriff auf das – subsidiär geltende – HmbDSG scheidet aus, denn §§ 9, 10 sind nur Auffangtatbestände, die spezielle Befugnisnormen für die Informationsverarbeitung im Polizeibereich nicht ersetzen können. Sie beziehen sich im übrigen nur auf die Informationsverarbeitung in Dateien, während eine Notwendigkeit für eine gesetzliche Regelung auch der Informationsverarbeitung in Akten besteht. Vordringlich ist die Schaffung klarer gesetzlicher Maßstäbe für die polizeiliche Informationserhebung (u. a. die polizeiliche Beobachtung), zumal die allgemeinen Datenschutzgesetze einen Erlaubnistatbestand für die Datenbeschaffung nicht enthalten. Nachfolgend skizziere ich kurz die Problemkomplexe, auf deren Lösung der Schwerpunkt der gesetzlichen Regelungen liegen sollte:

- Personenkontrollen:

  In unmittelbarem Zusammenhang mit dem Inkrafttreten des BPAG steht vor allem die Forderung, die Bestimmungen des Hamburgischen SOG über Personenkontrollen zu novellieren. Gerade im Hinblick auf die stark erweiterten technischen Möglichkeiten zur Kontrolle einer großen Anzahl von Personen, muß der Gesetzgeber klar formulieren, welche Arten der Personenkontrolle die Polizei unter welchen Voraussetzungen vornehmen darf. Entscheidend dabei ist die Konkretisierung des verfassungsrechtlichen Grundsatzes der Verhältnismäßigkeit.

  Ich begrüße es, daß die Überlegungen der Behörde für Inneres – soweit mir bekannt – nicht dahingehen, die entsprechenden Regelungen des Musterentwurfs für ein einheitliches Polizeigesetz des Bundes und der Länder einfach abzuschreiben, wie es die meisten anderen Bundesländer getan haben. Durch die §§ 9 ff des Musterentwurfs erhält die Polizei zusätzliche Befugnisse insbesondere zur vorbeugenden Verbrechensbekämpfung bereits im Vorfeld bestimmter Gefährdungen. Damit wird zugleich ein wichtiger Grundsatz des traditionellen Polizeirechts verlassen: der Grundsatz nämlich, daß sich Polizeimaßnahmen in erster Linie gegen sog. Störer zu richten haben. Vielmehr werden sehr viel stärker als bisher auch unbeteiligte Bürger dem Zugriff der Polizei ausgesetzt. Die Bedenken gegen diese erhebliche Ausweitung polizeilicher Befugnisse werden umso stärker, wenn gleichzeitig auch die technischen Möglichkeiten der Polizei nachhaltig verbessert werden. Umso wichtiger ist es, daß das SOG nicht nur nicht sämtliche Angebote des Musterentwurfs aufgreift, sondern zusätzliche Sicherungen schafft, wie es bislang allein der bremische Gesetzgeber versucht hat. Zur Identitätsfeststellung im Rahmen von Personenkontrollen gehört nach herkömmlichem Verständnis nicht nur die Feststellung der Identität einer unbekannten Person (etwa durch Vorlage von Personalpapieren) sondern auch die Feststellung, ob eine namentlich bekannte Person mit einer gesuchten identisch ist (Fahndungsabgleich). Auch die Voraussetzungen einer solchen Fahndungsüberprü-

fung sind im SOG – entsprechend den Voraussetzungen der Personenkontrollen – einschränkend zu regeln. Der Datenabgleich hat sich grundsätzlich auf den mit der Identitätsfeststellung verfolgten Zweck zu beschränken (d. h. z. B. kein routinemäßiger Fahndungsabgleich bei Verkehrskontrollen).

- Datenerhebung

  Die Polizei darf personenbezogene Daten nur erheben, wenn hierfür nicht nur eine gesetzliche Aufgabenumschreibung, sondern auch eine Befugnisnorm vorliegt. Nach dem Hamburgischen SOG kommt als Rechtsgrundlage z. Z. nur die polizeiliche Generalklausel in Betracht, die eine im Einzelfall bestehende Gefahr voraussetzt und die bei weitem nicht ausreicht, um die vorbeugende beobachtende Tätigkeit der Polizei zu rechtfertigen. Auch die Erhebung von Daten über andere Personen (insb. Nichtstörer) – vor allem auch im Rahmen einer Rasterfahndung – bedarf klarstellender gesetzlicher Regelungen.

- Erkennungsdienstliche Behandlung

  Die erkennungsdienstliche Behandlung als spezielle Form der Datenerhebung und -verarbeitung bedarf einer genaueren Regelung der Voraussetzungen in Bezug auf Nichtstörer und Unverdächtige. Fingerabdrücke, Fotografien und Messungen sind diskriminierend (Art. 1 Abs. 1 GG); sie sind deshalb nur als letztes Mittel einzusetzen. Für die Strafverfolgung bestimmt § 111 Abs. 3 StPO i. V. m. § 163b Abs. 2 S. 2 StPO, daß eine ed-Behandlung gegen den Willen des Nichtverdächtigen unzulässig ist. Im Rahmen vorbeugender Gefahrenabwehr sollten ed-Maßnahmen gegen den Willen der Person nur durchgeführt werden, wenn Angaben über die Identität verweigert wurden oder der Verdacht der Täuschung über die Identität begründet ist.

  Ferner sind die Voraussetzungen der Speicherung und Aufbewahrung von ed-Maßnahmen im einzelnen zu regeln. Als Zulässigkeitsvoraussetzung für die Speicherung kommt in Betracht, daß die Daten für die Dauer der Durchführung des Erkennungsdienstes oder wegen der Wiederholungsgefahr für weitere Straftaten gespeichert werden müssen.

  Die Vernichtung ist von Amts wegen durchzuführen, wenn die Voraussetzungen für die Speicherung entfallen sind (z. B. wenn die Identität inzwischen feststeht oder keine Wiederholungsgefahr besteht und das persönliche Interesse des Betroffenen , nicht ungerechtfertigt als potentieller Rechtsbrecher betrachtet zu werden, gegenüber dem öffentlichen Interesse an der Gefahrenabwehr überwiegt). Über das Recht, unter bestimmten Voraussetzungen die Vernichtung von ed-Unterlagen verlangen zu können, sollte der Betroffene bei Vornahme der Maßnahme belehrt werden.

Als weitere Komplexe, die mir dringend regelungsbedürftig erscheinen, sind aufzuzählen:

- Datenübermittlungen der Polizei (insbesondere Zusammenarbeit mit dem Verfassungsschutz),

- Löschungsregelungen sowie

- Auskunftsrechte für die Betroffenen (vgl. Nr. 3.9.2).

Nur wenn es gelingt, im Laufe des Jahres 1984 in die Landespolizeigesetze tragfähige und zugleich einschränkende Befugnisnormen für die polizeiliche Datenverarbeitung einzubauen, sind die Rahmenbedingungen für die Einführung des neuen Personalausweises gegeben. Die Landesregelungen haben sich allerdings auf den Bereich der polizeilichen Tätigkeit zur Gefahrenabwehr zu beschränken. Dringend erforderlich ist daneben die Regelung der Informationsverarbeitung im Bereich der Strafverfolgung durch den Bund.

5.2 Rechtsentwicklung im Bund

5.2.1 Spezifische Regelungen für den Sicherheitsbereich

Vorrangig für die Entwicklung des Datenschutzes auf Bundesebene sind zur Zeit – im Zusammenhang mit der geplanten Einführung des neuen Personalausweises – gesetzliche Regelungen für den Datenschutz im Sicherheitsbereich: also zum einen für die Informationsverarbeitung zu Strafverfolgungszwecken nach der StPO, des weiteren für die gefahrenabwehrende Tätigkeit der Polizeibehörden des Bundes. Polizeiorganisationen des Bundes (wie z. B. der Bundesgrenzschutz und das Bundeskriminalamt) dürfen nach der derzeitigen Rechtslage Personenkontrollen vornehmen, ohne daß irgendwelche näher bestimmten Voraussetzungen erfüllt sein müssen (vgl. § 17 Abs. 1 BGS-Gesetz, der über § 9 Abs. 3 BKA-Gesetz auch für das Bundeskriminalamt gilt). Diese Vorschriften sind dringend konkretisierungsbedürftig.

Die Strafprozeßordnung, die der Tätigkeit der Polizei auf dem Gebiet der Strafverfolgung zugrundeliegt, enthält zwar Regelungen über bestimmte Befugnisse (wie z. B. Identitätsfeststellung und ed-Maßnahmen), jedoch keine eingehenderen Regelungen zur generellen Informationsbeschaffung. Insbesondere enthält § 163 Abs. 1 StPO, wonach die Polizei Straftaten zu erforschen und alle keinen Aufschub gestattenden Anordnungen zu treffen hat, keine Befugniszuweisung, die eine gezielte Informationserhebung gestattet. § 163 StPO ist nach ganz herrschender Auffassung eine reine Aufgabenumschreibung, die nur Maßnahmen mit schlicht-hoheitlichen, nicht jedoch mit Eingriffscharakter abdeckt.

Die abweichende Auffassung, wonach § 163 Abs. 1 StPO – als strafprozessuale Generalklausel – die Polizei jedenfalls zu solchen Eingriffen ermächtigt, die ihrer Eingriffsintensität nach noch nicht die „Schwelle des Zwangscharakters" erreicht haben (sog. „Schwellen-Theorie"), wie es typischerweise bei den besonders geregelten Befugnissen in der StPO der Fall ist, ist nicht haltbar. Sie verkennt:
Eine solche Auslegung des § 163 StPO würde das in der StPO fein abgestimmte System von Strafverfolgungsmaßnahmen gegen Zeugen, Nichttatverdächtige, Tatverdächtige und Beschuldigte durchbrechen. Nach bisherigem Verständnis regelt die StPO abschließend, welche Maßnahmen gegen welchen der genannten Personenkreise zulässig sind. § 163 StPO läßt aber gerade offen, gegen welchen Personenkreis Eingriffsmaßnahmen erlaubt sind.
Auch im Bereich des Strafprozeßrechts bedarf es mithin noch ergänzender Regelungen.

5.2.2 Arbeitnehmerdatenschutz

Ebenso wichtig ist eine Verbesserung des Arbeitnehmerdatenschutzes. Das BDSG ist mit seinen viel zu allgemein gehaltenen Formulierungen nicht geeignet, den Arbeitnehmer vor überzogenen Informationsanforderungen des Arbeitgebers zu schützen. Hierzu bedarf es einer konkret auf die Besonderheiten des Arbeitsverhältnisses zugeschnittenen Regelung.

1. Vordringlich ist eine Bestimmung, die den Arbeitgeber auf die Verarbeitung solcher Daten beschränkt, die mit dem Arbeitsverhältnis zusammenhängen. Eine darüber hinausgehende Datenverarbeitung sollte auch mit Einwilligung des Arbeitnehmers nicht zulässig sein, da seine Entscheidungsfreiheit faktisch stark eingeschränkt ist (vgl. auch Nr. 4.8.4.3).

2. Ein wirksamer Schutz des Arbeitnehmers erfordert nicht nur eine bereichsspezifische Regelung der Verarbeitungsvoraussetzungen, sondern darüber hinaus die gesetzliche Absicherung der Mitbestimmungsrechte des Betriebsrats. Um jeden Zweifel an der Anwendung des § 87 Abs. 1 Nr. 6 BetrVG auf die mittelbare Überwachung auszuschließen (vgl. Nr. 4.8.4.1), ist diese Vorschrift so zu formulieren, daß die Einführung und der Ausbau von Personalinformationssystemen im weitesten Sinne, also auch solcher Verfahren, die zunächst nur abrechnungstechnischen Aufgaben dienen, der Mitbestimmung des Betriebsrats unterliegt.

3. BR und bDSB sind wegen ihrer sich überlagernden Kontrollaufgaben und Mitwirkungsrechte auf eine enge Zusammenarbeit angewiesen. Wegen des derzeitigen Bestellungsverfahrens und der organisatorischen Anbindung der bDSB an die Unternehmensleitung begegnen ihnen die BRe in aller Regel eher mißtrauisch. Deshalb – aber auch um die Stellung des bDSB zu stärken – sollten die Bestellung und die Abberufung des bDSB an die Zustimmung des Betriebsrats geknüpft werden und darüber hinaus die Kündigung des Arbeitsverhältnisses sowie die Abberufung aus der Funktion des bDSB vom Vorliegen eines wichtigen Grundes abhängig gemacht werden (vgl. Nr. 4.8.2.3).

5.2.3 Novellierung des BDSG

Die Datenschutzbeauftragten sind immer dafür eingetreten, das Datenschutzrecht vor allem bereichsspezifisch weiterzuentwickeln. Die Forderung, Sonderregelungen vor allem im Sicherheitsbereich, im Gesundheitswesen und für den Arbeitnehmerdatenschutz zu schaffen, ist nicht neu. Auf den vorhergehenden Seiten habe ich sie noch einmal begründet. Doch wird dadurch, daß der Gesetzgeber – wie ich hoffe – dieses Anliegen aufgreift, eine Überarbeitung des BDSG nicht entbehrlich. Auch wenn sich das BDSG im großen und ganzen in der Praxis bewährt hat, weist es gleichwohl erhebliche Mängel auf und ist es zunehmend ungeeigneter, Gefahren abzuwehren, die sich aus dem Einsatz neuer – bei Inkrafttreten des BDSG noch gar nicht bekannter oder jedenfalls noch nicht angewendeter – Techniken ergeben. Es besteht auch weitgehend Einigkeit darüber, daß das BDSG novellierungsbedürftig ist.

In dem seit Juni vorliegenden Referentenentwurf des Bundesinnenministers sehen die Datenschutzbeauftragten allerdings keinen geeigneten Beitrag zur Fortentwicklung des Datenschutzes, weil er

1. das geltende Datenschutzrecht teilweise verschlechtert,

2. hinter den bisherigen Entwürfen (CDU-Entwurf von 1980, SPD/FDP-Entwurf von 1980, Referentenentwurf von 1982) zurückbleibt,

3. wesentliche Forderungen der Datenschutzbeauftragten (Beschluß der Konferenz vom 21.6.1982) unberücksichtigt läßt und

4. den Anforderungen nicht gerecht wird, die sich aus der technischen Entwicklung ergeben.

Ich möchte mich jetzt nicht zu jeder einzelnen Vorschrift des Referentenentwurfs äußern und nicht jede Forderung erwähnen, die darin nicht berücksichtigt worden ist; aber ich fasse noch einmal zusammen, was ich an verschiedenen Stellen des Berichtes an kritischen Anmerkungen vorgebracht habe.

1. Unter Nr. 2.6.1 habe ich darauf hingewiesen,

   - daß der Dateibegriff neu definiert werden muß, um künftige, heute nicht voll absehbare Entwicklungen der DV-Technik einzufangen, ganz abgesehen davon, daß es richtiger wäre, die von Anfang an zu Unzuträglichkeiten führende Begrenzung der Anwendbarkeit des BDSG auf die dateigebundene Datenverarbeitung zu überwinden,

   - daß mit den in § 1 BDSG aufgezählten Phasen das Gesamtspektrum der Datenverarbeitung nicht abgedeckt ist,

   - daß den erhöhten Risiken, die mit dem direkten Zugriff Dritter auf automatisierte Dateien verbunden sind, durch strengere Anforderungen an die Zulassung von on-line-Anschlüssen Rechnung getragen werden muß.

Demgegenüber kehrt der Referentenentwurf zu einem viel zu starren Dateibegriff zurück, der auf Ordnungs- und Umordnungsfähigkeit abstellt, und gibt damit den noch im Vorjahr unternommenen Versuch, alle automatisierten Verfahren zu erfassen, wieder auf. Ebenso ärgerlich ist es, daß auch die Formulierung der Rückausnahme für Akten und Aktensammlungen im Entwurf 1982, die auf das Erschließen abstellte, durch eine engere Fassung (Auswerten) ersetzt worden ist.

Der neue Referentenentwurf verzichtet nicht nur auf die – im Vorjahr noch vorgesehene – Einbeziehung der Erhebung in den Anwendungsbereich des Gesetzes. Er läßt auch die „sonstige Nutzung" ungeregelt, so daß die besonderen Gefahren des Datenabgleichs, also der Verknüpfung von zuvor unabhängigen Dateien, weiterhin nicht hinreichend berücksichtigt werden.

Die Entscheidung über die Einrichtung eines automatisierten Verfahrens, das die Übermittlung durch Abruf ermöglicht, ist so bedeutsam, daß sie – jedenfalls im öffentlichen Bereich – durch Rechtssatz getroffen werden sollte. Es reicht nicht aus, daß die Festlegungen zu den Einzelheiten des Abrufverfahrens von den Beteiligten vereinbart werden, wie es der Referentenentwurf vorsieht.

2. Unter Nr. 4.5.1 habe ich eine Ergänzung des § 3 BDSG vorgeschlagen, durch die die Betroffenen vor Benachteiligungen bei Verweigerung der Einwilligung geschützt und die Widerruflichkeit der Einwilligung garantiert werden soll. Entsprechende Regelungen, die den Betroffenen davor bewahren wollten, wegen sozialer oder geschäftlicher Zwänge seinen eigenen Interessen zuwiderzuhandeln, hatte der Entwurf 1982 noch vorgesehen.

   Der Entwurf 1983 will statt dessen die Aufklärungspflicht auf die Fälle beschränken, in denen der Betroffene es verlangt. Dieser Vorschlag ist abzulehnen, da er die datenverarbeitenden Stellen zu der – irrigen – Auffassung verleiten könnte, die Wirksamkeit einer Einwilligung sei nicht mehr davon abhängig, daß den Betroffenen ihre Tragweite bekannt sei. Dieser Vorschlag dürfte i. ü. kaum mit der Zielsetzung vereinbar sein, die Datenverarbeitung für den betroffenen Bürger transparenter zu machen.

3. Kritische Anmerkung zur vorgesehenen Forschungsklausel habe ich unter Nr. 3.16.1 gemacht.

4. Die Datenschutzbeauftragten haben schon bei früheren Gelegenheiten gefordert, das Recht des Bürgers auf Auskunft, ohne das in aller Regel seine sonstigen Ansprüche nur auf dem Papier stehen, zu verstärken und deshalb auch für die Sicherheits- und Finanzbehörden das Abwägungsprinzip einzuführen. Ist schon das bestehende Auskunftsverweigerungsrecht problematisch, so kann der nunmehr vorgeschlagenen Befreiung von der Begründungspflicht, die die Position der Bürger weiter verschlechtert und das Verwaltungsverfahrensgesetz sowie die Rechtsprechung einiger Verwaltungsgerichte unterläuft, erst recht nicht zugestimmt werden (vgl. Nr. 3.9.2.4).

   Völlig unverständlich ist es auch, daß es im nicht-öffentlichen Bereich bei der Entgeltlichkeit der Auskunft, die nach allen bisherigen Vorschlägen aufgehoben werden sollte, bleiben soll. Hierfür gibt es keinen einleuchtenden Grund.

5. Zu den Kontrollbefugnissen der Datenschutzbeauftragten habe ich mich an mehreren Stellen des Berichts geäußert (Nrn. 1.1, 3.4.1.1, 3.9.1).

6. Auf die vorgesehene Neuregelung für die listenmäßige Datenübermittlung und den Wegfall des im Entwurf 1982 noch vorgesehenen Widerspruchsrechts bin ich unter Nr. 4.1.3.2 eingegangen.

7. Ferner verweise ich auf meine Vorschläge zur Verbesserung des Arbeitnehmerdatenschutzes (im Rahmen der §§ 23 und 24 BDSG) und zur Stärkung der Stellung des bDSB (im Rahmen des § 28 BDSG) unter Nr. 4.8.2.3.

Diese Hinweise mögen genügen, um die Ablehnung des neuen Referentenentwurfs aus dem Bundesinnenministerium durch die Konferenz der Datenschutzbeauftragten verständlich zu machen. Sie dürften darüber hinaus gezeigt haben, daß der Entwurf auch der eigenen Zielsetzung,

- im Interesse des betroffenen Bürgers praktische Verbesserungen im Datenschutz zu erbringen,

- das BDSG an die technologische Entwicklung auf dem Gebiet der Informationsverarbeitung anzupassen,

- zur Vereinheitlichung des Datenschutzes in der Bundesrepublik beizutragen und dem BDSG eine gewisse Schrittmacherfunktion auf diesem Rechtsgebiet zu erhalten und

- die Stellung des BfD zu verstärken sowie die Bedürfnisse der sonstigen Aufsichtsbehörden auszudehnen,

in keiner Weise gerecht wird.

Die öffentliche Diskussion zu den Themen Volkszählung, maschinenlesbarer Personalausweis, Personalinformationssysteme wie auch Bildschirmtext und andere neue Medien zeigt eine zunehmende Sensibilisierung zu Fragen des Datenschutzes. Vor diesem Hintergrund ist in der Öffentlichkeit die Erwartung entstanden, daß eine Novellierung des BDSG

- die bisher gewonnenen Erfahrungen sowie die neu aufgetretenen Probleme aufgreift und regelt und

- den Datenschutzinstanzen wirksamere Kontrollinstrumente an die Hand gibt.

Mit dem vorliegenden Referentenentwurf hat es der Bundesinnenminister indessen versäumt, den Datenschutz voranzubringen und die Befürchtungen der Bürger zu zerstreuen, wir trieben – zu Beginn des Orwell-Jahres – auf einer Woge der technischen Entwicklung dem Überwachungsstaat entgegen.

Hamburg, den 31.12.1983
Claus Henning Schapper

Anlage 1 (zu Nr. 3.8.4.1)
Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum Datenschutz im Personenstandswesen

1. Die Datenschutzbeauftragten begrüßen, daß – unbeschadet der Aufgabe der Länder (Artikel 83 GG), personenstandsrechtliche Vorschriften als eigene Angelegenheit auszuführen – Bund und Länder gegenwärtig gemeinsam prüfen, die in einer Verwaltungsvorschrift, der Dienstanweisung für die Standesbeamten und ihre Aufsichtsbehörden (DA), geregelten Mitteilungspflichten in einer Rechtsvorschrift zu verankern. Die Übermittlung personenbezogener Daten aus dem Bereich des Personenstandswesens stellt in der Regel einen Eingriff in die grundrechtlich geschützte Sphäre des Betroffenen dar und bedarf deshalb einer präzisen Rechtsgrundlage. Die Rechtsvorschrift sollte die einzelnen Datenübermittlungen konkret regeln. Allerdings darf sie sich nicht in einer bloßen Übernahme der DA erschöpfen.

2. Daher sollten die Bemühungen, die Mitteilungspflichten in einer Rechtsvorschrift zu verankern, mit einer Prüfung der Erforderlichkeit der bislang praktizierten Mitteilungen Hand in Hand gehen. Die Prüfung der Erforderlichkeit muß sich am Maß unabweislicher Bedürfnisse der Empfänger dieser Mitteilungen orientieren. Die insoweit maßgeblichen gesetzlichen Vorschriften müssen einer Überprüfung unterzogen werden, insbesondere im Hinblick auf ein gewandeltes Verständnis des verfassungsrechtlich garantierten Persönlichkeitsschutzes. Eine Reihe von Regelungen hat angesichts eines veränderten gesellschaftlichen Umfeldes und eines Wandels der Verwaltungsaufgaben ihren Sinn verloren.

3. Außerdem sollte darauf Bedacht genommen werden, daß

   - Datenübermittlungen den betroffenen Bürgern im Hinblick auf Inhalt, Adressat und zugrundeliegende Rechtsgrundlage transparent gemacht werden,

   - übermittelte Daten nur im Rahmen des Zwecks, zu dem sie übermittelt wurden, genutzt werden (Zweckbindung),

   - die notwendigen technisch-organisatorischen Maßnahmen der Datensicherung vorgesehen werden und

   - die Aufbewahrungsdauer, unter Berücksichtigung auch der Belange der Betroffenen, auf das erforderliche Maß beschränkt wird.

4. Vorbehaltlich weiterer eingehender Prüfungen empfehlen die Datenschutzbeauftragten schon jetzt:

   a) Das öffentliche Aufgebot sollte abgeschafft werden (§ 12 Ehegesetz, § 3 Personenstandsgesetz, §§ 127 f., insbesondere 135, 136 DA). Es erfüllt heute seinen ursprünglichen Zweck, Dritte zur Anzeige von Mängeln in der Ehefähigkeit der Verlobten und von Eheverboten zu veranlassen, nicht mehr.

   b) Die Pflicht des Standesbeamten, bei Eintragungen über alle umherziehenden Personen ohne festen Wohnsitz die Kriminalpolizei zu unterrichten (§§ 103 und 201 DA), muß gestrichen werden. Sie bedeutet eine pauschale Diskriminierung einer Personengruppe.

   c) Die Erhebung von Angaben über empfangene Versorgungsleistungen und deren Mitteilung an das Versorgungsamt (§§ 203 und 353 DA) sollte unterbleiben. Das Personenstandsgesetz enthält hierüber keine Rechtsgrundlage; auch ist im übrigen eine solche nicht ersichtlich. Es handelt sich schon bei der Erhebung dieser Angaben um Tätigkeiten, die mit den eigentlichen Aufgaben des Standesbeamten nichts zu tun haben.

5. Die Datenschutzbeauftragten empfehlen außerdem, Sterbeurkunden im Hinblick auf die übliche Vorlage solcher Urkunden bei Banken etc. von solchen Angaben zu entlasten, die mit detaillierten Orts- und Zeitangaben z. B. Hinweise darauf enthalten, daß der Verstorbene den Freitod gesucht hat (§ 336 DA). Solche Angaben bzw. der Rückschluß auf solche Fakten sind nicht erforderlich und durch das Personenstandsgesetz (§§ 37, 64 DA) nicht geboten. Hilfsweise sollte erwogen werden, zur Vorlage bei Banken etc. ein Papier zu schaffen, daß sich auf die für diesen Zweck notwendigen Daten beschränkt.

6. Angesichts der gegenwärtig zwischen den zuständigen Bundes- und Landesressorts geführten Diskussionen zu Fragen des Weges einer Unterrichtung der Meldebehörden über das Erlöschen des Verwandtschaftsverhältnisses bei Inkognito-Adoption Minderjähriger sind die Datenschutzbeauftragten der Ansicht, daß die DA eine Mitteilung des Standesbeamten über die Adoption an die Meldebehörde der leiblichen Eltern des adoptierten Kindes nicht vorsieht und nicht vorsehen sollte. Es sollte vermieden werden, daß – jedenfalls vom Standesbeamten – ein Informationsweg sowohl zur Meldebehörde des Annehmenden als auch zur Meldebehörde der bisherigen Verwandten führt. Die Datenschutzbeauftragten begrüßen die Auffassung, daß eine Mitteilungspflicht des Standesbeamten an die für den Wohnort der leiblichen Eltern zuständige Meldebehörde mit dem Offenbarungsverbot des § 1758 BGB nicht vereinbar wäre. Sie unterstützt das Vorhaben, dies in einer Rechtsvorschrift und in der DA (§ 98) klarer zum Ausdruck zu bringen.

Anlage 2 (zu Nr. 3.13.1.1)
Abgestimmte Stellungnahme der Landesbeauftragten für den Datenschutz zur „Anordnung über Mitteilungen in Strafsachen (MiStrA)" – Auszug –

I. Allgemeines

Die Landesbeauftragten und der Bundesbeauftragte sowie die Datenschutzkommission Rheinland-Pfalz haben bereits mit Beschluß vom 30.9.1980 zu der Anordnung über Mitteilungen in Strafsachen (MiStrA) Stellung genommen. Schwerpunkte dieses Beschlusses waren die Forderungen, die MiStrA so zu überarbeiten, daß nur noch die Vorschriften bestehen bleiben, für die eine gesetzliche Rechtsgrundlage besteht, oder andernfalls eine eindeutige gesetzliche Grundlage zu schaffen. Dabei sollte auch der Umfang der bisherigen Mitteilungspflichten reduziert werden.

Die Datenschutzbeauftragten begrüßen es, daß ein von den Justizverwaltungen eingerichteter Arbeitskreis die Anordnung über Mitteilungen in Strafsachen einer Überprüfung unterzogen hat.

Auf der Grundlage des vorgenannten Beschlusses ist zu dem vorliegenden Entwurf der Anordnung für Mitteilungen in Strafsachen (MiStrA) folgendes zu bemerken:

1. Mit Bedauern wird festgestellt, daß die im Beschluß genannten Forderungen und Anregungen nur zu einem geringen Teil aufgegriffen werden.

2. Eine Klärung der Frage steht noch aus, inwieweit für die Mitteilungen in Strafsachen bereits eine Rechtsgrundlage besteht oder ob eine weitergehende gesetzliche Grundlage geschaffen werden muß. Der Entwurf hält offensichtlich an der bisherigen Rechtsqualität als Verwaltungsvorschrift fest, ohne eine Begründung zu nennen, obwohl der Unterausschuß der Justizministerkonferenz selbst sich auf der Sitzung am 18. und 19. Mai 1981 für die Schaffung einer Rechtsgrundlage ausgesprochen hat. Weil derartige Mitteilungen für die Betroffenen einen Eingriff darstellen, bedürfen sie einer Rechtsgrundlage.

3. Der Grundsatz der Zweckbindung der Verwendung von Daten im Datenschutzrecht soll sicherstellen, daß Daten nur von denjenigen Stellen verwendet werden, die sie zur gesetzlichen Aufgabenerfüllung benötigen. Eine strenge Zweckbindung soll damit verhindern, daß Daten an andere Stellen gelangen und dort für andere als die ursprünglich vorgesehenen Zwecke Verwendung finden. Wegen der Sensibilität der aufgrund der MiStrA mitgeteilten Daten hat der Grundsatz der Zweckbindung besonderes Gewicht. Neben einer Regelung in Nr. 3 (vergl. die dortigen Anmerkungen) ist eine eindeutige Vorschrift in der MiStrA notwendig, die die Beachtung der Zweckbindung in allen Mitteilungsfällen sicherstellt.

4. Der vorliegende Entwurf sieht ohnehin eine Vielzahl von einzelnen Mitteilungsvorgängen vor. Eine Erweiterung dieses Katalogs durch relativ weitgehende Bestimmungen (vergl. Nr. 2 Abs. 2, Nr. 3 und Nr. 29) birgt die Gefahr in sich, daß die auf den Einzelfall bezogenen Regelungen und deren bewußte Beschränkungen umgangen werden. Damit wäre aber der Sinn der Einzelregelungen gefährdet, nämlich die mögliche Beeinträchtigung der durch Art. 1 Abs. 1 und Art. 2 Abs. 1 GG geschützten Persönlichkeitssphäre des Betroffenen zu begrenzen. Daher sollte die Neufassung eine abschließende Regelung der Mitteilungsvorgänge enthalten.

5. Im Hinblick auf die Auswirkungen, die die Mitteilungen für den Betroffenen haben können, sollten diese im Regelfall vom Richter oder Staatsanwalt veranlaßt werden. Nur in Fällen, in denen nach den Einzelregelungen kein Entscheidungsspielraum besteht, sollte die Geschäftsstelle zur Anordnung der Mitteilung befugt sein. Diese Umkehrung des im Entwurf und der geltenden Fassung der MiStrA enthaltenen Regel- und Ausnahmeverhältnisses drängt sich auch nach den Begründun-

gen des Arbeitskreises der Justizverwaltungen auf. Dieser Arbeitskreis lehnt bei einer Reihe von Bestimmungen eine Neuregelung deshalb ab, weil die Geschäftsstellen bei einem geänderten, dem Datenschutz aber eher Rechnung tragenden Vollzug überfordert wären.

6. Die Mitteilungen in Strafsachen sollen die zu benachrichtigenden Behörden in Kenntnis von den Vorgängen setzen, auf die sie im Rahmen des ihnen zugewiesenen Aufgabenbereichs zu reagieren haben. Ein strafrechtlich relevanter Sachverhalt läßt sich jedoch abschließend erst nach Abschluß des Strafverfahrens beurteilen. Damit den von den Mitteilungen Betroffenen nicht unnötige Nachteile entstehen, sollte der Grundsatz in der MiStrA ausdrücklich festgelegt werden, daß Mitteilungen erst nach rechtskräftigem Abschluß des Strafverfahrens erfolgen dürfen. Auch der Inhalt der Mitteilungen ist auf das im Einzelfall wirklich notwendige Mindestmaß zu beschränken. Das bedeutet, daß im Regelfall die Mitteilung der Tatsache einer Verurteilung unter Angabe der Straftat genügen wird. Ausnahmen hinsichtlich einer vorzeitigen Mitteilung oder eines umfangreicheren Inhalts der Mitteilungen müssen auf die Fälle beschränkt werden, in denen wegen der Bedeutung des möglicherweise verletzten Rechtsguts die begründete Annahme besteht, daß vorzeitige Maßnahmen veranlaßt sind oder die zu benachrichtigende Behörde nur aufgrund umfassenderer Kenntnis des dem Strafverfahren zugrundeliegenden Sachverhalts geeignete Maßnahmen treffen kann.

   Im einzelnen ist hier folgendes zu beachten:

   Soweit unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes Mitteilungen überhaupt erforderlich sind, sollten diese erst nach rechtskräftigem Urteil, das eine Verurteilung ausspricht, erfolgen. Diese Mitteilungen sollten sich entweder auf die Tatsache der Verurteilung oder auf den Abdruck des Urteilstenors beschränken.

   = Sollten Mitteilungen vorher erforderlich sein, dann dürfen diese grundsätzlich erst zum Zeitpunkt der Erhebung der öffentlichen Klage gemacht werden. Erst zu diesem Zeitpunkt ist bereits eine gewisse Erfolgsaussicht der Klage nach der Beurteilung des Staatsanwaltes anzunehmen. Diese vorzeitige Mitteilung kann nur dann veranlaßt sein, wenn begründete Anhaltspunkte vorliegen, daß die zu benachrichtigende Behörde Maßnahmen treffen muß, bevor das Verfahren abgeschlossen ist. Hierzu ist nur der Anklagesatz zu übermitteln. Keineswegs darf das wesentliche Ergebnis der Ermittlungen übersandt werden.

   = Mitteilungen über die Einleitung des Verfahrens sollten auf die wenigen Ausnahmefälle beschränkt bleiben, in denen begründete Anhaltspunkte vorliegen, daß die zu benachrichtigende Behörde sofortige Maßnahmen einleiten muß. Der Inhalt der Mitteilung ist auf die Formel des Strafvorwurfs zu beschränken.

     Gleiches gilt für Mitteilungen über den Erlaß eines Haftbefehls.

7. Der Betroffene ist grundsätzlich davon zu benachrichtigen, welchen Stellen Mitteilungen nach der MiStrA gemacht wurden. Von einer Benachrichtigung des Betroffenen kann ausnahmsweise nur dann abgesehen werden, wenn schwerwiegende Bedenken in der Person des Betroffenen entgegenstehen.

   Die Benachrichtigung könnte organisationstechnisch ohne großen Aufwand beispielsweise mit einem zusätzlichen Formblatt im Durchschreibeverfahren erfolgen. Wesentliche Kostenfolgen dürften damit wohl kaum verbunden sein.

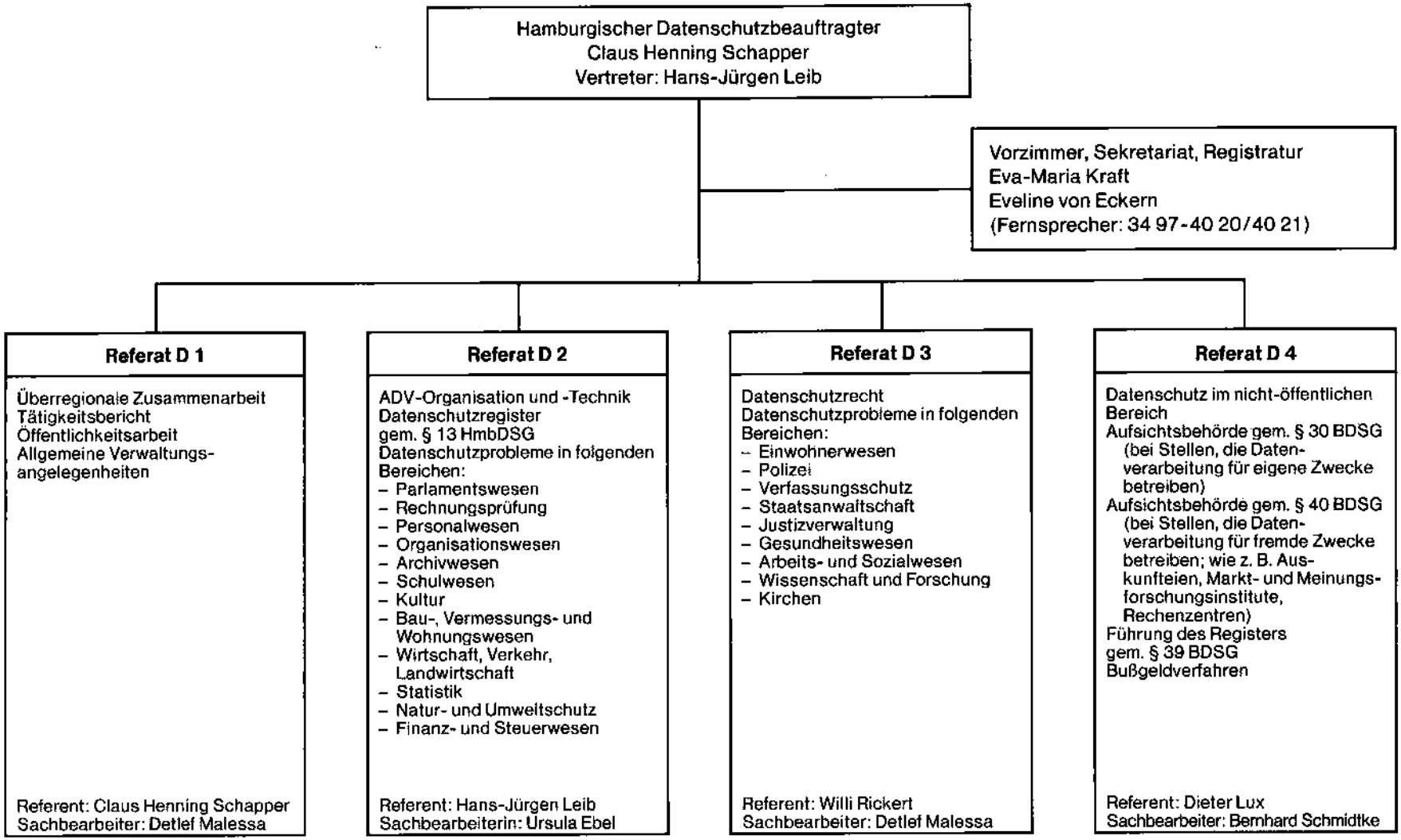
8. Die in der Mitteilung von Strafsachen liegenden Eingriffe sind auf das unbedingt erforderliche Maß zu begrenzen. Deshalb ist durch eindeutige Adressierung sicherzustellen, daß von diesen Mitteilungen nur die Personen in den zu benach-

richtigenden Behörden Kenntnis erlangen, welche diese Kenntnis zu ihrer Aufgabenerfüllung benötigen. (Beispielsweise sind Mitteilungen an den Leiter der Behörde oder die personalsachbearbeitende Stelle zu richten, wenn Mitteilungen öffentlich Bedienstete betreffen.) Außerdem sind derartige Mitteilungen in jedem Fall verschlossen zu versenden.

9. Die fahrlässige Begehung einer Straftat weist grundsätzlich auf ein geringeres Maß an strafrechtlicher Vorwerfbarkeit hin. Mitteilungen, die Fahrlässigkeitstaten betreffen, sollten daher grundsätzlich nicht im Rahmen der MiStrA mitgeteilt werden. Dies gilt insbesondere bei fahrlässigen Verkehrsstraftaten. Nur bei engem Bezug zur beruflichen Tätigkeit des von der Mitteilung Betroffenen und besonderem Gewicht des verletzten Rechtsguts sollten Ausnahmen gemacht werden. Die Prüfung, ob auch in diesen Fällen eine Mitteilung nicht erst nach rechtskräftigem Abschluß des Verfahrens erfolgen muß, sollte bei Fahrlässigkeitstaten besonders gründlich erfolgen.

10. Der Vollzug der Mitteilungen scheint nicht gleichmäßig zu erfolgen. Wegen der belastenden Wirkung, die die einzelnen Mitteilungen für die davon Betroffenen haben, entsteht hier eine nicht hinzunehmende Ungleichbehandlung. Möglicherweise ist diese Ungleichbehandlung ein Indiz dafür, daß manche Mitteilungspflichten als nicht mehr zeitgerecht empfunden werden; dies wäre ein Anlaß zu noch strengerer Prüfung der Erforderlichkeit.

Übersicht über die Organisation der Dienststelle des Hamburgischen Datenschutzbeauftragten



Nachtrag:
Ergänzende Anmerkungen nach Verkündung des BVerfG-Urteils zum Volkszählungsgesetz

1. Zu einer möglichen Volkszählung

Das Urteil des VerfG trifft eine Reihe von Feststellungen, die allgemein bei der Erhebung und Verarbeitung statistischer Daten zu beachten sein werden:
Anders als bei der Erhebung und Verarbeitung von Daten für den Verwaltungsvollzug kann bei der Datenerhebung für statistische Zwecke eine enge und konkrete Zweckbindung der Daten nicht verlangt werden, weil die Daten nach ihrer Aufbereitung für die verschiedensten, nicht von vornherein bestimmbaren Aufgaben verwendet werden sollen. Auch das strikte Verbot der Vorratsspeicherung gilt nicht für die statistische Datenerhebung und -verarbeitung.

Zum Ausgleich dafür, daß die Vielfalt der Verwendungs- und Verknüpfungsmöglichkeiten bei der Statistik nicht im voraus bestimmbar ist, sind an die Datenerhebung und -verarbeitung für statistische Zwecke besondere Anforderungen zu stellen:
- die Erhebung und Verarbeitung darf allein als Hilfe zur Erfüllung öffentlicher Aufgaben erfolgen,
- die Gefahr einer sozialen Abstempelung muß schon bei der Erhebung vermieden werden,
- es bedarf besonderer Vorkehrungen für Durchführung und Organisation zur Vermeidung einer Deanonymisierung, solange die Identifikationsmerkmale nicht gelöscht sind,
- es müssen Löschungsregelungen für die Identifikationsangaben getroffen werden,
- unverzichtbar ist schließlich eine wirksame Abschottung nach außen (Statistikgeheimnis).

Die Bundesregierung hat nach Verkündung des Urteils angekündigt, daß sie umgehend einen neuen Gesetzentwurf für eine Volkszählung vorlegen werde. Die Datenschutzbeauftragten werden darauf zu achten haben, daß der Entwurf den Anforderungen, die das Bundesverfassungsgericht in seinem Urteil aufgestellt hat, in wirksamer Weise entspricht:

Die Frage nach der Eigenschaft als Insasse einer Anstalt muß gestrichen werden.

Wenn der Gesetzgeber an der Erhebung des Haushaltszusammenhangs festhalten will, muß im Hinblick auf die damit in besonderen Fällen verbundene Gefahr der Diskriminierung dargetan werden, daß die Erhebung im überwiegenden Interesse der Allgemeinheit liegt und daß der Grundsatz der Verhältnismäßigkeit beachtet worden ist. Wenn dies nachgewiesen wird, muß die Erhebung des Haushaltszusammenhangs im Gesetz eindeutig geregelt werden.

Die Notwendigkeit, die Anschrift als Sachmerkmal und nicht nur als – möglichst frühzeitig zu löschendes – Indentifikationsmerkmal zu erheben, muß begründet und ggf. im Gesetz mit der notwendigen Klarheit geregelt werden.

Nach den Feststellungen des BVerfG liegen z. Z. zwar noch keine sicheren Erkenntnisse vor, die das Mittel der Totalerhebung schon jetzt als unverhältnismäßig erscheinen lassen. Der Gesetzgeber ist aber aufgefordert worden, die Methodendiskussion ständig zu verfolgen und aus einer Änderung der gegenwärtigen Anschauung die notwendigen Konsequenzen zu ziehen. Der vorgesehene Gesetzentwurf muß sich intensiv mit der Frage auseinandersetzen, ob angesichts der fortgeschrittenen Entwicklung der statistischen und sozialwissenschaftlichen Methoden eine Totalerhebung noch verhältnismäßig ist.

Das BVerfG hat erkennen lassen, daß es die gleichzeitige Durchführung von Melderegisterberichtigung und Volkszählung, in welcher Weise auch immer, für verfassungsrechtlich problematisch hält, weil „tendenziell Unvereinbares" miteinander verbunden wird. Wenn entgegen diesen Hinweisen an einer kombinierten Erhebung festgehalten werden soll, werden die dafür gegebenen Begründungen besonders sorgfältig zu prüfen und an den Maßstäben des BVerfG zu messen sein.

Das BVerfG hat die Weiterleitung von (noch nicht anonymisierten) statistischen Daten an andere Behörden für zulässig erklärt, wenn eine gesetzliche Ermächtigung vorliegt, die Daten für ausschließlich statistische Zwecke verwendet werden und in den empfangenden Behörden dieselben Vorkehrungen zum Schutze der Persönlichkeit (Statistikgeheimnis, Gebot der Anonymisierung) getroffen sind wie in den statistischen Ämtern. Ich werde mich dafür einsetzen, daß in Hamburg die Daten ausschließlich im Statistischen Landesamt ausgewertet werden.

Das BVerfG hat dem Gesetzgeber auferlegt, organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, die der Gefahr einer Verletzung der Persönlichkeitsrechte entgegenwirken. Der Gesetzgeber sollte die Chance wahrnehmen, nicht nur das Minimum ergänzender verfahrensrechtlicher Vorkehrungen zu treffen, die das BVerfG für unabdingbar hält, sondern darüber hinaus die Voraussetzungen zu schaffen, damit die Bevölkerung das für ein zuverlässiges Volkszählungsergebnis nötige Vertrauen faßt.

Eine aktuelle Aufgabe sehe ich in der Prüfung, ob das Hochschulstatistikgesetz den strengen Anforderungen des BVerfG standhält, insbesondere ob mit der zugelassenen Verwendung von Daten aus der Hochschulstatistik für Zwecke des Verwaltungsvollzugs tendenziell Unvereinbares miteinander verbunden wird und nicht wenigstens die Verwaltungsaufgaben präziser beschrieben werden müssen.

2. Zur Einführung des maschinenlesbaren Personalausweises

Das BVerfG hat in seinem Urteil Inhalt und Tragweite des im allgemeinen Persönlichkeitsrecht wurzelnden Grundrechts auf informationelle Selbstbestimmung näher definiert und ausgeführt, unter welchen Voraussetzungen es einschränkbar ist. Die dabei entwickelten Maßstäbe sind auch auf die Regelungen zur Einführung des neuen Personalausweises (vgl. dazu Nr. 3.8.2) anzuwenden. Sie geben den Forderungen der Datenschutzbeauftragten neue Aktualität und besonderes Gewicht. Nach dem Urteil des BVerfG kann jeder Bürger grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen. Dieses Recht darf nur nach Maßgabe der folgenden drei Voraussetzungen eingeschränkt werden:

- im überwiegenden Allgemeininteresse,
- auf einer gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben (Normenklarheit),
- im Rahmen der Verhältnismäßigkeit.

Die Beschränkung des informationellen Selbstbestimmungsrechts durch die Nutzung des neuen Personalausweises zur automatischen Erschließung sowie zur automatischen Einrichtung von Dateien, die nach dem BPAG in zwei Ausnahmefällen zugelassen ist, ist nach den vorstehenden Grundsätzen zu beurteilen:

- die generelle Erlaubnis, den Ausweis im nicht-öffentlichen Bereich zur automatischen Einrichtung von Dateien zu nutzen (vgl. Nr. 3.8.2.2.3), ist danach verfassungsrechtlich bedenklich;

- die Positionen der DSB zum Verbot der Protokollierung von Anfragen im Rahmen der polizeilichen Personenkontrollen (vgl. Nr. 3.8.2.2.1) sowie zum Ausschluß der Verwendung der Seriennummer durch die Polizei (vgl. Nr. 3.8.2.2.2) werden durch die Begründung des Urteils abgestützt.

Von unmittelbarer praktischer Bedeutung ist das Urteil auch für die zentralen Forderungen der Datenschützer nach flankierenden bereichsspezifischen Datenschutzregelungen im Polizei- und Strafverfahrensrecht (vgl. Nr. 3.8.2.1, 5.1.3, 5.2.1):

- Das BVerfG hat nunmehr in aller Deutlichkeit bekräftigt, ein Zwang zur Abgabe personenbezogener Daten – und darum geht es auch bei den polizeilichen Personenkontrollen mit Hilfe des Personalausweises – setzt voraus, „daß der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und die Angaben für diesen Zweck geeignet und erforderlich sind". Danach dürften keinerlei Zweifel darüber bestehen, daß die polizeilichen Personenkontrollen sowie die Verarbeitung personenbezogener Daten bei der Polizei eindeutiger und zugleich einengender Regelungen durch den Gesetzgeber bedürfen.

- Das BVerfG hat klargestellt, daß die Verwendung der Daten auf den gesetzlich bestimmten Zweck zu begrenzen ist. Angesichts der Gefahren der automatischen Datenverarbeitung ist ein amtshilfefester Schutz gegen Zweckentfremdung durch Weitergabe und Verwertungsverbote erforderlich. Daraus folgt, daß die bereichsspezifischen Vorschriften präzise und differenzierte Regelungen für die Übermittlung von Daten treffen müssen. Das gilt nicht zuletzt für den Informationsaustausch zwischen Polizei und Nachrichtendiensten.

- Große Bedeutung mißt das BVerfG ferner verfahrensrechtlichen Schutzvorkehrungen wie Aufklärungs-, Auskunfts- und Löschungspflichten zu. Daraus ergibt sich aus meiner Sicht, daß die bislang nach den Datenschutzgesetzen geltenden besonderen Beschränkungen der Auskunftsverpflichtung im Sicherheitsbereich beseitigt werden müssen (vgl. Nr. 3.9.2).

3. Zur Novellierung des BDSG

Die von den Datenschutzbeauftragten schon seit langem geforderte Novellierung des BDSG wird aufgrund der Ausführungen des BVerfG zum Schutz des Persönlichkeitsrechts unter den heutigen und künftigen Bedingungen der automatischen Datenverarbeitung noch dringlicher. Der Bundesinnenminister sollte allerdings den im Juni vorgelegten Referentenentwurf zurückziehen. Er ist keine geeignete Grundlage für die Fortführung der Diskussion.

Die Forderungen, die ich an verschiedenen Stellen des Berichts erhoben und die ich im Ausblick zusammengefaßt habe, sehe ich durch das Bundesverfassungsgericht bestätigt. An dieser Stelle möchte ich die Konsequenzen aufzeigen, zu denen das Volkszählungsurteil m. E. zwingt:

1. Die Erhebung und die „sonstige Verwendung" personenbezogener Daten müssen in den Anwendungsbereich der Datenschutzgesetze einbezogen werden.

2. Der Dateibegriff muß so weit gefaßt werden, daß er alle automatisierten Verfahren und alle Akten und Aktensammlungen umgreift, die mit Hilfe automatisierter Verfahren erschlossen werden können.

3. Ausnahmeregelungen für interne Dateien sind mit einem konsequenten Schutz der Betroffenen unvereinbar.

4. Der Betroffene ist in jedem Fall über die Tragweite seiner Einwilligung in die Datenverarbeitung sowie über die Rechtsgrundlage der Datenerhebung zu unterrichten, und zwar auch dann, wenn er dies nicht ausdrücklich verlangt.

5. Die Einführung von on-line-Übermittlungen ist im öffentlichen Bereich unter den Vorbehalt einer besonderen Rechtsvorschrift zu stellen.

6. Die Zweckbindung der Daten muß dadurch verstärkt werden,

   - daß die Datenweitergabe innerhalb derselben Behörde grundsätzlich den gleichen Einschränkungen unterworfen werden muß wie die Datenübermittlung an andere öffentliche Stellen,

   - daß bei der Datenübermittlung an andere öffentliche Stellen die Verantwortung der übermittelnden Stelle ungeschmälert bleiben muß,

   - daß bei der Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs der Empfänger die Daten nur für den Zweck verwenden darf, zu dessen Erfüllung sie ihm übermittelt wurden.

7. Das Recht des Bürgers auf Auskunft über seine Daten darf nicht eingeschränkt, sondern muß verstärkt werden. Es muß gegenüber allen Behörden bestehen, grundsätzlich auch gegenüber den Sicherheits- und Finanzbehörden.

8. Die Kontrollbefugnis der Datenschutzbeauftragten umfaßt die Einhaltung der Datenschutzgesetze und aller anderen Datenschutzvorschriften unabhängig davon, ob Daten in Dateien, in Akten oder in sonstiger Form festgehalten werden.
   Die Datenschutzbeauftragten haben das Recht, uneingeschränkt alle Akten einzusehen, die mit der Verarbeitung personenbezogener Daten in Zusammenhang stehen.
   Besondere Geheimhaltungsvorschriften können ihnen bei ihrer Tätigkeit nicht entgegengehalten werden.

Das Urteil des BVerfG gibt schließlich auch Veranlassung, die Vorschriften des 3. und 4. Abschnitts des BDSG zu überprüfen, die die Datenverarbeitung nicht-öffentlicher Stellen regeln. In der Begründung des Urteils heißt es u. a., daß mit dem Recht auf informationelle Selbstbestimmung eine Gesellschaftsordnung und eine Rechtsordnung nicht vereinbar wären, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.

Eine Reihe von Vorschlägen habe ich im Bericht gemacht, nur zwei Forderungen seien stichwortartig hinzugefügt: die Erweiterung des Umfangs der Benachrichtigungs-und Auskunftspflichten sowie die Erteilung kostenfreier Auskünfte auch im nicht-öffentlichen Bereich.