BÜRGERSCHAFT
DER FREIEN UND HANSESTADT HAMBURG

Drucksache 13/3308

13. Wahlperiode

17.02.89

Der Hamburgische Datenschutzbeauftragte

An die
Frau Präsidentin der Bürgerschaft

Betr.: Siebenter Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten

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

Dem Senat leite ich meinen Tätigkeitsbericht gleichzeitig zu.

Schapper

* Verteilt nur an die Abgeordneten der Bürgerschaft

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

Siebenter Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten

Zugleich Tätigkeitsbericht der Aufsichtsbehörde für den nicht-öffentlichen Bereich

vorgelegt zum 1. Januar 1989

Herausgegeben vom Hamburgischen Datenschutzbeauftragten
Claus Henning Schapper
Baumwall 7 · 2000 Hamburg 11 · Tel.: 349 12 20 44

Druck: Lütcke & Wulff, Hamburg 1

GLIEDERUNG

Seite

1.	**Zur Lage des Datenschutzes**	1
1.1	**Einige Anmerkungen zur Novellierung des Bundesdatenschutzgesetzes und des Bundesverfassungsschutzgesetzes**	1
1.2	**Nochmals: Zum Übergangsbonus**	2
1.3	**Zur Novellierung des HmbDSG**	2
1.4	**Verhältnis zur Verwaltung**	6
2.	**Entwicklung der Dienststelle**	8
2.1	**Ausstattung**	8
2.2	**Eingaben**	9
3.	**Beobachtung der automatisierten Datenverarbeitung**	9
3.1	**Umsetzung und Fortentwicklung von ADV-Richtlinien**	9
3.1.1	Bereich der zentralen ADV-Verfahren	9
3.1.2	Bereich der dezentralen Verfahren	10
3.2	**Risiken der Benutzung von Datex-P**	11
3.3	**Verarbeitung personenbezogener Daten im Rechenzentrum der Universität Hamburg**	12
3.3.1	Aufgaben und Einbindung des Rechenzentrums	12
3.3.2	Sicherungsmaßnahmen	12
3.3.3	Verarbeitung personenbezogener Daten	13
3.3.4	Forderungen/Anregungen	14
3.4	**Schriftgutvernichtung**	14
3.5	**Neue Medien**	15
3.5.1	Rundfunkfinanzierungsstaatsvertrag	15
3.5.1.1	Datenerhebung	16
3.5.1.2	Speicherung	16
3.5.1.3	Übermittlung	16
3.5.1.4	Löschung	17
3.5.1.5	Datenverarbeitung im Auftrag	17
3.5.2	Telekommunikation	17
3.5.2.1	Poststrukturgesetz	18
3.5.2.2	Gefahr der Dreiteilung des Datenschutzes	19
3.5.2.3	Parlamentsvorbehalt	20
3.5.2.4	Anforderungen an die Bestimmtheit von Verordnungsermächtigungen	21
3.5.2.5	Materielle Anforderungen an bereichsspezifische Regelungen	21
3.5.2.6	Sozialer Zwang muß vermieden werden	23
3.5.2.7	Unzureichende Bindungswirkung der Telekommunikationsordnung (TKO) für private Dienstanbieter	23
3.5.2.8	Zuständigkeit von Bund und Ländern	24
3.5.2.9	Einschränkung des Post- und Fernmeldegeheimnisses bei neuen Medien?	25
3.6	**Datenschutzrechtliche Rahmenbedingungen für die Arbeit von Medienarchiven**	25
3.6.1	Problemstellung	25

3.6.2	Technisierung und Automatisierung der Archive	26
3.6.3	Nutzung der Archive für andere als "eigene publizistische Zwecke"	27
3.6.4	Forderungen für die Novellierung des BDSG	28
3.6.5	Fazit	31
4.	**Einzelne Probleme des Datenschutzes im öffentlichen Bereich**	31
4.1	**Sozialwesen**	31
4.1.1	Akteneinsichtsrecht eines Deputierten der BAJS	31
4.1.2	Modellversuch im Rahmen des § 372 RVO	33
4.1.3	Einmalige Leistungen gem. § 21 BSHG	34
4.1.4	Amtspflegschaft und Amtsvormundschaft bei nichtehelichen Kindern	35
4.1.5	Verwendung der Rentenversicherungsnummer beim Zeitschriftenversand der AOK Hamburg	35
4.1.6	Projekt Sozialhilfe-Automation (PROSA)	36
4.1.7	Durchführung des Bundeserziehungsgeldgesetzes	38
4.1.8	Namentlicher Aufruf in den Sozialdienststellen der Bezirksämter	39
4.1.9	Maßnahmen zur Datensicherheit beim Versand besonders geschützter Sozialdaten	40
4.1.10	Prüfung im Bezirksamt Wandsbek	40
4.1.11	Einsatz eines dialogorientierten ADV-Systems im Landesbetrieb "Winterhuder Werkstätten"	42
4.1.12	Offenbarung von Sozialdaten auf Überweisungsträgern	42
4.2	**Personalwesen**	43
4.2.1	IuK-Projekte in der Personalverwaltung	43
4.2.2	Einsicht in Personalakten durch zukünftige Vorgesetzte	45
4.2.3	Bewerber- und Personalfragebögen	46
4.2.4	Aufbewahrung von Bewerbungsunterlagen	48
4.2.5	Ortszuschlag	49
4.2.6	Sicherheitsrichtlinien	50
4.3	**Statistik**	51
4.3.1	Landesstatistikgesetz	51
4.3.2	Volkszählung 1987	51
4.3.2.1	Automatisiertes Erinnerungs- und Mahnverfahren	52
4.3.2.2	Datenverarbeitungskonzept	53
4.3.2.3	Auftragsdatenverarbeitung in Nordrhein-Westfalen	54
4.3.2.4	Zeitpunkt der Vernichtung der Erhebungsunterlagen	55
4.3.2.5	Resümee	55
4.3.3	Hochschulstatistik	57
4.4	**Archivwesen**	58
4.5	**Schulwesen**	60
4.5.1	Berichte über Kinder in Vorschulklassen	60
4.5.2	Einsatz von Personalcomputern in der Schulverwaltung	61
4.6	**Automation des Gewerberegisters**	62
4.7	**Umweltschutz**	63
4.7.1	Veröffentlichung von Meßergebnissen aus der Überwachung von Gewerbebetrieben	63

4.7.2 Erlaß von Regelungen zur Durchführung des Datenschutzes im Bereich der Gesundheits- und Umweltämter ... 66
4.8 **Bauwesen** ... 66
4.8.1 Wohnraumdatei ... 66
4.8.2 Befragung im Harburger Binnenhafen ... 70
4.9 **Steuerwesen** ... 72
4.9.1 Fortdauer bzw. Erledigung alter Probleme ... 72
4.9.2 Änderungen des § 31 der Abgabenordnung (AO) ... 73
4.9.3 Auskunftsersuchen an Arbeitgeber zum Nachweis angeblicher Bewerbungskosten ... 74
4.9.4 Innenrevision im Bereich der OFD Hamburg und Bestimmungen über das Zeichnungsrecht in den Finanzämtern ... 75
4.9.5 Übermittlung von Lohnsteuerkarten an kirchliches Rechenzentrum ... 76
4.10 **Einwohnerwesen** ... 78
4.10.1 Ausländerzentralregister ... 78
4.10.2 Personenstandswesen ... 80
4.10.3 Online-Anschluß der Polizei an das Melderegister ... 82
4.10.4 Novellierung des Melderechtsrahmengesetzes ... 82
4.11 **Polizei** ... 84
4.11.1 Anforderungen an ein neues Polizeirecht ... 84
4.11.2 Einsatz von Personalcomputern ... 87
4.11.3 Bildaufzeichnungen durch Polizei und Verfassungsschutz ... 87
4.11.4 Polizeieinsatzzentrale ... 88
4.11.4.1 Beschreibung von HELP ... 88
4.11.4.2 Bewertung von HELP ... 89
4.11.5 Datenverarbeitung beim polizeilichen Staatsschutz ... 91
4.11.5.1 Bisherige Konsequenzen aus der Datenschutzkontrolle bei der Fachdirektion 7 ... 91
4.11.5.2 Speicherung von Volkszählungsgegnern ... 92
4.11.6 Löschung von Daten über Suizidversuche ... 92
4.11.7 Polizei in der Zentralambulanz für Betrunkene (ZAB) ... 92
4.12 **Novellierung des Bundesverfassungsschutzgesetzes** ... 93
4.12.1 Informationsverarbeitung ... 93
4.12.2 Nachrichtendienstliche Mittel ... 95
4.12.3 Trennungsgebot ... 95
4.12.4 Auskunft ... 96
4.13 **Justiz** ... 96
4.13.1 Stand der Gesetzgebung ... 96
4.13.2 Technikeinsatz ... 97
4.13.2.1 Datenverarbeitung in den Verwaltungen des Landgerichts und des Arbeitsgerichts ... 97
4.13.2.2 Prüfung der Datenverarbeitung beim Verwaltungsgericht ... 97
4.13.2.3 Personalcomputer für Richter ... 99
4.13.3 Telefonüberwachung gem. § 100a StPO ... 100
4.13.4 Erstellung eines zentralen privaten Handelsregisters ... 104
4.13.5 Gerichtsvollzieher ... 105

4.13.6 Einsicht in Justizakten zu Forschungszwecken ... 105
4.13.7 Veröffentlichung von Entmündigungsentscheidungen ... 106
4.13.8 Versendung amtsgerichtlicher Entscheidungen ... 107
4.14 **Wissenschaft und Forschung** ... 107
4.14.1 Erhebung von Studentendaten ... 107
4.14.2 Einzelne Forschungsprojekte ... 108
4.14.3 Gentechnologie ... 109
4.15 **AIDS** ... 110
4.15.1 HIV-Tests im Krankenhaus ... 110
4.15.2 HIV-Tests beim staatlichen Blutspendedienst ... 111
4.15.3 AIDS-Beratungsstellen der Gesundheitsämter ... 112
4.15.4 AIDS in polizeilichen Informationssystemen ... 113
4.16 **Gesundheitswesen** ... 114
4.16.1 Gesetzliche Grundlagen ... 114
4.16.1.1 Gesundheitsreformgesetz ... 114
4.16.1.2 Hamburgisches Krankenhausgesetz ... 115
4.16.1.3 Hamburgisches Maßregelvollzugsgesetz und Änderung des Gesetzes über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten ... 115
4.16.1.4 Änderung des Krebsregistergesetzes ... 116
4.16.2 Gesundheitsämter ... 117
4.16.3 Prüfung der Blutspenderverwaltung des Zentralinstituts für Transfusionsmedizin 119

5. Einzelne Probleme des Datenschutzes im nicht-öffentlichen Bereich ... 121
5.1 **Versandhandel/Interne Bonitätsprüfung** ... 121
5.2 **Kreditwirtschaft/SCHUFA** ... 121
5.2.1 Neues SCHUFA-Verfahren: kartellrechtliche Entwicklung ... 121
5.2.2 Erschleichen von SCHUFA-Auskünften ... 122
5.2.3 Identitätsprüfung und Verbreitungsverbot von SCHUFA-Daten bei nicht feststehender Identität ... 123
5.2.4 Löschen von Anfragen bei der SCHUFA ... 125
5.3 **Automatisierung des Zahlungsverkehrs - Zur Wirksamkeit der Sonderbedingungen für die Benutzung von ec-Geldautomaten** ... 125
5.4 **Versicherungswirtschaft** ... 132
5.4.1 Zentrale Dateien der Versicherungsverbände ... 132
5.4.1.1 Sonderwagnisdatei der Lebensversicherer ... 132
5.4.1.2 Zentrale Registrierstelle Rechtsschutz ... 135
5.4.1.3 Meldeverfahren der Kraftfahrzeug-Versicherer ... 136
5.4.1.4 Meldeverfahren der Unfallversicherer ... 145
5.4.1.5 Sachschadendatei ... 146
5.4.2 Einwilligungsklausel nach dem BDSG ... 150
5.4.3 Schweigepflichtentbindungsklausel ... 151
5.5 **Handels- und Wirtschaftsauskunfteien** ... 152
5.5.1 Automation bei Auskunfteien und neue Serviceleistungen ... 152
5.5.1.1 On-line-Verfahren bei Handelsauskunfteien ... 152
5.5.1.2 Marketing-Dienste der Handelsauskunfteien ... 155
5.5.2 Verbindung zwischen Inkasso- und Auskunfteiverkehr ... 156

5.6	**Arbeitnehmerdatenschutz**	158
5.7	**Sonstige Probleme**	160
5.7.1	Telefonmarketing	160
5.7.1.1	Darstellung und Abgrenzung	160
5.7.1.2	Datenschutzrechtliche Bewertung	161
5.7.2	Zusammenarbeit zwischen Vermietern und Auskunfteien	163
5.7.3	Zur datenschutzrechtlichen Kontrolle von Detekteien	164
5.7.4	Auskunftspflicht einer datenverarbeitenden Stelle im nicht-öffentlichen Bereich bei Anfragen von Strafverfolgungsbehörden	166

1. Zur Lage des Datenschutzes

1.1 Einige Anmerkungen zur Novellierung des Bundesdatenschutzgesetzes und des Bundesverfassungsschutzgesetzes.

Wieder einmal hat die Bundesregierung ein Paket mit Datenschutz- und Sicherheitsgesetzen beschlossen und zunächst einmal dem Bundesrat zur Stellungnahme zugeleitet. Vor drei Jahren hatten die wenigen Monate, die bis zum Ende der 10. Wahlperiode des Bundestages für die Beratung noch zur Verfügung standen, den Koalitionspartnern nicht ausgereicht, ihre Differenzen insbesondere über das Zusammenarbeitsgesetz (ZAG) auszuräumen und die Gesetzentwürfe über die parlamentarischen Hürden zu bringen. Auch diesmal ist völlig ungewiß, ob die Koalitionspartner sich noch einigen können. Die FDP-Minister haben vor der Kabinettsentscheidung eine mehrere Seiten lange Erklärung zu Protokoll gegeben, in der Vorbehalte und Wünsche des FDP-Präsidiums enthalten sind. Es handelt sich um eine Auflistung von — aus der Sicht der FDP — notwendigen Verbesserungen und noch erörterungsbedürftigen Punkten.

Mit ihrer Liste hat die FDP einige der von den Datenschutzbeauftragten geltend gemachten Forderungen und Bedenken aufgegegriffen. Wir können nur hoffen, daß die FDP möglichst viele ihrer Anliegen durchsetzt. Aber selbst wenn alle ihre Verbesserungsvorschläge berücksichtigt werden, bleiben Zweifel, ob die Gesetzentwürfe den verfassungsrechtlichen Anforderungen genügen.

Zur beabsichtigten Novellierung des Bundesdatenschutzgesetzes ist festzustellen, daß der Regierungsentwurf im wesentlichen die gleichen Mängel aufweist wie der in der 10. Legislaturperiode des Deutschen Bundestages vorgelegte Entwurf. Die Empfehlungen der Datenschutzbeauftragten sind leider ebensowenig berücksichtigt worden wie die zwischenzeitlich von einigen Bundesländern (Hessen, Bremen, Nordrhein-Westfalen) erlassenen, in wesentlichen Punkten vorbildlichen Neuregelungen. Es ist insbesondere verfehlt, das allgemeine Datenschutzrecht aufzusplitten in ein streng auf die Datenverarbeitung in Dateien bezogenes Bundesdatenschutzgesetz und ein den Datenschutz in Akten regelndes Verwaltungsverfahrensgesetz, das weite und wichtige Verwaltungsbereiche (z.B. Finanzverwaltung und Sozialverwaltung) ebensowenig erfaßt wie die Strafverfolgung und dessen Einhaltung sich überdies weitgehend der Datenschutzkontrolle entzieht.

Auch die in der Begründung des Regierungsentwurfs genannten Ziele der beabsichtigten Weiterentwicklung des Bundesdatenschutzgesetzes werden nicht erreicht:

— Die Anpassung an die Grundsätze des Urteils des Bundesverfassungsgerichts zum Volkszählungsgesetz ist in mehrfacher Hinsicht nicht gelungen: So enthält der Entwurf keine ausdrückliche Regelung der Datenerhebung, obwohl gerade diese den Bürger unmittelbar belastet; die geplante Regelung im Verwaltungsverfahrensgesetz reicht nicht aus. Auch erfährt der Grundsatz der Zweckbindung zu weitgehende Ausnahmen und die Transparenz der Datenverarbeitung, insbesondere das Recht des Betroffenen auf Auskunft, bleibt hinter den verfassungsrechtlichen Anforderungen zurück.

— Auch dem technologischen Fortschritt auf dem Gebiet der Informations- und Kommunikationstechnik (z.B. Arbeitsplatzcomputer, neue optische Speichermedien, Videoaufzeichnungen, Telekommunikation und Vernetzung) wird der Entwurf nicht gerecht. Der nicht entscheidend veränderte Dateibegriff und die Beibehaltung des bisherigen Katalogs technischer und organisatorischer Datensicherungsmaßnahmen vernachlässigen die technische Entwicklung.

— Die Kontrollbefugnis des Bundesbeauftragten für den Datenschutz wird insgesamt eingeschränkt, insbesondere durch den Ausschluß systematischer Kontrollen bei der Erhebung und Verwendung personenbezogener Informationen außerhalb von Dateien. Keinesfalls kann eine Einschränkung der Kompetenz der Landesbeauftragten durch den Bundesgesetzgeber hingenommen werden.

— Die Datenschutzvorschriften für den nicht-öffentlichen Bereich orientieren sich nicht an dem Grundsatz der Zweckbindung und räumen unvertretbare Verarbeitungsprivilegien ein.

Der Entwurf entspricht daher nicht den Erwartungen an ein zeitgemäßes Datenschutzrecht als Ausprägung des verfassungsrechtlich garantierten Rechts des Bürgers auf informationelle Selbstbestimmung. Ausführliche Anmerkungen zur Novellierung des BDSG finden sich im 4. Tätigkeitsbericht (4. TB, 6.1, S. 157 ff.) und im 6. Tätigkeitsbericht (6. TB, S. 1 ff.). Hierauf kann ich mich auch heute noch weitgehend beziehen.

Zur beabsichtigten Neufassung des Bundesverfassungsschutzgesetzes (BVerfSchG) habe ich unter 4.12 Stellung genommen.

1.2 Nochmals: Zum Übergangsbonus

Sollte das Paket mit den Datenschutz- und Sicherheitsgesetzen erneut im Bundestag scheitern, wären die Folgen insbesondere für die betroffenen Sicherheitsbehörden dramatisch. Nach — soweit ich sehe — übereinstimmender Auffassung in der Literatur und einer sich verfestigenden Rechtsprechung ist der Übergangsbonus, den der Gesetzgeber für die Schaffung gesetzlicher Grundlagen für die Informationstätigkeit beispielsweise der Polizei und der Nachrichtendienste in Anspruch nehmen kann, spätestens mit dem Ende dieser Wahlperiode des Bundestages verbraucht. Das bedeutet, daß ab 1991 Grundrechtseingriffe der Sicherheitsbehörden, die sich weiterhin nicht auf die erforderlichen bereichsspezifischen gesetzlichen Grundlagen stützen könnten, wegen fehlender verfassungsrechtlicher Legitimation als rechtswidrig angesehen werden müßten mit der Folge etwa, daß gleichwohl gespeicherte Daten gelöscht und dazugehörige Unterlagen vernichtet werden müßten.

Schon heute ist absehbar, daß zahlreiche Gesetze, die als Grundlage für Informationseingriffe von Sicherheitsbehörden unabdingbar sind, bis zum Ende dieser Legislaturperiode nicht verabschiedet werden. Das gilt z.B. für das Gesetz über das Bundeskriminalamt und das Gesetz über das Ausländerzentralregister, für die bislang erst — kaum als Diskussionsgrundlage geeignete — Arbeitsentwürfe vorliegen, aber auch für die notwendigen Änderungen der Strafprozeßordnung, für die der Bundesjustizminister erst vor einigen Wochen einen Referentenentwurf versandt hat. Die Bundesregierung hat selbst eingeräumt (in Beantwortung einer Großen Anfrage des SPD-Bundestagsfraktion), daß es ihr nicht mehr möglich sein wird, eine Vorlage zur Novellierung der StPO noch rechtzeitig im Bundestag einzubringen. Das heißt, daß derselbe Bürger, dessen Antrag auf Löschung seiner Daten in der Zentralen Namenskartei der Staatsanwaltschaft Frankfurt das OLG Frankfurt durch Beschluß vom 14. Juli 1988 zurückgewiesen hatte, im Jahre 1991 seinen Antrag mit Erfolg wiederholen kann. Eben dies hat ihm das OLG Frankfurt in der Begründung seiner Entscheidung bescheinigt. Hiernach wird auch ein Hamburger Bürger nicht mehr hinnehmen müssen, daß seine Daten über das Jahr 1990 hinaus in der Zentralkartei der hiesigen Staatsanwaltschaft gespeichert bleiben.

1.3 Zur Novellierung des HmbDSG

Das Berichtsjahr wurde mitgeprägt durch die Diskussion über die Novellierung des Hamburgischen Datenschutzgesetzes. Schon im letzten Tätigkeitsbericht habe ich darauf hingewiesen, daß gegen die Konzeption des von der Justizbehörde vorgelegten Entwurfs von mir keine grundlegenden Einwendungen zu erwarten sind. Er bietet die Chance, das Datenschutzrecht unter Verarbeitung der Impulse, die insbesondere die Rechtsprechung des Bundesverfassungsgerichts gegeben hat, angemessen, d.h. der Bedeutung des Grundrechts auf informationelle Selbstbestimmung entsprechend, fortzuentwickeln. Besonders hervorzuheben ist, daß der Anwendungsbereich des Gesetzes sich künftig auch auf die Datenverarbeitung in Akten erstrecken wird. Die Beschränkung auf die in Dateien gespeicherten Daten soll aufgegeben werden. Sie hat in der Vergangenheit verschiedentlich Anlaß zu Irritationen gegeben und die Neuregelung war verfassungsrechtlich geboten, da jede Datenverarbeitung — unabhängig von

der Verarbeitungsform — einen Eingriff in grundgesetzlich geschützte Rechtspositionen darstellt und deshalb einer gesetzlichen Ermächtigungsnorm bedarf.

Trotz dieser positiven Grundtendenz des Gesetzentwurfes komme ich nicht umhin festzuhalten, daß die Vorstellungen der Justizbehörde teilweise deutlich hinter früheren Entwürfen wie dem — von Hamburg mitgetragenen — Entwurf der SPD-geführten Länder für ein neues Bundesdatenschutzgesetz (vgl. Bundesrats-Drucksache 121/86 vom 28.2.1986) sowie hinter den neuen Datenschutzgesetzen der Länder Bremen, Nordrhein-Westfalen und Hessen zurückbleiben.

Ein modernes Datenschutzrecht hat sich im wesentlichen daran messen zu lassen, inwieweit es dem durch die Rechtsprechung des Bundesverfassungsgerichts geprägten Verfassungsverständnis vom allgemeinen Persönlichkeitsrecht entspricht und den diesem Recht durch die Möglichkeiten der Datenverarbeitung drohenden Gefahren wirksam begegnet. Dabei kommen der Ausgestaltung der Rechte der Betroffenen sowie der Unabhängigkeit des Datenschutzbeauftragten eine besondere Bedeutung zu. Schließlich muß das Datenschutzrecht wenigstens den gegenwärtigen technischen Möglichkeiten und — so weit wie möglich — der unverändert dynamischen Entwicklung der Datenverarbeitungstechnik Rechnung tragen.

Gemessen an diesen Vorgaben ist der vorgelegte Gesetzentwurf (trotz aller positiven Ansätze) noch verbesserungsfähig. Dazu habe ich eine Reihe von Vorschlägen unterbreitet, die bisher jedoch nicht aufgegriffen wurden. Die wichtigsten Anregungen möchte ich nachstehend skizzieren.

(1) Zum Schutz der Betroffenen halte ich es für erforderlich, daß der Katalog von Zweckdurchbrechungen und Übermittlungen von Daten an Dritte, der auf verschiedene Vorschriften verteilt ist, entscheidend eingeschränkt wird. Dieser Katalog liest sich derzeit so, als seien Übermittlungen und Zweckdurchbrechungen die Regel und nicht die Ausnahme, wie es die Rechtsprechung des Bundesverfassungsgerichts nahelegt. So soll z.B. generell die Übermittlung von personenbezogenen Verwaltungsdaten an private Dritte erlaubt sein, wenn dies im "öffentlichen Interesse" liegt. Durch solche Bestimmungen wird die vom Bundesverfassungsgericht geforderte Zweckbindung ausgehöhlt. Auch der Katalog der Ausnahmetatbestände, die eine Datenerhebung nicht beim Betroffenen, sondern ohne Kenntnis des Betroffenen bei Dritten gestatten, muß reduziert werden. So darf eine Datenerhebung beim Betroffenen nicht ohne weiteres durch eine zweckfremde Nutzung bzw. Übermittlung ersetzt werden.

Sofern Daten, die für einen bestimmten Zweck erhoben wurden, — ausnahmsweise — einem Dritten übermittelt oder für einen anderen Zweck benutzt werden, sollten die Betroffenen benachrichtigt werden. Nur so kann gewährleistet werden, daß die Rechte auf Auskunft, Berichtigung und Löschung wirksam wahrgenommen werden können.

(2) Daneben habe ich eine Reihe von Vorschlägen zum Arbeitnehmerdatenschutz eingebracht. So sollte die Erhebung medizinischer Daten bei ärztlichen Untersuchungen der Betroffenen vor Eingehung eines Beschäftigungsverhältnisses nur insoweit zulässig sein, als dies für die Feststellung seiner Eignung für die von ihm zu leistende Arbeit erforderlich ist und er vorher sein Einverständnis zu Art und Umfang der Informationserhebung erteilt hat. Der untersuchende Arzt darf der Personalstelle in der Regel nur das Ergebnis der Eignungsuntersuchung mitteilen. Auch die Erhebung psychologischer Daten im Zusammenhang mit der Eingehung eines Beschäftigungsverhältnisses darf nur zugelassen werden, soweit sie wegen besonderer Anforderungen an den Arbeitnehmer im Hinblick auf die von ihm zu leistende Arbeit erforderlich ist, vorhandene Bewerbungsunterlagen zur Beurteilung nicht bereits ausreichen, der Betroffene zuvor über Art und Umfang der Datenerhebung informiert wurde und sein Einverständnis hierzu erklärt hat. Allgemeine Persönlichkeitstests dürfen nicht zulässig sein. Daten im Zusammenhang mit psychologischen Tests sind Psychologen mit staatlich anerkannter wissenschaftlicher Abschlußprüfung vorzubehalten; diese Daten müssen nach Feststellung des Ergebnisses unverzüglich gesperrt werden. Der Personalstelle darf nur das Ergebnis der psychologischen Untersuchung mitgeteilt werden.

Darüber hinaus sollte eine Bestimmung aufgenommen werden, die dem Beschäftigten einen Unterrichtungsanspruch über sämtliche Datenübermittlungen sowie einen Auskunftsanspruch über personenbezogene Auswertungsprogramme bzw. Einzelauswertungen (etwa Telefondatenerfassung, Kontrolle des Zugangs zu Sicherheitszonen u.ä.), in die seine Daten einbezogen sind, zubilligt. Schließlich sollten sämtliche Übermittlungen von Beschäftigtendaten an zukünftige Arbeitgeber oder Beschäftigungsbehörden von der Einwilligung der Betroffenen abhängig gemacht werden, es sei denn, daß eine Abordnung oder Versetzung vorbereitet wird, die der Zustimmung des Beschäftigten nicht bedarf.

(3) Ferner bin ich der Absicht entgegengetreten, die Nutzung und Verarbeitung personenbezogener Daten, die aus "allgemein zugänglichen Quellen" stammen, voraussetzungslos zuzulassen. Ich habe darauf hingewiesen, daß auch die Verwendung von personenbezogenen Daten aus "allgemein zugänglichen Quellen" schutzwürdige Belange der Betroffenen verletzen kann. In der Begründung des Gesetzentwurfs wird — unter Rückgriff auf Formulierungen des Bundesverfassungsgerichts — selbst darauf hingewiesen, daß es bei den bestehenden Möglichkeiten der Datenverarbeitung keine "belanglosen" Daten mehr gibt. So können auch Daten aus "allgemein zugänglichen Quellen" durch die Verknüpfung mit vorhandenen Verwaltungsdaten und dadurch entstehende zusätzliche Auswertungsmöglichkeiten eine neue Qualität erlangen. Es ist deshalb konsequent zu fordern, daß jede Form der Datenerhebung und -verarbeitung den allgemeinen Vorschriften des Datenschutzgesetzes unterworfen wird. Darüber hinaus ist jetzt schon abzusehen, daß über die Frage, welche Quellen zu den allgemein zugänglichen zu zählen sind, eine ständige Auseinandersetzung entstehen wird.

(4) Zum Teil enthält der Entwurf noch Regelungen, die sich in der Vergangenheit nicht bewährt haben. Hier ist in erster Linie die Definition von "Akten", für die verschiedene Regelungen des Gesetzes nicht gelten, zu erwähnen. Diese Definiton hat schon im geltenden Recht zu erheblichen Auslegungsschwierigkeiten geführt. So hat eine Behörde die Auffassung vertreten, eine Datensammlung, die alle Merkmale einer Datei trage (hier: personenbezogene Protokollformulare), sei gleichwohl als Akte anzusehen, weil der Bearbeiter erklärt habe, er wolle die Möglichkeiten einer Datei nicht nutzen; die damit verbundenen Manipulationsmöglichkeiten seien gesetzesimmanent. Dem sollte durch das neue Recht ein Ende gesetzt werden.

(5) Die bisherige Sonderregelung für öffentliche Kreditinstitute, nach der sie der umfassenden Kontrolle des HmbDSB nach dem HmbDSG entzogen waren und von ihm stattdessen in seiner Eigenschaft als Aufsichtsbehörde nach dem BDSG kontrolliert wurden, muß gestrichen werden. Es ist kein sachlicher Grund zu erkennen, gerade die öffentlich-rechtlichen Kreditinstitute anders zu behandeln als die übrigen öffentlich-rechtlichen Wettbewerbsunternehmen. Die bisherige Aufsicht der nach dem BDSG zuständigen Behörden ist auf einen konkreten Anlaß (d.h. auf die Fälle, in denen ein Betroffener sich beschwert) beschränkt. Die öffentlich-rechtlichen Kreditinstitute werden sich sicherlich selbst nicht darauf berufen wollen, daß sie dadurch, daß sie einer strengeren Datenschutzkontrolle unterworfen werden, Wettbewerbsnachteile erleiden könnten.

(6) In einigen Fällen sehe ich sogar eine Verschlechterung gegenüber dem bisher erreichten Standard. So gibt es keine überzeugende Begründung, daß für die Datenverarbeitung in Akten, die bei Gerichten im Rahmen der Rechtspflege sowie bei der Staatsanwaltschaft und ihren Hilfsbeamten (!) bei der Verfolgung von Straftaten und der Strafvollstreckung geführt werden, die Zweckbindungs- und Übermittlungsvorschriften nicht gelten und die Rechtspositionen der Betroffenen geschwächt werden sollen. So sollen die Betroffenen keinen Anspruch auf Auskunft, Berichtigung, Sperrung, Löschung und Schadensersatz haben. Zwar ist es unstreitig, daß für die Datenverarbeitung der Gerichte und Strafverfolgungsbehörden bereichsspezifische Rechtsgrundlagen erforderlich sind. Daran wird zum Teil gearbeitet. Es ist aber abzusehen, daß diese erst in einigen Jahren in Kraft treten werden. Für die Zwischenzeit benötigt die Justiz jedoch den Orientierungsrahmen des Hamburgischen Datenschutzgesetzes, der ihr

jetzt genommen werden soll. Weiter muß beachtet werden, daß die neu zu schaffenden Rechtsgrundlagen voraussichtlich nicht so umfassend sein werden, daß sie die Bestimmungen des Hamburgischen Datenschutzgesetzes vollständig verdrängen werden. Dann besteht das Bedürfnis weiter, den allgemeinen Grundsätzen des Datenschutzrechts auch im Bereich der Justiz Geltung zu verschaffen.

(7) Im bisherigen Entwurf wird es versäumt, wichtige technische Entwicklungen durch entsprechende Schutzvorschriften gesetzgeberisch zu begleiten.

So gibt der verstärkte Einsatz der Videotechnik Anlaß, einige Grundsätze gesetzlich zu regeln. Die technische Entwicklung hat ein Niveau erreicht, das eine inhaltliche Auswertung der aufgezeichneten Bilder und den Abgleich der so gewonnenen Informationen mit vorhandenen Datenbeständen in naher Zukunft ermöglicht. Im übrigen sind die Bildaufzeichnungen selbst als Eingriff in das informationelle Selbstbestimmungsrecht zu werten. Unabhängig von der Schaffung bereichsspezifischer Rechtsgrundlagen sollte deshalb ein Auffangtatbestand in das Datenschutzgesetz aufgenommen werden, mit dem ein generelles Verbot von heimlichen Videoüberwachungen und -aufzeichnungen kodifiziert wird, das nur durch eng begrenzte spezialgesetzliche Erlaubnistatbestände durchbrochen werden kann. Dazu würden vor allem bereichsspezifische Eingriffsgrundlagen für die Sicherheitsbehörden gehören.

Auch die Möglichkeit, ferngesteuerte Messungen und Beobachtungen in Wohnungen oder Geschäftsräumen (Fernmessen) vorzunehmen oder mit Hilfe von Übertragungseinrichtungen in solchen Räumen andere Wirkungen auszulösen (Fernwirken) muß im Datenschutzgesetz geregelt werden, wie es etwa in Nordrhein-Westfalen und Hessen geschehen ist.

Von erheblicher Bedeutung ist auch die Forderung nach einem von den datenverarbeitenden Stellen zu führenden Geräteverzeichnis, die inzwischen Eingang in die Datenschutzgesetze von Hessen (§ 6 Abs. 3 HDSG) und Bremen (§ 6a Abs. 3 BrDSG) gefunden hat. Derartige Verzeichnisse sind angesichts der stürmischen Ausweitung dezentraler Datenverarbeitungsanlagen einerseits erforderlich, um den für die Sicherstellung des Datenschutzes verantwortlichen Behördenleitungen einen Überblick über die eingesetzten Verfahren zu verschaffen. Andererseits sind von der eingesetzten Technik die nach § 8 zu treffenden technischen und organisatorischen Maßnahmen abhängig. Schließlich würde ein Geräteverzeichnis datenschutzrechtliche Kontrollen erleichtern. Dies gilt ebenso für meine Forderung, den datenverarbeitenden Stellen aufzugeben, Vernetzungspläne bereitzuhalten.

Die Erfahrungen der letzten Jahre haben gezeigt, daß gerade beim Einsatz dezentraler Technik eine professionelle, auch Datenschutzanforderungen gerecht werdende Datenverarbeitung nicht immer gewährleistet war, insbesondere eine ordnungsgemäße Freigabe nicht erfolgte und eine Dokumentation nicht vorlag. Deshalb sollte im Gesetz der Grundsatz verankert werden, daß die Verarbeitung personenbezogener Daten nur mit freigegebenen und dokumentierten Verfahren zulässig ist. Nur auf diesem Wege ist eine ordnungsgemäße Datenverarbeitung zu gewährleisten.

(8) Die Neufassung des Gesetzes sollte darüber hinaus Gelegenheit sein, die Stellung des Datenschutzbeauftragten zu überdenken und zu erwägen, ihm eine dem Rechnungshof vergleichbare Rechtsstellung einzuräumen. Dies würde seine Unabhängigkeit, die das Bundesverfassungsgericht als eines der Kernstücke der Sicherung des Rechts auf informationelle Selbstbestimmung bezeichnet hat, stärken. Diesem Ziel dient auch mein Vorschlag, eine einmalige Amtszeit des Datenschutzbeauftragten von acht Jahren vorzusehen.

Auf jeden Fall muß auf die immer noch vorgesehene Rechtsaufsicht des Senats über den Datenschutzbeauftragten verzichtet werden. Die Rechtsaufsicht könnte dazu benutzt werden, in Konfliktfällen die Rechtsauffassung des Senats gegenüber dem Datenschutzbeauftragten durchzusetzen. Dies wäre nicht nur mit dessen Unabhängigkeit, sondern auch mit seinem gesetzlichen Auftrag unvereinbar. Entsprechend ist eine Rechtsaufsicht in Nordrhein-Westfalen und Bremen nicht mehr vorgesehen; in Hessen und Berlin gab es sie nie.

Beseitigt werden muß auch eine jetzt noch bestehende Lücke in der Datenschutzkontrolle im Sicherheitsbereich. Nach § 20 Abs. 4 des geltenden Hamburgischen Datenschutzgesetzes darf die Einhaltung von Datenschutzvorschriften u.a. beim Landesamt für Verfassungsschutz, den Behörden der Staatsanwaltschaft und der Polizei nicht überwacht werden, soweit der Senat im Einzelfall feststellt, daß die Einsicht in Unterlagen und Akten die Sicherheit des Bundes oder eines Landes gefährdet. Daran will der Entwurf festhalten, obwohl dies mit der einschlägigen Rechtsprechung des Bundesverfassungsgerichts kaum vereinbar ist. Ich habe vorgeschlagen, für die Fälle, in denen der Senat feststellt, daß derartige Sicherheitsbelange tangiert sind, die Konrolle dem Datenschutzbeauftragten persönlich vorzubehalten. Entsprechende Regelungen finden sich in den neuen Datenschutzgesetzen von Nordrhein-Westfalen und Hessen.

1.4 Verhältnis zur Verwaltung

Auch im Berichtsjahr fehlt es nicht an Beispielen, die belegen, daß die Verwaltung dem Datenschutz nicht immer den ihm zukommenden Stellenwert beigemessen hat. So habe ich die Erfahrung machen müssen, daß es der Verwaltung häufig schwerfällt, die Erkenntnis, daß es bestimmte Datenschutzprobleme gibt und daß sie in bestimmter Weise gelöst werden müssen, in konkrete Maßnahmen umzusetzen. Es hat den Anschein, als ob die Datenschutzprobleme, sofern sie mit anderen Vorhaben konkurrieren, auf der Prioritätenliste ziemlich weit unten rangieren. Im übrigen wurde der Datenschutzbeauftragte entgegen häufig wiederholten Zusagen weiterhin in einigen Fällen überhaupt nicht, in anderen Fällen verspätet oder unzureichend an datenschutzrelevanten Vorhaben und Projekten beteiligt, gestellte Fragen wurden verspätet oder unzureichend beantwortet. Beispiele:

— Bereits im Juni 1985 hatte ich schriftliche "Empfehlungen zum Verfahren der Vernichtung von Schriftgut in den Behörden der Freien und Hansestadt Hamburg" gegeben. Aufgrund einer Zeitungsmeldung über einen Aktenfund griff ich das Problem der Schriftgutvernichtung im Frühjahr 1987 mit einer Umfrage bei allen Behörden wieder auf und konnte nur feststellen, daß eine Umsetzung meiner Empfehlungen noch nicht in Angriff genommen worden war. Mit Schreiben vom Juni 1987 übermittelte ich dem Senatsamt zur weiteren Konkretisierung meiner Empfehlungen von 1985 den Entwurf eines Mustervertrages zur Regelung von Auftragsverhältnissen zur Schriftgutvernichtung zwischen öffentlichen Stellen und privaten Auftragnehmern. Daraufhin wurde im Sommer 1987 eine Arbeitsgruppe aus Vertretern des Senatsamtes für den Verwaltungsdienst, der Finanzbehörde, der Baubehörde und einiger Bezirksämter eingesetzt, um den Behörden durch die Veröffentlichung von Hinweisen zur Schriftgutvernichtung und eines Mustervertrages in den Mitteilungen für die Verwaltung bei der ordnungsgemäßen Organisation der Schriftgutvernichtung Hilfestellung zu geben. Doch ist es bis heute nicht zu einer Veröffentlichung gekommen, weil offenbar immer noch an dem Entwurf gearbeitet wird, s. Nr. 3.4.

— Die bereits in meinem letzten TB (vgl. 4.2.4, S. 40) angekündigten neuen Richtlinien und Formulare des Personalamtes für die Ortszuschlagsberechnung bei einer in den Haushalt aufgenommenen Person sind immer noch nicht erlassen. Der erste Entwurf vom Januar 1988 enthielt wieder Formulierungen, die ich vorher schon mehrfach kritisiert hatte. In einem Gespräch mit dem Personalamt im März konnte hinsichtlich des Erhebungsformulars weitgehend Einigkeit erzielt werden. Im Mai 1988 hieß es in der Stellungnahme des Senats zu meinem letzten Tätigkeitsbericht, das Personalamt habe "inzwischen in Übereinstimmung mit dem Hamburgischen Datenschutzbeauftragten einen neuen Fragebogen über den Ortszuschlag entwickelt, in dem der Fragenumfang wesentlich beschränkt werden konnte". Dies entsprach nicht den Tatsachen, denn erst am 19. Juli 1988 erhielt ich einen weiteren Entwurf, zu dem ich am 1. August 1988 noch einmal Stellung nahm. Mein Erinnerungsschreiben vom 4. November 1988 führte zu einem Brief vom 21. November, in dem es heißt: "Das Personalamt ist jedoch bemüht, in dieser Angelegenheit nunmehr baldmöglichst zu einer abschließenden Entscheidung zu kommen. Es bittet Sie, sich noch etwas zu gedulden". Unmittelbar vor Redaktionsschluß erhielt ich am

21. Dezember 1988 nochmals überarbeitete Hinweise und Musterformulare, die einem Teil meiner Bedenken Rechnung tragen und "nunmehr umgehend an die Behörden und Ämter" versendet werden sollen.

— Im letzten Tätigkeitsbericht (vgl. 4.2.2, S. 38) hatte ich mitgeteilt, daß ich es nach jahrelangen Erörterungen mit dem Personalamt nunmehr für wichtig hielte, die bereinigten Bewerberfragebögen in den Ämtern und Behörden zügig einzusetzen. Bereits im November 1987 hatte das Personalamt nämlich mitgeteilt, die für die Gestaltung der Vordrucke zuständigen Stellen seien um die Änderung des Musterfragebogens für Bewerber sowie um die Einführung eines Vordruckes für Einzustellende gebeten worden. Auf mein Erinnerungsschreiben vom 31. März 1988 erhielt ich am 6. Juni 1988 ein Schreiben, in dem der gesichert geglaubte Kompromiß aus meiner Sicht wieder in Frage gestellt wurde. Seit einem Schriftwechsel hierzu mit dem Leiter des Personalamtes vom 24.6./17.8.1988 hat es in der Einführung eines einheitlichen Bewerberfragebogens keine Fortschritte gegeben.

  Auch die Behörde für Inneres ließ sich Zeit: Am 6. Juni 1988 bat ich um Zusendung der in der Innenbehörde verwendeten Bewerberfragebogen. Ich erhielt sie nach Erinnerung am 12. August 1988. Auf meine umfangreiche Stellungnahme und Kritik vom 22. August 1988 bekam ich am 7. November 1988 die Antwort, die Behörde habe "die Polizei und die Feuerwehr gebeten zu prüfen, ob und mit welchen evtl. Ergänzungen die Musterentwürfe (des Personalamtes) eingeführt werden können".

— Im Sommer 1987 wurde von mir die "Arbeitsdatei PIOS-Innere Sicherheit" (APIS) bei der für den polizeilichen Staatsschutz zuständigen Fachdirektion 7 überprüft. Es zeigte sich, daß zahlreiche Datensätze eingegeben worden waren, die nach der Errichtungsanordnung nicht hätten gespeichert werden dürfen. Den Prüfbericht habe ich der Behörde für Inneres im November 1987 mit der Bitte um Stellungnahme übersandt. Mit Schreiben vom 15. Februar 1988, 6. September 1988 und 12. September 1988 teilte die Innenbehörde mit, daß einige der beanstandeten Fälle inzwischen gelöscht worden seien. Eine umfassende Stellungnahme zur Speicherpraxis der Polizei unterblieb mit dem Hinweis darauf, daß die Polizei eine grundlegende Überprüfung der Speicherungspraxis eingeleitet habe, die noch nicht abgeschlossen sei. Nachdem der Polizeipräsident auf der Sitzung des Rechtsausschusses vom 12. September 1988 mitgeteilt hatte, daß eine Überprüfung des Hamburger APIS-Bestandes zur Löschung von 35 % der Datensätze geführt hätte, habe ich die Behörde für Inneres am 15. September 1988 erneut gebeten, eine abschließende Stellungnahme zum Prüfbericht abzugeben, wobei von mir insbesondere die Frage nach den neuen Kriterien und ihrer Anwendung gestellt wurde. Bis heute hat die Innenbehörde darauf trotz nochmaliger Erinnerung nicht geantwortet.

— Im August habe ich die Behörde für Inneres gebeten mir mitzuteilen, wann die einzelnen Erhebungspapiere der Volkszählung vernichtet werden sollen und wie die Vernichtung organisiert werden soll. Erst aufgrund wiederholter Erinnerungsschreiben und nach der Androhung einer förmlichen Beanstandung hat die Behörde für Inneres mir Anfang Dezember einen Terminplan für die Vernichtung der einzelnen Erhebungsunterlagen übersandt. Ein Konzept zur Vernichtung dieser Unterlagen liegt dem Statistischen Landesamt offensichtlich bis heute nicht vor, jedenfalls war die Behörde für Inneres nicht in der Lage, mir ein derartiges Konzept bis zum Redaktionsschluß zuzusenden.

— Vor über vier Jahren hat das UKE in der Erkenntnis, daß die geltende Dienstanweisung über die Führung und Herausgabe von Krankengeschichten inhaltlich nicht mehr der Rechtsprechung zum Datenschutz und zum Akteneinsichtsrecht entsprach, einen Neuentwurf zur Diskussion gestellt. Die Dienstanweisung ist aber trotz meiner mehrfachen Hinweise auf die Dringlichkeit einer Neuregelung bis heute nicht beschlossen worden. Zuletzt habe ich im September den Erlaß der Dienstanweisung beim UKE angemahnt, auf mein Schreiben aber nicht einmal eine Eingangsbestätigung, geschweige denn eine inhaltliche Rückäußerung erhalten.

— Seit Anfang 1987 planen die gesetzlichen Krankenkassen und der Vertrauensärztliche Dienst der Landesversicherungsanstalt Hamburg einen Modellversuch zur Kosten- und Leistungstransparenz auf dem Krankenhaussektor, dessen Vorbereitungsphase Mitte 1988 angelaufen ist (näheres dazu unter 4.1.2). Weder die AOK noch die LVA, die beide als öffentlich-rechtliche Körperschaften der Kontrolle des Hamburgischen Datenschutzbeauftragten unterstehen, haben mich an den Vorarbeiten für das Konzept des Modellversuchs beteiligt, obwohl in großem Umfang sensible personenbezogene Daten verarbeitet werden sollen und aus früheren Modellversuchen in anderen Bundesländern die datenschutzrechtliche Brisanz derartiger Vorhaben bekannt sein mußte.

  Erst zehn Tage vor Beginn der ersten Phase des Modellversuchs und nachdem die personellen und organisatorischen Voraussetzungen für die Durchführung des Vorhabens bereits geschaffen waren, bin ich von der Krankenhausgesellschaft und einem Krankenhaus beteiligt worden und habe festgestellt, daß das Konzept aus datenschutzrechtlicher Sicht einer grundlegenden Überarbeitung bedarf.

2. Entwicklung der Dienststelle

2.1 Ausstattung

Im Berichtszeitraum hat sich die personelle Ausstattung meiner Dienststelle gegenüber dem Vorjahr nicht verändert und liegt weiterhin bei 11 Planstellen. Ein Beschluß der Bürgerschaft über den Haushaltsplan für 1989 lag bei Redaktionsschluß dieses Berichts zwar noch nicht vor, jedoch erwarte ich aufgrund des vom Senat in die Bürgerschaft eingebrachten Stellenplanentwurfs für das kommende Jahr die Zuweisung von zwei weiteren Stellen des höheren Dienstes, um die im 6. Tätigkeitsbericht (2.1, S. 13) skizzierten Aufgaben in Angriff nehmen zu können. Hierfür bin ich sehr dankbar, auch wenn meine Forderung nach einer weiteren Sachbearbeiterstelle nicht berücksichtigt wurde, die erforderlich ist, um die vorhandenen Defizite bei der Prüfung der umfangreichen polizeilichen Datenverarbeitung abbauen zu können. Außerdem benötige ich vor allem für die Erledigung der immer zahlreicher werdenden Schreibaufträge zumindest eine weitere Schreibkraft. Entsprechende Anträge habe ich zum Stellenplan 1990 formuliert.

Seit wir im September 1987 unsere Diensträume im Millerntor-Hochhaus wegen einer Asbest-Verunreinigung verlassen haben (vgl. 6. TB, 2.1, S. 13), ist die Dienststelle nach wie vor in zwei verschiedenen Dienstgebäuden an der Drehbahn und am Klosterwall notdürftig untergebracht. Ein geordneter Dienstbetrieb ist deshalb weiterhin nicht möglich, ganz abgesehen davon, daß seit 15 Monaten ratsuchende Bürger große Mühe haben, die Dienststelle des Datenschutzbeauftragten ausfindig zu machen oder auch nur telefonisch zum zuständigen Sachbearbeiter vorzudringen. Seit Mitte des Jahres sind wenigstens die Akten wieder zugänglich.

Mittlerweile hat die Justizbehörde die angemieteten Flächen im Gebäude Millerntorplatz 1 fristlos gekündigt. Damit steht fest, daß meine Dienststelle dorthin nicht wieder zurückkehren wird. Kurz vor Redaktionsschluß zeichnete sich ab, daß wir mit großer Wahrscheinlichkeit Anfang des kommenden Jahres frei werdende Räume am Baumwall 7, die bisher vom Hafenärztlichen Dienst der Gesundheitsbehörde genutzt wurden, beziehen können. Büroräume in der City-Nord hatte ich abgelehnt, da ich meine, daß der Datenschutzbeauftragte in der Innenstadt (im weiteren Sinne) untergebracht sein muß, um für die Bürger erreichbar zu sein.

Mein besonderer Dank gilt an dieser Stelle allen Mitarbeiterinnen und Mitarbeitern, die es trotz widriger äußerer Umstände möglich gemacht haben, daß auch dieser Tätigkeitsbericht einigermaßen rechtzeitig erstellt werden konnte.

2.2 Eingaben

Im Berichtszeitraum erreichten mich 377 Eingaben. Davon entfielen 245 auf den öffentlichen und 132 auf den nicht-öffentlichen Bereich. Die bis zum Redaktionsschluß abgeschlossenen Eingaben betrafen im einzelnen folgende Bereiche:

A) Öffentlicher Bereich		195
davon Sicherheitsbereich	37	
Gesundheits- und Sozialbereich	30	
Volkszählung	75	
übrige Bereiche	53	
B) Nicht-öffentlicher Bereich		105
davon Versandhandel	7	
Versicherungswirtschaft	25	
Kreditwirtschaft	7	
Sonstige des 3. Abschnitts	46	
Auskunfteien	17	
Sonstige des 4. Abschnitts	3	

3. Beobachtung der automatisierten Datenverarbeitung

3.1 Umsetzung und Fortentwicklung von ADV-Richtlinien

3.1.1 Bereich der zentralen ADV-Verfahren

Im Berichtsjahr habe ich die Prüfung des Personalamtsverfahrens fortgesetzt, die sich wegen der Kompliziertheit der Materie und des Fehlens gerade solcher Bestandteile in der Dokumentation, die u.a. externen Kontrollorganen den Einstieg erleichtern sollen, recht schwierig gestaltet. Ich hoffe, die Prüfung im nächsten Jahr abschließen und in meinem 8. Tätigkeitsbericht eine Bewertung abgeben zu können. Ein Schwerpunkt wird dabei das Problem der Einhaltung der ADV-Richtlinien sein.

Nicht nur beim Personalamtsverfahren habe ich insofern Defizite festgestellt, sondern z.B. auch beim Verfahren "Kartei des produzierenden Gewerbes", einer Anwendung des Statistischen Landesamtes. Durch einen Zufall bin ich darauf gestoßen, daß in diesem Verfahren — ähnlich wie in dem von mir beanstandeten Verfahren zur Gebäudevorerhebung (s. 6. TB, Nr. 3.4.1) — gegen das der Datensicherheit dienende Prinzip der Trennung von Test- und Produktionsbetrieb verstoßen wurde.

Ich habe festgestellt, daß in diesem Verfahren Originaldatenbestände arbeitstäglich in eine Testdatei des Statistischen Landesamtes überspielt wurden. In der Testdatei wurden die Originaldaten im online-Testbetrieb von Mitarbeitern des StaLa bearbeitet. Der geänderte Bestand wurde am selben Tag nachmittags wieder in die Produktionsdatei zurückübertragen, wo er dann unter Produktionsbedingungen ausgewertet wurde.

Das Überspielen von Daten aus Produktionsdateien in Testdateien ist in der DVZ nicht ohne weiteres möglich, weil das Sicherungssystem der DVZ dies grundsätzlich zu verhindern hat. Das Sicherungssystem ist so konzipiert, daß es den Zugriff auf Originaldaten nur freigegebenen Programmen unter einer besonderen Laufart gestattet. Auf Testdatenbestände dürfen alle bei der Programmerstellung Beteiligten zugreifen und die Daten auch beliebig, insbesondere mit den auszutestenden, noch nicht freigegebenen Programmen verarbeiten. Im Testbetrieb läßt das System den Zugriff nur auf Testdatenbestände zu. Im geregelten Ausnahmefall — wofür es eine spezielle "Laufart" gibt — kann das Überspielen von Originaldaten in Testdateien jedoch erfolgen.

Nach Angaben des Statistischen Landesamtes, die vom Senatsamt und der DVZ bestätigt wurden, war die beschriebene Verfahrensweise 1982 aus Praktikabilitätsgründen nach Absprache mit dem Senatsamt für den Verwaltungsdienst "offiziell" gewählt worden. Sie ist auch entsprechend in der Verfahrensdokumentation beschrieben und seither so praktiziert worden.

Ich habe Bedenken gegen eine derartige Verfahrensgestaltung, weil sie die strikte Trennung zwischen Produktionsbetrieb und Testbetrieb aufhebt. Hier ist nicht — wie beim Verfahren Gebäudevorherbung — mit "echten" Daten getestet worden, sondern es wurde ein Teil der Produktion, ein Arbeitsgang im Gesamtarbeitsablauf — nämlich der Änderungsdienst — aus der Produktionsumgebung hinausverlagert in die Testumgebung. Das Ergebnis wurde anschließend wieder in die Produktionsumgebung überführt.

Die Behörde für Inneres hat darauf hingewiesen, daß durch diese Verfahrensweise keine konkrete Gefährdung der statistischen Geheimhaltung von Einzeldaten zu erwarten war oder eingetreten sei. Es sei organisatorisch gesichert gewesen, daß auf die Daten nur die fachlich zuständige Stelle zugreifen konnte. Allerdings habe es an einer zusätzlichen technischen Absicherung durch Beschränkung der Zugriffsberechtigung auf eine spezielle User-ID gefehlt. Dieser Mangel sei aber seit Februar 1988 behoben. Auch sei die Richtigkeit und die Ordnungsmäßigkeit der eingesetzten Programme gewährleistet gewesen.

Aufgrund von Hinweisen aus der Verwaltung und der DVZ bin ich zu der Überzeugung gelangt, daß auch andere Verfahren bzw. andere Behörden, gerade was die DVZ-Laufarten angeht, sich nicht immer streng an die vom Senatsamt für den Verwaltungsdienst entwickelten ADV-Richtlinien halten. Ich habe es daher begrüßt, daß das Senatsamt — Organisationsamt — und die DVZ einen Arbeitskreis eingesetzt haben, der eine Überprüfung der Abgrenzung von Test und Produktion vornehmen und Vorschläge für eine Neuregelung der DVZ-Laufarten erarbeiten soll. An dieser Arbeitsgruppe bin ich laufend beteiligt worden. Das endgültige Ergebnis der Arbeit dieser Gruppe liegt noch nicht vor. Die bisherigen Gspräche und Vorschläge lassen jedoch ein befriedigendes Ergebnis erwarten, wenn auch noch nicht für alle Probleme eine praxisgerechte Lösung gefunden wurde.

Nach allem sehe ich mich veranlaßt, vom Senat zu fordern, daß die ADV-Richtlinien für die hamburgische Verwaltung noch einmal ausdrücklich für verbindlich erklärt werden, daß als notwendig erkannte Modifikationen umgehend in die Richtlinien eingearbeitet werden und daß danach Verstöße gegen die Richtlinien nicht mehr geduldet werden. Die Stellungnahmen, die die Behörden und auch der Senat (z.B. in seiner Stellungnahme zu meinem 6. TB) bisher abgegeben haben, wenn ich Verstöße gegen die Richtlinien gerügt habe, halte ich für ausgesprochen unbefriedigend. Sie lassen Zweifel daran aufkommen, daß die ADV-Organisation der hamburgischen Verwaltung den Anforderungen gerecht wird, die § 8 Abs. 1, Anlage Nr. 10 HmbDSG (Organisationskontrolle) an diese Organisation stellt. Besonders gefährlich kann eine nicht konsequent durchgehaltene Organisationskontrolle dann werden, wenn im Zuge des verstärkten IuK-Einsatzes in der Verwaltung — wie geplant — die Vernetzung von dezentralen Anlagen mit den Anlagen der DVZ vorangetrieben wird.

3.1.2 Bereich der dezentralen Verfahren

Auf die Risiken, die mit der Verarbeitung personenbezogener Daten auf dezentralen Anlagen (PC, Arbeitsplatzrechner, Abteilungsrechner) verbunden sind, habe ich wiederholt hingewiesen (s. u.a. 6. TB, Nr. 3.5). In diesem Zusammenhang habe ich auch das Problem angesprochen, daß nach dem Einzug der ADV in die Fachabteilungen die Vermittlung der erforderlichen Kenntnisse bei diesem Personenkreis über die vom Senatsamt für den Verwaltungsdienst erlassenen generellen Regelungen und die jeweils selbst zu treffenden technischen und organisatorischen Maßnahmen zur Sicherstellung des Datenschutzes, der Datensicherheit und der Betriebssicherheit noch nicht gewährleistet ist. Daraus können Gefahren für den Datenschutz erwachsen. Das Senatsamt für den Verwaltungsdienst hat dies durchaus erkannt und im April 1988 in den Mitteilungen für die Verwaltung eine Neufassung der "Hinweise zur Durchführung des Hamburgischen Datenschutzgesetzes und zu datenschutzrechtlichen Regelungen des Sozialgesetzbuchs/Bundesdatenschutzgesetzes" sowie die ergänzenden "Vorläufigen Hinweise für die Verarbeitung personenbezogener Daten auf Personal-

computern (PC) in der Verwaltung" veröffentlicht (MittVw 1988, S. 61 ff.). Die "Hinweise" und die "Ergänzung" sind zur Vermittlung der notwendigen Kenntnisse an alle, die zur Erfüllung einer Fachaufgabe automatisierte Lösungen entwickeln, durchaus geeignet, wenn ich auch einer verbindlichen Regelung mit den entsprechenden Regelungsgegenständen den Vorzug vor "Hinweisen" geben würde.

Ich habe aber auch im Berichtsjahr wiederholt die Erfahrung machen müssen, daß dezentrale Geräte angeschafft worden waren und Verfahren darauf entwickelt wurden, ohne daß die damit beauftragten Mitarbeiter die ADV-Richtlinien oder die "Hinweise" kannten.

Ich fordere daher die Behörden auf, die Verpflichtung aus § 16 Satz 1 HmbDSG, eigenverantwortlich die Ausführung der Datenschutzbestimmungen in ihrem Bereich sicherzustellen, konsequenter zu erfüllen als bisher. In jeder Behörde muß dafür gesorgt werden, daß zur Ausstattung einer Dienststelle oder eines einzelnen Arbeitsplatzes mit ADV-Technik immer auch die Ausstattung mit den einschlägigen ADV-Richtlinien und Hinweisen gehört, und die Verteilung von Ergänzungen und Änderungen muß so organisiert werden, daß sie zuverlässig alle erreicht, die es angeht. Der Erlaß von Regelungen mag eine zentrale Aufgabe sein. Aber die Umsetzung der Regelungen bis in die letzte Untergliederung innerhalb der Behörden ist Sache der einzelnen Behörde. Meine Prüfungen in verschiedenen Fachbehörden haben aber ergeben, daß hier noch erhebliche Defizite bestehen, vgl. 4.5.2, 4.13.2.2, 4.13.3.

3.2 Risiken der Benutzung von Datex-P

Bereits in meinem 5. Tätigkeitsbericht (5. TB, 3.1, S. 7) habe ich auf Mißbrauchsrisiken bei Datex-P hingewiesen. Bei Datex-P handelt es sich um einen paketvermittelten Dienst der Deutschen Bundespost zur digitalisierten Datenübertragung, der von öffentlichen und nicht-öffentlichen Stellen in starkem Maße in Anspruch genommen wird. Gefahren ergeben sich u.a. im Zusammenhang mit einer mißbräuchlichen Verwendung der Teilnehmerkennung, die im Datex-P-Dienst die Funktion eines Kontos für die Inanspruchnahme des Dienstes hat. Ihr werden die Gebühren zugeordnet, die bei Verbindungen unter ihrer Angabe anfallen. Unter Nutzung der Teilnehmerkennung kann jeder von jedem beliebigen Anschluß auf Kosten des Inhabers der Kennung den Dienst in Anspruch nehmen. Aus diesem Grund muß die Kennung besonders sorgfältig geheimgehalten werden. Gleichwohl werden immer raffiniertere Versuche unternommen, die wertvolle Teilnehmerkennung anderer Datex-P-Benutzer auszuspähen. Von einem solchen — zunächst erfolgreichen — Versuch habe ich im Berichtsjahr erfahren:

Ein Mitarbeiter der Universität hatte von einem Datex-P-Anschluß aus Kontakt zu einer Mailbox in München aufgenommen, über die sog. "public domain software" angeboten wurde. Das Mailbox-Programm hat einen Verbindungsabbruch simuliert und sich (fälschlich) als Datex-P-Knoten der Post ausgegeben und den Benutzer zu erneutem Verbindungsaufbau aufgefordert. Dieser Aufforderung ist der Universitätsmitarbeiter nachgekommen. Da im Rahmen der Anmeldeprozedur auch die Teilnehmerkennung abgefragt wird, hat der Mailbox-Betreiber so die Kennung der Universität erfahren.

Die Universität hat — nachdem sie Verdacht geschöpft hatte — die Teilnehmerkennung des Anschlusses durch die Post sperren lassen. Zu monieren ist allerdings, daß außer der Sperrung der Kennung die betroffene Stelle zunächst nichts unternommen hat. Der Universitätsverwaltung wurde — trotz ausdrücklicher Aufforderung — eine genaue Darstellung des Sachverhalts nicht gegeben. Bei frühzeitiger und ausführlicher Unterrichtung hätten auch die anderen universitären Datex-P-Nutzer frühzeitig gewarnt werden können. Dies ist aber unterblieben.

Die Universität hat inzwischen ein Rundschreiben versandt, in dem auf die Mißbrauchsmöglichkeiten und auf Gegenmaßnahmen hingewiesen wird. Da die geschilderten Risiken sich nicht auf universitäre Benutzer beschränken, soll der die Gegenmaßnahmen betreffende Teil des Rundschreibens hier zitiert werden:

"Wie können Sie sich gegen derartige Gefahren schützen? Brechen Sie in derartigen Fällen die aufgebaute Verbindung physikalisch ab, indem Sie den Hörer auflegen, und — wenn Sie wollen — bauen Sie die Verbindung neu über das Postnetz wieder auf.

Sobald Sie auch nur Zweifel haben, ob nicht Ihre Teilnehmer-Kennung in falsche Hände geraten sein könnte, so veranlassen Sie bitte umgehend eine Sperrung Ihrer Teilnehmer-Kennung und fordern Sie von der Deutschen Bundespost einen Ausdruck der im fraglichen Zeitraum hergestellten Teilnehmer-Verbindungen an."

3.3 Verarbeitung personenbezogener Daten im Rechenzentrum der Universität Hamburg

3.3.1 Aufgaben und Einbindung des Rechenzentrums

Das Rechenzentrum ist eine Betriebseinheit i.S.v. § 110 Hamburgisches Hochschulgesetz und als zentrale Einrichtung dem Akademischen Senat zugeordnet. Es hat die Aufgabe, Datenverarbeitungsanlagen für Lehre und Forschung und in Ausnahmefällen auch für die Verwaltung zu betreiben. Es berät die Benutzer, leistet benutzerorientierte Forschungs- und Entwicklungsarbeit und bietet Lehrveranstaltungen über Programmiersprachen und die Nutzung von Datenverarbeitungsanlagen an (vgl. § 2 der Organisationsbestimmungen für das Rechenzentrum der Universität Hamburg vom 11.7.1985).

Grundsätzliche Fragen der Benutzung sind in der Benutzungsordnung geregelt. Darüber hinaus gibt es Bestimmungen für die Vergabe von Betriebsmitteln des Rechenzentrums (Beantragung von Problemnummern, Rechenzeiten, Verbrauchsmitteln, Zugangskontrolle).

Das Rechenzentrum ist lokal mit verschiedenen Universitätsinstituten, dem HWWA-Institut für Wirtschaftsforschung und der TU Hamburg-Harburg verbunden. Darüber hinaus ist das RZ mit einem Datex-P-Anschluß und über einen HfD-Anschluß (Standleitung) an das Europäische Forschungsnetz (EARN) angeschlossen. Dieses Netz verfügt über Schnittstellen zu anderen internationalen Forschungsnetzen.

3.3.2 Sicherungsmaßnahmen

Da die vom Datenschutzrecht vorgeschriebenen Sicherheitsmaßnahmen (vgl. § 8 Abs. 1 HmbDSG) sich an der Schutzwürdigkeit der verarbeiteten personenbezogenen Daten zu orientieren haben und im RZ keine personenbezogenen Daten verarbeitet werden dürfen, zielen die vom RZ getroffenen Maßnahmen vor allem darauf ab, eine unberechtigte Inanspruchnahme von Betriebsmitteln zu verhindern und die Betriebssicherheit zu gewährleisten.

Prinzipiell hat jeder Benutzer eine Problemnummer, die nur Zugriff auf seine eigenen Datenbestände erlaubt; es gibt aber auch Problemnummern, die einer Benutzergruppe (z.B. Fachbereich Medizin) zugeordnet sind. In diesen Fällen können alle autorisierten Benutzer aus dieser Gruppe auf die ihr gehörenden Datenbestände zugreifen.

Den einzelnen Benutzern werden jeweils nur Betriebsmittel zugeteilt (Rechenzeit, Speicherkapazität auf einer Platte usw.). Im Rahmen dieser Zuteilungen können die Teilnehmer frei disponieren, d.h. auch Dateien anlegen, ändern und löschen. Eine Freigabe von Programmen — wie es z.B. bei der kommerziellen Datenverarbeitung üblich ist — entfällt hier, da gerade die Entwicklung angemessener Software-Produkte ein wesentlicher Forschungsgegenstand ist. Welche Daten im einzelnen verarbeitet werden und welche Programme dabei eingesetzt werden, wird vorab also nicht kontrolliert; dagegen ist aber — im Rahmen der Aufgabenbestimmung des Rechenzentrums — auch nichts einzuwenden.

Die befugten Benutzer haben die Möglichkeit, im Rahmen ihrer Berechtigungen Datenbestände im Wege des Filetransfers auf dezentrale Anlagen zu überspielen (download) und auf dezentralen Anlagen gespeicherte Daten an den Großrechner zu übertragen (upload).

Jeder Benutzer hat ein nur ihm bekanntes Paßwort zu wählen. Das Paßwort muß periodisch (z.Z. alle 30 Tage) gewechselt werden. Die Benutzung des Systems wird durch das Sicherheitssystem RACF kontrolliert.

Die Systemaktivitäten werden durch ein entsprechendes Softwareprodukt (SMF) ausführlich protokolliert und selektiv auf einem Systemmonitor angezeigt.

3.3.3 Verarbeitung personenbezogener Daten

Aufgrund seiner wissenschaftlichen Aufgabenstellung ist das RZ der Universität Hamburg nur eingeschränkt mit anderen kommerziellen bzw. Verwaltungsrechenzentren vergleichbar. Insbesondere hinsichtlich der Sicherheitsmaßnahmen bleibt eine solche wissenschaftliche und damit "offene" Einrichtung zwangsläufig hinter kommerziellen Rechenzentren zurück. Aus diesem Grund hat der Akademische Senat bereits 1977 festgestellt, daß im Rechenzentrum keine personenbezogenen Daten — auch nicht für wissenschaftliche Zwecke — verarbeitet werden sollen.

Dieser Grundsatzbeschluß ist zwar nicht in die verbindlichen Organisationsbestimmungen für das Rechenzentrum übernommen worden, aber eine entsprechende Formulierung findet sich im Anmeldeformular, das jeder Benutzer zu unterschreiben hat. Es handelt sich um folgende Formulierung:

"Es handelt sich um eine wissenschaftliche Arbeit; personenbezogene Daten i.S.d. Datenschutzgesetzes werden nicht verarbeitet."

Ich habe stichprobenartig mehr als hundert Dateien der Fachbereiche Psychologie und Medizin überprüft. Dabei habe ich eine Verarbeitung von Daten, die ohne Zusatzwissen einzelnen namentlich gekennzeichneten Personen zugeordnet werden können, nicht festgestellt. Gleichwohl werden in großem Umfang Einzelangaben über natürliche Personen verarbeitet, die einzelnen Menschen über laufende Nummern, Patientennummern, Codes o.ä. zugeordnet werden können.

Das Hamburgische Datenschutzgesetz definiert in § 4 Abs. 1 personenbezogene Daten als Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Nach meinen Prüfungen waren in einer Vielzahl von Dateien zwar keine Daten bestimmter natürlicher Personen gespeichert; die Identität der Personen kann jedoch mit entsprechendem Zusatzwissen festgestellt werden. Es handelt sich also um Daten bestimmbarer natürlicher Personen. Dies bedeutet, daß im Rechenzentrum entgegen den Beschlüssen des Akademischen Senats doch personenbezogene Daten verarbeitet werden.

Im Hinblick auf das Mißbrauchsrisiko der zwar ohne Namen, aber mit anderen Ordnungsmerkmalen (z.B. lfd. Nr. der Testperson) gespeicherten Daten ist zu differenzieren zwischen dem Zugriff durch Mitarbeiter der speichernden Stelle (z.B. FB Psychologie) und durch sonstige Dritte (z.B. Mitarbeiter des Rechenzentrums und anderer Institute). Im letzten Fall ist das Mißbrauchsrisiko verhältnismäßig gering einzuschätzen, da hier regelmäßig kein Zusatzwissen, das eine individuelle Zuordnung ermöglichen würde, vorhanden ist.

Gleichwohl stellt die Speicherung personenbezogener Daten auch in der geschilderten Form einen Eingriff in das informationelle Selbstbestimmungsrecht des Betroffenen dar, da die speichernde Stelle aufgrund ihrer Kenntnisse die "anonymisierten" Daten ohne weiteres wieder einzelnen natürlichen Personen zuordnen kann. Dies bedeutet, daß auch bei der "anonymisierten" Speicherung von Einzeldatensätzen die Bestimmungen des Hamburgischen Datenschutzgesetzes und sonstige datenschutzrechtliche Spezialregelungen (z.B. § 203 StGB — Ärztliche Schweigepflicht) Anwendung finden müssen. Die Speicherung und Verarbeitung personenbezogener Daten ist gem. § 5 Abs. 1 HmbDSG nur zulässig, wenn eine Rechtsvorschrift sie erlaubt oder der Betroffene eingewilligt hat. Davon kann nur dann abgewichen werden, wenn durch geeignete technische Maßnahmen sichergestellt ist, daß eine individuelle Zuordnung der Datensätze zu natürlichen Personen auch der speichernden Stelle mit vertretba-

rem Aufwand nicht möglich ist. Dies wäre z.B. dann der Fall, wenn Identifikationsmerkmale (z.B. Patientennummer) ganz weggelassen oder so verfremdet werden, daß sie auch mit Zusatzwissen einen Rückgriff auf die einzelne Person nicht mehr ermöglichen.

3.3.4 Forderungen/Anregungen

Angesichts der dargestellten Problematik müßten nach der Beschlußlage des Akademischen Senats streng genommen alle Dateien mit Daten von bestimmbaren natürlichen Personen gelöscht werden, da personenbezogene Daten ja nicht im Rechenzentrum verarbeitet werden dürfen. Dies wäre aber im Hinblick auf das nur geringe Risiko nicht angemessen.

M.E. würde es genügen, wenn das Rechenzentrum die Benutzer auf die Tragweite des Verbots der Verarbeitung personenbezogener Daten hinweist und Sanktionen für die Nichtbeachtung vorsieht. Dabei sollte insbesondere darauf hingewirkt werden, daß auf Identifikatoren, die eine Zuordnung zu bestimmten natürlichen Personen ermöglichen, weitgehend verzichtet wird. Sofern dies vom Forschungsansatz her im Einzelfall nicht zu leisten ist, also ein Rückgriff auf die Daten bestimmter Personen für den Forschungszweck unerläßlich ist, müssen die für den jeweiligen Bereich zuständigen Fachbereiche bzw. angeschlossenen Institutionen Ausnahmegenehmigungen erteilen. Dabei ist darauf zu achten, daß das für eine De-Anonymisierung erforderliche Zusatzwissen (z.B. Listen mit namentlicher Zuordnung von gespeicherten Codes) getrennt von den übrigen Daten aufbewahrt, geheimgehalten und vor unberechtigtem Zugriff besonders gesichert wird. Die aufgrund dieser Ausnahmegenehmigungen angelegten Dateien unterliegen voll dem Datenschutzgesetz einschließlich der Meldepflichten gem. § 13 Abs. 4 HmbDSG.

Das Verbot sollte in einer ausdrücklichen Regelung in den Organisationsbestimmungen oder in der Benutzerordnung ausdrücklich festgeschrieben werden. Ferner habe ich vorgeschlagen, daß das RZ selbst — stichprobenartig — die Einhaltung des Verbots der Verarbeitung personenbezogener Daten überwacht.

3.4 Schriftgutvernichtung

In meinem 6. Tätigkeitsbericht (S. 18 f.) habe ich geschildert, welche Probleme bei der Phase der Löschung von Daten auftreten können. Ich habe darauf hingewiesen, daß die Verwaltung noch nicht genug getan hat, um jederzeit eine geordnete, datenschutzrechtlich einwandfreie Vernichtung von Datenträgern aller Art (Akten, Magnetbänder, Disketten, Platten von Diktiergeräten, Carbonkassetten, Mikrofilmmaterial) sicherzustellen. Und ich habe über das Vorhaben des Senatsamtes für den Verwaltungsdienst und der Finanzbehörde berichtet, durch eine Veröffentlichung von "Hinweisen zur Schriftgutvernichtung" und eines "Mustervertrages" für die Auftragsvergabe an private Vernichtungsunternehmen den Behörden Hilfestellung bei der Bewältigung dieser Aufgabe zu geben.

Im Berichtsjahr ist dieses Vorhaben des Senatsamtes und der Finanzbehörde immer noch nicht in die Tat umgesetzt worden. Im Verlaufe mehrerer Abstimmungsrunden unter den beteiligten Behörden wurden immer wieder neue und alte Argumente gegen die Form der Regelung bzw. die Art der Veröffentlichung (1), gegen die Praktikabilität der Regelungen (2) und gegen einzelne Klauseln bzw. Formulierungen (3) vorgetragen. Wenn auch einzelne Bedenken und Anregungen berechtigt und nützlich gewesen sein mögen, so bedaure ich gleichwohl die Folge dieses nicht gerade zügigen Vorgehens, daß nämlich den Behörden bis heute keine Handreichung zur Schriftgutvernichtung zur Verfügung gestellt worden ist.

(1) Das Senatsamt für den Verwaltungsdienst hatte im Februar 1988 den Entwurf einer Bekanntmachung in den Mitteilungen für die Verwaltung vorgelegt, in dem berücksichtigt worden war, daß

— die Gestaltung innerbehördlicher organisatorischer Regelungen grundsätzlich in die eigene Zuständigkeit der Behörden fällt,

— detaillierte Regelungen nach dem Ergebnis des Erfahrungsaustauschs mit den beteiligten Behörden sowohl wegen der Unterschiedlichkeit der örtlichen und organisatorischen Verhältnisse als auch aus Gründen der Wirtschaftlichkeit nicht getroffen werden können,

— und der sich deswegen auf wesentliche generelle Vorgaben beschränkte.

In der Bekanntmachung wurde auf einen von der Finanzbehörde im Januar 1988 vorgelegten, ebenfalls zur Veröffentlichung in den MittVw vorgesehenen Mustervertrag für die Vergabe von Aufträgen zur Vernichtung entbehrlicher Informationsträger hingewiesen.

Ich hatte den Entwürfen der Bekanntmachung und des Mustervertrages zugestimmt und eine baldige Veröffentlichung erwartet. Im August übersandte das Senatsamt dann jedoch einen neuen Entwurf für die Bekanntmachung in den MittVw. Die Bekanntmachung enthielt jetzt nur noch die "Grundsätze der Erfassung und Verwertung von Altpapier und anderen verbrauchten Datenträgern", während ein Informationsschreiben "nähere Erläuterungen sowie Hinweise zur praktischen Umsetzung" enthielt. Begründet wurde dies damit, daß eine Behörde im Rahmen des Abstimmungsverfahrens die ursprüngliche Bekanntmachung als zu umfangreich und detailliert kritisiert und darauf hingewiesen hatte, eine so umfassende Verfahrensregelung widerspreche den Bemühungen der Verwaltung um eine Eindämmung der Vorschriftenflut. Ich hielte es für wünschenswert, wenn in der Bekanntmachung als zu beachtender Grundsatz nicht — wie vorgesehen — nur die umweltfreundliche Beseitigung der Datenträger, sondern auch eine datenschutzrechtlich einwandfreie Beseitigung genannt wird. Im übrigen habe ich der Veröffentlichung auch in der neuen Form zugestimmt, wenngleich mir nicht einleuchtet, inwiefern es der Verwaltungsvereinfachung dienen soll, wenn die — erwiesenermaßen notwendigen — Informationen zum Problem nicht im Zusammenhang gegeben, sondern auf mehrere Unterlagen verteilt werden.

(2) Bedenken, die Regelungen seien nicht praktikabel, sind gegen die Vorgaben zur Sammlung von Datenträgern mit geschützten Daten erhoben worden. Gerade zu diesem Problem werden jedoch keine starren Regeln vorgeschrieben, sondern es werden Erfahrungen und Lösungswege aufgezeigt, im übrigen werden die Behörden und Ämter jedoch aufgefordert, "durch geeignete Maßnahmen sicherzustellen, daß das gesammelte Material bis zur Vernichtung oder bis zum Abtransport vor dem Zugriff durch Unbefugte geschützt ist (z.B. verschlossene Sammelbehälter; Aufstellung der Behälter in verschlossenen Räumen)." Die Kritik geht also fehl, denn den Behörden steht jede Lösungsmöglichkeit, die sie für praktikabel halten, offen — wenn diese Lösung nur die in der Regelung genannten Anforderungen erfüllt.

(3) Bei den Stellungnahmen zu einzelnen Klauseln handelte es sich mehr oder weniger um redaktionelle Änderungsvorschläge. Lediglich eine Stellungnahme enthielt den datenschutzrechtlich nicht akzeptablen Vorschlag, für einen bestimmten Aktenvernichtungsbetrieb eine Ausnahmeklausel in dem Mustervertrags-Entwurf vorzusehen. Dieser Vorstoß konnte jedoch keinen Erfolg haben, weil die Anforderungen, die bei der Schriftgutvernichtung zu erfüllen sind, sich nach der Art der in dem Schriftgut gespeicherten Daten zu richten haben und nicht nach den — möglicherweise eingeschränkten — Möglichkeiten eines potentiellen Auftragnehmers.

Ich muß also feststellen, daß es auch 1988 leider nicht gelungen ist, der hamburgischen Verwaltung Hinweise zur Schriftgutvernichtung an die Hand zu geben. Ich muß daher befürchten, daß dieses Problem auch 1988 noch nicht überall befriedigend gelöst worden ist. Spektakuläre Aktenfunde sind allerdings — glücklicherweise — ausgeblieben.

3.5 Neue Medien

3.5.1 Rundfunkfinanzierungsstaatsvertrag

Die Datenschutzbeauftragten der öffentlichen Rundfunkanstalten haben mit einem Entwurf vom 3. März 1988, der auch von den Justitiaren der Rundfunkanstalten beraten

wurde, eine Ergänzung des Staatsvertrages über die Höhe der Rundfunkgebühr (Rundfunkfinanzierungsstaatsvertrag) um datenschutzrechtliche Bestimmungen vorgeschlagen.

Ich habe mich gegenüber der Senatskanzlei im Grundsatz positiv zu dem Vorhaben, den Staatsvertrag um eine bereichsspezifische Datenschutzregelung zu ergänzen, geäußert. Ich habe aber zugleich darauf hingewiesen, daß nach meiner Ansicht die vorgeschlagenen Formulierungen das Ziel einer verfassungsrechtlich einwandfreien Rechtsgrundlage für die Datenverarbeitung beim Gebühreneinzug nicht erreichen.

3.5.1.1 Datenerhebung

Der Entwurf hatte vorgesehen, daß die zuständige Rundfunkanstalt personenbezogene Daten, die für den Einzug der Rundfunkgebühren erforderlich sind, über Personen, bei denen die begründete Vermutung besteht, daß sie ein Rundfunkempfangsgerät zum Empfang bereithalten, erheben darf. Diese Formulierung könnte als Erweiterung des Art. 5 Abs. 4 des Staatsvertrages ausgelegt werden, der ausschließlich die Offenbarung durch den Betroffenen erlaubt. Neben der Datenerhebung beim Betroffenen würde so auch die Datenerhebung bei Dritten erlaubt, ohne daß die Voraussetzungen eines solchen Eingriffes genauer spezifiziert würden.

3.5.1.2 Speicherung

Es ist notwendig, in einer zu schaffenden bereichsspezifischen Datenschutzregelung die Art der gespeicherten Daten genau zu beschreiben. Der Hinweis auf die Erforderlichkeit der Daten im Hinblick auf die Aufgabenerfüllung bringt hier keine weiteren über das allgemeine Datenschutzrecht hinausgehenden Klärungen. Für bedenklich halte ich es, wenn in diesem Zusammenhang die Speicherung auch für andere Zwecke (für Werbe- und Informationsmaßnahmen) zugelassen werden sollte.

3.5.1.3 Übermittlung

Auch die Daten, deren Übermittlung zulässig sein soll, und die Übermittlungszwecke müßten genauer umschrieben werden, als dies im Entwurf geschehen ist. Von besonderer Bedeutung ist hier die Einrichtung von automatisierten Abrufverfahren. Ich bin der Auffassung, daß automatisierte Abrufverfahren — durch die ja in besonderer Weise in das Recht auf informationelle Selbstbestimmung eingegriffen wird — nur eingerichtet werden dürfen, wenn für die konkrete Aufgabenerfüllung ein Direktzugriff erforderlich ist. Ich sehe nicht, warum dies bei der Übermittlung von Gebührendaten zwischen den Landesrundfunkanstalten der Fall sein soll.

Die bei der Einrichtung von automatisierten Abrufverfahren zu beachtenden datenschutzrechtlichen Bestimmungen dürfen nicht hinter den in den neueren Landesdatenschutzgesetzen (Hessen, Nordrhein-Westfalen, Bremen) getroffenen Regelungen zurückbleiben. Auch der Referentenentwurf für ein neues Hamburgisches Datenschutzgesetz sieht vor, daß automatisierte Abrufverfahren nur auf Grundlage einer Rechtsverordnung zulässig sind, wobei die Verordnung den Datenempfänger, die Datenart und den Zweck des Abrufs festzulegen hat. Die Verordnung hat Maßnahmen zur Datensicherung und zur Datenschutzkontrolle vorzusehen.

Der Entwurf enthielt eine Klausel, wonach öffentliche Stellen, die personenbezogene Daten von Rundfunkteilnehmern verarbeiten, diese Daten an die zuständige Rundfunkanstalt für die ihr im Rahmen des Rundfunkgebühreneinzugs obliegenden Aufgaben übermitteln dürfen. Damit sollte offenbar die Übermittlung von Daten durch die Sozialleistungsträger an die Landesrundfunkanstalten erlaubt werden, u.a. sollte der Grund der Befreiung von der Rundfunkgebühr übermittelt werden dürfen, was bisher nicht zulässig war. Abgesehen davon, daß auch in dieser Vorschrift eine genaue Benennung der zu übermittelnden Daten fehlte und mithin die erforderliche Normenklarheit nicht gegeben war, hielte ich es für systemwidrig, das Sozialgeheimnis durch einen Länderstaatsvertrag zum Rundfunkgebührenwesen einzuschränken, zumal es

sehr zweifelhaft erscheint, ob datenschutzrechtliche Spezialregelungen des Bundesrechts (hier: SGB X) überhaupt durch Landesrecht verdrängt werden können.

3.5.1.4 Löschung

Es muß eine Frist festgelegt werden, in der personenbezogene Daten nach dem Ende des Teilnehmerverhältnisses regelhaft zu löschen sind. Der Entwurf sah vor, daß personenbezogene Daten über Ordnungswidrigkeitenverfahren spätestens fünf Jahre nach Abschluß des jeweiligen Verfahrens zu löschen seien. Ich habe nicht nachvollziehen können, für welchen Zweck die Daten über Ordnungswidrigkeitenverfahren so lange gespeichert bleiben dürfen, zumal der Anspruch auf Rundfunkgebühren gem. Art. 5 Abs. 3 nach vier Jahren verjährt.

3.5.1.5 Datenverarbeitung im Auftrag

Natürlich steht es den Landesrundfunkanstalten — wie anderen öffentlichen und nichtöffentlichen Stellen auch — offen, ihre Daten im Auftrag verarbeiten zu lassen. Da die Regelungen des Staatsvertrages die entsprechenden Regelungen der Landesdatenschutzgesetze verdrängen sollen, muß an die Auftragsverhältnisse aber zumindest der Maßstab angelegt werden, den die neueren Datenschutzgesetze aufstellen in bezug auf

— die Auswahl des Auftragnehmers (insbesondere Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen),

— die Form der Beauftragung,

— die Weisungsgebundenheit des Auftragnehmers.

Sofern einer anderen Institution nicht nur die Datenverarbeitung im engeren Sinne, sondern auch Teile der im Gebührenstaatsvertrag geregelten Fachaufgaben übertragen werden sollen (wie dies de facto gegenüber der Gebühreneinzugszentrale schon geschieht), kann nicht mehr von der Konstruktion der "Datenverarbeitung im Auftrag" ausgegangen werden; diese Institution wäre dann selbst als "speichernde Stelle" im Sinne des Datenschutzrechts anzusehen. Wenn dies beabsichtigt wird, ist hierfür eine eigene Rechtsgrundlage notwendig.

Aufgrund der hier referierten datenschutzrechtlichen Bedenken gegen den vorgelegten Entwurf, die auch von anderen Datenschutzbeauftragten und zum Teil auch von den zuständigen Landesbehörden geteilt werden, haben die Länder darauf verzichtet, die zunächst vorgesehene Datenschutzklausel bei der Modifikation des Rundfunkfinanzierungsstaatsvertrages zu berücksichtigen. Gleichwohl ist festzuhalten, daß die Bemühungen fortgesetzt werden müssen und hoffentlich zu einem alsbaldigen Ergebnis führen werden.

3.5.2 Telekommunikation

Mit nahezu 28 Millionen Teilnehmern — davon mehr als 27 Millionen Telefonkunden — ist das öffentliche Telekommunikationsnetz bereits heute eng geknüpft. Immer mehr Leistungen werden unter Einsatz von Telekommunikationstechnik abgewickelt; neue Medien dringen in immer weitere Anwendungsgebiete vor. Die wirtschaftliche und auch die datenschutzrechtliche Bedeutung der Telekommunikation (TK) nimmt mit der Telematisierung großer Lebensbereiche ständig zu. Bei der TK fällt eine Vielzahl personenbezogener Daten an; die Post gehört bereits heute zu den bedeutendsten Datenverarbeitern in der Bundesrepublik. Die Ausgestaltung datenschutzrechtlicher Regelungen entfaltet mithin erhebliche Breitenwirkung. So betrifft die Entscheidung darüber, welche Verbindungsdaten gespeichert werden dürfen und wann sie zu löschen sind, nahezu jeden Bürger.

In Bezug auf die Tiefe des Eingriffs in das Recht auf informationelle Selbstbestimmung ist die TK im Begriff, eine neue Qualität zu erreichen: Mit dem Übergang zu digitaler Vermittlungstechnik fallen an zentraler Stelle weitaus mehr Kommunikationsdaten an

als bei analoger Vermittlung. Diese Daten sind einem hohen Mißbrauchsrisiko ausgesetzt, da sich aus ihnen detaillierte Angaben über das Kommunikationsverhalten der Teilnehmer gewinnen lassen. Während bei herkömmlicher (analoger) Vermittlungstechnik die Verbindungsdaten — wie z.B. die angerufene Telefonnummer — in keiner Vermittlungseinrichtung in auswertbarer Weise anfallen, ist dies bei digitalen Vermittlungsstellen anders: Die Verbindung wird nicht mehr schrittweise aufgebaut, sondern in einem Akt durchgeschaltet, wobei die gesamte angewählte Rufnummer und die Nummer des Ausgangspunktes der Verbindung gespeichert werden.

Die Planungen der Deutschen Bundespost sehen vor, beim Übergang zu ISDN

— Rufnummern der Anschlüsse, von denen Wählverbindungen aufgebaut werden,

— Rufnummern der Anschlüsse, zu denen Wählverbindungen aufgebaut wurden,

— in Anspruch genommene Telekommunikations-Dienstleistungen (z.B. Telefax-Dienst) und Dienstleistungsmerkmale (z.B. Anruf-Weiterleitung) sowie

— Datum, Beginn oder Dauer und Ende der Verbindung

in wenigen regionalen Gebührenrechenzentren zusammenzuführen und dort erst 80 Tage nach Rechnungstellung zu löschen. In dieses Verfahren sollen die Daten aller Teilnehmer einbezogen werden (BT-Drs. 11/2853, S. 8 — Antwort der Bundesregierung auf eine Kleine Anfrage der Fraktion der GRÜNEN). Abgesehen davon, daß sich diese Planungen nicht mit den Bestimmungen der TKO vereinbaren lassen, würde ihre Umsetzung in den Gebührenrechenzentren in bislang unbekanntem Umfang Kommunikationsdateien entstehen lassen, mit deren Hilfe sich umfassende Kommunikationsprofile einzelner Teilnehmer und Teilnehmergruppen gewinnen lassen.

Auch gegenüber dem jeweiligen Kommunikationspartner werden in stärkerem Maße als bisher personenbezogene Daten offenbart. Zu der bei modernen Nebenstellenanlagen ohnehin möglichen Aufzeichnung und Auswertung der Zielnummern kommt mit der Einführung von ISDN die Möglichkeit zur Feststellung und Auswertung der Anschlüsse, von denen Verbindungen ausgehen (Anrufer), und zwar auch dann, wenn die Verbindung nicht von einem ISDN-Anschluß aufgebaut worden ist, sonderen von einem normalen analogen Telefonapparat.

Neue Techniken gestatten zunehmend auch die Überwachung der Kommunikationsinhalte. Dies gilt zunächst für die Dienste, bei denen digitalisierte Daten und Texte übermittelt werden (z.B. Teletex, Btx-Mitteilungsdienst, Datex-P). Mittels geeigneter Programme lassen sich Mitteilungen mit interessanten Inhalten herausfiltern und aufzeichnen. Sobald leistungsfähige Spracherkennungssysteme entwickelt sein werden, kann auf die gleiche Weise auch die Sprachkommunikation, also auch der Telefonverkehr, automatisiert überwacht werden.

3.5.2.1 Poststrukturgesetz

Im Verlauf des Jahres 1988 haben die Pläne der Bundesregierung zur Umstrukturierung des Telekommunikationswesens Gestalt angenommen. Die Bundesregierung hat im September 1988 den Entwurf eines Gesetzes zur Neustrukturierung des Post- und Fernmeldewesens und der Deutschen Bundespost (PostStruktG) — BT-Drs. 11/2854 vom 2.9.1988 —, mit dem das Post- und Fernmeldewesen grundlegend verändert werden soll, im Bundestag eingebracht. Datenschutzrechtlich bedeutsam ist, daß zeitgleich mit der fortschreitenden Digitalisierung und Integration bisher getrennt betriebener Netze im ISDN das Netzmonopol der Deutschen Bundespost eingeschränkt und ihr Dienstmonopol weitgehend aufgehoben werden soll. Im einzelnen ist folgendes geplant:

— Im Fernmeldewesen soll das Postmonopol zur Ausnahme, der Wettbewerb zur Regel werden. Das Netzmonopol soll zwar bestehen bleiben, wird aber auf die Leitungsbereitstellung beschränkt. Bereits auf der Ebene der Leitungsvermittlung können so private Anbieter in Konkurrenz zur Telekom treten. Für verschiedene Funkdienste wird auf das Netzmonopol völlig verzichtet.

— Alle TK-Dienste außer dem Telefondienst, der auch in Zukunft allein von der Post abgewickelt werden soll, können in Zukunft auch von privaten Unternehmen angeboten werden, die unter Nutzung posteigener Übertragungsleitungen Anlagen zur Vermittlung, Speicherung und Verarbeitung von Informationen Fernmeldedienstleistungen für Dritte erbringen dürfen (Art. 3 § 1 Abs. 4 E-PostStrukG). Eine datenschutzrechtliche Bindung der privaten Dienstanbieter ist nicht vorgesehen. Lediglich Betreiber von Fernmeldeanlagen, die Telekommunikationsleistungen für andere erbringen (diese müssen nicht unbedingt mit den Dienstanbietern identisch sein), haben ihren Betrieb sowie Änderungen und Aufgabe beim Bundesminister für Post und Telekommunikation anzuzeigen.

— Auch das Endgerätemonopol der Post soll aufgehoben werden. Bei der Zulassung von Endgeräten durch das Ministerium für Post und Telekommunikation sind lediglich technische Prüfungen zur Sicherstellung der Funktionsfähigkeit des TK-Netzes vorgesehen.

Die von der Bundesregierung vorgesehenen Maßnahmen dienen dem gemeinsamen Ziel, neue Märkte für Telekommunikationsleistungen und -endgeräte zu fördern, das wirtschaftliche Wachstum zu steigern und die internationale Wettbewerbsfähigkeit der Hersteller- und der Anwenderindustrie zu stärken.

Bei der Konzentration auf diese wirtschaftspolitischen Ziele wird leider häufig übersehen, daß die Nutzung von Fernmeldeanlagen mit individuellen und gesellschaftlichen Risiken verbunden ist, die sich mit den laufenden technischen Änderungen und mit der Ausweitung des Geräteeinsatzes und des Telekommunikationsverkehrs noch verstärken werden. Die zur Entscheidung anstehenden ordnungspolitischen Änderungen tragen diesen Risiken nicht Rechnung. Die vorgesehene Deregulierung erhöht vielmehr die Risiken und schwächt bisherige Einrichtungen zur Risikobewältigung.

3.5.2.2 Gefahr der Dreiteilung des Datenschutzes

Die Verwirklichung dieses Entwurfs hätte faktisch eine Dreiteilung des Datenschutzes bei der TK zur Folge:

— Für die Post gelten — soweit sie im Monopol Leistungen erbringt — weiterhin die Vorschriften des BDSG für öffentliche Stellen (zweiter Abschnitt).

— Soweit die Post im Wettbewerb mit privaten TK-Anbietern steht, gelten für sie zwar die Kontrollvorschriften für den Öffentlichen Bereich (§§ 15-21 BDSG), finden aber die materiell-rechtlichen Regelungen für die Datenverarbeitung nicht-öffentlicher Stellen (dritter Abschnitt) Anwendung.

— Für private TK-Anbieter gelten allein die Vorschriften des dritten BDSG-Abschnittes.

Während für die Post jedoch zusätzliche — wenn auch verbesserungsbedürftige — bereichsspezifische Regelungen gelten (nämlich die TKO), gibt es für die privaten TK-Anbieter solche speziellen Datenschutzvorschriften nicht, so daß sich hier die Regelungsdefizite und Mängel des BDSG besonders gravierend auswirken:

— Durch die Beschränkung auf Datenverarbeitung in Dateien stehen Inhaltsdaten, die nicht als Dateien i.S.d. BDSG gespeichert werden, nicht unter dem Schutz des Gesetzes. Dies betrifft z.B. Fax- und Textdienste, die auch im privaten Bereich an Bedeutung gewinnen werden.

— Die Erhebung von Daten wird nicht normiert. Gerade weil sich in diesem Bereich durch das automatisierte Entstehen von Verbindungsdaten und die Verbreitung neuer Dienste zusätzliche Risiken auftun, sind hier besondere Regelungen notwendig.

— Bei der TK ist es i.d.R. schwierig, die speichernde Stelle i.S.v. § 2 Abs. 2 Nr. 1 BDSG zu bestimmen, bei der der Betroffene seine Rechte geltend machen kann und der die Verpflichtung zur Datensicherung (§ 6 BDSG) obliegt.

— Nicht eindeutig feststellbar ist bei der TK häufig auch, ob es sich um Datenverarbeitung nicht-öffentlicher Stellen für eigene oder für fremde Zwecke handelt und ob dementsprechend der dritte oder der vierte Abschnitt des BDSG Anwendung findet.

Das BDSG geht mit seinen Bestimmungen von der Vertragsfreiheit der Beteiligten aus. Dies bedeutet, daß die Gewährleistung des Datenschutzes in starkem Maße in die Dispositionsfreiheit der Anbieter gestellt wird, wobei die Chancen des Kunden, die Vertragsbestimmungen zu beeinflussen, recht gering sind.

So ist die Speicherung bzw. Übermittlung von Daten gem. §§ 23, 24 BDSG zulässig im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen oder nach Abwägung der berechtigten Interessen der Beteiligten oder der Allgemeinheit mit den schutzwürdigen Belangen des Betroffenen. Die privatwirtschaftlichen TK-Anbieter und der Wettbewerbsbereich der Telekom dürften Verbindungsdaten also durchaus auch für Werbezwecke speichern, da das Nutzungsverhalten der Kunden Anhaltspunkte dafür liefern könnte, wie sich die Geschäftsbeziehungen noch ausbauen ließen. Die BDSG-Novelle erlaubt sogar generell, personenbezogene Daten — nach Gruppen geordnet — für Zwecke der Werbung oder Markt- oder Meinungsforschung zu übermitteln; die Bundesregierung geht dabei davon aus, daß in diesen Fällen ein entgegenstehendes berechtigtes Interesse des Betroffenen nicht besteht (§ 26 Abs. 2 Nr. 2 E-BDSG).

Auch in bezug auf die Kontrolle der Einhaltung von datenschutzrechtlichen Bestimmungen würde die vorgesehene Liberalisierung des Fernmeldewesens einen Rückschritt bedeuten. Nach § 19 BDSG unterliegt die Post als Teil der Bundesverwaltung der umfassenden Kontrolle durch den Bundesbeauftragten für den Datenschutz. Demgegenüber hat die für den privaten Bereich zuständige Aufsichtsbehörde gem. § 30 BDSG nur im Einzelfall das Recht, die Ausführung der Datenschutzvorschriften zu überwachen. Sie kann nur dann prüfend tätig werden, wenn ein Betroffener begründet darlegt, daß er bei der Verarbeitung von Daten in seinen Rechten beeinträchtigt wird (Anlaßkontrolle).

Ob die Vorschriften des BDSG für alle privaten TK-Dienste überhaupt verbindlich sind, ist durchaus nicht sicher, denn § 1 Abs. 3 BDSG nimmt personenbezogene Daten, die durch Unternehmen und Hilfsunternehmen der Presse, des Rundfunks und des Films für eigene publizistische Zwecke verarbeitet werden, von seinem Schutz aus (sog. "Medienprivileg", vgl. Ziff. 3.6.1). Zumindest in bestimmten Teilbereichen (z.B. bei Mailboxen und "elektronischen Pin-Wänden") weisen TK-Dienste presseähnliche Funktionen auf. Für diese Dienste sind also — sofern sie von Privaten angeboten werden — möglicherweise nicht einmal die einschlägigen BDSG-Bestimmungen anwendbar, sondern die — in bezug auf den Schutz des Rechts auf informationelle Selbstbestimmung noch unbefriedigenderen — Regelungen des Presserechts.

3.5.2.3 Parlamentsvorbehalt

Das Bundesverfassungsgericht hat wiederholt festgestellt, daß die für die Gestaltung der Lebensumstände wesentlichen Entscheidungen — zumal wenn sie mit Grundrechtseingriffen verbunden sind — unter Parlamentsvorbehalt stehen (vgl. BVerfGE 33, 125, S. 158 f.; BVerfGE 47, 46, S. 79; BVerfGE 49, 89, S. 132). Dies trifft auch auf die bei der TK zu erlassenden datenschutzrechtlichen Regelungen zu.

Damit das Grundrecht auf informationelle Selbstbestimmung auch auf diesem Gebiet gewährleistet bleibt, müssen bereichsspezifische, für öffentliche wie für private Netz- und Dienstbetreiber gleichermaßen verbindliche Datenschutzregelungen im Gesetz verankert werden. Dies bedeutet zwar nicht, daß der Gesetzgeber alle von den Betreibern im einzelnen zu treffenden Maßnahmen konkret vorzuschreiben hätte. Dies wäre angesichts der Komplexität der bei der TK eingesetzten Technik auch lebensfremd (vgl. BVerfGE 56, 1, S. 13). Das Parlament muß aber den Rahmen für diesbezügliche Entscheidungen festlegen und die datenschutzrechtlichen Mindestanforderungen definieren.

3.5.2.4 Anforderungen an die Bestimmtheit von Verordnungsermächtigungen

Aufgrund der hohen Bedeutung von Eingriffen in das informationelle Selbstbestimmungsrecht bei der TK sind an den Bestimmtheitsgrad datenschutzrechtlicher Verordnungsermächtigungen strenge Maßstäbe anzulegen. Von den verschiedenen im Paket vorgesehenen Verordnungsermächtigungen weist nur die Ermächtigung des Art. 1 § 26 Abs. 2 EPostStruktG Bezug zur Gewährleistung des Datenschutzes auf. Diese Verordnungsermächtigung bleibt mit ihrem allgemeinen Verweis auf "Regelungsgrundsätze des BDSG" (Gesetzesbegründung) zu pauschal und genügt nicht den an eine bereichsspezifische Datenschutzregelung zu stellenden Ansprüchen, zumal diese Grundsätze durch den Verweis auf die Berücksichtigung der berechtigten Interessen des jeweiligen Unternehmens, die ebenfalls zu beachten sind, noch relativiert werden.

Der bloße Hinweis auf die "Beachtung des Grundsatzes der Verhältnismäßigkeit, insbesondere der Beschränkung der Erhebung und Verarbeitung auf das Erforderliche" wiederholt einerseits nur den allgemein gültigen Verhältnismäßigkeitsgrundsatz, läßt andererseits mit dem einfachen Hinweis auf das "Erforderliche" offen, worauf die Erforderlichkeit zu beziehen ist: Gerade der Umfang und die Art von Daten, die für bestimmte Dienste erforderlich sind, muß ein Kriterium für die Einführung von Diensten sein.

Welche Daten bei der TK erforderlich und wie sie zu verarbeiten sind, muß bereichsspezifisch geregelt werden. Bereichsspezifischen Regelungen muß es auch vorbehalten bleiben, die Zwecke der Verarbeitung enger zu definieren und festzulegen, in welchen Fällen eine zweckfremde Verwendung von Daten zulässig ist.

3.5.2.5 Materielle Anforderungen an bereichsspezifische Regelungen

Aus meiner Sicht müßte eine bereichsspezifische Datenschutzregelung für die TK folgende Komplexe umfassen:

— Die Datenverarbeitung (Erhebung, Speicherung und Übermittlung) muß auf das unerläßliche Ausmaß beschränkt werden. Verbindungsdaten müssen von der Übermittlung ausgeschlossen sein, da sie ein besonders hohes Mißbrauchsrisiko in sich bergen.

— Personenbezogene Daten müssen einer strengen dienstbezogenen Zweckbindung unterworfen werden. Es reicht nicht aus — wie z.B. mit § 454 TKO —, den Zweck der Verarbeitung allein auf "Telekommunikationszwecke" zu beschränken. Dieser Begriff ist unscharf und läßt die Auswertung und Übermittlung von Daten für sehr verschiedenartige Zwecke zu (z.B. für technische Test- und Meßverfahren im Rahmen von Kapazitätsplanungen, Gebührenermittlungen bzw. Nachweis von Forderungen der Post gegenüber privaten Dienstanbietern). Das Zweckbindungsgebot muß so gefaßt werden, daß im Rahmen eines Dienstes anfallende Daten auch nur für die Abwicklung des jeweiligen Dienstes verarbeitet werden dürfen und — nachdem der Zweck erfüllt ist — zu löschen sind. So müssen Verbindungsdaten nach Auslösen der Verbindung generell gelöscht werden. Ausnahmen — etwa für die Sicherstellung des Datenschutzes — dürfen nur aufgrund besonderer Vorschriften in einem eng begrenzten Rahmen erlaubt werden.

— Ein formalisiertes Zulassungsverfahren muß gewährleisten, daß die Dienstbetreiber die Datenschutzvorschriften einhalten. Eine bloße Anzeigepflicht (Art. 3 § 1a Abs. 1 PostStrukG) reicht nicht aus. Die Genehmigungsbehörde sollte dazu verpflichtet werden, darauf zu achten, daß der jeweilige Dienst datenschutzfreundlich gestaltet wird, so daß die dabei anfallenden personenbezogenen Daten minimiert werden.

— Dienstanbieter und Netzbetreiber müssen zu einer umfassenden Information über die technischen Bedingungen und Risiken der jeweiligen Dienste verpflichtet werden, da jeder Kommunikationsdienst technisch bedingte Risiken in sich birgt, die für den Teilnehmer angesichts der Komplexität und Vielfalt der eingesetzten Systeme in der Regel nicht ohne weiteres erkennbar sind. Die Kenntnis der grundle-

genden Bedingungen und Risiken, die mit einer Inanspruchnahme eines Telekommunikationsdienstes verbunden sind, ist eine Grundvoraussetzung dafür, daß sich der informierte und verantwortungsbewußte Bürger für oder gegen eine Inanspruchnahme des jeweiligen Angebotes entscheiden kann. Eine solche Informationspflicht würde auch die Markttransparenz verbessern, wenn verschiedene Betreiber ähnliche oder auf den ersten Blick sogar identische Dienste anbieten.

— Dienstanbieter und Netzbetreiber müssen dazu verpflichtet werden, geeignete technische und organisatorische Maßnahmen zur Sicherstellung des Datenschutzes zu ergreifen. Sie müssen gewährleisten, daß die übertragenen und gespeicherten Daten nur den dazu Berechtigten zur Kenntnis gelangen. So muß technisch sichergestellt werden, daß

  - die Anzeige der Kennung des Anschlusses, von dem eine Verbindung ausgeht, beim Empfänger nur mit Zustimmung und mit Kenntnis des Anrufers und des Empfängers erfolgen kann,
  - die Speicherung von Nutzungsdaten in Vermittlungseinrichtungen ausgeschlossen ist,
  - personenbezogene Daten über Teilnehmer durch Dritte nicht ausgelesen werden können,
  - bei der Gebührenspeicherung nutzungsneutrale oder zumindest teilnehmerseitige Formen der Speicherung Vorrang vor netz- bzw. betreiberseitiger Speicherung bekommen,
  - betreiber- und netzseitig Verschlüsselungsdienste angeboten werden.

  Die Maßnahmen haben sich am Stand der Technik zu orientieren.

— Auch bei Inanspruchnahme von Diensten privater Anbieter muß der Benutzer sichergehen können, daß die gesetzlichen Schutzvorschriften nicht vertraglich oder im Rahmen von allgemeinen Geschäftsbedingungen außer Kraft gesetzt werden. Es darf sich nicht um dispositives Recht handeln, das — je nach Marktverhältnissen — durch Private ausgehandelt und abgeschwächt oder aufgehoben wird. Sichergestellt werden muß vielmehr, daß die Betreiber von Netzen und die Anbieter von Diensten jeweils den gesetzlich fixierten datenschutzrechtlichen Mindeststandard zu beachten haben. Durch geeignete Regelungen muß auch sichergestellt werden, daß die Datenschutzbestimmungen nicht nur für den Anbieter eines Dienstes (als "Konzessionsnehmer" der Post) gelten, sondern auch für etwa von ihm beauftragte Dritte (Subunternehmer), die an der Erbringung von Diensten beteiligt sind. Zu denken ist etwa an eine Vorschrift entsprechend Art. 9 Abs. 6 Btx-Staatsvertrag vom 18. März 1983, wonach personenbezogene Daten nur abgefragt und gespeichert werden dürfen, soweit dies für das Erbringen der Leistung, den Abschluß oder die Abwicklung von Vertragsverhältnissen erforderlich ist.

— Eine effektive Datenschutzkontrolle muß gewährleistet werden; die für Telekommunikationsdienste zu treffenden Kontrollregelungen dürfen nicht hinter den Stand des Btx-Staatsvertrages und der Mediengesetze zurückfallen. Das bedeutet, daß den zuständigen Datenschutzkontrollinstanzen ein umfassendes Überwachungs- und Kontrollrecht in bezug auf die Einhaltung der Datenschutzvorschriften auch durch Private zugestanden wird und bei Verstößen angemessene und wirksame Sanktionsmechanismen zur Verfügung gestellt werden.

— In Anlehnung an Bestimmungen für andere Technikbereiche sollte die Einführung einer Gefährdungshaftung bei der Verletzung des informationellen Selbstbestimmungsrechts durch Netzbetreiber oder Dienstanbieter erwogen werden, da angesichts der für den Teilnehmer bestehenden Intransparenz des Telekommunikationswesens ein Verschuldensnachweis nur schwer zu führen sein dürfte.

— Den Teilnehmern müßte bezüglich der über sie gespeicherten Daten ein umfassendes Auskunfts-, Sperrungs- und Löschungsrecht eingeräumt werden. Entsprechend

den Regelungen des Art. 9 Abs. 7 Btx-Staatsvertrag müßte festgelegt werden, bei welcher Stelle (Dienstanbieter, Netzbetreiber, Anbieter von Informations-Dienstleistungen) die Rechte eingefordert werden können.

Die genannten Regelungen müssen unabhängig davon gelten, ob die personenbezogenen Daten in Dateien oder nicht dateiförmig gespeichert werden. Vor allem ist zu gewährleisten, daß auch elektronisch gespeicherte und übertragene Mitteilungen geschützt sind. Die Einbeziehung von Kommunikationsinhalten in den Schutz des Gesetzes ist insbesondere deshalb notwendig, weil private Dienstanbieter an Art. 10 GG (Post- und Fernmeldegeheimnis) nicht gebunden sind.

3.5.2.6 Sozialer Zwang muß vermieden werden

In der Vergangenheit ist wiederholt das Argument vorgebracht worden, restriktive Datenschutzregelungen seien bei der Telekommunikation deshalb nicht notwendig, weil es jedermann freistehe, einen Dienst in Anspruch zu nehmen oder nicht. Dem ist entgegenzuhalten, daß es bereits heute faktisch keine Freiwilligkeit etwa bei der Inanspruchnahme des Telefondienstes gibt, da das Telefon — wie auch das Rundfunkgerät — heute zur technischen Grundausstattung eines jeden Haushalts und Unternehmens gehört. Es ist absehbar, daß die Freiwilligkeit der Entscheidung über den Anschluß in Zukunft bei einer zunehmenden Anzahl anderer Dienste ebenfalls faktisch reduziert wird. Auch wenn ein formeller Anschlußzwang nicht vorliegt, kann doch von einer wirklich freien Entscheidung zur Teilnahme oder Nichtteilnahme kaum die Rede sein.

Auch deshalb ist es notwendig, die Datenverarbeitung durch die Dienstbetreiber (Post und Private) restriktiv zu handhaben und die Datenverarbeitung — auch bei Vorliegen entsprechender Einverständniserklärungen — gesetzlich auf das erforderliche Maß zu begrenzen.

Wird bei den Teilnehmern die Einwilligung zur Datenverarbeitung im Rahmen eines TK-Dienstes eingeholt, so sind an die Einwilligungserklärung besondere Anforderungen zu stellen:

— Auf die Einwilligung muß schriftlich besonders hingewiesen werden, wenn die Einwilligung zusammen mit anderen Erklärungen erteilt wird.

— Die Einwilligung muß eine umfassende Information über die Tragweite der Einwilligung, die Verwendung der Daten, insbesondere beabsichtigte Übermittlungen voraussetzen.

— Der Dienstanbieter sollte verpflichtet werden, den Betroffenen auch darüber aufzuklären, welche Folgen eine eventuelle Verweigerung der Einwilligung hat.

— Einwilligungen, die auf der Grundlage unangemessener Drohungen, fehlender oder ungenügender Information oder in sonstiger, gegen Treu und Glauben verstoßender Weise erlangt wurden, müssen unwirksam sein.

— Wenn die Einwilligung im Rahmen der Zustimmung zu allgemeinen Geschäftsbedingungen abgegeben wurde, darf sie nur insoweit wirksam sein, als die Datenverarbeitung, in die eingewilligt wurde, für die Diensterbringung notwendig ist.

— Verweigert ein Betroffener die Einwilligung, dürfen ihm keine Nachteile entstehen, die über die unmittelbaren Kosten der Verweigerung hinausgehen.

— Der Betroffene muß das Recht haben, seine Einwilligung jederzeit zu widerrufen, ohne daß ihm dadurch unangemessene Kosten entstehen.

3.5.2.7 Unzureichende Bindungswirkung der Telekommunikationsordnung (TKO) für private Dienstanbieter

Die TKO fußt auf der Verordnungsermächtigung des § 14 Postverwaltungsgesetz. Danach erläßt der Bundesminister für das Post- und Fernmeldewesen Rechtsverordnungen über die Bedingungen und Gebühren für die Benutzung der Einrichtungen des

Post- und Fernmeldewesens (Benutzungsverordnungen). Die TKO legt fest unter welchen Bedingungen Posteinrichtungen von Dritten genutzt werden dürfen, und bindet dadurch — z.B. über die Definition von Schnittstellen — indirekt auch Private. Ansonsten richtet sich die TKO an die Bundespost, die verpflichtet wird, zu definierten Bedingungen Dienste bereitzustellen. Die Datenschutzbestimmungen der §§ 449 ff. TKO binden ausschließlich die Post.

Gem. Art. 1 § 60 Abs. 1 EPostStrukG treten die aufgrund des § 14 Postverwaltungsgesetz erlassenen Rechtsverordnungen zwei Jahre nach dem Inkrafttreten des Postverfassungsgesetzes außer Kraft, soweit sie nicht vorher aufgehoben worden sind. Materiell tritt die Verordnungsermächtigung gem. Art. 1 § 26 EPostStrukG an die Stelle der Verordnungsermächtigung des § 14 Postverwaltungsgesetz. Durch die vorgesehenen Veränderungen ergibt sich die Notwendigkeit, die TKO zu überarbeiten.

Ob die TKO für die zu bildende Telekom insgesamt bindend sein wird, bleibt unklar, da nicht nur die Struktur der Post, sondern auch die durch sie zu erledigenden Aufgaben grundlegend umgestaltet werden sollen. Ebenfalls offen ist, inwieweit die überarbeitete TKO auch für den Wettbewerbsbereich gelten soll. Art. 1 § 26 Abs. 2 EPostStrukG verpflichtet die Bundesregierung lediglich für den Telefondienst und einen Teilbereich anderer von der Post angebotener Dienste zum Erlaß datenschutzrechtlicher Verordnungen.

Deutlich ist hingegen bereits heute, daß Rechtsverordnungen auf der Grundlage der Verordnungsermächtigung des Art. 1 § 26 Abs. 2 EPostStrukG keine Bindungswirkung für private Anbieter von Telekommunikationsdiensten entfalten können. Das Postverfassungsgesetz soll die Organisation des Postwesens und — zum Teil — das Verhältnis der Unternehmen der Deutschen Bundespost zu Dritten regeln. Es normiert nicht das Verhältnis von Anbietern privater Telekommunikationsdienste, die mit Art. 3 Nr. 1 Abs. 4 EPostStrukG pauschal zugelassen werden, zu deren Kunden. Von privaten Betreibern wären dann lediglich die Vorschriften des BDSG für den privaten Bereich zu beachten, was zu erheblichen datenschutzrechtlichen Verschlechterungen für die Teilnehmer führen würde.

Auch aufgrund der anderen vorgesehenen Verordnungsermächtigungen wird die Bundesregierung keine Möglichkeit haben, verbindliche Datenschutzregelungen für Private zu erlassen. Während der Entwurf des Fernmeldeanlagengesetzes vorsieht, daß zur Vermeidung von Wettbewerbsbeeinträchtigungen (Art.2 § 1a Abs. 2 PostStruktG) und zur Gewährleistung eines ordnungsgemäßen öffentlichen Fernmeldeverkehrs (Art.2 § 2a Abs. 1) dem Bundesminister für Post und Telekommunikation Verordnungsermächtigungen eingeräumt werden und die Voraussetzungen, unter denen Personen Fernmeldegeräte an das Netz der Post anschließen dürfen (Ausbildung, Kenntnisstand usw.) detailliert mit Art. 2 § 2a Abs. 2 geregelt werden sollen, fehlt auch hier jeglicher für private Betreiber verbindliche Hinweis auf die Einhaltung datenschutzrechtlicher Regelungen oder Mindeststandards.

3.5.2.8 Zuständigkeit von Bund und Ländern

Die Zuständigkeit zum Erlaß von Regelungen im Bereich der TK ist geteilt: Zwar unterliegt das Post- und Fernmeldewesen gem. Art. 73 Nr. 7 GG einer ausschließlichen Gesetzgebungskompetenz des Bundes; das Bundesverfassungsgericht hat jedoch in seinem Fernsehurteil festgestellt, daß das Post- und Fernmeldewesen nur den sendetechnischen Bereich, nicht aber den inhaltlichen Bereich umfaßt (BVerfGE 12, 205, S. 225). Gleichwohl hat aber die Gestaltung der fernmeldetechnischen Infrastruktur erhebliche Auswirkungen auf den in Länderkompetenz befindlichen Nutzungsbereich der Neuen Medien. Dem muß durch eine geeignete Form der Entscheidungsfindung, an der auch die Länder angemessen beteiligt werden, Rechnung getragen werden.

Kompetenzrechtliche Probleme treten vor allem bei den Mehrwertdiensten auf, da deren Zusatzfunktionen (Speichern, zum Abruf bereithalten, verändern, Wirkungen auslösen, Retrievel-Methoden bereitstellen, Programmauswahl usw.) Nutzungen dar-

stellen, die über den Bereich der Bereitstellung einer technischen Fernmeldeinfrastruktur hinausgehen. Das PostStrukG enthält keine Regelungen über die Beteiligung der Länder; dies ist allerdings insoweit konsequent, als im Nutzungsbereich gerade keine Kompetenz des Bundes besteht.

Wenn entsprechende Länderregelungen ergehen, sei es wie beim Rundfunk durch Ländergesetze oder wie beim Bildschirmtext durch Staatsvertrag, stellt sich die Frage, in welchem Verhältnis diese zu der pauschalen Dienstzulassung durch Bundesrecht stehen. Ich habe Zweifel, ob der Bund von Verfassung wegen überhaupt berechtigt ist, Dienste, die keine reinen Übertragungsdienste sind, generell zu erlauben. Die Regelung der Bedingungen für die Zulassung von Mehrwertdiensten kann m.E. nur Sache der Länder sein. Wenn mit der zitierten Vorschrift lediglich die Telekom gebunden werden soll, zu nicht diskriminierenden Bedingungen Vorleistungen für private Mitbewerber zu erbringen, müßte dies entsprechend verdeutlicht werden.

Zu fordern ist eine "Schnittstellen-Regelung", die postseitig Verfahren der Zulassung unter Einbeziehung der Länder sowie Umfang und zulässige Nutzungen der bei Mehrwertdiensten anfallenden Netzdaten und "durchgereichten" Nutzungsdaten enthält (zu letzterem vgl. z.B. § 458 Abs. 2 TKO für Fernwirkdienste).

3.5.2.9 Einschränkung des Post- und Fernmeldegeheimnisses bei neuen Medien?

Durch Art. 10 GG werden das Post- und Fernmeldegeheimnis geschützt. Dieses Grundrecht wird durch verschiedene einfachgesetzliche Regelungen eingeschränkt. Das G10-Gesetz ermächtigt die Verfassungsschutzbehörden und andere Geheimdienste, unter bestimmten Umständen Sendungen zu öffnen, einzusehen sowie den Fernschreibverkehr mitzulesen, den Fernmeldeverkehr abzuhören und auf Tonträger aufzuzeichnen. § 100a StPO gestattet den Strafverfolgungsbehörden die Überwachung und Aufnahme des Fernmeldeverkehrs auf Tonträger.

Es mag bereits zweifelhaft sein, ob neue TK-Dienste, insbesondere Mehrwertdienste, überhaupt voll in den Schutzbereich des Art. 10 GG fallen. Sicherlich können jedoch Eingriffe in neue TK-Dienste nicht auf das G10-Gesetz und die Vorschriften des § 100a StPO gestützt werden. Die gesetzlichen grundrechtsbeschränkenden Vorschriften beziehen sich auf bestimmte Formen der Überwachung (Mitlesen des Fernschreibverkehrs, Abhören des Telefonverkehrs und Aufzeichnen auf Tonträger). Damit ist die Überwachung von in digitaler Form übertragenen Daten nicht gestattet. Wenn der Gesetzgeber Eingriffe auch in diese neuen Dienste erlauben wollte, müßte er dies in den bereichsspezifischen gesetzlichen Regelungen ausdrücklich zulassen.

Die gesetzlichen Vorschriften zur Beschränkung des Post- und Fernmeldegeheimnisses beziehen sich zudem auf reine Übertragungsdienste. Außer der Übertragungsfunktion werden aber bei neuen Diensten, z.B. Btx, vielfältige andere Funktionen (z.B. Speichern und Weiterverarbeitung von Informationen) angeboten, so daß diese Dienste nicht mehr als reine Fernmeldedienste angesehen werden können. Ihre Überwachung bedeutet somit im übrigen vielfach nicht nur einen Eingriff in das Fernmeldegeheimnis, sondern auch in andere Grundrechte (z.B. in die von Art. 13 GG geschützte Unverletzlichkeit der Wohnung bei Überwachung von TEMEX — Fernwirkdiensten).

3.6 Datenschutzrechtliche Rahmenbedingungen für die Arbeit von Medienarchiven

3.6.1 Problemstellung

Nachdem ich mich bereits in meinem 4. TB mit datenschutzrechtlichen Fragen im Zusammenhang mit der Arbeit von Medienarchiven auseinandergesetzt habe (vgl. 4. TB, 6.2.2.10, S. 165 ff.), hat mich der von der Bundesregierung beschlossene Entwurf für ein neues Datenschutzgesetz (im folgenden zitiert als "EBDSG") im Berichtsjahr erneut veranlaßt, mich diesem Thema zuzuwenden.

Die Presse und der Rundfunk sind für ihre Berichterstattung auf Hintergrundinformationen und Informationen über die Vorgeschichte von aktuellen Ereignissen angewiesen.

Sie unterhalten deshalb — z.T. umfangreiche — Archive, in denen vornehmlich bereits veröffentlichtes Material (Artikel aus Zeitungen, Zeitschriften und Meldungen von Nachrichtenagenturen) gesammelt werden. Einem funktionsfähigen Archivwesen kommt große Bedeutung für die Qualität journalistischer Arbeit zu; es ist mithin eine wesentliche Bedingung für die Aufgabenerfüllung von Presse, Funk und Film. Die Arbeit der Archive ist grundrechtlich durch Art. 5 Abs. 1 GG geschützt.

Datenschutzrechtlich bedeutsam ist die Informationsverarbeitung durch Medienarchive nur insoweit, als dabei personenbezogene Daten gespeichert oder übermittelt werden. Die Bestimmungen des BDSG kommen für Medienarchive nur dann zur Anwendung, wenn personenbezogene Daten

— dateiförmig (§ 1 Abs. 2 BDSG) und

— nicht ausschließlich zu eigenen publizistischen Zwecken (§ 1 Abs. 3 BDSG)

verarbeitet werden.

Das informationelle Selbstbestimmungsrecht wird in besonderer Weise dort gefährdet, wo die archivierten Informationen Dritten — auch außerhalb des publizistischen Bereichs — zur Verfügung gestellt werden. Wenn es sich z.B. bei den Empfängern von übermittelten Daten um Arbeitgeber handelt, könnten diese die Informationen über politische oder religiöse Anschauungen bei personalpolitischen Entscheidungen (Einstellung, Beförderung, Entlassung) nutzen. Öffentliche Stellen könnten sich über lange Zeit zurückliegende Straftaten bzw. Ordnungswidrigkeiten von Kritikern informieren. Die Liste der Mißbrauchsmöglichkeiten ließe sich mühelos verlängern.

Die Möglichkeiten des Mißbrauchs von in Medienarchiven zusammengefaßten Informationen hängen eng von der Organisationsform der Archive und der eingesetzten Technik ab. Wie in anderen Bereichen steigt auch hier das Mißbrauchsrisiko mit dem Umfang, der Integration und der Komfortabilität der eingesetzten automatisierten Verfahren.

3.6.2 Technisierung und Automatisierung der Archive

In der Vergangenheit wurden Archive fast ausschließlich als "Ausschnittarchive" betrieben, wobei die einzelnen Informationseinheiten nach einer bestimmten Systematik abgelegt wurden und nur in der gleichen Systematik wieder erschlossen werden konnten. Den Mißbrauchsmöglichkeiten waren bei dieser Form der Datenhaltung verhältnismäßig enge Grenzen gesetzt. Es handelte sich auch nicht um Dateien i.S.v. § 2 Abs. 3 Nr. 3 BDSG.

Durch den zunehmenden Einsatz automatisierter Systeme auch im Archivwesen ändert sich die Lage entscheidend. Dabei sind drei Stufen zu unterscheiden:

a) Es werden — bei ansonsten unveränderter manueller Ablagetechnik — zu jedem archivierten Dokument ein oder mehrere "Deskriptoren" (Hinweise auf Fundstellen) automatisiert gespeichert, die eine Erschließung des Dokumentenbestandes erleichtern und ihn (sofern je Dokument mehrere Deskriptoren erfaßt werden) einer — zumindest logischen — Umsortierung und einer Auswertung nach einer anderen als der Anlagesystematik zugänglich machen. Gleichwohl wird damit nicht das gesamte Archiv zur Datei, da es zur Erschließung und Umsortierung des Datenbestandes erheblicher manueller Anstrengungen bedarf.

b) Die archivierten Dokumente werden auf einem optischen Medium gespeichert (Mikrofilm, Mikrofiche, Bildplatte); zugleich werden — wie im unter a) beschriebenen Verfahren — Deskriptoren in einer gesonderten Datenbank gespeichert. Wird nach einem Suchbegriff oder einer Kombination von Suchbegriffen recherchiert, liefert das System die gefundenen Dokumente auf einem Bildschirm oder über Drucker im Faksimile. Ob es sich im datenschutzrechtlichen Sinne um eine Datei handelt, muß konkret geprüft werden (vgl. 6. TB, S. 14 ff.). Sofern nach einem vorgegebenen Schema mehrere Deskriptoren je Dokument gespeichert werden, ist für die Gesamtheit der so verwalteten Dokumente von einer Datei auszugehen.

c) Die archivierten Texte werden vollständig in einer Datenbank gespeichert und automatisch indexiert (Volltextdatenbank). Eine (fast beliebige) automatisierte Erschließung der gespeicherten Texte, ihre Auswertung und Umsortierung ist möglich. Hier handelt es sich zweifelsfrei um eine dateiförmige Speicherung.

3.6.3 Nutzung der Archive für andere als "eigene publizistische Zwecke"

§ 1 Abs. 3 BDSG nimmt personenbezogene Daten, die "durch Unternehmen oder Hilfsunternehmen der Presse, des Rundfunks oder des Films ausschließlich zu eigenen publizistischen Zwecken verarbeitet werden", von seinem Schutz aus. Bei dieser Art der Datenverarbeitung sind lediglich die gem. § 6 Abs. 1 BDSG vorgeschriebenen technischen und organisatorischen Sicherungsmaßnahmen zu treffen. Das so formulierte "Medienprivileg" bedeutet aber keineswegs, daß im publizistischen Bereich das Recht auf informationelle Selbstbestimmung keine Geltung hätte und deshalb keinerlei Beschränkungen der Datenverarbeitung erforderlich wären. Das "Medienprivileg" des BDSG nimmt lediglich die DV der Medien zu eigenen publizistischen Zwecken vom Geltungsbereich des BDSG aus.

Überschreiten Medienarchive die vom BDSG definierte Grenze der Verarbeitung "zu eigenen publizistischen Zwecken", kommt hingegen das BDSG zur Anwendung: Gibt ein Presseunternehmen personenbezogene Daten aus einer Datei nicht nur gelegentlich an andere weiter, dann unterliegt diese Datei voll dem Bundesdatenschutzgesetz (Hinweise zur Anwendung des BDSG, Amtl. Anzeiger Hamburg v. 7.6.78, S. 953).

Der oben beschriebene verstärkte Technikeinsatz in den Archiven ist i.d.R. mit sehr hohen Investitionskosten verbunden. Demgegenüber fallen die mit der einzelnen Recherche verbundenen Kosten kaum noch ins Gewicht. Es liegt also für die Medienunternehmen nahe, die gespeicherten Informationen effektiver zu verwerten, indem die Daten auch anderen Personen, Unternehmen und Institutionen — auch außerhalb des Medienbereichs — zur Verfügung gestellt werden. Dabei sind folgende Fälle zu unterscheiden:

a) Ein Presseunternehmen stellt einem anderen Presseunternehmen, das selbst kein Archiv betreibt, sein Archiv zur Mitnutzung zur Verfügung. Es hängt von der rechtlichen und organisatorischen Stellung des Archivs ab, ob es sich noch um eigene publizistische Zwecke handelt. Dies ist jedenfalls dann zu verneinen, wenn es sich um ein Archiv einer Zeitung oder Zeitschrift handelt, nicht aber um ein Archiv eines Verlages mit mehreren Publikationsobjekten. Gleiches gilt auch für die gegenseitige Unterstützung von Medienarchiven.

b) Die (gelegentliche) Erfüllung von Leserwünschen nach Auszügen aus archivierten eigenen oder auch fremden Erzeugnissen (sog. "Leserservice") stellt keine Umwidmung des Zweckes eines Medienarchivs dar und führt nicht dazu, daß das BDSG Anwendung findet. Der Leserservice ist eine Dienstleistung von Zeitungen an ihre Leser und hat vornehmlich die Aufgabe, die Bindung der Leserschaft an das betreffende Blatt zu stärken. Dies spricht dafür, den Leserservice im Rahmen der massenmedialen Aufgabe der Presse zu sehen und ihn zur Datenverarbeitung für eigene publizistische Zwecke zu rechnen.

c) Hingegen kann die Mitteilung personenbezogener Daten an Dritte außerhalb des Leserservice nicht unter das "Medienprivileg" subsumiert werden. Dies gilt vor allem dann, wenn Einzelanfragen, die sich auf bestimmte Personen beziehen, beantwortet oder personenbezogene Daten im Wege der Online-Recherche bzw. durch Überlassung maschinenlesbarer Datenträger zur Verfügung gestellt werden.

d) Eine Sonderstellung nehmen die Archive von Nachrichtenagenturen ein. Ihre Zweckbestimmung liegt gerade darin, daß sie Vorleistungen in Form von laufenden Meldungen oder — zunehmend — auch als aufbereitete Informationen für die Presse erbringen. Insofern unterliegen auch sie als Hilfsunternehmen der Presse dem "Medienprivileg". Während es noch hinzunehmen ist, daß zu den Abnehmern der Mitteilungsdienste der Nachrichtenagenturen auch Unternehmen außerhalb der

Presse und öffentliche Stellen gehören, wäre es sehr problematisch, wenn darüber hinaus für diesen Abnehmerkreis gezielte Einzelauskünfte erteilt oder Online-Recherchen zugelassen würden. Dies wäre auch bei Hilfsunternehmen der Presse keine Nutzung zu eigenen publizistischen Zwecken.

Will ein Medienunternehmen seine Archivalien kommerziell für andere als die eigenen publizistischen Zwecke nutzen und will es vermeiden, daß die dem publizistischen Zweck nicht angemessenen datenschutzrechtlichen Speicherungs-, Auskunfts- und Löschungsvorschriften Anwendung finden, so hat es dafür zu sorgen, daß die für eigene publizistische Zwecke gespeicherten Daten wirkungsvoll von den (auch) kommerziell angebotenen Datenbeständen abgeschottet werden. Dies würde eine Übernahme von Daten aus dem "publizistischen" in den "kommerziellen" Teil der Archive nicht ausschließen. Es müßte aber gewährleistet werden, daß die Übernahme nach festen nachprüfbaren Regeln geschieht und sich auf bereits veröffentlichtes Material beschränkt.

Andernfalls besteht die Gefahr, daß die Medienarchvie zu nicht dem Datenschutzrecht und der Datenschutzaufsicht unterliegenden Ersatzauskunfteien werden oder umgekehrt — bei voller Geltung des BDSG — für alle Daten die Funktionsfähigkeit der Archive im Hinblick auf ihre eigentliche journalistisch-redaktionelle Aufgabe beeinträchtigt wird.

3.6.4 Forderungen für die Novellierung des BDSG

Das "Medienprivileg" des BDSG ist bereits frühzeitig als präzisierungs- und verbesserungsbedürftig kritisiert worden (vgl. z.B. Bull, Ziele und Mittel des Datenschutzes, 1981, S. 50; 4. TB des HmbDSB, S. 165 ff., 5. TB des Bayerischen LfD, S. 5 ff.). Die Kritik geht davon aus, daß die seinerzeit erwartete gesetzliche Spezialregelung durch das Presserechtsrahmengesetz ausgeblieben ist, rechtliche Schutzbestimmungen über die von der Rechtsprechung entwickelten Grundsätze des allgemeinen Persönlichkeitsrechts hinaus aber erforderlich sind. Es kann dahingestellt bleiben, ob die zu schaffenden Regelungen besser im Presserecht oder im BDSG untergebracht wären. Die anstehende Novellierung des BDSG böte jedenfalls die Chance, diese Forderungen aufzugreifen und somit den Datenschutzbelangen besser als bisher Rechnung zu tragen.

Der Referentenentwurf des BMI vom 5.11.1987 berücksichtigt die von Datenschutz-Aufsichtsbehörden aufgestellten Forderungen im wesentlichen, auch wenn in einzelnen Punkten noch Verbesserungen erfolgen können:

a) Stärkung der Rechte des Betroffenen gegenüber den Pressearchiven, soweit sie dem "Medienprivileg" unterliegen

Auch wenn in Medienarchiven fast ausschließlich Daten aus allgemein zugänglichen Quellen (u.a. Pressemeldungen) gesammelt werden, können für den Betroffenen Gefährdungen entstehen, weil

— über die Richtigkeit des aus allgemein zugänglichen Quellen stammenden Materials Meinungsverschiedenheiten bestehen können und

— durch die Zusammenstellung von Material aus verschiedenen Quellen und über eine längere Zeit hinweg ein Persönlichkeitsbild entstehen kann, das der Zeitungsleser oder Rundfunkhörer aus seinen im allgemeinen punktuellen Eindrücken zu gewinnen nicht in der Lage ist.

Aus diesen Gründen sollten dem Betroffenen folgende Rechte gegenüber Medienarchiven eingeräumt werden:

— Ein Auskunftsrecht, soweit er durch eine Berichterstattung in seinen schutzwürdigen Belangen beeinträchtigt wird, jedenfalls dann, wenn die Daten in Dateien oder in personenbezogen erschließbaren Akten gespeichert werden,

— eine Verpflichtung der Medien, nach dem Presserecht zugelassene Gegendarstellungen (§ 11 Hamburgisches Pressegesetz) zu den entsprechenden Archivdaten zu

nehmen und dort so lange aufzubewahren, wie auch die dazugehörigen Daten gespeichert werden.

§ 37 Abs. 2 und 3 EBDSG räumen dem Betroffenen nur gegenüber den Rundfunkanstalten des Bundesrechts ein Gegendarstellungsrecht und einen Auskunftsanspruch über die zu seiner Person gespeicherten Daten ein, wenn er durch eine Berichterstattung in seinem Persönlichkeitsrecht beeinträchtigt wird. Diese Bestimmungen müßten auf alle Medien ausgeweitet werden.

Sofern die Regelungen des § 37 EBDSG in dieser Weise erweitert würden, wäre eine deutliche Verbesserung der Rechtslage für die Wahrung des Rechts auf informationelle Selbstbestimmung auch gegenüber den Medien erreicht.

b) Abgrenzung des Geltungsbereiches des "Medienprivilegs"

In der Vergangenheit ist es wiederholt zu Schwierigkeiten bei der Abgrenzung des "Medienprivilegs" gekommen. So haben sich — unter Verkennung des vom Gesetzgeber verfolgten Zieles — auch Verlage von Adressbüchern und ähnlichen Publikationen darauf berufen. § 37 Abs. 4 EBDSG stellt klar, daß Verlage von Adressen-, Telefon-, Branchen- oder vergleichbaren Verzeichnissen, soweit sie keine meinungsbildende journalistische Tätigkeit ausüben, nicht unter das "Medienprivileg" fallen. Damit und mit der Ersetzung des Begriffs "publizistische Zwecke" (§ 1 Abs. 3 BDSG) durch die Formulierung "journalistisch-redaktionelle Zwecke" (§ 37 Abs. 1 EBDSG) wird deutlich gemacht, daß es sich nicht um eine Sonderregelung für jegliche Veröffentlichungen, sondern nur für die durch die Pressefreiheit geschützten Medien und deren Hilfsunternehmen handelt.

Im Hinblick auf die vielfältigen, heute von den Archiven wahrgenommenen Aufgaben bringt der Referentenentwurf keine weiteren Klarstellungen. Es wäre darüber nachzudenken, das "Medienprivileg" so zu formulieren, daß

— der Leserservice,

— die kollegiale Hilfe von Medienarchiven untereinander und

— die Unterstützung für Medien, die selbst keine eigenen Archive unterhalten

eindeutig darunter fallen.

c) Ergänzung der Vorschriften für die Datenverarbeitung für fremde Zwecke

Sofern Medienarchive Daten nicht ausschließlich für eigene publizistische Zwecke verarbeiten, kommen für sie die Bestimmungen des 4. Abschnittes BDSG (Datenverarbeitung für fremde Zwecke), speziell die Vorschriften über Auskunfteien (§§ 32-35), zur Anwendung. Die Regelungen des BDSG über Benachrichtigung und Auskunftserteilung (§ 34), Berichtigung, Sperrung und Löschung (§ 35) sind auf die Tätigkeit von Auskunfteien zugeschnitten und passen teilweise nicht für die Arbeit der Pressearchive. Die Bestimmungen müßten so geändert werden, daß sie den Besonderheiten der Verarbeitung bereits publizierten und für dokumentarische Zwecke gespeicherten Materials gerecht werden. Der Referentenentwurf trägt dem weitgehend Rechnung, ist in einigen Punkten jedoch noch verbesserungsbedürftig:

— De lege lata dürfen Daten nur gespeichert werden, soweit kein Grund für die Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden. Abweichend hiervon ist das Speichern zulässig, wenn die Daten unmittelbar aus allgemein zugänglichen Quellen entnommen sind (§ 32 Abs. 1 BDSG).

  Nach dem Referentenentwurf soll die Speicherung von Daten zum Zwecke ihrer Übermittlung zulässig sein, sofern kein Grund für die Annahme besteht, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Speicherung hat oder wenn die Daten aus allgemein zugänglichen Quellen stammen und die schutzwürdigen Belange des Betroffenen das Interesse der speichernden Stelle nicht offensichtlich überwiegen (§ 27 Abs. 1 EBDSG). Die vorgeschlagene Regelung

bedeutet eine Verbesserung der Stellung der Betroffenen bei gleichzeitiger Wahrung der berechtigten Interessen der speichernden Stellen, da bislang eine Abwägung zwischen den Interessen des Betroffenen und den Interessen der speichernden Stelle überhaupt nicht vorgesehen war.

— Nach geltendem Recht ist der Betroffene zu benachrichtigen, wenn erstmals ihn betreffende Daten übermittelt werden, es sei denn, daß er auf andere Weise von der Speicherung Kenntnis erlangt hat (§ 34 Abs. 1 BDSG) oder die Übermittlung listenmäßig oder sonst zusammengefaßt wird und sich auf die in § 32 Abs. 3 benannten Merkmale beschränkt.

  Angesichts der Tatsache, daß es sich bei dem Archivgut um sehr umfangreiches Material handelt, das zumeist Veröffentlichungen entstammt, und die Anschriften der Betroffenen zumeist der speichernden Stelle nicht bekannt sind, ist eine derartige Benachrichtigungspflicht für Archive nicht praktikabel. Der Referentenentwurf sieht dementsprechend vor, daß die Benachrichtigung des Betroffenen über die erstmalige Speicherung der zu seiner Person gespeicherten oder übermittelten Daten unterbleiben kann, soweit die Daten allgemein zugänglichen Quellen entnommen sind oder sich auf denjenigen beziehen, der die Daten selbst veröffentlicht hat (Autor) (§ 30 Abs. 1 EBDSG).

— Nach geltendem Recht (§ 34 Abs. 2 BDSG) ist dem Betroffenen Auskunft über die zu seiner Person gespeicherten Daten zu erteilen. Nur wenn durch die Auskunftserteilung überwiegende berechtigte Interessen einer dritten Person geschädigt würden bzw. die öffentliche Sicherheit und Ordnung gefährdet würde (§ 34 Abs. 4), hat der Betroffene kein Recht auf Auskunft.

  Das Auskunftsrecht ist Voraussetzung dafür, daß der Betroffene weitere Rechte (z.B. Berichtigung, Löschung) in Anspruch nehmen kann. Es ist deshalb notwendig, dieses Recht zu stärken, indem z.B. Herkunft und Empfänger der Daten ebenfalls in das Auskunftsrecht einbezogen werden. Der Referentenentwurf trägt dem grundsätzlich zwar Rechnung, schränkt die Auskunftsverpflichtung der speichernden Stelle bei der Datenverarbeitung für fremde Zwecke bezüglich Herkunft und Empfänger von Daten aber auf diejenigen Fälle ein, in denen der Betroffene begründete Zweifel an der Richtigkeit der Daten geltend macht.

  Diese auf die Besonderheiten von Auskunfteien zugeschnittene Regelung muß für die Pressearchive modifiziert werden: Da hier bereits veröffentlichtes Material gespeichert ist, dürfte die Auskunft über die Datenherkunft keine Probleme bereiten. Eine Beschränkung auf Fälle, in denen begründete Zweifel an der Richtigkeit der Daten bestehen, wie im Entwurf vorgesehen, erscheint deshalb ungerechtfertigt. Andererseits wäre die Auskunftserteilung über Datenempfänger bei Pressearchiven völlig unrealistisch, da diese eine Aufzeichnung sämtlicher Übermittlungsvorgänge für alle personenbezogenen Daten voraussetzen würde. Da die Speicherung dokumentweise erfolgt, also i.d.R. gar nicht auf die einzelne Person als Ordnungsmerkmal abstellt, müßten alle Übermittlungen (d.h. auch alle Einsichtnahmen von Dritten in das Archiv) vorsorglich aufgezeichnet und abrufbar dokumentiert werden. Dies wäre aber nicht angemessen.

— Das BDSG sieht vor, daß personenbezogene Daten

  - zu berichtigen sind, wenn sie unrichtig sind (§ 35 Abs. 1),
  - zu sperren sind, wenn ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen läßt. Sie sind ferner am Ende des fünften Kalenderjahres nach ihrer Einspeicherung zu sperren (§ 35 Abs. 2),
  - zu löschen sind, wenn ihre Speicherung unzulässig war oder — auf Verlangen des Betroffenen — am Ende des fünften Kalenderjahres nach der Einspeicherung. Daten über gesundheitliche Verhältnisse, strafbare Handlungen, religiöse oder politische Anschauungen sind zu löschen, wenn ihre Richtigkeit von der speichernden Stelle nicht bewiesen werden kann (§ 35 Abs. 3).

Diese Regelungen sind für die dem BDSG unterliegenden Medienarchive unpraktikabel, denn diese dokumentieren bereits veröffentlichtes Material — weitgehend unabhängig von seinem Wahrheitsgehalt. An die Stelle von Berichtigungs-, Sperrungs- und Löschungsregelungen sollte daher ein Gegendarstellungsrecht treten. Die im geltenden Recht vorgesehene 5-Jahres-Frist für Sperrung und Löschung sollte für die Archive entfallen, da die Möglichkeit bestehen bleiben muß, auch nach Ablauf des 5-Jahres-Zeitraumes auf die archivierten Informationen zurückzugreifen. Zu erwägen wäre allenfalls, für die in §35 Abs. 3 S.3 BDSG aufgezählten besonders sensiblen Daten an der 5-Jahres-Frist festzuhalten. Dem steht allerdings entgegen, daß damit ein erheblicher zusätzlicher Aufwand verbunden wäre und neue Datenschutzprobleme entstehen könnten (Einrichtung zusätzlicher Dateien mit sensiblen, der Löschungsfrist unterliegenden Daten).

Der Referentenentwurf trägt den Forderungen nach modifizierten Berichtigungs-, Sperrungs- und Löschungsregelungen Rechnung: Daten, die unrichtig sind oder deren Richtigkeit bestritten wird, müssen bei der Datenverarbeitung für fremde Zwecke (außer wenn es sich um Daten über gesundheitliche Verhältnisse, strafbare Handlungen, Ordnungswidrigkeiten sowie religiöse oder politische Anschauungen handelt und ihre Richtigkeit von der speichernden Stelle nicht bewiesen werden kann) nicht berichtigt, gesperrt oder gelöscht werden, wenn sie aus allgemein zugänglichen Quellen stammen und zu Dokumentationszwecken gespeichert sind. Auf Verlangen des Betroffenen ist diesen Daten für die Dauer der Speicherung seine Gegendarstellung beizufügen. Die Daten dürfen nicht ohne Gegendarstellung übermittelt werden (§ 31 Abs. 5 EBDSG). Die 5-Jahres-Frist für die Löschung bzw. Sperrung ist zwar in modifizierter Form in den Entwurf übernommen worden (§ 31 Abs. 2 Nr. 4 EBDSG), gilt aber gerade nicht für die aus öffentlichen Quellen unmittelbar gewonnenen und zu Dokumentationszwecken für fremde Zwecke verarbeiteten Daten.

3.6.5 Fazit

Auch wenn der Referentenentwurf einer BDSG-Novelle den Besonderheiten der Medienarchive, insbesondere soweit sie nicht dem "Medienprivileg" unterliegen, z.T. Rechnung trägt, muß hier noch in einigen Feldern nachgebessert werden.

Wenn die Bestimmungen des § 37 Abs. 2 EBDSG (Gegendarstellungsrecht) und § 37 Abs. 3 (Auskunftsrecht für den Betroffenen) nicht nur bei Rundfunkanstalten, sondern bei allen Medien Anwendung fänden, würde damit auch wesentlichen datenschutzrechtlichen Forderungen bezogen auf den journalistisch-redaktionellen Bereich entsprochen. Dies würde auch die Medienarchive betreffen, sofern sie im Rahmen ihrer eigentlichen Aufgabenstellung tätig sind.

Darüberhinaus sind weitere Datenschutzregelungen im Presserecht notwendig, soweit sie vom allgemeinen Datenschutzrecht nicht geregelte Sachverhalte betreffen (z.B. Abschottung der Daten für journalistisch-redaktionelle Zwecke von den durch das BDSG geschützten Daten, da an die für eigene publizistische Zwecke gespeicherten Daten insbesondere hinsichtlich der Sperrungs-, Löschungs- und Berichtigungsregelungen andere Maßstäbe anzulegen sind als an die auch für Dritte außerhalb der Presse zugänglichen Informationen).

4. Einzelne Probleme des Datenschutzes im öffentlichen Bereich

4.1 Sozialwesen

4.1.1 Akteneinsichtsrecht eines Deputierten der BAJS

Zu dem Spannungsverhältnis von Sozialdatenschutz und Akteneinsichtsrecht eines Deputierten hatte ich bei der Prüfung der Frage Stellung zu nehmen, ob einem Deputierten der BAJS Einblick in die Selbstkostenrechnung der "Vereinigung städtischer

Kinder- und Jugendheime e.V." gewährt werden darf oder ob der Schutz von Betriebs- und Geschäftsgeheimnissen Vorrang hat, da die personenbezogenen Daten dem Sozialdatenschutz unterliegen. Die Selbstkostenrechnung ist Basis für Verhandlungen über den Pflegesatz, den der Träger der Sozial- oder Jugendhilfe für die Betreuung eines Hilfebedürftigen in einer Einrichtung des Trägers der Freien Jugendhilfe bezahlt. Die Berechnungen enthalten Details über die innerbetriebliche Situation der Einrichtung und damit Geschäftsgeheimnisse i.S.v. § 35 SGB I.

Für ein uneingeschränktes Akteneinsichtsrecht scheint die Entstehungsgeschichte des § 14 Verwaltungsbehördengesetz zu sprechen: Das OVG Hamburg hat sich in seinem Urteil vom 28. April 1986 (Aktenzeichen OVG Bs IV (VII) 38/85) mit ihr auseinandergesetzt und zu belegen versucht, daß eine Beschränkung der Akteneinsicht auf die Aufgabenbereiche der Deputation vom Gesetzgeber im Jahre 1926 nicht gewollt war und daß sich daran bei den nachfolgenden Novellierungen nichts geändert hat. Hieraus darf nicht der Schluß gezogen werden, die Akteneinsicht sei — einmal abgesehen von den in § 14 Verwaltungsbehördengesetz erwähnten entgegenstehenden gesetzlichen Vorschriften oder Gesichtspunkten des Staatswohls — uneingeschränkt zu gewähren. Eine verfassungskonforme Auslegung muß vielmehr zu einer Begrenzung auf die für die rechtmäßige Aufgabenerfüllung des Deputierten erforderliche Informationserhebung führen. Gesichtspunkte der Erforderlichkeit sind um so stärker zu beachten, je sensibler die in den Akten enthaltenen Daten sind.

Allerdings darf der Begriff der "Aufgaben" der Deputierten nicht zu eng gefaßt werden. Die Aufzählung in § 3 der Geschäftsordnung für die Deputation der Behörde für Arbeit, Jugend und Soziales ist nicht abschließend. Die Deputierten haben das Recht, Beratungsgegenstände von grundsätzlicher Bedeutung von sich aus aufzugreifen und zur Beratung zu stellen (§ 4 der Geschäftsordnung). Um eigene Initiativen ergreifen zu können, muß ihnen zugestanden werden, sich umfassend über die Arbeit ihrer Behörde zu informieren. Zu den Aufgaben der Deputierten gehört es aber nicht, die Verwaltung ihrer Fachbehörden zu kontrollieren, das ist die verfassungsmäßige Aufgabe der Bürgerschaft. Nicht verwehrt werden kann dem Deputierten aber die Befugnis, aus vorangegangenen Entscheidungen der Behörde Schlußfolgerungen zu ziehen und Verbesserungsvorschläge im Sinne einer Qualitätskontrolle zu machen.

Die Gewährung von Akteneinsicht ist, sofern sie sich auf die Beschaffung der zur Aufgabenerfüllung erforderlichen Informationen beschränkt, eine zulässige "Offenbarung" von Sozialdaten i.S.d. §§ 67 ff. SGB X. Nicht erforderlich ist allerdings eine Preisgabe personenbezogener Daten, wenn die Vorlage anonymisierter Aktenauszüge für die Wahrnehmung der Aufgabe ausreicht. Als Mitglied des obersten Leitungsorgans ist der Deputierte in den Entscheidungsfindungsprozess und damit in die Erfüllung der gesetzlichen Aufgaben seiner Fachbehörde im Rahmen der behördenintern geregelten Zuständigkeiten eingebunden. Die Weitergabe von Daten erfolgt daher, soweit sie sich im Rahmen dieser Zuständigkeitsregelungen hält, ebenso befugt wie eine Beteiligung des Vorgesetzten oder der Rechtsabteilung an einer Entscheidung. Eine andere Qualität hat selbstverständlich die Weitergabe von Sozialdaten zwischen Behördenteilen, die unterschiedliche Aufgaben zu erfüllen haben.

In dem mir zur Prüfung vorgelegten Fall wurde Akteneinsicht in einen für die Aufstellung des Haushaltsplans relevanten Vorgangs verlangt. Ein Mitwirkungsrecht der Deputierten an der Aufstellung und Durchführung des Haushaltsplans ihrer Behörde ist unbestritten, eine sinnvolle Mitwirkung aber nur möglich, wenn Informationen über das Zustandekommen von Haushaltsansätzen zugänglich gemacht werden. Entscheidend ist hier die Frage, ob der Anspruch des Deputierten auf Informationen durch Vorlage anonymisierter Selbstkostenrechnungen befriedigt werden kann. Gegen einen Mißbrauch des Informationsrechts, wie er von der Behörde offenbar befürchtet wurde, hat sie geeignete Vorkehrungen zu treffen, z.B. indem sie den Deputierten auf seine Amtsverschwiegenheit und evtl. strafrechtliche Konsequenzen hinweist.

4.1.2 Modellversuch im Rahmen des § 372 RVO

Seit Beginn der 80er Jahre fördert die Bundesregierung wissenschaftlich begleitete "Modellversuche zur Erhöhung der Leistungs- und Kostentransparenz in der gesetzlichen Krankenversicherung", um die daraus gewonnenen Erkenntnisse für kostendämpfende Maßnahmen und Strukturveränderungen nutzbar zu machen. Während bisher vorwiegend der ambulante Sektor und die Arzneimittelversorgung untersucht wurden, wendet sich das Interesse nunmehr verstärkt der stationären Versorgung zu, deren Kosten immerhin fast 1/3 der Leistungsausgaben der gesetzlichen Krankenversicherung ausmachen.

Auf Initiative der Spitzenorganisationen der Krankenversicherung und der Rentenversicherung hat die Arbeitsgemeinschaft für Gemeinschaftsaufgaben der Krankenversicherung (AGKV) das Konzept für einen Modellversuch entwickelt, mit dessen Hilfe die Informationsbasis der gesetzlichen Krankenkassen über Notwendigkeit und Dauer der Krankenhausbehandlung und über Planungsdaten für den stationären Sektor verbessert werden soll. Aus Kosten- und Kapazitätsgründen soll das Transparenzprojekt nicht wie zunächst geplant in drei Modellregionen, sondern nur in Hamburg erprobt werden, das bei den Kosten der stationären Versorgung angeblich eine Spitzenposition einnimmt: Dem Konzept für den Modellversuch ist zu entnehmen, daß die Ausgaben z.B. der AOK Hamburg je Mitglied für die Krankenhauspflege um 24 % über dem Bundesdurchschnitt liegen. Die Gründe für diese Entwicklung sollen mit Hilfe der durch den Modellversuch gewonnenen Informationen aufgeklärt und mit dem Ziel der Kostensenkung und Effizienzsteigerung beeinflußt werden.

Als Rechtsgrundlage für den Modellversuch bedarf es einer vertraglichen Vereinbarung gem. § 372 Reichsversicherungsordnung (RVO) zwischen den Verbänden der Krankenkassen und der Krankenhausträger. Bisher sind die Vertragsverhandlungen zwischen der Arbeitsgemeinschaft der Krankenkassen-Verbände in Hamburg und der Hamburgischen Krankenhausgesellschaft (HKG), dem Zusammenschluß der staatlichen und freien und gemeinnützigen Krankenhausträger, noch nicht abgeschlossen, gleichwohl läuft seit Anfang Juli eine Vorbereitungsphase für den Modellversuch.

Leider haben die beteiligten Verbände es versäumt, den HmbDSG an den Vorarbeiten für das Konzept des Modellversuchs zu beteiligen. Als die HKG mich 10 Tage vor dem geplanten Beginn der sog. "Übergangsphase" um Stellungnahme zu dem Konzept gebeten hat, wartete bereits ein eigens für den Modellversuch eingerichtetes Krankenhausdezernat des Vertrauensärztlichen Dienstes mit acht Ärzten, vier Datenerfassungskräften und einer Dokumentationsfachkraft auf den Beginn der Datenflüsse.

Nach dem ursprünglichen Konzept des Modellversuchs sollten in der "Übergangsphase" die Entlassungsanzeigen aller Hamburger Krankenhäuser für die Versicherten der am Modellversuch beteiligten allgemeinen Ortskrankenkassen, Ersatzkassen und Betriebskrankenkassen über den Vertrauensärztlichen Dienst der zuständigen Krankenkasse zugeleitet werden. Beim VÄD war geplant, die Daten zu erfassen und in einer zentralen Datei personenbezogen zu speichern und auszuwerten.

Der eigentliche Modellversuch sollte ursprünglich am 1. Januar 1989 beginnen. Ab diesem Zeitpunkt war vorgesehen, die Kostenübernahme für einen stationären Aufenthalt auf der Grundlage eines Verweildauer-Anhaltszahlenkatalogs zu befristen und nur in gesondert zu begründenden Einzelfällen zu verlängern. Dann sollten für jeden Versicherten nicht nur die Entlassungsanzeige, sondern bereits eine Aufnahmeanzeige und evtl. erforderliche Verlängerungsanzeigen dem VÄD zur Auswertung zugeleitet werden. Aus der Gesamtzahl der Krankenhauspatienten sollte er sich die für Einzelfallprüfungen geeigneten Fälle aussuchen, alle Verlängerungsanzeigen im Hinblick auf Notwendigkeit und Dauer der stationären Behandlung prüfen und Auswertungen für Pflegesatzverhandlung, Bedarfs- und Großgeräteplanung, Forschung und Gesundheitsberichterstattung erstellen.

Bei allem Verständnis für das berechtigte Anliegen der Krankenkassen nach Schaffung von mehr Transparenz und besseren Planungsgrundlagen und nach Beschränkung

der Krankenhausbehandlung auf das erforderliche Maß konnte ich mich mit diesem Konzept nicht einverstanden erklären.

Für die Errichtung einer kassenübergreifenden, zentralen Patientendatei beim VÄD gibt es weder nach geltendem Recht in der Reichsversicherungsordnung noch zukünftig im Gesundheitsreformgesetz eine gesetzliche Grundlage. Das Sozialgesetzbuch X verbietet in § 96 Abs. 3 ausdrücklich die Bildung einer Zentraldatei mehrerer Leistungsträger für Daten ärztlich untersuchter Leistungsempfänger. Eine Ausnahme von diesem Verbot kommt, nach einem Änderungsvorschlag des Gesundheitsreformgesetzes, allenfalls für die Träger der Unfallversicherung in Betracht. Eine zentrale Datensammlung beim VÄD ist auch zur Erfüllung seiner Aufgaben nicht erforderlich. Die RVO geht davon aus, daß die Krankenkassen in "geeigneten Fällen" den VÄD gutachterlich einschalten, der Entwurf des Gesundheitsreformgesetzes definiert die "geeigneten Fälle" als solche, in denen eine Überprüfung durch den Medizinischen Dienst "nach Art, Schwere, Dauer oder Häufigkeit der Erkrankung oder nach dem Krankheitsverlauf erforderlich ist". Zulässig ist danach eine Einzelfallprüfung, nicht aber eine Speicherung und Durchrasterung aller Krankenhausfälle in einer zentralen Datei beim VÄD. Es muß Aufgabe der einzelnen Krankenkassen bleiben, die geeigneten Fälle für eine Einzelfallprüfung aus ihrem Versichertenbestand auszuwählen. Nur in diesen Fällen ist eine Übermittlung personenbezogener Daten zur Erstellung eines Gutachtens im Rahmen der Aufgaben des VÄD erforderlich und zulässig. Für die Suche nach "geeigneten Fällen" dürfen sich die Krankenkassen der Kriterien bedienen, die der VÄD mit Hilfe des bei ihm angesiedelten medizinischen Sachverstands vorgibt.

Für die Entwicklung solcher allgemeiner Auswahlkriterien und für die Verbesserung der Informationsgrundlagen z.B. für Pflegesatzverhandlungen und Bedarfsplanungen ist eine Speicherung personenbezogener Daten nicht notwendig und schon deswegen unzulässig. Soweit es für bestimmte Auswertungen erforderlich ist, eine Fallbeziehbarkeit der Daten sicherzustellen, muß von der Möglichkeit einer geeigneten Verschlüsselung der Patientendaten Gebrauch gemacht werden. Das Konzept des Modellversuchs bedarf einer grundlegenden Überarbeitung unter datenschutzrechtlichen Gesichtspunkten, auch wenn dadurch der Start des Projekts verzögert wird.

Für die "Übergangsphase" habe ich daher mit der Arbeitsgemeinschaft der Krankenkassen-Verbände und der Hamburgischen Krankenhausgesellschaft vereinbart, die Daten aus den Entlassungsanzeigen faktisch zu anonymisieren, indem weder der Name noch das genaue Geburtsdatum oder die Adresse des Patienten gespeichert werden. Auch die Versicherungsnummer oder eine Fall- oder Aufnahmenummer des Krankenhauses darf der Entlassungsanzeige nicht entnommen werden. Bestimmte Implausibilitäten, wie ein Widerspruch zwischen Verschlüsselung und Klartext der Diagnose oder die Angabe nicht existierender ICD-Nummern dürfen vor der Erfassung der Daten aufgeklärt werden. Unzulässig ist dagegen eine Verknüpfung von Verweildauer und Diagnose für den Einzelfall. Nach Abspeicherung des Datensatzes ist eine Wiederherstellung des Personenbezugs beim VÄD ausdrücklich untersagt. Einzelfallprüfungen in "geeigneten Fällen" dürfen wie in der Vergangenheit nur auf Anstoß der Krankenkassen vorgenommen werden.

Für eine endgültige Bewertung der Zulässigkeit des Modellversuchs sind die Regelungen des Gesundheitsreformgesetzes für den medizinischen Dienst richtungweisend. Nicht zuletzt aufgrund der Forderungen der Datenschutzbeauftragten sind in das Gesetz Vorschriften für eine konkretere Fassung der Aufgaben und Befugnisse des medizinischen Dienstes und für eine strenge Zweckbindung der Datenverarbeitung aufgenommen worden. Auf dieser Grundlage wird zu entscheiden sein, inwieweit das Konzept für den Modellversuch zu ändern ist.

4.1.3 Einmalige Leistungen gem. § 21 BSHG

Im letzten Tätigkeitsbericht (6. TB, 4.1.5) hatte ich davon berichtet, daß in der Fachlichen Weisung der Behörde für Arbeit, Jugend und Soziales zu § 21 BSHG u.a. auf bestehende Lieferverträge zwischen dem Beschaffungsreferat der BAJS und verschie-

denen Lieferanten hingewiesen wird. Sofern ein Antragsteller die Voraussetzungen zur Gewährung einer einmaligen Hilfe gem. § 21 BSHG erfüllte, wurde vom Sozialamt ein Bestellschein an die Lieferfirma gesandt, auf dem Name und Anschrift des Hilfeempfängers vermerkt waren. Damit wurde dem Lieferanten offenbart, daß der Empfänger der Ware Sozialhilfe erhält.

Die BAJS hatte zugesagt, daß ein Bestellschein künftig vom Sozialamt nur dann an die Lieferfirma geschickt würde, wenn der Hilfeempfänger vorher seine ausdrückliche Einwilligung gem. § 67 SGB X dazu gegeben hat. Bei Verweigerung der Einwilligung würde die Hilfe als Geldleistung und nicht als Sachleistung erbracht.

Offenbar wurde nicht in allen Sozialämtern entsprechend verfahren. Mehrere Hilfeempfänger beschwerten sich bei mir darüber, daß von Hamburger Sozialämtern nach wie vor Lieferfirmen beauftragt würden, ohne daß für die damit verbundene Offenbarung von Sozialdaten eine Einwilligung der Betroffenen vorliege. Die BAJS hat zugesagt, alle Sozialämter noch einmal auf die bestehende Rechtslage hinzuweisen.

Ein Hilfeempfänger berichtete mir darüber hinaus in diesem Zusammenhang folgendes: Ihm sei ein Kleiderschrank bewilligt worden. Nachdem er seine Einwilligung zur Offenbarung seiner Daten an eine Möbelfirma verweigert habe, sei ihm ein Betrag von DM 50,— angeboten worden. Da er sich nicht in der Lage sah, für diesen Betrag einen gebrauchten Schrank zu beschaffen, willigte er schließlich ein, den Schrank vom Sozialamt bei einer Möbelfirma bestellen zu lassen. Von einer "freiwilligen" Einwilligung im Sinne des § 67 SGB X kann in diesem Fall keine Rede sein.

Ich habe der BAJS mitgeteilt, daß m.E. in den Fällen, in denen eine Einwilligung zur Offenbarung von Sozialdaten nicht erteilt wird, den Betroffenen wenigstens der Betrag auszuzahlen ist, den der bewilligte Gegenstand bei einer Bestellung durch das Sozialamt kosten würde.

4.1.4 Amtspflegschaft und Amtsvormundschaft bei nichtehelichen Kindern

In meinem 6. Tätigkeitsbericht (6. TB, 4.1.2) hatte ich das an Hamburger Jugendämtern praktizierte Verfahren bei der Beschaffung von Informationen über das Einkommen von Vätern nichtehelicher Kinder kritisiert.

Die Behörde für Arbeit, Jugend und Soziales (BAJS) hatte seinerzeit zugesagt, für die Zukunft sicherzustellen, daß die Verfahrensregularien des § 74 Nr. 2 SGB X in jedem Einzelfall streng beachtet werden. Die BAJS war aber nicht bereit, auf Anfragen bei Arbeitgebern zu verzichten, um das Arbeitseinkommen von Unterhaltspflichtigen zu ermitteln, obwohl es für diese Anfragen m.E. keine Rechtsgrundlage gibt. Die Diskussion zu dieser Frage wurde von der BAJS im Frühjahr 1988 abgebrochen mit der Begründung, sie werde das Verfahren nur ändern, wenn der Senat sich in seiner Stellungnahme zum 6. Tätigkeitsbericht meiner Auffassung anschließe. Sie hat es dann aber offenbar versäumt, dem Senat die Kontroverse darzustellen, so daß er sich dazu gar nicht äußern konnte. Infolgedessen besteht das von mir kritisierte Verfahren weiter, so daß sich eine förmliche Beanstandung wohl nicht vermeiden läßt.

4.1.5 Verwendung der Rentenversicherungsnummer beim Zeitschriftenversand der AOK Hamburg

Die AOK Hamburg versorgt seit Jahren etwa 350.000 Mitglieder mit der Zeitschrift "bleib gesund" im Postversand. Von einem Versicherten der AOK wurde ich darauf hingewiesen, daß der Adreßaufkleber dieser Zeitschrift in gespiegelter (und damit einfach zu entschlüsselnder) Form die Rentenversicherungsnummer enthält. Auf meinen Hinweis, daß dieses Verfahren einen Verstoß gegen das Sozialgeheimnis darstelle (§ 35 SGB I), teilte die AOK mit, daß eine große Zahl der Mitglieder-Zeitschriften von der Bundespost als "unzustellbar" zurückgesandt werde, weil diese Mitglieder versäumt hatten, der AOK ihre neue Anschrift mitzuteilen. Die Kenntnis der Versicherungsnummer sei als Ordnungsbegriff von erheblicher Bedeutung, um den maschinell geführten Datenbestand mit den von der Bundespost mitgeteilten neuen Anschriften zu aktualisieren.

Im Ergebnis stimmte die AOK aber mit mir überein, daß dieses Verfahren nicht datenschutzkonform ist. Künftig wird die Versicherungsnummer für den Zeitschriftenversand — auch in gespiegelter Form — nicht mehr verwendet. Statt dessen wird Basis des Ordnungsbegriffs allein das Geburtsdatum des Mitglieds sein, das in verschlüsselter Form ausgedruckt wird. Kommt die Zeitschrift zurück, wird die Schlüsselzahl maschinell entschlüsselt. Gegen dieses Verfahren habe ich keine datenschutzrechtlichen Bedenken.

4.1.6 Projekt Sozialhilfe-Automation (PROSA)

Das IuK-Vorhaben "Reorganisation der Arbeitsabläufe in den Sozialdienststellen der Bezirke durch umfassende Technikunterstützung" wird von der Verwaltung als Prioritätsvorhaben behandelt. In dem im Dezember 1986 vom Senat beschlossenen IuK-Gesamtplan 1987-1989 wurde dieses Projekt bereits als dringlich und unabweisbar ausgewiesen. Inzwischen firmiert es als "Projekt Sozialhilfe-Automation (PROSA)".

Ziel des Projektes ist es, eine umfassende Arbeitsunterstützung für z.Z. rund 1.000 Sozialhilfe-Sachbearbeiter zu schaffen. Dies soll durch Dialogisierung des operativen Verfahrens "Sozialhilfe" und durch Einführung von IuK-Technik zur Bürounterstützung und -kommunikation erreicht werden.

Weiteres Ziel ist daneben, die Transparenz der mit der Sozialhilfe verbundenen sozialpolitischen und finanziellen Aspekte inhaltlich zu verbessern und zeitnäher zu gewährleisten.

Darüber hinaus mißt der Senat diesem Projekt grundsätzliche Bedeutung im Rahmen seiner auf Modernisierung der Verwaltung durch umfassende und konsequente Nutzung von IuK-Technik gerichteten Organisationspolitik bei (vgl. 3. TB, 3.1). So sollen im Rahmen von PROSA Standards zur Schaffung einer ausbaubaren, zukunftssicheren Infrastruktur für die Informationsverarbeitung im Bürobereich der gesamten Verwaltung gewonnen werden. Deshalb sollen alle in diesem Bereich vorhandenen Bürofunktionen (wie z.B. Textverarbeitung, Aktenhaltung, Dokumentation, Terminverwaltung, Bürokommunikation) daraufhin untersucht werden, ob und inwieweit jeweils eine Technikunterstützung in Betracht kommt.

Stand des Projekts:

Anfang März 1988 wurde vom Senat eine Projektorganisation eingesetzt, die sich aus einer Lenkungsgruppe, einer Projektgruppe und einem Senatsbeauftragten, der die Funktion des Projektleiters wahrnimmt, zusammensetzt. Die Federführung für PROSA liegt bis auf weiteres beim Senatsamt für den Verwaltungsdienst.

Aufgabe der Lenkungsgruppe ist es, Einzelheiten des Projektauftrages festzulegen und Entscheidungswege zwischen den beteiligten Behörden projektorientiert zu straffen. Der Hamburgische Datenschutzbeauftragte ist — als Person — vom Senat zum Mitglied dieser Lenkungsgruppe berufen worden. Da ich in der Vergangenheit mehrfach Anlaß hatte, mich über meine mangelnde Beteiligung an datenschutzrechtlich relevanten Vorhaben der Verwaltung zu beschweren, begrüße ich diese Entscheidung grundsätzlich. Der gesetzlich verankerten Unabhängigkeit des Datenschutzbeauftragten hätte es allerdings eher entsprochen, ihm — ähnlich wie dem Rechnungshof — eine Mitwirkung anzubieten. Darauf muß ich auch deshalb Wert legen, weil andernfalls — wegen gleichzeitiger Beteiligung an einer Vielzahl von Automations-Vorhaben — die Kapazitäten und damit die Dispositionsmöglichkeiten der Dienststelle allzusehr eingeengt werden könnten.

Die Entscheidung des Senats habe ich so verstanden und dies auch dem Senat mitgeteilt, daß der Hamburgische Datenschutzbeauftragte — wie es § 20 Abs. 2 HmbDSG vorsieht — die Lenkungsgruppe bei Bedarf in Fragen des Datenschutzes beraten, nicht aber in Entscheidungen eingebunden werden soll. Der Datenschutzbeauftragte muß es sich vorbehalten, anderer Meinung zu sein als die Mehrheit der Lenkungsgruppe, ihre Beschlüsse zu kritisieren und seine Position etwa gegenüber dem Senat deutlich zu machen. Im Hinblick auf seine sonstigen Verpflichtungen hätte ich es im Sinne

einer kontinuierlichen und sachkundigen Begleitung des Projekts für wünschenswert gehalten, daß der Datenschutzbeauftragte sich in Sitzungen der Lenkungsgruppe vertreten lassen kann, wenn er selbst verhindert ist. Dies wurde vom Senat leider abgelehnt.

In der Projektgruppe sind inzwischen Vorüberlegungen zu einem Datenschutzkonzept für PROSA erarbeitet worden. Ziel dieser Überlegungen ist es, die normativen Vorgaben für ein Datenschutzkonzept zusammenzustellen, erkennbare Problembereiche zu skizzieren sowie Lösungsansätze zu entwickeln.

Besondere Datenschutzprobleme ergeben sich als Folge von Gesetzesbestimmungen, die für die Arbeit der Sozialämter von grundlegender Bedeutung sind. So erscheinen einige Regelungen des Bundessozialhilfegesetzes, durch die die Sozialämter veranlaßt werden, umfangreiche Ermittlungen bis in den sehr privaten Lebensbereich der Hilfeempfänger, in Einzelfällen bis in die Intimsphäre hinein anzustellen, aus datenschutzrechtlicher Sicht außerordentlich problematisch:

Nach § 3 Abs. 1 BSHG richten sich Art, Form und Maß der Sozialhilfe "nach der Besonderheit des Einzelfalles, vor allem nach der Person des Hilfeempfängers, der Art seines Bedarfs und den örtlichen Verhältnissen". Durch diesen Grundsatz unterscheidet sich die Sozialhilfe z.B. von der Sozialversicherung, die einzelnen typischen Notlagen durch im wesentlichen tatbestandlich typisierte und im vorhinein festgelegte Leistungen zu begegnen sucht. Um dem Grundsatz der Individualisierung gerecht zu werden, muß das Sozialamt zunächst ermitteln, ob und inwieweit dem Hilfesuchenden Mittel und Kräfte fehlen, eine bestimmte Notsituation aus eigener Kraft zu überwinden. Die wesentlichen Fakten, die für die Entscheidung über Art, Form und Maß der Hilfe erheblich sind, müssen aktenkundig gemacht werden, um die Entscheidung (z.B. für spätere Rechtsmittelverfahren) nachvollziehbar zu machen.

Wegen des Grundsatzes des Nachrangs der Sozialhilfe (§ 2 Abs. 1 BSHG: "Sozialhilfe erhält nicht, wer sich selbst helfen kann oder wer die erforderliche Hilfe von anderen, besonders von Angehörigen oder von Trägern anderer Sozialleistungen erhält") werden nicht nur beim Hilfesuchenden selbst, sondern auch bei potentiell unterhalts- bzw. leistungspflichtigen Dritten Daten erhoben. Beispielsweise wird in diesem Zusammenhang ermittelt, ob es sich, wenn ein Hilfesuchender einen Mitbewohner hat, um eine reine Wohngemeinschaft (z.B. zum Zwecke der Teilung der Mietkosten) oder um eine eheähnliche Gemeinschaft handelt. Im letzteren Fall gilt die gesetzliche Vermutung, daß der Hilfesuchende von seinem Mitbewohner Leistungen zum Lebensunterhalt erhält, soweit dies nach seinem Einkommen und Vermögen erwartet werden kann (§ 122 i.V.m. § 16 BSHG).

Die Zahl derjenigen, die in Hamburg Sozialhilfe beziehen und damit von der beschriebenen Problematik betroffen sein können, wurde Ende 1987 vom Statistischen Landesamt auf 155.000 geschätzt. Das sind rund 10 % der Einwohner Hamburgs. Dazu kommt noch die nicht quantifizierbare Zahl von notwendigen Datenspeicherungen über Dritte, die nicht selbst Hilfeempfänger sind.

Schon die konventionelle Datenverarbeitung (Speicherung in Akten, Datenübermittlungen per Telefon oder Papier) hat somit ein Volumen erreicht, das kaum noch angemessen kontrollierbar ist und — wie ich aus zahlreichen Gesprächen und Schreiben erfahren habe — für viele Betroffene inzwischen undurchschaubar und — auch deshalb — beängstigend ist.

Mit der Einführung der automatisierten Verarbeitung sensibelster Daten aus dem privaten und beruflichen Lebensbereich der Betroffenen erhöht sich die Gefahr einer Verletzung des Rechts der Betroffenen auf informationelle Selbstbestimmung weiter. Bereits in seinem "Mikrozensus-Beschluß" von 1969 bezog sich das Bundesverfassungsgericht auf das Menschenbild des Grundgesetzes, das dem einzelnen Bürger "einen unantastbaren Bereich privater Lebensgestaltung" gewährt, "der der Einwirkung der öffentlichen Gewalt entzogen ist". Mit der Menschenwürde ist es nach diesem Beschluß nicht zu vereinbaren, wenn der Staat das Recht für sich in Anspruch nehmen

könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren (vgl. BVerfGE 27, 1 ff.). 1983 hat das Bundesverfassungsgericht diese Auffassung im "Volkszählungsurteil" (BVerfGE 65, 1 ff.) noch einmal bekräftigt: "Schon bislang ist anerkannt, daß die zwangsweise Erhebung personenbezogener Daten nicht unbeschränkt statthaft ist, namentlich dann, wenn solche Daten für den Verwaltungsvollzug (etwa bei der Besteuerung oder der Gewährung von Sozialleistungen) verwendet werden sollen". Ein überwiegendes Allgemeininteresse, das Voraussetzung für die Datenerhebung ist, bestehe regelmäßig "nur an Daten mit Sozialbezug unter Ausschluß unzumutbarer intimer Angaben und von Selbstbezichtigungen".

Die Akzeptanz von PROSA wird auch davon abhängen, inwieweit es der Verwaltung gelingt, dem informationellen Selbstbestimmungsrecht der Betroffenen — auch und insbesondere unter den Bedingungen der modernen Datenverarbeitung — Geltung zu verschaffen.

4.1.7 Durchführung des Bundeserziehungsgeldgesetzes

Das Bundeserziehungsgeldgesetz (BErzGG) vom 6.12.1985 ist am 1.1.1986 in Kraft getreten. Das Gesetz regelt die Gewährung von Erziehungsgeld und Erziehungsurlaub.

Ein Erziehungsgeld in Höhe von monatlich DM 600,– wird für Kinder, die nach dem 31.12.1985 geboren sind, bis zur Vollendung des 10. Lebensmonats und für Kinder, die nach dem 31.12.1987 geboren sind, bis zur Vollendung des 12. Lebensmonats gewährt. Bis zur Vollendung des 6. Lebensmonats ist das Erziehungsgeld grundsätzlich eine einkommensunabhängige Leistung. Der Anspruch entfällt jedoch, wenn die Person, die das Kind betreut, eine Erwerbstätigkeit von 19 und/oder mehr Wochenstunden ausübt oder eine einer solchen Erwerbstätigkeit gleichzusetzende Sozialleistung mit Lohnersatzfunktion bezieht. Vom Beginn des 7. Lebensmonats an sind Einkommensgrenzen zu berücksichtigen. Übersteigt das Einkommen der/des Berechtigten und ggf. des Ehegatten die Einkommensgrenze, ist das Erziehungsgeld zu mindern oder es entfällt. Daneben sind auf das Erziehungsgeld Mutterschaftsgeld und entsprechende Leistungen nach beamten- oder soldatenrechtlichen Vorschriften anzurechnen.

Für die Durchführung des Gesetzes sind die Länder zuständig. Nach § 10 Abs. 1 Satz 1 BErzGG bestimmen die Landesregierungen oder die von ihnen bestimmten Stellen die für die Ausführung des Gesetzes zuständigen Behörden. Für eine bis zum 31.12.1988 befristete Übergangszeit hatte der Gesetzgeber die Möglichkeit der Übertragung der Durchführung des Gesetzes auf die Bundesanstalt für Arbeit zugelassen (§§ 10 Abs. 1 Satz 2 und 3 und § 39 Abs. 2 BErzGG). Hamburg hat diese Möglichkeit genutzt und die Durchführung des BErzGG im Rahmen einer Verwaltungsvereinbarung der Bundesanstalt für Arbeit übertragen, die auch für die Abwicklung aller noch im Jahre 1988 begonnenen Fälle zuständig bleibt.

Ab 1.1.1989 wird das BErzGG von den Einwohnerämtern der Bezirksämter — Kerngebiete — ausgeführt. Die Aufgabenerledigung soll durch den Einsatz moderner IuK-Technik unterstützt werden. Die Einwohnerämter werden mit insgesamt 14 Terminals und 8 Arbeitsplatzdruckern ausgestattet. Vorgesehen ist der Einsatz eines Dialogverfahrens im Verbund mit der Datenverarbeitungszentrale.

Im einzelnen war seitens der Projektgruppe zunächst geplant, mit dem ADV-Verfahren folgende Aufgaben zu erledigen:

— Das Erziehungsgeld zu berechnen,

— einen Bescheid zu schreiben,

— die für die Zahlung erforderlichen Unterlagen zu erstellen, den Sachbearbeitern — auch außerhalb der Akte — die wesentlichen Informationen zu liefern,

— Dokumentationen aufgrund datenschutzrechtlicher und haushaltsrechtlicher Vorschriften zu erstellen,

— Statistiken zu erstellen.

Gegen die zusätzliche, für die Antragsbearbeitung nicht erforderliche Erhebung von Daten zu statistischen Zwecken (z.B. Beruf, Erziehungsurlaub, differenzierte Angaben zum Familienstand wie ledig, geschieden, verwitwet, dauernd getrennt lebend) habe ich Einwendungen erhoben. Die BAJS teilte mir daraufhin mit, daß das Bundesministerium für Jugend, Familie, Frauen und Gesundheit (BMJFFG) darum gebeten habe, möglichst viele Daten für statistische Zwecke zu erheben, da "der Legitimierungsdruck gegenüber der Öffentlichkeit, vermutlich auch innerhalb des Kabinetts, aber auch gegenüber dem Parlament erheblich zu sein scheine". Diese Begründung ist für mich nicht nachvollziehbar. Inwieweit kann die Kenntnis, welchen Beruf die Antragsteller haben, die Zahlung von Erziehungsgeld legitimieren?

Abgesehen von der Zweckbestimmung ist aber entscheidend, daß es keine Rechtsgrundlage für die zusätzliche Erhebung von Daten zu statistischen Zwecken gibt. Nach dem Urteil des Bundesverfassungsgerichts zur Volkszählung darf die Verwaltung in das informationelle Selbstbestimmungsrecht von Betroffenen nur aufgrund einer bereichsspezifischen und normenklaren gesetzlichen Grundlage eingreifen. Antragsteller und Antragstellerinnen haben nach § 60 Abs. 1 SGB I lediglich die Tatsachen anzugeben, die für die Leistung erheblich sind. Die Verwaltung hat sich letztlich meiner Rechtsauffassung angeschlossen. Der mir z.Z. vorliegende automatisierte Datensatz enthält keine Angaben, die ausschließlich für statistische Zwecke erhoben und verarbeitet werden.

Der erste Entwurf eines Vordruckes, der von Antragstellern auszufüllen ist, wurde unter meiner Beteiligung überarbeitet und von der Projektgruppe inzwischen im wesentlichen datenschutzrechtlichen Erfordernissen angepaßt. Es wurde z.B. die Frage gestrichen, ob das Kind adoptiert sei, ebenso die Frage nach der Nicht-Ehelichkeit des Kindes.

Die Verwaltung hatte die Frage nach der Adoption zunächst für erforderlich gehalten, weil der Gesetzgeber beabsichtige, 1989 oder 1990 für Adoptivkinder einen längeren Anspruchszeitraum zu schaffen. Man wollte vermeiden, schon nach relativ kurzer Zeit einen neuen Vordruck erstellen zu müssen. Unabhängig davon, daß nach meiner Kenntnis in der Bonner Koalition noch streitig ist, ob, ggf. wann und für welche Berechtigten der Anspruchszeitraum für Erziehungsgeld verlängert wird, ist jedenfalls derzeit eine Rechtsnorm, die die Erhebung dieses Datums erlauben würde, nicht in Sicht. Ich weise vorsorglich schon jetzt darauf hin, daß eine Erhebung des Datums Adoption auch dann nur auf freiwilliger Basis zulässig wäre, wenn es zu einer Gesetzesänderung kommen würde, mit der adoptierten Kindern ein längerer Anspruchszeitraum geschaffen würde als anderen Berechtigten. Es müßte den Antragstellern überlassen bleiben, ob sie die Tatsache der Adoption preisgeben wollen, um ein höheres Erziehungsgeld zu beziehen.

Eine abschließende datenschutzrechtliche Beurteilung ist mir beim derzeitigen Stand des Projektes noch nicht möglich (z.B. liegt zum Zeitpunkt der Erstellung dieses Berichts eine Verfahrensdokumentation noch nicht vor). Ich gehe aber zunächst davon aus, daß die Verwaltung die erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherung trifft (§ 6 BDSG nebst Anlage).

4.1.8 Namentlicher Aufruf in den Sozialdienststellen der Bezirksämter

Im letzten Tätigkeitsbericht (6. TB, 4.1.1) hatte ich gerügt, daß Hilfeempfänger in den Wartezonen der Sozialämter durch namentlichen Aufruf ins Büro der Sachbearbeiter gebeten werden. Ich hatte dem Senatsamt für Bezirksangelegenheiten vorgeschlagen, in den Wartezonen (ähnlich wie im Arbeitsamt und in vielen Arztpraxen) ein Zahlensystem einzuführen. Mein Vorschlag wurde vom Senatsamt für Bezirksangelegenheiten aufgegriffen. Inzwischen sind zwei Modellversuche in den Sozialdienststellen Altona/Kern und St. Pauli abgeschlossen. Nach Einschätzung des Senatsamtes haben beide Versuche gezeigt, daß "Wartemarken ein geeignetes Instrument sein können, den namentlichen Aufruf des Publikums zu vermeiden und gleichzeitig zu einer Entkrampfung der Situation in den Wartezonen beizutragen". Die Modellversuche sollten

auch Erkenntnisse darüber bringen, ob der Verzicht auf den namentlichen Aufruf von den Betroffenen als Verbesserung empfunden wird. Eine Fragebogen-Aktion brachte folgendes Ergebnis:

Von 1.437 ausgegebenen Fragebögen wurden 533 (37 %) wieder abgegeben. In 288 Fragebögen (rund 54 % des Rücklaufs) wurde geantwortet: "Ich finde das neue Verfahren gut." 245 Befragte äußerten Gleichgültigkeit, wenige Befragte äußerten den Wunsch, weiterhin namentlich aufgerufen zu werden.

Ich begrüße es, daß inzwischen in weiteren Sozialdienststellen auf den namentlichen Aufruf des Publikums verzichtet wird, und erwarte, daß die in einigen Dienststellen noch bestehenden organisatorischen Probleme im Interesse der Betroffenen zügig gelöst werden.

4.1.9 Maßnahmen zur Datensicherheit beim Versand besonders geschützter Sozialdaten

Im Berichtszeitraum sind mir zwei ausgefüllte Krankenhauskosten-Übernahmeanmeldungen mit Diagnose-Angaben (in einem Fall mit der Diagnose AIDS) und weiteren sensiblen Daten zugegangen, die ein Sozialamt offen an das anmeldende Krankenhaus zurücksenden wollte, die aber als Irrläufer in dem Postfach für eine Schule gelandet sind. Eine Nachfrage beim stellvertretenden Sozialamtsleiter ergab, daß der offene Versand dieser Schriftstücke nicht etwa ein bedauerliches Versehen war, sondern die Regel ist.

Bereits im letzten Tätigkeitsbericht (6. TB, 4.1) hatte ich als Beispiel für ein Verwaltungshandeln, das längst hätte aufgegeben werden müssen, die unverschlossene Weitergabe von Betroffenen-Daten beanstandet. Die Dienstvorschrift der BAJS zum Schutz der Sozialdaten vom 14. April 1987, die auch in den bezirklichen Sozialämtern anzuwenden ist, regelt unter Punkt 2.3 ausdrücklich, daß Schriftstücke mit sensiblem Inhalt verschlossen zu versenden sind. Unabhängig davon, daß vom Sozialamt laufend gegen § 35 Sozialgesetzbuch I und die entsprechende Dienstvorschrift verstoßen wurde, offenbart dieser Fall einen erschreckenden Mangel an Sensibilität für die Belange der Betroffenen.

Das Senatsamt für Bezirksangelegenheiten ist inzwischen meiner Forderung nachgekommen und hat erneut alle Bezirksämter auf ihre Verantwortung für die Sicherstellung des Datenschutzes, insbesondere beim Versand von Schriftstücken mit sensiblem Inhalt, hingewiesen.

4.1.10 Prüfung im Bezirksamt Wandsbek

Die nachstehende Schilderung zeigt, daß eine verbesserte Datensicherung in vielen Bereichen schon durch kleine technische und organisatorische Veränderungen zu erreichen wäre. Dieser Fall mag aber auch als Beispiel dafür gelten, wieviel Aufwand ich teilweise treiben muß, um Maßnahmen zur Datensicherung, die eigentlich selbstverständlich sein sollten, durchzusetzen.

Anfang 1988 erhielt ich durch einen Bediensteten des Bezirksamts Wandsbek einen Hinweis darauf, daß in einem Dienstgebäude, in dem das Jugendamt, das Sozialamt und Teile des Amtes für Soziale Dienste untergebracht sind, Defizite hinsichtlich der technischen und organisatorischen Datensicherung bestehen (§ 6 Bundesdatenschutzgesetz).

Bei einer von mir im Februar 1988 durchgeführten Prüfung im Jugendamt und im Amt für Soziale Dienste habe ich folgende Feststellungen getroffen:

— Das Haus hat keinen Pförtner. Zwar ist ab 16.00 Uhr (außer montags) kein Zugang mehr möglich. Wer zu diesem Zeitpunkt aber bereits im Gebäude ist, kann sich weitgehend ungehindert bewegen.

— Die Türen der Diensträume haben einfache Schlösser. Die Schlüssel hängen auf fast allen Stockwerken offen in den Teeküchen, die frei zugänglich sind. Darüber

hinaus wurde mir berichtet, daß viele Mitarbeiter bei Verlassen der Räume die Schlüssel ohnehin auf den Türen stecken lassen.

— Die Akten lagern in einigen Zimmern auch nach Dienstschluß völlig offen, da abschließbare Schränke nicht vorhanden sind.

— Abgelegte Akten des Jugendamtes und des Amtes für Soziale Dienste lagern auf dem Boden und im Keller. Der Keller ist von außen zugänglich. In den Türen sind zwar Sicherheitsschlösser, die Schließzylinder ragen jedoch zentimeterweit aus dem Schließblech hervor.

— Das Geschäftszimmer des Jugendamtes ist frei zugänglich. In diesem Raum befinden sich Akten des Jugendamtes und ein Brett mit allen Schlüsseln der 5. Etage. Mir wurde berichtet, daß der Raum auch dann unverschlossen bleibt, wenn er nicht besetzt ist, damit alle Mitarbeiter Zugang zu ihren Schlüsseln und den Akten haben.

Im Ergebnis bedeutet dies, daß Unbefugte, die hinreichend selbstbewußt auftreten, vor allem in den Nachmittagsstunden kaum Schwierigkeiten haben werden, sich beliebige Akten zu beschaffen. Das Reinigungspersonal hat ungehinderten Zugang. Dies heißt, daß unbefugt Einsicht genommen werden kann, daß Akteninhalte manipuliert und ganze Akten entfernt werden können.

Ich habe das Bezirksamt sofort nach Abschluß der Prüfung aufgefordert, geeignete Maßnahmen zu treffen, um die festgestellten Mißstände zu beseitigen. Zwei Monate später wurde mir mitgeteilt, daß noch geprüft werde, durch welche organisatorischen oder baulichen Maßnahmen bzw. eine veränderte Büroausstattung (z.B. Schränke mit Sicherheitsschlössern) eine bessere Datensicherung möglich sei. Mir wurde weiter mitgeteilt, es zeichne sich ab, daß Maßnahmen größeren finanziellen Umfangs erforderlich seien, für die laufende Haushaltsmittel nicht vorhanden seien. Es müßten ggf. Haushaltsmittel zum nächstmöglichen Termin eingeworben werden.

Daraufhin habe ich mit dem Bezirksamt ein Gespräch geführt, in dem Einigkeit darüber erzielt wurde, daß kurzfristig jedenfalls solche organisatorischen und baulichen Maßnahmen zur besseren Datensicherung zu ergreifen sind, die mit geringem finanziellen Aufwand durchführbar sind. Ich habe gefordert,

— dafür zu sorgen, daß die Schlüssel in der Teeküche nicht mehr frei zugänglich sind (z.B. abschließbarer Schlüsselschrank, zu dem jeder Bedienstete einen Schlüssel erhält),

— darauf zu achten, daß das Geschäftszimmer des Jugendamtes, in dem sich Akten des Jugendamtes und ein Brett mit allen Schlüsseln der 5. Etage befinden, abgeschlossen wird, wenn sich niemand in dem Zimmer aufhält,

— Keller- und Bodenräume, in denen Akten des Jugendamtes und des Amtes für Soziale Dienste lagern, mit geeigneten Sicherheitsschlössern auszustatten,

— festzustellen, in welchen Bereichen besonders sensible Daten anfallen, um dort vorrangig abschließbare Schränke anzuschaffen,

— alle Bediensteten (incl. der Reinigungskräfte) in geeigneter Form noch einmal darauf hinzuweisen, daß nicht besetzte Büros abzuschließen sind und die Einhaltung dieser Anweisung im Rahmen der Dienstaufsicht zu kontrollieren,

— zu klären, ob die Aktenlagerung in den Archiven so organisiert ist, daß nach Ablauf von Aufbewahrungsfristen die Aktenvernichtung unverzüglich stattfinden kann.

Nach weiteren drei Monaten und mehreren Nachfragen teilte das Bezirksamt mit, daß inzwischen die nachstehenden Maßnahmen durchgeführt seien:

In jedem Stockwerk des Gebäudes wurde ein mit einem Sicherheitsschloß versehener Schlüsselkasten aus Stahl installiert, in dem die Schlüssel nach Dienstschluß verwahrt werden. Alle Bediensteten des Gebäudes wurden angewiesen, bei Verlassen der Zimmer die Türen zu verschließen und beim Verlassen des Gebäudes die Schlüssel in den

Schlüsselkasten zu hängen. Die Türen zu den Archivräumen im Keller und auf dem Boden wurden mit einem Sicherheitsschloß versehen. Für die Beschaffung von Stahlschränken und -karteikästen zur sicheren Unterbringung von Datenbeständen wurden in das Bezirksprogramm 1990 — 1993 insgesamt DM 600.000,– eingestellt.

Ich habe die Beschaffung von Stahlschränken und -karteikästen für die Büros, in denen nach meiner Ansicht abschließbare Schränke vorhanden sein sollten, nicht gefordert, habe aber gegen ein "Mehr" an Datensicherheit natürlich nichts einzuwenden. Trotz mehrfacher Nachfrage hat mir das Bezirksamt bisher nicht mitgeteilt, in welchen Bereichen wegen der besonderen Sensibilität der Daten vorrangig — aus noch vorhandenen Haushaltsmitteln — abschließbare Schränke angeschafft werden. Auch die Frage nach der Organisation der Aktenlagerung in den Archiven blieb bisher unbeantwortet.

4.1.11 Einsatz eines dialogorientierten ADV-Systems im Landesbetrieb "Winterhuder Werkstätten"

Die Behörde für Arbeit, Jugend und Soziales (BAJS) beabsichtigt, beim Landesbetrieb "Winterhuder Werkstätten" ein dialogorientiertes ADV-System einzuführen. Der Landesbetrieb ist ein Dienstleistungsunternehmen, das mehrere Werkstätten für Behinderte in Hamburg betreibt. Das geplante Verfahren soll der wirtschaftlichen Erfüllung der Aufgaben des Landesbetriebes nach § 26 Landeshaushaltsordnung und § 55 Abs. 3 Schwerbehindertengesetz dienen.

Im einzelnen sollen folgende Aufgabenbereiche mit dem System unterstützt werden:

— Finanzbuchhaltung, Anlagenbuchhaltung,

— Kostenrechnung, Lagerwirtschaft,

— Wirtschaftsplanung,

— Leistungsabrechnung mit Kunden/Lieferanten,

— Lohnabrechnung behinderter Mitarbeiter.

Für statistische Zwecke war zunächst geplant, über die für die Lohnabrechnung erforderlichen Daten hinaus eine Vielzahl sensibler personenbezogener Daten der behinderten Arbeitnehmer im System zu speichern und auszuwerten (z.B. Angaben darüber, ob die Betroffenen vor der Aufnahme in der Werkstatt im Heim oder bei ihren Eltern gelebt haben, ob sie beschäftigt oder arbeitslos waren, welche Schule sie ggf. besucht haben, in welchem Maße sie geistig, psychisch, physisch behindert sind, warum sie die Werkstatt ggf. wieder verlassen haben).

Die automatisierte Speicherung und Auswertung dieser Daten wäre ein Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen, für den eine Rechtsgrundlage nicht vorhanden ist. Ich habe deshalb gegen eine Speicherung von Daten der behinderten Arbeitnehmer, die zur Lohnabrechnung nicht erforderlich sind, Bedenken erhoben. Der Landesbetrieb ist meiner Argumentation gefolgt und hat zugesagt, auf die automatisierte Verarbeitung dieser Daten zu verzichten.

Das dargestellte Beispiel zeigt, wie wichtig es ist, daß die für ein Automations-Vorhaben jeweils zuständigen Stellen nicht nur bei großen Projekten wie PROSA (vgl. 4.1.6), sondern auch bei vergleichsweise kleinen Vorhaben Datenschutz-Aspekte rechtzeitig in ihre Überlegungen einbeziehen. Dies ist insbesondere dann sicherzustellen, wenn es sich um so sensible Daten wie die behinderter Menschen handelt.

4.1.12 Offenbarung von Sozialdaten auf Überweisungsträgern

Im 5. und 6. Tätigkeitsbericht (5. TB, 5.14 und 6. TB, 4.16) hatte ich gerügt, daß die Hamburgischen Sozialhilfedienststellen bei der Übersendung von Sozialhilfeleistungen auf Konten der Empfänger den Verwendungszweck auf dem Überweisungsträger angeben. Da die gesetzlichen Offenbarungsbefugnisse der §§ 68 bis 77 SGB X die damit verbundene Mitteilung, daß der Konteninhaber Sozialhilfe erhält, nicht abdecken, halte

ich die jetzige Praxis für rechtswidrig. Ich habe deshalb wiederholt eine Änderung des Verfahrens gefordert. Bisher hatte sich die BAJS meiner Rechtsauffassung — die von der Bürgerschaft geteilt wird — nicht angeschlossen.

Kurz vor Redaktionsschluß hat mir die BAJS mitgeteilt, sie sei weiterhin bemüht, eine Lösung zu finden, die sowohl den Belangen des Datenschutzes als auch denen der Sozialdienststellen Rechnung trage. Sie hat angeregt, das Gespräch über diese Thematik wieder aufzunehmen. Ich bin dazu gern bereit.

4.2 Personalwesen

4.2.1 IuK-Projekte in der Personalverwaltung

In den letzten Jahren wurden mir mehrere IuK-Projekte bekannt, die die Praxis der Personalverwaltung in Zukunft entscheidend verändern werden.

— In der Vergangenheit beschäftigte mich die Lehrerindividualdatei der Schulbehörde (LID) und ihre beabsichtigte Modernisierung. Mit Schreiben vom 12.10.1988 teilte die Schulbehörde mit, daß im Senatsamt für den Verwaltungsdienst aufgrund der in der Schulbehörde erstellten Datenstrukturanalyse eine Projektgruppe zum möglichen Einsatz von IuK-Technik in der gesamten hamburgischen Personalverwaltung gebildet worden sei und die Projektgruppe "Modernisierung der LID" daraufhin die Erledigung ihres Arbeitsauftrages festgestellt habe.

— Im Januar 1988 hatte ich einen ersten — und bisher einzigen — Kontakt zu dem IuK-Projekt "Automation des Ist-Stellenplans" des Senatsamtes für den Verwaltungsdienst — Organisationsamt —. Der "Ist-Stellenplan" verzeichnet auch die aktuelle bzw. zukünftige Besetzung von Stellen, enthält also personenbezogene Daten der Bediensteten (z.B. Name, Gehaltsgruppe, Daten des Beschäftigungsverhältnisses). Unabhängig von dem zentralen Projekt haben bereits einzelne Fachbehörden für ihren Bereich den Ist-Stellenplan selbst automatisiert bzw. dies geplant. Für derartige dezentrale "Insel-Lösungen" sollen in Zukunft allerdings keine Haushaltsmittel mehr zur Verfügung stehen, weil das zentrale IuK-Projekt des Organisationsamtes Priorität habe.

— Ende Oktober 1988 erhielt ich den Entwurf einer Senatsdrucksache zur "Zentralisierung der Beihilfefestsetzung für Beamte, Angestellte und Arbeiter". Bereits im letzten Jahr (1987) hatte die Projektgruppe "Einsatz neuer IuK-Technik in der Personalverwaltung" ihren Bericht "Möglichkeiten zur Vereinfachung und Rationalisierung des Beihilfeabrechnungsverfahrens" vorgelegt. Vorgeschlagen wird die Bündelung der spezifischen Sachverstand erfordernden Beihilfeabrechnung bei der zentralen Besoldungs- und Versorgungsstelle, verbunden mit der Einführung eines online-Zugriffs der Sachbearbeiter auf eine zentrale Datei (Dialogverfahren). In meiner Stellungnahme zum Senatsdrucksachenentwurf habe ich das Ziel, nämlich die Abschottung der Beihilfebearbeitung von der übrigen Personalverwaltung, begrüßt. Unerwähnt bleiben in dem Entwurf jedoch die notwendigen Datensicherungsmaßnahmen, die einen Mißbrauch der zentralen Beihilfedateien — z.B. eine Verknüpfung mit anderen zentralen Dateien — ausschließen.

— In einem Gespräch im Personalamt Ende März 1988 erfuhr ich eher beiläufig von der Verfügung Senator Pawelczyks vom 10. März 1988 über die Einsetzung einer Projektgruppe "Personalverwaltung", die auch zur Einstellung der Modernisierung der LID führte.

Die Projektgruppe "Personalverwaltung" soll prüfen,

- ob und in welchem Umfang es durch eine Neuverteilung der Aufgaben — insbesondere der Verlagerung der Besoldungsaufgaben der Besoldungs- und Versorgungsstelle auf die jeweiligen Behörden — möglich, sinnvoll und wirtschaftlich ist, die Personalverwaltung zu reorganisieren;

- ob und in welchem Umfang das Dialog-Verfahren zur Sachbearbeiter-Unterstützung in der Besoldungs- und Versorgungsstelle für einen Einsatz in den Personalabteilungen (der Fachbehörden, Bezirks- und Senatsämter) geeignet ist und inwieweit eine Anpassung an die dortigen Arbeitsabläufe bzw. die Kenntnisse der Personalsachbearbeiter erforderlich ist;
- wie diese Anpassung grob zu gestalten und zu realisieren ist.

Da die Verfügung auf Anforderungen des Datenschutzes ausdrücklich Bezug nimmt, bat ich das Personalamt um eine frühzeitige Beteiligung und einen vollständigen Überblick über die von den IuK-Untersuchungen betroffenen Einzelgebiete der Personalverwaltung.

Ich erhielt am 29. Mai 1988 das Ergebnisprotokoll der ersten Projektausschußsitzung mit dem Hinweis, daß "alle Vorlagen für den Projektausschuß und die Protokolle der regelmäßig stattfindenden Sitzungen (alle sechs Wochen) dem Datenschutzbeauftragten zur Unterrichtung über den Projektfortgang zugehen sollen". Erst am 14. September, also nahezu fünf Monate später, wurde mir die Niederschrift der vierten Ausschußsitzung zugesandt, der ich entnehmen konnte, daß inzwischen der Entwurf einer "Voruntersuchung zur Reorganisation der hamburgischen Personalverwaltung" (Stand: 30.6.1988) erstellt und in der dritten Sitzung des Projektausschusses am 12. Juli 1988 erörtert worden war. Erst auf meine telefonische Anforderung ging die umfangreiche Dokumentation Ende September bei mir ein.

Obwohl die in Aussicht genommene Rückverlegung von Personalverwaltungsaufgaben von der Besoldungs- und Versorgungsstelle auf die einzelnen Personalstellen der Behörden, verbunden mit der Anwendung eines elektronischen Dialog-Verfahrens, eine ganze Reihe datenschutzrechtlicher und datensicherungstechnischer Fragen aufwerfen dürfte — und dies bestätigt die Durchsicht des Voruntersuchungsentwurfs —, wurde ich bisher weder an der Diskussion des Grundsätzlichen (Datenschutz bei zentraler/dezentraler Datenverarbeitung), noch an Erörterungen/Planungen zu einzelnen Problemen (z.B. Zugriffsberechtigungen, Protokollierungen, Personalstrukturdatei) beteiligt. Nach der Einsetzungsverfügung hat die Projektgruppe "bis zum 31.12.1988 einen Bericht mit Entscheidungsvorschlägen vorzulegen", der "auch Datenschutz- und Sicherheitsaspekten Rechnung zu tragen" hat. Eine eingehende Auseinandersetzung mit Datenschutzfragen war mir allein aufgrund der übersandten Protokolle und Voruntersuchungsentwürfe bisher nicht möglich. Sie wurde von der Projektgruppe auch nicht erwartet, da sie ihre Arbeit lediglich als Vorstudie versteht, die für eine allgemeine Diskussion mit anderen Behörden noch nicht gedacht sei. Inzwischen hat das Personalamt angeregt, ein gemeinsames Gespräch über datenschutzrechtliche Implikationen des Projekts zu führen.

— Zusammen mit den Bundesländern entwickelt der Bund derzeit ein "informationstechnisches System zur Unterstützung bei Kostenrechnungen im Dienstbereich (ISKD)", bei dem trotz prinzipieller Aggregation und Anonymität der übermittelten Abrechnungsdaten der Bediensteten Datenschutzfragen eine Rolle spielen.

Auf Bundesebene legte im Juli 1988 eine interministerielle Arbeitsgruppe ihren "Bericht zur strukturellen Fortentwicklung des Personalaktenrechts im öffentlichen Dienst" vor, der sich eingehend mit Möglichkeiten und Grenzen von Personalinformationssystemen bzw. "automatisierten Personalverwaltungssystemen" auseinandersetzt. Er macht Regelungsvorschläge und formuliert als "Zwischenergebnis":

"Gleichwohl sollte die Chance nicht vertan werden, im Zuge der Novellierung des Personalaktenrechts eine Rechtsgrundlage zu schaffen, die es den personalaktenführenden Stellen freistellt, sich die Technologie der Zukunft schon heute nutzbar zu machen. Daß dies nicht ohne entsprechende Modifikationen und Begrenzungen geschehen kann, ist angesichts des erheblichen Gefährdungspotentials, das für die Rechtsgüter des Einzelnen in jeder Art und in jedem einzelnen Vorgang der automatischen Datenverarbeitung liegt, einsichtig."

Der Bericht der interministeriellen Arbeitsgruppe soll nicht nur gesetzliche Regelungen für die Bundesverwaltung, sondern auch — über Ergänzungen des Beamtenrechtsrahmengesetzes — für die Landespersonalverwaltungen vorbereiten.

Angesichts aller genannten IuK-Projekte und -Planungen im Personalwesen drängt sich mir die Frage auf, in welchem Verhältnis die mir als Einzelprojekte beschriebenen Vorhaben zueinander stehen. Besteht zwischen einzelnen oder allen Projekten ein Zusammenhang? Liegt den Einzelprojekten ein gemeinsames Konzept zugrunde? Meine Bitte an das Personalamt, mir einen Überblick über die derzeitigen IuK-Planungen im Personalbereich zu verschaffen, blieb aber bis heute unerfüllt.

In meinem 3. Tätigkeitsbericht 1984 (3.2, S. 23-30) hatte ich seinerzeit bestehende elektronische Personaldateien beschrieben und die Frage "Gibt es in der hamburgischen Verwaltung ein integriertes Personalinformationssystem?" verneint. In meinem 5. Tätigkeitsbericht 1986 (5.2.2, S. 36) bemerkte ich dagegen bezüglich der LID, die umfassende Zielsetzung der Modernisierung der Lehrerindividualdatei lasse den Schluß zu, daß hier ein in Teilen auf andere Behörden übertragbares Personalinformationssystem entstehe. Vor allem vor dem Hintergrund, daß die Modernisierung der LID gerade wegen des zentralen IuK-Projektes "Personalverwaltung" aufgegeben wurde, erscheint angesichts der dargestellten Fortentwicklung des IuK-Einsatzes in der Personalverwaltung eine erneute Diskussion über "Personalinformationssysteme in der Hamburger Verwaltung" geboten. Selbst wenn die einzelnen IuK-Projekte keinem einheitlichen IuK-Konzept folgen sollten, so bleibt die Frage, ob es nicht dennoch ein einheitliches Datenschutz-/Datensicherungskonzept für alle Projekte zusammen geben muß, um auch den Mißbrauch durch unzulässige Verbindungen/Zugriffe/Verknüpfungen zwischen den Systemen verhindern zu können. Im weiteren Verlauf der IuK-Planungen im Personalwesen werde ich hierauf und auf den Themenkomplex "Personalinformationssysteme" besonderes Gewicht legen. Dabei wird mir möglicherweise auch der Erfahrungsaustausch mit den anderen Datenschutzbeauftragten helfen, mit denen ich die Einrichtung eines neuen Arbeitskreises "Personalwesen" vereinbart habe.

4.2.2 Einsicht in Personalakten durch zukünftige Vorgesetzte

In meinem 6. Tätigkeitsbericht (4.2.1, S. 36) konnte ich davon berichten, daß in der Baubehörde in Zukunft ohne eine schriftliche Einwilligung die Personalakte eines verwaltungsinternen Bewerbers nicht mehr angefordert bzw. vorgelegt wird.

Mein Bemühen, diesen Grundsatz, zumindest aber eine Unterrichtung des Betroffenen von der Personalakten-Versendung, auch in anderen Behörden — insbesondere im Personalamt — Praxis werden zu lassen, war nicht erfolgreich. Zwar hatte das Personalamt in einer Besprechung der Personalabteilungsleiter am 23. September 1987 meine Anregung weitergegeben, "die Beschäftigten in der Regel darüber zu unterrichten, wenn die Personalakten zur Vorbereitung oder Durchführung von Entscheidungen in Personalangelegenheiten einer anderen Dienststelle des Dienstherrn/Arbeitgebers Freie und Hansestadt Hamburg zur Einsicht überlassen werden" (Niederschrift der Personalabteilungsleiter-Besprechung). In der Stellungnahme des Senats zum 6. Tätigkeitsbericht (Senatsdrucksache vom 25.5.1988) heißt es dann jedoch: Der Senat halte es "nicht für erforderlich und zweckmäßig zu bestimmen, daß die Beschäftigten bei Erwägungen über Versetzungen oder Abordnungen innerhalb der hamburgischen Verwaltung über die Versendung der Personalakte zu unterrichten sind". Ob sich dies nur auf — ggf. zwangsweise durchzuführende — Versetzungen und Abordnungen von Beamten bezieht oder auch auf jede "vorsorgliche" Personalaktenübersendung an Dienstvorgesetzte anderer Behörden, die eine Stelle zu besetzen haben, bleibt offen. Ziffer 31 (1) der Anordnung über die Führung und Verwaltung der Personalakten von 1971, die trotz meiner Kritik offensichtlich nicht geändert werden soll, erlaubt jedenfalls ganz allgemein eine Personalakten-Übersendung ohne Kenntnis des Betroffenen. In einem Schreiben vom 17. August 1988 stellt das Personalamt dementsprechend fest, daß es den Dienstvorgesetzten gestattet sein müsse, im Stadium personalplanerischer Überlegungen Personalakten aus anderen Behörden ohne Kenntnis der Betroffenen

einzusehen. Andererseits bezeichnet das Personalamt dies ausdrücklich als Ausnahme und bekräftigte in einer Personalabteilungsleiterbesprechung am 10. November noch einmal die Anregung, in der Regel den Betroffenen von einer Weitergabe seiner Personalakte zu unterrichten.

Die interpretationsfähigen Stellungnahmen des Personalamtes vermitteln den Eindruck, daß sich an der seit Jahren gepflegten Praxis nur wenig ändern wird. Dagegen habe ich mehrfach meine Rechtsauffassung deutlich gemacht, daß das Grundrecht des einzelnen, "wissen zu können, wer was wann und bei welcher Gelegenheit über ihn weiß" (Bundesverfassungsgericht), nicht hinter eher taktischen Planungs- und Organisationsinteressen der Verwaltung zurückstehen darf. Der Betroffene darf nicht zum Objekt von Entscheidungen des Dienstherrn werden, sondern hat jedenfalls bei einer Offenbarung seiner persönlichen Daten gegenüber anderen ein legitimes Interesse, sich bereits mit "Erwägungen" über seine Person bzw. seine weitere dienstliche Verwendung auseinanderzusetzen.

4.2.3 Bewerber- und Personalfragebögen

— Musterfragebogen des Personalamtes —

In meinem 6. Tätigkeitsbericht (4.2.2, S. 37), berichtete ich von der Diskussion um Musterentwürfe des Personalamtes für einen "Fragebogen für Bewerber" und einen "Fragebogen für Einzustellende". Am 25. November 1987 hatte mir das Personalamt mitgeteilt, daß "die für die Gestaltung der Vordrucke zuständigen Stellen" um die Änderung bzw. Einführung der Fragebogen gebeten wurden. Ein Jahr nach dieser Ankündigung habe ich weder neue Formulare erhalten noch eine Änderung der Behördenpraxis feststellen können.

Hinsichtlich der Frage, ob auch bei der Bewerbung für Angestellten- und Arbeiterfunktionen ein allgemeines Führungszeugnis verlangt werden darf, hatte das Personalamt sich seinerzeit bereiterklärt, "der von Ihnen empfohlenen differenzierten Lösung für Bewerber um Berufung in das Beamtenverhältnis einerseits und Bewerber um Einstellung als Arbeitnehmer andererseits näherzutreten und in dem Zusammenhang bei Bewerbungen um Einstellung als Angestellte ein Führungszeugnis nicht mehr allgemein zu fordern". Ich wertete diesen Satz als Verzicht auf die Vorlage eines Führungszeugnisses bei Arbeitern und Angestellten. In der Stellungnahme des Senats zum 6. Tätigkeitsbericht ist hiervon nicht viel übrig geblieben. In einem neuen Entwurf des Personalamtes zur Änderung der Durchführungsrichtlinien zum Bundeszentralregistergesetz heißt es nun:

"Ausgewählte Bewerber um Einstellung für eine Tätigkeit als Angestellter der Vergütungsgruppe Vb bis I bzw. Kr VII bis Kr XII BAT (entspricht dem gehobenen und höheren Dienst) sowie als übertariflich beschäftigte Angestellte haben ein Führungszeugnis vorzulegen ... (Dies gilt) auch für ausgewählte Bewerber um Einstellung für eine Tätigkeit als Angestellte der Vergütungsgruppe X bis Vc bzw. Kr I bis Kr VI BAT (entspricht dem einfachen und mittleren Dienst) sowie als Arbeiter, wenn die Art des zu besetzenden Arbeitsplatzes die Kenntnis über anhängige Verfahren und Vorstrafen erforderlich macht (z.B. Kraftfahrer, Kassierer, Erzieher)."

Auf den Meinungswandel angesprochen, erklärte das Personalamt mit Schreiben vom 17. August 1988, es sei der von mir "empfohlenen Lösung eben nur nähergetreten und nicht etwa beigetreten".

Demgegenüber bekräftige ich meine bereits im 6. Tätigkeitsbericht geäußerte Rechtsauffassung, daß das Arbeitsrecht auch für den öffentlichen Dienst das Fragerecht des Arbeitgebers auf "einschlägige" Vorstrafen, also solche, die für die in Aussicht genommene Tätigkeit relevant sind, beschränkt. Dies kann auch nicht mit dem vom Personalamt angeführten Argument umgangen werden, auch Angestellte würden heute von der und für die Freie und Hansestadt Hamburg und nicht mehr für einzelne Arbeitsplätze eingestellt. Das Fragerecht kann und muß auch in diesem Fall darauf beschränkt sein, welche Anforderungen der konkrete Arbeitsplatz stellt, für den eine bestimmte Behörde

einen Arbeitnehmer sucht. Bei einem späteren Arbeitsplatzwechsel kann die Frage nach "einschlägigen" Vorstrafen noch einmal — ggf. mit anderem Inhalt — gestellt werden.

— Ausnahmeregelung für Heimpersonal —

Aufgrund meiner Ausführungen im 6. Tätigkeitsbericht zum Führungszeugnis und zur Frage nach anhängigen Strafverfahren wandte sich auch die Arbeits- und Sozialbehörde an mich. Sie hatte Sorge, daß bei der Auswahl von Personal für Anstalten, Heime und Behindertenwerkstätten ein Schutz der abhängigen und nicht selten hilflosen Heimbewohner/Behinderten kaum gewährleistet werden könne, wenn nicht auch nach weniger schweren bzw. im Zentralregister gelöschten Delikten gefragt werden dürfe.

Da es hier nicht nur um den Datenschutz der Bewerber, sondern ganz entscheidend um den Schutz Dritter geht, teile auch ich die Meinung, daß in diesem Falle das Fragerecht sich nicht auf die in ein Führungszeugnis aufzunehmenden Vorstrafen beschränken muß. In einer gemeinsamen Besprechung wurde aber auch Einigkeit über die Grenzen dieser Ausnahme erzielt: "Voraussetzung für die Zulässigkeit ist allerdings, daß nicht automatisch alle Bewerber befragt werden, sondern nur die, die in die engere Wahl für die Einstellung kommen (2-stufiges Verfahren) und daß die Frage für den Arbeitsplatz relevant ist. Dies ist z.B. der Fall bei Fragen nach Delikten wie Diebstahl, Betrug, Urkundenfälschung, Körperverletzung oder bei Drogendelikten" (Ergebnisniederschrift).

— Bewerber- und Personalbögen der Justiz- und der Innenbehörde —

Angesichts des offensichtlich sehr langwierigen Verfahrens zur Einführung allgemein verbindlicher Bewerber- und Personalfragebögen habe ich im letzten Jahr die gegenwärtig verwendeten Fragebögen der Justizbehörde und der Innenbehörde überprüft. Es ergab sich, daß bereits im Bewerberfragebogen viele Fragen gestellt werden, die nicht für die Auswahl, also die Einstellungsentscheidung, sondern erst für die spätere Lohn-/Gehaltsabrechnung bzw. die Personalverwaltung von Bedeutung sind. Dazu gehören insbesondere Angaben zum Familienstand, zum Ehegatten, zu Kindern, aber auch zum Wehrdienst, zur Ersatzkassen-Mitgliedschaft und zum Rentenbezug.

Andere Fragen können Teil einer Sicherheitsüberprüfung sein. Diese muß aber der grundsätzlichen Einstellungsentscheidung nachfolgen. Eine "vorsorgliche" Datenerhebung im Bewerbungsbogen auch für diesen Zweck ist unverhältnismäßig. Dies gilt z.B. für die Wohnanschriften der letzten zehn Jahre, die Personalien der Eltern des Bewerbers sowie die Frage: "Seit wann wohnen Sie in der Bundesrepublik?"

Einige Fragen halte ich überhaupt für unzulässig, weil sie einen unangemessenen Eingriff in die Privatsphäre des Bewerbers darstellen, ohne für den Dienstherrn erforderlich zu sein. So fragt die Polizei z.B.:

— "Haben Sie vor Ihrem 18. Lebensjahr längere Zeit außerhalb des Elternhauses gelebt? (z.B. Heime, Internate o.ä.) Von — bis, Name und Anschrift".

— Beruf bzw. Tätigkeit von Vater und Mutter

— Art, Höhe und Tilgungstermin "geldlicher Verpflichtungen oder Schulden", monatliche Tilgung. (Hier sollte eine Frage nach geordneten wirtschaftlichen Verhältnissen genügen. Anderenfalls wäre zur richtigen Beurteilung eine detaillierte Aufstellung der Einkommens-, Vermögens- und Belastungsverhältnisse erforderlich. Eine solche halte ich für unverhältnismäßig.)

Darüber hinaus erklärt sich der Polizeibewerber formularmäßig durch seine Unterschrift "damit einverstanden, daß über meinen Leumund Auskünfte eingeholt werden". Die Polizei fühlt sich dadurch ermächtigt, an andere (Polizei-) Dienststellen folgende Anfrage zu richten: "Im Wege der Amtshilfe wird gebeten mitzuteilen, ob anhand von Dateien, Karteien usw. Erkenntnisse vorliegen, die gegen eine mögliche Einstellung sprechen könnten. Dabei sind sowohl abgeschlossene als auch zur Zeit anhängige Straf- oder Ermittlungsverfahren sowie evtl. milieubedingte Kenntnisse von Interesse".

Diese Nachfrage geht über Eintragungen im Bundeszentralregister weit hinaus und umfaßt z.B. auch Ermittlungsvorgänge nach einer Einstellung des Verfahrens. Ob und wie in der Praxis "milieubedingte Kenntnisse" von bloßen Gerüchten, Mutmaßungen, auch Vorurteilen abzugrenzen sind, halte ich für ungeklärt. Auf die erwähnte Einwilligung des Bewerbers kann sich die Polizei bei einer derart vagen Formulierung nicht stützen.

Die Feuerwehr geht in der Erforschung der Vergangenheit noch weiter als die Polizei: Sie fragt nicht nur nach den Personalien des Vaters ("bei ehelicher Geburt") bzw. der Mutter ("bei nichtehelicher Geburt"), sondern auch noch nach denen des Großvaters ("väterlicherseits") bzw. "Großvater (mütterlicherseits) bzw. Großmutter bei nichtehelicher Geburt der Mutter". Der Bewerber muß also die eheliche Abstammung (dann interessieren die Feuerwehr nur die männlichen Vorfahren) oder nichteheliche Abstammung seiner selbst und sogar seiner Mutter offenbaren, ohne daß dies als Kriterium für die Auswahl nach Eignung, Befähigung und fachlicher Leistung herangezogen werden dürfte. Auch wenn eine nichteheliche Abstammung heute zumindest in Hamburg kaum noch einen sozialen Makel bedeutet, halte ich derart intime Fragen für einen schwerwiegenden Verstoß gegen das informationelle Selbstbestimmungsrecht.

Die Innenbehörde hat auf meine Stellungnahme vom 22. August 1988 bisher nur eine Zwischennachricht gegeben.

Auf meine Kritik an den Fragebogen der Justizbehörde hat diese einige Änderungen der Formulare angekündigt. Dies gilt insbesondere für eine Trennung der Bewerbungsfragen von den Personalverwaltungsfragen. Darüber hinaus soll in Zukunft die Adressenangabe des derzeitigen Arbeitgebers des Bewerbers ebenso freiwillig sein wie die — nun gesondert erbetene — Einwilligung in die Anforderung der Personalakte. Bezüglich einzelner anderer Fragen ist die Diskussion mit der Justizbehörde noch nicht abgeschlossen.

— Personalkarteikarte für Dienststellenleiter; Formular für Ernennungsvorschläge —

Die Eingabe eines Behördenbediensteten veranlaßte mich, die vom Senatsamt für Bezirksangelegenheiten herausgegebene Karteikarte für Dienststellenleiter zu überprüfen und eine Änderung anzuregen. Zwar räume ich ein, daß neben der Personalabteilung auch die jeweilige Dienststellen-/Fachamtsleitung über einen gewissen Grundstock an Personaldaten der Mitarbeiter/innen für Personalplanungszwecke muß verfügen können. Dazu gehören meiner Auffassung nach jedoch nicht Angaben über Geburtsort, Familienstand und Kinder. Die Rubrik "Bemerkungen" könnte zur Eintragung einerseits überflüssiger, andererseits besonders mißbrauchsgefährdeter Angaben ("fleißig", "gesellig" usw.) verleiten. Das Senatsamt für Bezirksangelegenheiten hat inzwischen die beanstandeten Fragen/Angaben aus dem Formular herausgenommen und den Bezirksämtern neue Karteikarten zugesandt.

Auch das von den Behörden verwandte Formular P 10.105 "Ernennungsvorschlag" des Personalamtes weist Angaben über Familienstand und Kinderzahl auf, die ich für einen Ernennungsvorschlag nicht für erforderlich halte. Das Personalamt erklärte sich bereit, bei einer Neuauflage des Vordrucks auf diese Fragen zu verzichten.

4.2.4 Aufbewahrung von Bewerbungsunterlagen

Aufgrund eines Beschlusses des Arbeitsgerichts Hamburg vom 23. Februar 1988 hatte ich mich gutachterlich zu der Frage zu äußern: Bestehen Bedenken gegen die Praxis des Senatsamtes für den Verwaltungsdienst — Prüfungsamt für den öffentlichen Dienst —, die Prüfungsunterlagen erfolgloser Bewerber vier Jahre lang aufzubewahren?

In meinem 2. Tätigkeitsbericht 1983, S. 47 ff., hatte ich Datenspeicherung und Verfahren des Prüfungsamtes ausführlich dargestellt. Wenige Monate nach meiner damaligen Untersuchung erging das Volkszählungsurteil des Bundesverfassungsgerichts, das insbesondere an die Ermächtigungsgrundlage für Eingriffe in das informationelle Selbstbestimmungsrecht strenge Anforderungen stellt. Mangels spezialgesetzlicher

Regelungen für die Aufbewahrung von Prüfungsunterlagen kommt hierfür nur § 9 HmbDSG in Betracht. Dessen generalklauselartige Formulierung "Das Speichern ist zulässig, wenn es zur rechtmäßigen Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgabe erforderlich ist" kann jedoch den Anforderungen des Volkszählungsurteils an eine normenklare, für den Bürger nachvollziehbare Eingriffsermächtigung heute nicht mehr genügen. Für die Übergangszeit bis zum Erlaß einer tragfähigen gesetzlichen Grundlage kann nach dem Bundesverfassungsgericht nur noch geduldet werden, was "im konkreten Fall für die geordnete Weiterführung eines funktionsfähigen Betriebs unerläßlich ist." Dies mag für eine Praxis gelten, die verhindern soll, daß ein abgelehnter Bewerber sich in kürzesten Zeitintervallen erneut bewirbt und mangels entsprechender Hinweise auch erneut geprüft wird. Eine Liste mit Namen, Prüfungstermin und Ergebnis reicht dazu aus; eine Aufbewahrung der vollständigen Bewerbungsunterlagen ist dazu jedoch nicht "unerläßlich".

Ebenso hat im Ergebnis das Bundesarbeitsgericht bereits am 6. Juni 1984 entschieden. Über dieses Urteil hatte ich in meinem 3. Tätigkeitsbericht, S. 122, ausführlich berichtet, ohne allerdings das Prüfungsamt noch einmal speziell auf diese Rechtsprechung hinzuweisen. Auch der gegenwärtig diskutierte Entwurf eines neuen hamburgischen Datenschutzgesetzes trifft eine Regelung in diesem Sinne, wenn er in § 28 Abs. 4 Satz 1 vorsieht: "Personenbezogene Daten, die vor der Eingehung eines Beschäftigungsverhältnisses erhoben wurden, sind unverzüglich zu löschen, sobald feststeht, daß ein Beschäftigungsverhältnis nicht zustandekommt".

Eine Erörterung mit dem Leiter des Prüfungsamtes ergab allerdings, daß die derzeitige Kommunikationsstruktur zwischen dem zentralen Prüfungsamt und den dezentralen Beschäftigungsbehörden es heute nicht zuläßt, den Zeitpunkt der Erfolglosigkeit einer Bewerbung — und damit das Ende der Aufbewahrungszeit — früh und eindeutig festzulegen. Dieses verwaltungsorganisatorische Problem kann jedoch an der grundsätzlichen Forderung, Prüfungsunterlagen erfolgloser Bewerber zu löschen, nichts ändern. Hier sind zur Gewährleistung des Datenschutzes neue Formen des Informationsaustausches unvermeidlich.

Der Rechtsstreit, den das Arbeitsgericht zu entscheiden hat — ein Urteil liegt noch nicht vor —, weist über die allgemeine Problematik hinaus noch die Besonderheit auf, daß der Kläger eine Arbeitsbeschaffungsmaßnahme (ABM) wahrnehmen sollte, aber auch für ein späteres Dauerarbeitsverhältnis in Betracht kam. Deswegen unterzog er sich der Eingangsprüfung bereits kurz nach Antritt der ABM. Nach Nichtbestehen der Prüfung wurde ihm sofort gekündigt mit der Folge, daß er auch die ABM, für die eine Eignungsprüfung selbst nicht erforderlich ist, nicht wahrnehmen konnte. Ich halte diese Praxis nicht für angemessen. Der für eine Dauerbeschäftigung in Betracht kommende Bewerber wird hier schlechter gestellt als eine "normale" ABM-Kraft. Die Eignungsprüfung sollte vielmehr erst am Ende der ABM stattfinden, wenn der Bewerber an einer Daueranstellung dann noch selbst interessiert ist.

4.2.5 Ortszuschlag

Aus dem Ortszuschlagsrecht habe ich mit dem Personalamt vor allem die Regelung bei Aufnahme einer Person in die Wohnung des Antragstellers intensiver erörtert (Zur allgemeinen Problematik der Datenerfassung im Ortszuschlagsrecht vgl. 6. TB, 4.2.4, S. 39 ff.).

Einem Entwurf des Personalamtes für "Hinweise zum Ortszuschlag/Anwärter-Verheiratetenzuschlag" habe ich in mehreren Punkten widersprochen. So soll der Ortszuschlag entgegen der bisherigen Praxis in Zukunft auch dann anteilig gekürzt werden, wenn zwei im öffentlichen Dienst beschäftigte Mitbewohner jeweils unabhängig voneinander eine weitere Person (Kind) aufgenommen haben und ihr jeweils Unterhalt zahlen. Bislang trat die Ortszuschlags-Kürzung nur ein, wenn beide Mitbewohner für dieselbe aufgenommene Person (anteilig) Unterhalt zahlten. Datenschutzrechtlich ist dies insofern relevant, als die beabsichtigte Neuregelung weitere Datenerhebungen notwendig macht. Auch die automatische Versendung von Vergleichsmitteilungen an den Arbeit-

geber des Mitbewohners ohne sein Wissen habe ich kritisiert. Das Personalamt ist allerdings bereit, auf den Austausch einer Vergleichsmitteilung zu verzichten, wenn der Antragsteller eine Bescheinigung des Arbeitgebers des Mitbewohners vorlegt, nach der dieser keinen erhöhten Ortszuschlag geltend gemacht hat. Diese Möglichkeit, eine Vergleichsmitteilung mit den eigenen Daten zu vermeiden, muß dem Antragsteller jedoch bereits im Fragebogen angeboten werden.

Einen zunächst vorgelegten Entwurf für eine siebenseitige "Ergänzende Erklärung zum höheren Ortszuschlag wegen Aufnahme einer Person in die Wohnung" zog das Personalamt zurück und übernahm weitgehend einen von mir eingebrachten Formulierungsvorschlag. Dieser reduziert den Umfang der Fragen erheblich und kommt so mit zwei Seiten aus. An die Stelle detaillierter Angaben zu einer die Wohnung des Antragstellers mitbewohnenden Person tritt die Erklärung des Antragstellers, daß er — bei Beanspruchung des vollen Ortszuschlages — entweder allein mit der aufgenommenen Person lebt oder der/die Mitbewohner/in versichert habe, einen eigenen Anspruch auf erhöhten Ortszuschlag wegen der aufgenommenen Person nicht zu stellen. Nur wenn die mitbewohnende Person im öffentlichen Dienst beschäftigt ist (oder der Antragsteller hierüber im Zweifel ist), ist auch die Beschäftigungsbehörde anzugeben. Weitere Beschäftigungsdaten werden nicht erhoben. Das Formular enthält ferner die Einverständniserklärung für Vergleichsmitteilungen an die Beschäftigungsbehörde des Mitbewohners. Ich habe angeregt, im Formular alternativ auch noch die angesprochene Möglichkeit zu schaffen, eine entsprechende Bestätigung der Beschäftigungsbehörde des Mitbewohners vorzulegen.

Meine schon mehrfach geäußerten Bedenken gegen den allgemeinen Ortszuschlag-Fragebogen P 10.025 mußte ich in diesem Jahr leider wiederholen. Nach wie vor wird der verheiratete Antragsteller danach gefragt, ob der Ehegatte berufstätig ist, wo er arbeitet und — unabhängig davon, ob der Arbeitgeber zum öffentlichen Dienst gehört oder nicht — mit wieviel Wochenstunden, unter welcher Personalnummer. Es werden hinsichtlich des Ehegatten ferner Sonder-, Mutterschafts-, Erziehungsurlaubszeiten, Krankengeld-Bezugszeiten sowie die Art des Beschäftigungsverhältnisses abgefragt. Ich halte es beispielsweise für unzulässig, daß der Dienstherr erfährt, daß die Frau des Antragstellers als Verkäuferin bei Karstadt mit 30 Wochenstunden teilzeitbeschäftigt ist und von März bis April Krankengeld nach der RVO bezogen hat.

Auf meine in einem Schreiben vom 1. August 1988 zusammengefaßten Bedenken und Anregungen hat das Personalamt bislang nicht reagiert.

4.2.6 Sicherheitsrichtlinien

Am 1. Mai 1988 traten neue "Richtlinien (des Bundes) für die Sicherheitsüberprüfung von Personen im Rahmen des Geheimschutzes" in Kraft. Das Bundesinnenministerium empfiehlt und geht davon aus, daß diese Sicherheitsrichtlinien von den Ländern übernommen werden. Auf meine Anfrage antwortete die Behörde für Inneres — Landesamt für Verfassungsschutz — im April 1988, sie werde einen Entwurf für hamburgische Sicherheitsrichtlinien erstellen, "der einige spezifisch hamburgische Belange und Formulierungserfordernisse berücksichtigt, im wesentlichen aber die Bundesrichtlinien wortgetreu wiedergeben wird".

Wie der Bundesbeauftragte für den Datenschutz habe auch ich Bedenken gegen die neuen Sicherheitsrichtlinien. Sie können die durch das Volkszählungsurteil des Bundesverfassungsgerichts geforderte normenklare gesetzliche Grundlage für die Datenerhebungen des Verfassungsschutzes nicht ersetzen. Den neuesten Beschluß des Bundesverfassungsgerichts vom 10. Februar 1988 (Deutsches Verwaltungsblatt 1988, S. 530), die Datenerhebungen im Rahmen von Sicherheitsüberprüfungen seien durch § 55 Bundesbeamtengesetz legitimiert, kann ich nicht nachvollziehen. § 55 BBG enthält lediglich die allgemeine Beratungs- und Unterstützungspflicht gegenüber den Vorgesetzten sowie die Pflicht, deren Anordnungen auszuführen. Über Voraussetzungen und Umfang von Sicherheitsüberprüfungen lassen sich dieser Vorschrift die notwendigen normenklaren Vorgaben nach meiner Auffassung nicht entnehmen.

Es kommen also — für eine Übergangszeit — nur solche Datenverarbeitungen in Betracht, die für die Staatssicherheit unerläßlich sind. Mit einer Ausdehnung der Sicherheitsüberprüfung auf Ehegatten, Verlobte und Lebensgefährten gehen die Sicherheitsrichtlinien aber noch über die bisherigen Grundrechtseingriffe weit hinaus. Sie berühren nicht nur das Recht des Bediensteten auf informationelle Selbstbestimmung, sondern auch den Grundrechtsschutz Dritter.

4.3 Statistik

4.3.1 Landesstatistikgesetz

Leider ist die Erstellung eines Hamburgischen Landesstatistikgesetzes im Jahr 1988 kaum vorangekommen. Ich komme deshalb nicht umhin festzustellen, daß es für einen großen Teil der Verarbeitung personenbezogener Daten durch das Statistische Landesamt nach wie vor an einer verfassungsgemäßen Rechtsgrundlage mangelt (vgl. 4. TB, 4.3.5, S. 43; 5. TB, 5.3.3, S. 46 und 6. TB, 4.3.1, S. 43).

4.3.2 Volkszählung 1987

Die mit Stichtag 25. Mai 1987 bundesweit durchgeführte Volkszählung ist in Hamburg nicht so zügig abgewickelt worden, wie dies dem erkennbaren Willen des Gesetzgebers entsprochen hätte und auch von den Statistikern vor der Erhebung zugesagt worden war. Das Ziel, zeitnah flächendeckend genaue Daten über die Bevölkerung, den Gebäude- und Wohnungsbestand und die Arbeitsstätten zu erhalten, ist nicht erreicht worden. In Hamburg hat sich allein die Erhebungsphase, in der versucht wurde, bei den Auskunftspflichtigen Auskünfte zu erhalten, über einen Zeitraum von nahezu 18 Monaten hingezogen. Erst mit Ablauf des 15. November 1988 hat die Erhebungsstelle des Statistischen Landesamtes die Erhebung bei den Auskunftspflichtigen abgeschlossen.

So hat es mich auch nicht verwundert, daß das Statistische Landesamt Ende November nicht — wie von den Datenschutzbeauftragten und der Öffentlichkeit erwartet — die Endergebnisse der Volkszählung in Form einer amtlichen Bevölkerungszahl bekanntgeben konnte, sondern lediglich vorläufige, zum großen Teil ungeprüfte Eckzahlen vorgelegt hat. Mit der Feststellung einer amtlichen Bevölkerungszahl ist in Hamburg nicht vor Ende März 1989 zu rechnen. Auch wenn einzelne andere Länder (z.B. Hessen), in denen weniger Probleme mit der Erhebungsorganisation aufgetreten sind, bereits zu einem amtlichen Ergebnis gelangt sind, ist bundesweit ein Abschluß der Aufbereitungsarbeiten für die Volkszählung noch lange nicht erreicht. Im Gegenteil: Das Statistische Bundesamt hat kurz vor der Bekanntgabe von bundesweiten Eckzahlen im November 1988 die Statistischen Landesämter aufgefordert, auf die Feststellung der amtlichen Bevölkerungszahl vorerst zu verzichten, bis weitere, auch länderübergreifende sachlogische Konsistenzprüfungen stattgefunden haben. Bis auf weiteres seien also keine "endgültigen" Zahlen, sondern lediglich "erste" statistische Ergebnisse bekanntzugeben, die unter dem Vorbehalt von Änderungen aus statistischen Verfahren, aber ggf. auch aus Rechtsmittelverfahren stehen. Besonders gravierend ist in diesem Zusammenhang die Forderung des Statistischen Bundesamtes, bis zum Abschluß dieser Prüfungen das Ausgangsmaterial (d.h. die personenbezogenen Erhebungsunterlagen) nicht zu vernichten.

Es ist klar, daß die Durchführung weiterer, im bundeseinheitlichen Verarbeitungskonzept des Statistischen Bundesamtes überhaupt nicht vorgesehener Plausibilitäts- und Konsistenzprüfungen weitere Verzögerungen in der Abwicklung der Volkszählung und damit verbunden auch in der Durchführung der gesetzlich vorgeschriebenen grundrechtssichernden Maßnahmen, insbesondere der Vernichtung der Erhebungsunterlagen und der Anonymisierung der automatisiert gespeicherten Daten nach sich ziehen werden.

Ich bin der Auffassung, daß dieses Vorgehen der gesetzlich vorgesehenen, aber auch verfassungsrechtlich gebotenen Durchführung grundrechtssichernder Maßnahmen

zum frühestmöglichen Zeitpunkt widerspricht. Das Volkszählungsgesetz schreibt in § 15 Abs. 2 vor, daß die Erhebungsvordrucke einschließlich der Hilfsmerkmale zum frühestmöglichen Zeitpunkt, spätestens zwei Wochen nach Feststellung der amtlichen Bevölkerungszahl des Landes, zu vernichten sind. Diesem kommt auch für die gesetzlich ebenfalls gebotene Anonymisierung des automatisierten Datenbestandes (§ 15 Abs. 3 VZG) entscheidende Bedeutung zu. Ich hatte bereits frühzeitig darauf hingewiesen, daß sich die Erhebungs- und Aufbereitungsorganisation an einer zügigen Erhebung zu orientieren habe und vermeidbare Fehler und Mängel es nicht rechtfertigen können, daß sich Trennung und Löschung verzögern. Der Termin der Feststellung der amtlichen Bevölkerungszahl stellt keine autonome Größe dar; er ist vielmehr im Kontext des Gebots zur möglichst frühzeitigen Durchführung der grundrechtssichernden Maßnahmen zu sehen. Es darf deshalb nicht in das Belieben der Statistischen Ämter gestellt sein, wann und unter welchen Voraussetzungen sie die Erhebungsunterlagen vernichten und die Daten in der gesetzlich vorgeschriebenen Weise anonymisieren.

Für Hamburg läßt sich feststellen, daß im Statistischen Landesamt zum Jahreswechsel 1988/1989 noch sämtliche Melderegisterangaben, die für die Organisation der Zählung vom Einwohnermeldeamt übermittelt worden waren, vorhanden sind, ferner sämtliche ausgefüllten Haushaltsmantelbögen, Personen- und Wohnungsbögen, die dazugehörigen von den Zählern ausgefüllten Adressenlisten und die in der Erhebungsstelle Volkszählung angelegten Regionallisten. Darüber hinaus besteht ein automatisierter — wenn auch noch nicht vollständig plausibilisierter — Datenbestand mit Erhebungsdaten, wobei eine Verknüpfung der verschiedenen Datenbestände (z.B. über die Haushaltsheftnummer und die genaue Anschrift) jederzeit möglich ist. Ich halte die gleichzeitige automatisierte Speicherung von Organisations- und Erhebungsdaten deshalb und auch wegen der seit dem Erhebungsstichtag vergangenen Zeit für sehr problematisch.

Im Zusammenhang mit der Volkszählung habe ich auch im Jahr 1988 eine Vielzahl von Bürgeranfragen beantworten und Eingaben von Petenten nachgehen müssen. Im folgenden möchte ich nur auf einige der Problemkomplexe eingehen, die mich im Jahr 1988 im Zusammenhang mit der Volkszählung beschäftigt haben und die von grundsätzlicher Bedeutung sind:

4.3.2.1 Automatisiertes Erinnerungs- und Mahnverfahren

Die Erhebungsstelle Volkszählung hatte sich bereits 1987 für Zwecke der Vollzähligkeitskontrolle und der Abwicklung von Erinnerungs- und Mahnverfahren gegenüber säumigen Auskunftspflichtigen von der Meldebehörde die in § 11 Abs. 1 VZG genannten Merkmale übermitteln lassen (vgl. 6. TB, 4.4.4.5, S. 63). Diese Daten wurden in der Datenbank "ERA" (Einwohnerregisterauszug) gespeichert und standen den Sachbearbeitern in den Zählungsdienststellen on-line zur Verfügung.

Ich hatte gegen die Errichtung dieser Datenbank unter der Bedingung keine Einwände erhoben, daß die einzelnen Datensätze zum frühestmöglichen Zeitpunkt, d.h. nach Eingang der ausgefüllten Erhebungsunterlagen des jeweiligen Betroffenen bei der Erhebungsstelle, gelöscht würden. Obwohl die Mehrzahl der Hamburger Bürger ihrer Auskunftspflicht bereits im Jahr 1987 nachgekommen war, die Erhebungsunterlagen mithin in der Erhebungsstelle bereits vorlagen, wurde die ERA-Datei erst im Zuge der Abschlußarbeiten für die einzelnen Zählungsbezirke seit dem Frühjahr 1988 sukzessive reduziert. Auf meine seit August 1988 wiederholt gestellten Fragen nach dem aktuellen ERA-Bestand hat das Statistische Landesamt zunächst nicht geantwortet. Erst mit Schreiben vom 30. November 1988 wurde mir von der Behörde für Inneres mitgeteilt, daß sich am Stichtag 24. November 1988 noch Datensätze über 62.629 Personen in der ERA-Datenbank befunden hätten. Dabei habe es sich um folgende Fallgruppen gehandelt:

— Personen, die nach dem Zählungsstichtag unbekannt verzogen sind,

— verstorbene Personen,

— säumige Auskunftspflichtige.

Die Behörde für Inneres hat mir zugleich zugesichert, daß die verbliebenen ERA-Daten Anfang Dezember gelöscht würden. Dabei war auch vorgesehen, die vorhandenen Sicherungskopien innerhalb der kommenden zwei Wochen ebenfalls zu löschen. Inzwischen hat sich aber herausgestellt, daß der am 6. Dezember 1988 erfolgten Löschung der "aktiven" ERA-Datenbank eine Löschung der Sicherungskopien erst mit 100-tägiger Verzögerung (d.h. erst Mitte März 1989) folgen soll. Der Datenbestand ist gemeinsam mit den Datenbeständen anderer Behörden in einer physischen ADABAS-Datenbank gehalten und im Rahmen einer automatisierten Archivierung auf ein Magnetband überspielt worden. Für diese Form der automatisierten Datensicherung ist eine 100-tägige Löschungsfrist vorgesehen.

Auch wenn mit der Löschung der aktiven ERA-Datenbestände ein on-line-Zugriff auf die dort gespeicherten personenbezogenen Daten nicht mehr möglich ist, muß ich doch feststellen, daß durch das unflexible Sicherungsverfahren die Speicherungsdauer entgegen dem Gebot des § 15 Abs. 3 HmbDSG in unzulässiger Weise ausgeweitet wurde. Das Gesetz schreibt vor, daß personenbezogene Daten zu löschen sind, wenn ihre Kenntnis für die speichernde Stelle zur Erfüllung der Aufgaben nicht mehr erforderlich ist. Ich bin der Auffassung, daß sich durch eine andere Organisation des ERA-Datenbestandes und durch vorausschauende Planung dieses Problem hätte vermeiden lassen.

4.3.2.2 Datenverarbeitungskonzept

Ich habe wiederholt darauf hingewiesen, daß dem rechtzeitigen Vorliegen eines verbindlichen Datenverarbeitungskonzeptes für die Volkszählung erhebliche verfassungsrechtliche Bedeutung zukommt (vgl. 6. TB, 4.4.3.1). Ohne Kenntnis eines solchen Konzeptes ist eine effektive Datenschutzkontrolle vor allem im Hinblick auf das automatisierte Verfahren kaum möglich. Während mir der erste Teil des Aufbereitungskonzeptes für die Volkszählungsdaten kurz vor dem Erhebungsstichtag (25. Mai 1987) zugestellt wurde, mußte ich auf die noch fehlenden Teile lange Zeit warten. Erst am 28. September 1988, d.h. lange nach Beginn der Aufbereitungsarbeiten, wurden die fehlenden Bestandteile nachgereicht. Es handelte sich dabei um einige zusätzliche Datenflußpläne und um Beschreibungen der "Satzarten", in denen Volkszählungsdaten im Verlauf des Verarbeitungsprozesses anfallen. Die mir gegenüber als verbindlich bezeichneten Unterlagen über durchzuführende Arbeitsgänge schließen die Bildung eines anonymisierten bzw. mit verfremdeten Orts- und Hilfsmerkmalen ausgestatteten Datenbestandes mit ein. Mit Verwunderung habe ich deshalb zur Kenntnis genommen, daß das Statistische Landesamt — wie bereits oben erwähnt — weitere, in dem mir übersandten Verarbeitungskonzept nicht enthaltene Arbeitsschritte vorhat, um die Plausibilität und Konsistenz des Erhebungsmaterials zu verbessern. Über diese zusätzlichen Verarbeitungsschritte bin ich erstmals mit Schreiben vom 5. Dezember 1988, und zwar nur andeutungsweise, unterrichtet worden. Ein aufgrund dieses Schreibens am 14. Dezember 1988 geführtes Gespräch hat mir von den geplanten zusätzlichen Verarbeitungsgängen folgendes Bild vermittelt (eine ausführliche schriftliche Beschreibung lag mir bis zum Redaktionsschluß noch nicht vor):

— Es ist vorgesehen, etwaige Doppelerfassungen, wie sie z.B. aufgrund von Umzügen während der langen Dauer der Erhebungsphase vorgekommen sein mögen, anhand der Haushaltsmantelbögen festzustellen. Dabei soll der automatisiert gespeicherte Erhebungsdatenbestand anhand bestimmter Merkmale (Alter, Geburtsjahr, Geschlecht und Staatsangehörigkeit) durchgesucht und Fälle mit gleichen Merkmalskombinationen selektiert werden. Die so erzielten "Treffer" sollen anhand der aus dem Melderegister übermittelten Daten (Meldeliste) und anderer Erhebungsunterlagen (z.B. Haushaltsmantelbögen) auf Namensgleichheit hin überprüft werden. Bei namensgleichen Fällen wird auf Doppelzählung geschlossen und der automatisierte Datenbestand entsprechend bereinigt.

— In ca. 18.000 Fällen ist übersehen worden, daß in Personenbögen Angaben über den Haupt- bzw. Nebenwohnsitz nicht ausgefüllt wurden. In diesen Fällen soll auf

die Angaben über Haupt- bzw. Nebenwohnung im Melderegisterauszug zurückgegriffen werden.

— Das Statistische Landesamt vermutet, daß die Zahl der festgestellten Wohnungen und Haushalte überhöht ist. Für Überprüfungszwecke stehen die im Frühjahr 1988 vernichteten Erhebungsunterlagen aus der Gebäudevorerhebung nicht mehr zur Verfügung. Das Statistische Landesamt hatte vor, die Ergebnisse der Wohnungszählung mit der Stromzählerdatei der HEW abzugleichen. Dem lag die Überlegung zugrunde, daß im allgemeinen je Wohnung ein Stromzähler vorhanden ist. Für den Abgleich hat das Statistische Landesamt die HEW aufgefordert, die Zahl der Stromzähler je Gebäude zur Verfügung zu stellen. Für diese Prüfung soll ebenfalls ein Melderegisterauszug herangezogen werden, um festzustellen, ob ein Gebäude bewohnt ist oder nicht. Ich habe der Behörde für Inneres gegenüber deutlich gemacht, daß ich die Übermittlung personenbezogener Daten für Zwecke der Volkszählung nur im Rahmen der im Volkszählungsgesetz ausdrücklich festgelegten Grenzen für zulässig halte. Der vorgesehene gebäudeweise Abgleich der Stromzählerdatei der HEW mit den Daten der Wohnungszählung würde einen unzulässigen, weil im Gesetz nicht vorgesehenen, Übermittlungsvorgang darstellen. Zumindest in den Fällen, in denen sich nur ein Stromzähler in einem Gebäude befindet, ist ein Rückschluß auf persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (personenbezogene Daten i.S.v. § 4 Abs. 1 HmbDSG) möglich. Es handelt sich nicht nur für die HEW um personenbezogene Daten (ihnen ist ja der jeweilige Anschlußinhaber bekannt), sondern auch in Bezug auf den vom Statistischen Landesamt beabsichtigten Verwendungszweck. Aus der Zählerzahl je Gebäude soll auf die Wohnungszahl geschlossen werden. Dies bedeutet, daß bei Vorhandensein nur eines Stromzählers in einem Wohngebäude davon ausgegangen werden könnte, daß die in diesem Haus wohnenden Personen nicht in verschiedenen, sondern nur in einer Wohnung leben. In diesen Fällen sollen — wenn aufgrund der Angaben des Auskunftspflichtigen oder der Ersatzvornahme bisher von mehreren Wohnungen ausgegangen worden ist — die Wohnungszahl entsprechend reduziert und die Betroffenen einer gemeinsamen Wohnung zugeordnet werden. Die Erörterung dieses Verfahrens mit der Innenbehörde ist noch nicht abgeschlossen.

4.3.2.3 Auftragsdatenverarbeitung in Nordrhein-Westfalen

Anfang Mai 1988 war ich von der Behörde für Inneres darüber informiert worden, daß beabsichtigt sei, zur Vermeidung weiterer Verzögerungen in der Aufbereitung der Volkszählungsdaten einen Teil der maschinellen Erfassungs- und Verarbeitungsaufgaben durch das Landesamt für Datenverarbeitung und Statistik Nordrhein-Westfalen abwickeln zu lassen. Ich hatte diesem Vorhaben unter der Bedingung zugestimmt, daß

— für die in Nordrhein-Westfalen durchgeführten Arbeitsgänge der für Hamburg gültige Sicherheitsstandard gewährleistet wird,

— die bei der maschinellen Erfassung eingesetzten Verfahrensteile ordnungsgemäß nach einem Abnahmetest freigegeben werden,

— ein klar definiertes Auftragsdatenverarbeitungsverhältnis i.S.v. § 3 HmbDSG festgeschrieben und Unterauftragsverhältnisse (z.B. von Signierarbeiten in Heimarbeit) ausgeschlossen werden,

— der Transport der Erhebungsunterlagen angemessen gesichert wird,

— sichergestellt wird, daß beim Auftragnehmer nach Abgabe der beschriebenen Magnetbänder an das Statistische Landesamt Hamburg keine Hamburger Volkszählungsdaten dort maschinell gespeichert bleiben.

Die Arbeiten wurden wie vorgesehen durch das Landesamt für Datenverarbeitung und Statistik Nordrhein-Westfalen abgewickelt. Ich hatte keinen Anlaß zu Beanstandungen.

4.3.2.4 Zeitpunkt der Vernichtung der Erhebungsunterlagen

Ich hatte die Behörde für Inneres bereits frühzeitig (im November 1987) darauf hingewiesen, daß — vermeidbare — Verzögerungen auch eine datenschutzrechtliche Qualität bekommen, sofern sie dazu führen, daß sich auch die im Volkszählungsgesetz vorgeschriebenen grundrechtssichernden Maßnahmen verzögern. Ich hatte dabei die Auffassung geäußert, daß das seinerzeit im Senat zur Entscheidung anstehende Zwangsgeldverfahren aufgrund der organisatorischen Gegebenheiten und des Verarbeitungskonzeptes des Statistischen Landesamtes in Hamburg erhebliche Verzögerungen nach sich ziehen würde und damit die Zulässigkeit der gesamten weiteren Verarbeitung und Verwertung der Erhebungsdaten in Frage gestellt würde. Aus diesem Grund hatte ich seinerzeit empfohlen, zur Vermeidung weiterer Verzögerungen für die noch fehlenden Daten eine Ersatzvornahme gem. § 11 Abs. 1 VZG vorzunehmen. Der Senat war damals meinen Empfehlungen nicht gefolgt und hatte sich für die Durchführung eines Erzwingungsverfahrens entschieden, das erst durch Senatsbeschluß vom 15. November 1988 abgeschlossen wurde. Aufgrund der Tatsache, daß mittlerweile einige Flächenländer, bei denen sich — wegen ihrer zweigliedrigen Erhebungsorganisation (Länder/Gemeinden) — die Durchführung der Volkszählung naturgemäß erheblich komplizierter gestaltet als in einem Stadtstaat, ihre Bevölkerungszahlen feststellen konnten, hatte ich es für selbstverständlich gehalten, daß auch in Hamburg bis zum 25. November 1988 bei entsprechend zweckmäßiger Erhebungsorganisation die amtliche Bevölkerungszahl hätte festgestellt werden können.

Aufgrund der weiter oben beschriebenen, vom Statistischen Landesamt für unabdingbar gehaltenen zusätzlichen sachlogischen Prüfungen sind für die einzelnen Papiere nunmehr folgende Vernichtungszeitpunkte vorgesehen:

— Haushaltsmantelbögen im Januar 1989,

— Melderegisterauszug Mitte Februar 1989,

— Personen- und Wohnungsbögen ab Ende Februar 1989 bis März 1989,

— Regional- und Adreßlisten bis Ende März 1989.

Von den Unterlagen aus der Arbeitsstättenzählung sollte mit der Vernichtung der Adreßlisten umgehend (d.h. noch im Dezember 1988) begonnen werden. Mit dem Abschluß der Vollzähligkeitskontrolle einschließlich der Blockseitenzuordnung aller Sätze sollen ab Mitte Februar 1989 sukzessive auch die Deckblätter der Arbeitsstättenbögen (mit den Hilfsmerkmalen) vernichtet werden. Ab Anfang März 1989 sollen ebenfalls sukzessive die Regionallisten und die Datenteile sämtlicher Arbeitsstättenbögen vernichtet werden.

Ich bin der Auffassung, daß bei zweckmäßiger Erhebungsorganisation die Unterlagen hätten zu einem früheren Zeitpunkt vernichtet werden können und daß somit das Gebot der möglichst frühzeitigen Vernichtung (§ 15 Abs. 2 VZG) nicht eingehalten wurde. Sofern weitere vermeidbare und von der Statistik zu verantwortende Verzögerungen in der Datenaufbereitung auftreten sollten, werde ich nicht umhin können, dies gegenüber dem Senat förmlich zu beanstanden.

4.3.2.5 Resümee

Auch wenn der formelle Schlußpunkt der Zählung, die Feststellung der amtlichen Bevölkerungszahl, auf Bundes- und auf Landesebene noch nicht erreicht ist, möchte ich an dieser Stelle ein — wenn auch vielleicht noch ergänzungsbedürftiges — Resümee ziehen.

Nach dem für den Datenschutz wegweisenden Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 hätte man erwarten müssen, daß bei dem neuen Anlauf zu einer derartigen "Totalerhebung" die im Volkszählungsurteil aufgestellten Grundsätze sowohl im Gesetzgebungsverfahren als auch bei der Umsetzung des Gesetzes penibel beachtet würden. Ich muß jedoch konstatieren, daß die Praxis in mancherlei Hinsicht diesen Erwartungen nicht entsprach.

Bereits im Gesetzgebungsverfahren zum Volkszählungsgesetz 1987 waren Zweifel daran laut geworden, ob die Alternativen zu einer Totalerhebung mit Auskunftszwang mit der gebotenen Gründlichkeit diskutiert worden sind. Ich hatte daraufhin vorgeschlagen, den flächendeckend zu erhebenden Merkmalskatalog auf ein Mindestmaß zu begrenzen. Diesem — vom Hamburger Senat aufgegriffenen — Vorschlag war die Bundesregierung seinerzeit nicht gefolgt.

In der Erhebungsphase hatte sich dann herausgestellt, daß die im Gesetz zugelassenen Datenquellen für eine reibungslose Abwicklung der Zählung z.T. nur bedingt geeignet waren. Gleichwohl konnte ich es nicht hinnehmen, wenn die Statistik versuchte, diesen Mangel dadurch zu heilen, daß sie auch auf andere als die gesetzlich zugelassenen Datenbestände zugriff.

Als besonders problematisch erscheint mir die Art und Weise, wie das Datenverarbeitungsverfahren für die VZ geplant, erstellt und modifiziert wurde (vgl. 4.3.2.2). Die Datenschutzbeauftragten von Bund und Ländern haben die Statistik dazu aufgefordert, rechtzeitig, d.h. vor Beginn der Erhebung, ein vollständiges DV-Konzept vorzulegen. Dazu war das Statistische Bundesamt, unter dessen Federführung die "Verbundprogramme" von einigen Statistischen Landesämtern erstellt wurden, nicht bereit oder nicht in der Lage. So ist es nicht in erster Linie von dem Statistichen Landesamt Hamburg zu verantworten, daß die Datenverarbeitungskonzeption nicht planmäßig im voraus erstellt wurde, was eine effiziente und zügige Datenverarbeitung sehr gefördert und auch die Datenschutzkontrolle sehr vereinfacht hätte. Stattdessen scheint das DV-Konzept sukzessive, mit nur geringem zeitlichen Vorlauf vor oder erst begleitend zu den jeweils als nächstes anstehenden Aufgaben, entstanden zu sein. Entsprechend zögerlich wurde ich informiert. Aus dieser Vorgehensweise resultieren nicht nur Verfahrensfehler, hierin ist auch eine Hauptursache für die aufgetretenen Verzögerungen zu sehen.

Auch hinsichtlich der Zuverlässigkeit und Genauigkeit vor allem der kleinräumigen Ergebnisse sind Zweifel angebracht. Allein in Hamburg hat es — trotz entschiedener Versuche, Auskunftsunwillige doch noch zur Teilnahme an der Zählung zu bewegen — mehr als 65.000 Fälle (3,8 %) gegeben, in denen auf Angaben der Auskunftspflichtigen verzichtet werden mußte und stattdessen einige wenige Grundangaben aus dem Melderegisterbestand nachgetragen wurden (Ersatzvornahme gem. § 11 Abs. 1 VZG). Da aber die Meldedaten recht ungenau sind, haben so auch die im Melderegister enthaltenen Fehler in den Erhebungsdatenbestand Eingang gefunden.

Dort, wo das Gesetz eine Ersatzvornahme nicht zuläßt (bei der Mehrzahl der Merkmale der Personenzählung und bei der gesamten Gebäude-, Wohnungs- und Arbeitsstättenzählung), waren die Statistiker ohnehin auf Schätzungen angewiesen, wenn keine Antworten der Auskunftspflichtigen vorlagen. Derartige Schätzungen sind aber sehr risikobehaftet. Hierzu ein Beispiel: Bundesweit war die Statistik davon ausgegangen, daß die tatsächliche Zahl der Wohnungen von den Fortschreibungsergebnissen der letzten Wohnungszählung nach unten abweicht. Als in Hamburg die Auszählung der Wohnungsbögen ergeben hatte, daß die Zahl hier höher liegt als die Fortschreibung, trauten die Statistiker diesem Ergebnis selbst nicht und verminderten das Zählungsergebnis pauschal um einige 10.000 Wohnungen. Diese "korrigierte" Zahl wurde dann unter der Überschrift "Informationen aus der Volkszählung 1987" veröffentlicht. Nun bemühen sich die Statistiker, durch Heranziehung zusätzlicher Quellen die Ergebnisqualität zu verbessern, was datenschutzrechtliche Probleme aufwirft (vgl. 4.3.2.2).

Es ist nicht meine Aufgabe, zu beurteilen, ob sich der für die Volkszählung getriebene personelle und materielle Aufwand gelohnt hat. Angesichts der aufgetretenen Pannen und Versäumnisse ist eine positive Bilanz der Zählung aus Sicht des Datenschutzes leider nicht möglich. Deshalb halte ich es für besonders wichtig, intensiver als bisher über datenschutzfreundliche Alternativen zur Totalerhebung mit Auskunftspflicht nachzudenken. Ebenso möchte ich der Statistik empfehlen, Datenschutz nicht als Hemmschuh, sondern als Chance zu begreifen. Nur so wird es sich vermeiden lassen, daß die Akzeptanz statistischer Erhebungen beim Bürger noch weiter nachläßt.

4.3.3 Hochschulstatistik

In meinem 6. Tätigkeitsbericht (6. TB, 4.3.2, S. 43 ff.) hatte ich kritisiert, daß die Behörde für Wissenschaft und Forschung und das Statistische Landesamt trotz fehlender Rechtsgrundlage die Verarbeitung der Daten von Studenten und Prüfungskandidaten ausgeweitet hatten. Ich hatte insbesondere Bedenken dagegen geäußert, daß auch Hamburger Hochschulen Daten für die bundesweite Verlaufsstatistik zuliefern, obwohl gerade diese Statistik in besonderer Weise in das Recht auf informationelle Selbstbestimmung der Betroffenen eingreift. Zu dieser Frage hat der Senat in seiner Stellungnahme folgendes ausgeführt:

"Eine Zusammenführung von Studentendaten und Prüfungsdaten in einer Studienverlaufsdatei erfolgt — entgegen der Vermutung des HmbDSB — wegen der noch ungeklärten Rechtslage derzeit nicht. Das Statistische Bundesamt hat lediglich eine methodische Prüfung vorgenommen, ob eine solche Zusammenführung technisch möglich ist, und ist zu einem positiven Ergebnis gelangt. Eine Studienverlaufsstatistik mit Studentendaten wird in Hamburg nicht geführt.

Bei der Lieferung von Studentendaten an das Statistische Bundesamt und den dort laufenden Aktivitäten handelt es sich überwiegend um noch unveröffentlichte Arbeiten zur Erprobung und Vervollständigung des statistischen und technischen Verfahrens. Es werden derzeit vom Statistischen Bundesamt lediglich vereinzelt Arbeitsunterlagen in statistischer (anonymisierter) Form erstellt und z.B. dem Sekretariat der Kultusministerkonferenz zur Verfügung gestellt." (Bürgerschafts-Drs. 13/1734, S. 6)

Ich ging aufgrund der zitierten Stellungnahme des Senats davon aus, daß — da sich Hamburg ja nicht an der Verlaufsstatistik beteiligt und die Daten nicht in einer Verlaufsdatei zusammengeführt werden — ein Verzicht auf die Übermittlung der ausschließlich für die Verlaufsstatistik bestimmten Daten ohne Probleme möglich sein müßte. Deshalb war ich sehr überrascht, als meine entsprechenden Vorschläge von der Behörde für Inneres mit der Begründung zurückgewiesen wurden, daß — sofern die Hochschulen die Merkmale Geburtsdatum und Geburtsort der Studenten nicht an das Statistische Landesamt übermittelten — die Studentenverlaufsstatistik nicht mehr durchgeführt werden könne, da diese Daten zur Bildung des für eine Zusammenführung der Fälle unerläßlichen Identifikationsmerkmales unbedingt notwendig seien.

Meine aufgrund dieser widersprüchlichen Äußerungen vorgenommenen Ermittlungen haben ergeben, daß die Hamburger Hochschulen sehr wohl Daten zu der bundesweiten Verlaufsstatistik beisteuern und mithin die Senatsstellungnahme von unzutreffenden Tatsachen ausgeht. Die Hochschulen liefern die Studentendaten an das Statistische Landesamt. Dort werden sie für die automatisierte Weiterverarbeitung und Auswertung erfaßt und auf Magnetbändern an das Statistische Bundesamt geliefert. Darüber hinaus werden die Banddatensätze durch das Statistische Landesamt für die stichtagsbezogene Hochschulstatistik ausgewertet.

Das Statistische Bundesamt führt zentral eine Studienverlaufsdatei mit Individualdatensätzen, die über einen Identifikator (bestehend aus Namensbestandteilen und Geburtsdaten) zusammengeführt werden können. Daten aus dieser Datei wurden und werden für planerische und bildungspolitische Zwecke zwar ausgewertet, wurden aber im Hinblick auf die bestehenden Rechtsunsicherheiten bislang nicht veröffentlicht. Doch wurden die Ergebnisse dem Hochschulstatistikausschuß und dem Sekretariat der Kultusminister der Länder zur Verfügung gestellt.

Während die Verlaufsstatistik über Studenten im geltenden Hochschulstatistikgesetz zumindest erwähnt wird (wenn auch eine genaue Spezifikation der erhobenen Hilfs- und Erhebungsmerkmale fehlt), ist dies bei der Statistik der Prüfungskandidaten und Prüfungsabsolventen (Prüfungsstatistik) nicht der Fall.

Auch für die Prüfungsstatistik werden aber an den Hamburger Hochschulen (bei Prüfungskandidaten und Prüfungsämtern) Daten erhoben, durch das Statistische Landesamt erfaßt und für periodische Veröffentlichungen ausgewertet und an das Statisti-

sche Bundesamt übermittelt. Der übermittelte Datensatz beinhaltet einen strukturgleichen Identifikator wie die Studienverlaufsstatistik, so daß die technische Voraussetzung für die Zusammenführung von Prüfungs- und Studienverlaufsdaten gegeben ist. Gleichwohl wird von der BWF und von dem Statistischen Landesamt versichert, daß bislang (bis auf wenige methodische Voruntersuchungen) von dem Statistischen Bundesamt eine derartige Zusammenführung nicht erfolgt ist.

Statistisches Landesamt und BWF rechtfertigen die Datenlieferung an das Statistische Bundesamt — einschließlich des nur für Zwecke der Verlaufsstatistik erforderlichen Identifikationsschlüssels — mit der Notwendigkeit, für eine evtl. im zu novellierenden Hochschulstatistikgesetz vorgesehene Verlaufsstatistik, die sowohl Studenten- als auch Prüfungsdaten umfassen könnte, Vorsorge zu treffen.

Diese Begründung kann ich nicht hinnehmen. Die langfristige Speicherung von Hilfs- (Identifikations-) und Erhebungsdaten stellt einen besonders gravierenden Eingriff in das informationelle Selbstbestimmungsrecht dar und ist nur auf Grundlage eines bereichsspezifischen verfassungskonformen Gesetzes zulässig. Da eine bereichsspezifische Regelung fehlt, muß die weitere Zulieferung von Daten für die Verlaufsstatistik unterbleiben, zumal die Einführung der Verlaufsstatistik eine Ausweitung der bisherigen Praxis darstellt und somit nicht auf einen "Übergangsbonus" bei der Umsetzung der Grundsätze des Volkszählungsurteils des Bundesverfassungsgerichts gestützt werden kann.

4.4 Archivwesen

Im Juni 1988 legte das Staatsarchiv den anderen Behörden den Entwurf eines hamburgischen Archivgesetzes zur Abstimmung vor. Damit ist es der von mir seit langem geforderten gesetzlichen Grundlage für die Archivnutzung einen großen Schritt näher gekommen. Ein Teil meiner Anregungen gegenüber dem Referentenentwurf (vgl. 6. TB, 4.5, S. 66) wurde berücksichtigt. Insgesamt begrüße ich deswegen den Entwurf als Versuch, das Grundrecht auf freie Forschung und Wissenschaft mit dem Recht von Betroffenen auf informationelle Selbstbestimmung in Einklang zu bringen. Der Entwurf orientiert sich an dem inzwischen verabschiedeten Bundesarchivgesetz und dem baden-württembergischen Archivgesetz. Folgende noch verbleibende Problempunkte habe ich in meiner Stellungnahme aufgegriffen:

— Anbietung von Unterlagen, die besonderen Geheimhaltungsvorschriften unterliegen —

Der Hamburger Gesetzentwurf normiert eine unbeschränkte Anbietungspflicht auch solcher Unterlagen, die besonderen Geheimhaltungsbestimmungen unterliegen. Das baden-württembergische Archivgesetz fordert in diesen Fällen dagegen bereits vor Übergabe an das Archiv "geeignete Maßnahmen" zur Berücksichtigung schützenswerter Belange des Betroffenen, z.T. eine Anonymisierung. Das Bundesarchivgesetz verpflichtet das Archiv, die Belange Betroffener in demselben Umfang zu berücksichtigen wie die abgebende Verwaltungsstelle. Die völlig unbeschränkte Anbietungspflicht des Hamburger Entwurfs ist insbesondere für die strafrechtlich geschützten Geheimnisse nach § 203 StGB datenschutzrechtlich nicht hinnehmbar. Ich habe deswegen zumindest eine dem Bundesarchivgesetz ähnliche Regelung gefordert.

— Anbietungspflicht trotz Aufbewahrungsvorschriften? —

Nach § 3 des Gesetzentwurfs sind "die Registraturbildner verpflichtet, alle Unterlagen, die sie zur Erfüllung ihrer Aufgaben nicht mehr benötigen, fortlaufend auszusondern, dem Staatsarchiv anzubieten und ihm nach Feststellung der Archivwürdigkeit abzuliefern". Die bisherige Behördenabstimmung über den Gesetzentwurf zeigt deutlich, daß die Frage, wann eine Behörde Unterlagen "zur Erfüllung ihrer Aufgaben nicht mehr benötigt", weiterer Klärung bedarf. Ist dieser Zeitpunkt erreicht, wenn ein bestimmtes Verwaltungsverfahren (rechtskräftig) abgeschlossen ist? Oder ist die Aufgabenerfüllung erst dann beendet, wenn auch alle erdenklichen weiteren Zwecke, z.B. die Abwicklung von Schadensersatzansprüchen gegenüber dem Staat, erledigt sind? Kön-

nen bloße Verwaltungsvorschriften über Aufbewahrungsfristen eine solche weitere Aufgabe begründen, oder gehen hier die gesetzlichen Vorschriften des § 15 HmbDSG (Sperrung, Löschung) bzw. des § 3 Archivgesetzentwurf (Anbietungspflicht) vor?

Ich meine, im Archivrecht kann das Kriterium "zur Erfüllung der Aufgaben nicht mehr benötigt" nicht anders verstanden werden als im Datenschutzrecht. Danach ist der konkrete Zweck der Datenerfassung und -speicherung ausschlaggebend. Ist dieser ursprüngliche Zweck erfüllt, dürfen die Daten nicht für andere zukünftige Zwecke, "auf Vorrat", aufbewahrt werden. Dies setzt sich auch gegenüber verwaltungsinternen Aufbewahrungsvorschriften durch: Nur für gesetzliche Aufbewahrungsfristen trifft das Hamburger Datenschutzgesetz — ebenso wie das Bundesdatenschutzgesetz — besondere Regelungen: § 13 Abs. 3 Nr. 3 HmbDSG geht ausdrücklich davon aus, daß selbst gesetzliche Aufbewahrungsvorschriften keine eigene "Aufbewahrungs-Aufgabe" der Verwaltungsstelle begründen, sondern immerhin zu einer Sperrung der nicht mehr für die unmittelbare Aufgabenerfüllung benötigten Daten führen. Rein verwaltungsinterne Aufbewahrungsfristen können nach dem HmbDSG eine Löschung dagegen nicht verhindern. Hier kommt allenfalls für eine Übergangszeit bis zum Erlaß in Vorbereitung befindlicher Gesetzesvorschriften eine analoge Behandlung, also eine Sperrung der Daten bzw. Unterlagen, in Betracht, wenn eine Löschung die Funktionsfähigkeit des betreffenden Verwaltungsbereichs gefährden würde.

Nach § 3 Abs. 2 Archivgesetzentwurf sind dem Staatsarchiv sowohl gesperrte (z.B. noch aufzubewahrende) als auch zu löschende Unterlagen anzubieten. Weder gesetzliche noch verwaltungsinterne Aufbewahrungsfristen können danach die Anbietungspflicht aussetzen und eine Übernahme durch das Staatsarchiv bzw. die anderenfalls gebotene Löschung nach § 3 Abs. 4 Archivgesetzentwurf ausschließen. Andererseits bestimmt § 3 Abs. 5 des Archivgesetzentwurfs jedoch: "Archivwürdige Unterlagen können (!) bereits vor Ablauf der durch Rechts- oder Verwaltungsvorschriften bestimmten Aufbewahrungsfristen vom Staatsarchiv übernommen werden". Als Regel geht der Gesetzentwurf mithin von der Aufbewahrung durch die Verwaltungsstelle — ohne Anbietungspflicht — aus. Dieser Regelungswiderspruch sollte nach meiner Auffassung wie folgt aufgelöst werden: Unterlagen, die allein wegen bestehender Rechtsvorschriften (nicht: Verwaltungsvorschriften) über Aufbewahrungsfristen gesperrt und nicht gelöscht werden, können, müssen aber nicht bis zum Ablauf der Frist dem Staatsarchiv angeboten werden. In diesem Fall erfolgt die Aufbewahrung im Staatsarchiv für die und im Auftrag der Verwaltungsstelle. Diese bleibt bis Fristablauf speichernde Stelle im Sinne des Datenschutzgesetzes mit allen sich daraus ergebenden Pflichten.

— "Personenbezogenes Archivgut" —

Anders als "normales" Archivgut unterliegt personenbezogenes Archivgut besonderen Schutzfristen, vor deren Ablauf eine Nutzung grundsätzlich nicht möglich ist. § 5 Abs. 3 Satz 3 des Archivgesetzentwurfs definiert "personenbezogenes Archivgut" als Archivgut, das personenbezogene Daten "enthält". Diese Begriffsbestimmung geht über die Formulierungen im Bundes- und im baden-württembergischen Archivgesetz hinaus. Dort wird ein "Bezug" des Archivguts auf natürliche Personen — "nach seiner Zweckbestimmung" (Baden-Württemberg) — gefordert. Zumindest dem Wortlaut nach dehnt der Hamburger Entwurf den Datenschutz damit auch auf Sachakten aus, die etwa Adressen von Empfängern und Absendern dienstlicher Korrespondenz "enthalten". Der Hinweis in der Gesetzesbegründung, das Recht des Betroffenen auf Auskunft und Einsicht bei personenbezogenen Daten finde seine Grenze "in dem zur Ermittlung der personenbezogenen Daten notwendigen unverhältnismäßigen Verwaltungsaufwand", läßt jedoch vermuten, daß der Datenschutz in der Praxis kaum weitergehen wird als bei Anwendung der Definitionen des Bundesarchivgesetzes oder des baden-württembergischen Archivgesetzes. Um Unsicherheiten zu vermeiden und eine gewisse Rechtseinheitlichkeit zu gewährleisten, habe ich angeregt, sich der Begriffsbestimmung des Bundesarchivgesetzes anzuschließen, also personenbezogenes Archivgut dann anzunehmen, wenn es sich auf natürliche Personen "bezieht".

— Rechte der Betroffenen —

Nach § 6 Abs. 2 des Hamburgischen Archivgesetzentwurfs hat der Betroffene lediglich einen Anspruch darauf, daß das Staatsarchiv dem Archivgut eine Gegendarstellung des Betroffenen hinzufügt, wenn er die Richtigkeit seiner personenbezogenen Angaben bestreitet und ein Gegendarstellungsinteresse glaubhaft macht. Es fehlt ein echter Berichtigungsanspruch. Ähnlich wie es das Bundesarchivgesetz und das baden-württembergische Archivgesetz vorsehen, habe ich eine Ergänzung des § 6 um folgende Formulierung vorgeschlagen: "Wird die Unrichtigkeit personenbezogener Angaben festgestellt, so ist dies zu berichtigen oder in den Unterlagen zu vermerken. Der Betroffene hat hierauf einen Anspruch."

Ferner habe ich mich gegen die Beschränkung der Auskunfts- und Gegendarstellungsrechte des Betroffenen auf Archivgut öffentlicher Hamburger Stellen gewandt. Mit der Übernahme des Archivgutes auch von Bundesbehörden und privaten "Registraturbildnern" ist das Staatsarchiv für alle Unterlagen speichernde Stelle im Sinne des Datenschutzgesetzes geworden und kann hinsichtlich der Betroffenenrechte nicht nach der Herkunft des Archivguts differenzieren.

4.5 Schulwesen

4.5.1 Berichte über Kinder in Vorschulklassen

In den Vorschulklassen der hamburgischen Grundschulen wird am Ende des Vorschuljahres vom Klassenleiter über jedes Kind ein Bericht angefertigt, der die Entwicklung des Kindes während des Besuches der Vorschule und den Entwicklungsstand nach Ablauf des Vorschuljahres darstellen soll. Der Bericht wird in den bei Schuleintritt anzulegenden Schülerbogen übernommen.

Grundlage der Berichte sind von den Klassenleitern während des Vorschuljahres zu führende "Beurteilungsbögen zur Feststellung der Lernausgangslage von Schulanfängern". Zu beantworten sind u.a. folgende Fragen:

1. Persönlichkeitsbereich

1.1. Kontaktfähigkeit: Ist das Kind aktiv im Kontakt? Knüpft es schnell und ungezwungen Beziehungen? Oder ist es eher passiv, scheu, gehemmt im Umgang mit anderen?

1.2. Emotionale Zuwendungsfähigkeit: Kann das Kind anderen spontan seine Gefühle, Sympathie, Zuneigung zeigen? Oder ist es eher ausdrucksgehemmt, gleichgültig, distanziert?

1.3. Soziales Einfühlungsvermögen: Kann das Kind Mitleid zeigen, andere trösten, sich für Schwächere einsetzen? Oder wirkt es gleichgültig gegenüber den Problemen anderer?

1.4. Verantwortungsbewußtsein: Zeigt das Kind Verantwortungsbewußtsein für andere? Behandelt es ihm anvertraute Dinge sorgfältig? Oder verhält es sich passiv, wenn andere Hilfe brauchen? Behandelt es ihm anvertraute Dinge nachlässig?

1.5. Konfliktverhalten: Trägt das Kind Konflikte physisch-aggressiv aus? Oder zeigt es andere Konfliktverhaltensweisen? (Wenn ja, welche?)

1.6. Kooperationsverhalten: Wie weit kann das Kind eigene Interessen für Gruppenziele zurückstellen, sich gruppenorientiert verhalten? Hält es sich an gemeinsam vereinbarte Regeln? Oder ist es stark egozentrisch, denkt nur an seine Interessen, schließt keine Kompromisse?

1.7. Selbstkontrolle: Ist das Kind in der Lage, Bedürfnisbefriedigung aufzuschieben? Oder bricht es z.B. Regeln, weil diese mit seinen momentanen Bedürfnissen kollidieren?

1.8. Gefühlsstabilität: Wirkt das Kind ausgeglichen, gefühlsstabil, belastbar? Oder wirkt es eher empfindlich, leicht frustriert, gefühlslabil?

1.9. Selbstsicherheit: Wirkt das Kind sicher und angstfrei, äußert es seine Wünsche? Oder wirkt es eher ängstlich, unsicher, sagt nicht, was es will?

1.10. Kritikfähigkeit: Kann das Kind Vorgegebenes in Frage stellen, fragt es nach den Gründen für Sachverhalte, oder nimmt es alles ungeprüft und kritiklos hin?

1.11. Selbständigkeit: Kann sich das Kind bei Problemen selbst helfen? Entwickelt es Initiative oder bleibt es ohne fremde Hilfe und Anregung passiv und hilflos?

1.12. Kreativität: Sind die Arbeiten und Problemlösungen des Kindes originell, einfallsreich? Oder verwendet es überwiegend stereotype, wenig differenzierte Klischees?

1.13. Weitere Erläuterungen zum Persönlichkeitsbereich.

Ähnlich detaillierte Fragen werden gestellt zur Motorik, Wahrnehmungsfähigkeit, Merkfähigkeit, Konzentration, sprachlichen Fähigkeit und zu den Interessen des Kindes.

In einem weiteren Feld können Verhaltensweisen, die nicht durch das vorgegebene Schema erfaßt werden, mit Angabe des Datums, an dem entsprechende Beobachtungen gemacht werden, notiert werden.

Eine Rechtsgrundlage für die Übernahme dieser Beurteilungen in die bei Beginn der Schulpflicht anzulegende Schülerakte gibt es nicht. Die gegenwärtige Praxis beruht auf den von der Behörde für Schule und Berufsbildung (BSB) im Jahre 1975 erlassenen "Richtlinien für die Erziehung in Vorschulklassen", die nicht die Qualität von Rechtsvorschriften haben. Ich halte das Berichtsverfahren deshalb schon aus "formalen" Gründen für rechtswidrig. Es bedarf im übrigen sicher keiner weiteren Erläuterung, daß diese Berichte geeignet sind, Schulanfängern einen unbelasteten Start erheblich zu erschweren. Hinzu kommt eine problematische Ungleichbehandlung gegenüber solchen Kindern, die keine Vorschule besuchen und für die lediglich das Ergebnis der "Schulreife-Untersuchung" in der Schülerakte vermerkt wird.

Inzwischen habe ich mit der BSB Gespräche darüber geführt, ob an der Erstellung und Übernahme der Berichte in die Schülerakten weiter festgehalten werden soll. Die Behörde hat ihre Überlegungen zwar noch nicht abgeschlossen, es zeichnet sich jedoch ab, daß die Berichte in der gegenwärtig praktizierten Form abgeschafft werden. Es wird erwogen, den Bericht durch folgendes Verfahren zu ersetzen: Die Lehrer erstellen einen individuell konzipierten Berichtstext, in dem lediglich deutlich werden muß, ob der Vorschüler nach dem Besuch der Vorschulklasse schulreif ist. Dieser Bericht wird in einer Ausfertigung den Eltern zugeleitet; eine weitere Ausfertigung wird zunächst zur Schülerakte genommen, nach einer kurzen Aufbewahrungsfrist aber vernichtet. Falls auf schriftliche Berichte ganz verzichtet werden wird, soll sichergestellt sein, daß die Leiter von Vorschulklassen bereits während des Schuljahres mit den Eltern der Vorschulkinder engen Kontakt halten und sie über den Entwicklungsstand informieren, wie dies schon bisher geschehen sollte. In jedem Fall soll in der Schülerakte vermerkt werden, ob das Kind am Ende des Besuches der Vorschulklasse schulreif ist.

4.5.2 Einsatz von Personalcomputern in der Schulverwaltung

Ich habe im Berichtsjahr in einem Gymnasium überprüft, ob beim Einsatz von Personalcomputern in der Schulverwaltung die gem. § 8 Abs. 1 HmbDSG zu treffenden Datensicherungsmaßnahmen ergriffen wurden.

In dem überprüften Gymnasium wird zur Erleichterung der Verwaltung der gymnasialen Oberstufe zur Erstellung von Stundenplänen, Klassen- und Kurslisten, zur Auflagenkontrolle und Berechnung von Bedingungen für Übergänge und Abschlüsse auf einem PC ein von der Schule käuflich erworbenes Programmpaket eines externen Softwareentwicklers eingesetzt. Das Programmpaket ist nicht durch die Behörde für

Schule und Berufsbildung oder eine andere zuständige Stelle geprüft und freigegeben worden, es gibt keine ordnungsgemäße Dokumentation, und es ist deshalb auch nicht ersichtlich, welche Rechts- und/oder Verwaltungsvorschriften jeweils in der aktuellen Version des Programmpakets berücksichtigt worden sind. Bei dem Verfahren handelt es sich um eine Anwendung mit verbindlicher Verarbeitungslogik, d.h. zur Erfüllung konkreter rechtlich umschriebener Aufgaben. Ein fehlerhaftes Funktionieren könnte gravierende Folgen, u.a. erhebliche Regreßansprüche nach sich ziehen (z.B. wegen fehlerhafter Entscheidungen aufgrund einer unrichtigen Auflagenkontrolle bzw. Errechnung von Durchschnittsnoten usw.).

Ich habe der BSB meine Auffassung mitgeteilt, daß die Ordnungsmäßigkeit der Datenverarbeitung bei dem geprüften Verfahren nicht gewährleistet ist. Ich habe zugleich angeregt, darauf zu dringen, daß der Softwarelieferant eine vollständige und einwandfreie Dokumentation abliefert und auch den Nachweis erbringt, daß die Software ordnungsgemäß funktioniert. Ich habe die BSB gebeten sicherzustellen, daß in den Schulen bei der Verarbeitung personenbezogener Daten nur technisch und fachlich einwandfreie Software zum Einsatz kommt.

Daraufhin hat die BSB mitgeteilt, die hier dargestellten Probleme im Zusammenhang mit gekaufter Software beträfen nicht Fragen des Datenschutzes und insbesondere der Datensicherung, sondern in erster Linie Fragen vertrags- und haftungsrechtlicher Art. Dem habe ich widersprochen:

Gem. § 16 Satz 2 Nr. 2 HmbDSG haben die Behörden dafür zu sorgen, daß die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme überwacht wird. Eine wirksame Überwachung setzt aber die Kenntnis der logischen Struktur und eine Offenlegung der Programmfunktionen voraus, kann also nur bei Vorliegen einer angemessenen Dokumentation erfolgen. Dies gilt sowohl für selbsterstellte als auch für käuflich erworbene Software.

Auch bei extern erworbener Software muß ein geordnetes Freigabeverfahren erfolgen, wobei auch die Erfüllung datenschutzrechtlicher Vorgaben geprüft werden muß. Es muß sichergestellt werden, daß

— die eingesetzten Programme geeignet sind, die Fachaufgabe zu erledigen (also richtige Ergebnisse liefern),

— sich die gespeicherten personenbezogenen Daten auf das erforderliche Maß beschränken und

— die erforderlichen Datensicherungsmaßnahmen getroffen werden.

Der von der BSB geäußerten Auffassung, ein solches geordnetes Test- und Freigabeverfahren sei bei gekaufter Software entbehrlich, da das richtige Funktionieren — mit echten Daten — stichprobenartig durch den Anwender geprüft werde, kann ich nicht folgen, zumal ich in der Schule keine Dokumentation dieser Prüfung vorgefunden habe.

4.6 Automation des Gewerberegisters

In meinem 6. Tätigkeitsbericht, S. 67 ff. führte ich aus, daß die gegenwärtig manuell geführten Gewerbekarteien der bezirklichen Wirtschafts- und Ordnungsämter (WI-Dienststellen) durch eine zentrale Datenbank mit On-line-Zugriff der zuständigen Sachbearbeiter ersetzt werden soll.

Vor allem hinsichtlich der Frage nach der notwendigen Rechtsgrundlage für dieses automatisierte Verfahren fanden weitere Erörterungen statt mit der Behörde für Wirtschaft, Verkehr und Landwirtschaft und den an dem Projekt beteiligten Stellen. In einem Schreiben vom 21. April 1988 habe ich allen Beteiligten einschließlich der regelmäßigen Empfänger der Gewerbeanzeigen meine Position noch einmal deutlich gemacht:

Die Gewerbeordnung legt nur den Zweck der Gewerbeanzeigen fest — nämlich die Gewerbeüberwachung —, regelt aber nicht die Nutzung des daraus entstandenen Registers, insbesondere die Übermittlung personenbezogener Daten an Dritte. Die Versendung von Durchschriften bzw. Ausdrucken der Gewerbeanzeigen an verschiedene Stellen sowie Auskünfte aus dem Register an private Dritte stellen selbständige Eingriffe in das informationelle Selbstbestimmungsrecht der Gewerbetreibenden dar und bedürfen nach dem Volkszählungsurteil des Bundesverfassungsgerichts einer eigenen gesetzlichen Grundlage. Darüber hinaus erfordert die regelmäßige Übermittlungsart eine spezielle Rechtsgrundlage, die auch eine Rechtsverordnung — mit entsprechender gesetzlicher Ermächtigung — sein kann.

Mit Schreiben vom 26. Mai 1988 erklärte sich die Wirtschaftsbehörde daraufhin bereit, "die Federführung für die vom Hamburgischen Datenschutzbeauftragten verlangte landesrechtliche Regelung dieser Übermittlungen zu übernehmen". Die Behörde für Arbeit, Jugend und Soziales meldete bereits ihren Bedarf an der Übermittlung der Gewerbeanzeigen für "Überwachungs- und Kontrollaufgaben im Bereich des sozialen, medizinischen und technischen Arbeitsschutzes sowie der technischen Überwachung" an. Von einem Gesetzentwurf der Wirtschaftsbehörde bzw. konkreten Vorbereitungen dazu habe ich bisher keine Kenntnis erhalten. Bis zum Erlaß einer gesetzlichen Grundlage ist eine regelmäßige Weiterleitung der Gewerbeanzeigen an die interessierten Stellen indessen nicht zulässig.

Unabhängig von der Rechtsgrundlage waren auch inhaltliche Problempunkte bei der Ausgestaltung des geplanten automatisierten Gewerberegisters zu erörtern. So z.B. der Umfang der Daten, den ein örtlich nicht zuständiger, aber von einem Dritten befragter Sachbearbeiter von der zentralen Datenbank abfragen darf, um die für die Auskunft zuständige Stelle herauszufinden. Ich stehe nach wie vor auf dem Standpunkt, daß nicht jeder Sachbearbeiter der 22 WI-Dienststellen auf alle gespeicherten Daten aller Hamburger Gewerbetreibenden Zugriff haben muß und darf (die WI-Dienststellen würden einen solchen allgemeinen Zugriff dagegen sehr begrüßen). Andererseits soll die bislang sehr umständliche Befragung nötigenfalls aller WI-Dienststellen durch die Automation gerade entscheidend vereinfacht und beschleunigt werden. Um dem befragten Sachbearbeiter die schnelle Benennung der örtlich zuständigen Stelle zu ermöglichen, habe ich dem Zugriff auf folgende Daten zugestimmt: Interne Gewerbenummer (Aktenzeichen); im Handels-, Genossenschafts- oder Vereinsregister eingetragener Name des Gewerbebetriebes, Familienname, Vorname, Geburtsjahr des Gewerbetreibenden; Anschrift der Betriebsstätte und die angemeldete Tätigkeit. Ob darüber hinaus auch nicht mehr aktuelle Daten als Suchmerkmale notwendig sind, ist noch nicht abschließend geklärt (z.B. für die Anfrage: "Herr A. hatte vor zehn Jahren einmal in Wandsbek einen Kfz-Handel betrieben, wo betreibt er heute welches Gewerbe?").

Insgesamt ist ein Großteil der Detailregelungen des Verfahrens noch nicht endgültig geklärt. Eine abschließende Stellungnahme kann ich erst abgeben, wenn mir alle Bildschirmmasken und die jeweils ausgelösten Verfahren schriftlich beschrieben vorliegen.

4.7 Umweltschutz

4.7.1 Veröffentlichung von Meßergebnissen aus der Überwachung von Gewerbebetrieben

Ein Bezirksamt bat mich um Stellungnahme zu der Frage, ob und ggf. in welchem Umfang eine nach § 52 Bundes-Immissionsschutzgesetz (BImSchG) tätige Überwachungsbehörde Ergebnisse aus Luft- und Lebensmittelmessungen veröffentlichen darf. Das Bezirksamt war aufgefordert worden, die Ergebnisse von Messungen des Gehalts an Lösungsmitteln (PER) in der Abluft von Chemischen Reinigungen und der Schadstoffkonzentration in Wohnungen, Geschäften und Lebensmitteln in unmittelbarer Nähe von Chemischen Reinigungen zu veröffentlichen, und zwar in einer Form, die es dem Publikum erlauben sollte, aus den Meßergebnissen Konsequenzen u.a. beim Einkaufsverhalten zu ziehen. Die Veröffentlichung sollte also unter Angabe der jeweiligen Chemischen Reinigung, benachbarter Geschäfte usw. erfolgen.

Da leider noch keine bereichsspezifische Regelung für das Auskunftsrecht über Umweltdaten erlassen wurde (s. dazu 6. TB, 4.7 — Einsichtsrecht in Umweltakten) und auch das BImSchG keine spezielle Vorschrift zu der anstehenden Frage enthält, mußte zur Beurteilung auf die Generalklausel des § 30 Verwaltungsverfahrensgesetz (VwVerfG) zurückgegriffen werden. (Das Hamburgische Datenschutzgesetz ist in diesem Fall nicht anwendbar, weil es sich bei den zu veröffentlichenden Daten durchweg nicht um Daten einer natürlichen Person, sondern um Firmendaten handelt und weil die Daten in Listen und Akten, nicht in Dateien verarbeitet wurden.) § 30 VwVerfG gewährt den an einem Verwaltungsverfahren Beteiligten einen Anspruch darauf, daß ihre Geheimnisse, insbesondere die zum persönlichen Lebensbereich gehörenden Geheimnisse sowie die Betriebs- und Geschäftsgeheimnisse, von der Behörde nicht unbefugt offenbart werden. Regelungszweck des § 30 VwVerfG ist es, die an einem Verwaltungsverfahren Beteiligten davor zu schützen, daß Tatsachen, an deren Geheimhaltung die Beteiligten ein Interesse haben, durch die Behörde nicht unbefugt offenbart werden. Weder kommt es darauf an, ob die Beteiligten natürliche oder juristische Personen sind; noch kommt es auf die Art der Geheimnisse an, also darauf, ob es sich um personenbezogene Daten ("zum persönlichen Lebensbereich gehörende Geheimnisse") oder um Betriebs- oder Geschäftsgeheimnisse handelt. Maßgebend ist, ob die Beteiligten ein legitimes Interesse an der Geheimhaltung der betreffenden Daten bekunden bzw. ob — falls die Beteiligten sich nicht geäußert haben — ein vernünftiger Betrachter ein solches Interesse annehmen würde und daß betreffende Daten nicht schon offenkundig sind.

§ 30 VwVerfG verbietet die Offenbarung von Geheimnissen jedoch nicht ausnahmslos, sondern nur dann, wenn sie unbefugt ist.

"Unbefugt" ist ein unbestimmter Rechtsbegriff, der der vollen Nachprüfung durch die Verwaltungsgerichte unterliegt. Eine Befugnis kann sich ergeben aus gesetzlichen Mitteilungspflichten, aus der Einwilligung der Betroffenen, aber auch aus einer Güterabwägung, wonach das Geheimhaltungsinteresse hinter noch wichtigeren anderen Interessen zurücktreten muß. Dies ist insbesondere dann der Fall, wenn im Einzelfall die Offenbarung zur Aufgabe der Behörde gehört, um z.B. vor schädlichen Nebenwirkungen von Arzneien, Lebensmitteln etc. zu warnen. Allerdings ist bei der Güterabwägung ein strenger Maßstab anzulegen. Konfliktsfälle werden sich insbesondere dort ergeben, wo der Geheimhaltungsanspruch des Beteiligten gegenüber der Behörde dem Informationsanspruch der Öffentlichkeit und insbesondere dem nach den Pressegesetzen der Länder eingeräumten Informationsanspruch der Presse gegenübertritt. Zur Frage, ob höherrangige Rechtsgüter eine Offenbarung erfordern oder zulassen, kann auch die Rechtsprechung der Strafgerichte zu §§ 203 und 300 StGB herangezogen werden. Eine absolute Schranke für die Offenbarung von Geheimnissen im weitesten Sinne stellt — zumindest soweit sie ohne Einwilligung des Betroffenen erfolgen würde — in jedem Falle der vom Grundgesetz gewährte unantastbare Bereich privater Lebensgestaltung dar.

Nach Abwägung des Geheimhaltungsinteresses der Beteiligten gegenüber dem Informationsinteresse Dritter bin ich zu dem Ergebnis gekommen, daß die Offenbarung der Meßdaten aus höherrangigem Interesse der Allgemeinheit (1) und aus höherrangigem Interesse einzelner Bürger (2) befugt sein kann.

(1) Das Interesse der Allgemeinheit an den Meßdaten — Aufklärung über die Gefahren durch Selbstbedienungsreinigungen — dürfte insoweit gegenüber den schutzwürdigen Belangen der Beteiligten überwiegen, als es darum geht, über

— die Eigenschaften von PER (Fähigkeit, Mauern zu durchdringen, Anreicherung in fetthaltigen Nahrungsmitteln, gesundheitliche Gefahren usw.),

— die generelle Problematik des PER-Einsatzes in Chemischen Reinigungen,

— die im Bezirk festgestellte Zahl von Reinigungen mit erhöhten PER-Werten,

— die in den Reinigungen gemessenen Werte ohne Angabe der zugehörigen Reinigungen,

— die Meßergebnisse in der Umgebung von (namentlich nicht genannten) Reinigungen, in Lebensmitteln, die Art der Lebensmittel ohne Angabe der Geschäfte, aus denen die Lebensmittel stammten,

— die Zahl belasteter Wohnungen und Meßwerte aus Wohnungen ohne Angabe der Lage der Wohnungen

— und weitere Daten in dieser nicht personen- oder firmenbezogenen Art

zu informieren. Zu einer solchen Veröffentlichung gehört selbstverständlich auch, daß die Behörde die Bevölkerung über die Maßnahmen unterrichtet, die sie zur Abwendung der Gefahr getroffen hat (wie z.B. Schaffung rechtlich zulässiger Betriebsbedingungen, Verkaufsverbot für gesundheitsgefährlich belastete Lebensmittel, Schließung von Anlagen usw.). Eine solche Veröffentlichung wäre zwar ein Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen. Dieser Eingriff wäre aber verhältnismäßig, weil die schutzwürdigen Belange der Betroffenen und das berechtigte Interesse der Allgemeinheit unter Einsatz des die Betroffenen am wenigsten belastenden Mittels zu einem angemessenen Ausgleich gebracht würden. Mit einer bloßen "Schadensmeldung" würde die noch bestehende Gefahr als schwerer dargestellt als sie (hoffentlich) tatsächlich — nämlich nach Herstellen eines gesetzmäßigen Zustandes — noch ist. Der Eingriff wäre für die Betroffenen nicht mehr verhältnismäßig, wenn die Bürger durch die Veröffentlichung bloß der hohen PER-Belastungen im Zeitpunkt der Messungen veranlaßt würden, aus Angst vor Schäden vorsichtshalber in Geschäften in der Umgebung von Chemischen Reinigungen gar nicht mehr zu kaufen oder Wohnungen in der Nähe von Reinigungen nicht mehr zu mieten.

Das Interesse der Allgemeinheit mag zwar auch darauf gerichtet sein zu erfahren, welche Reinigungen für bestimmte Belastungen verantwortlich sind, in welchen Geschäften besonders hohe PER-Verunreinigungen in Lebensmitteln festgestellt worden sind usw. Insoweit ist das Interesse der Allgemeinheit jedoch nicht gewichtiger als das Interesse der Beteiligten an der Geheimhaltung, jedenfalls solange nicht, wie die Verwaltung ihrer Überwachungsaufgabe, die dem Schutz der Bevölkerung vor den mit dem Betrieb der chemischen Anlagen verbundenen Gefahren dient, ordnungsgemäß nachkommt. Kommt die Überwachungsbehörde ihren Verpflichtungen jedoch nicht nach, ist also der Schutz vor gesetzlich unzulässigen gesundheitlichen Beeinträchtigungen nicht gewährleistet, weil die Überwachungsbehörde ungesetzliche Zustände beim Betrieb Chemischer Reinigungen nicht abstellt, so könnte es zu einer anderen Beurteilung kommen. Diese hier für den PER-Fall geltenden Überlegungen sind keineswegs neu. Die Gesetzesinitiative Hamburgs mit dem Entwurf eines Gesetzes über den Auskunftsanspruch des Bürgers über Umweltdaten (SDrs. Nr. 222 v. 31.3.1987) beruht auf diesen Überlegungen ebenso wie der Gesetzesentwurf der GRÜNEN (BTDrs. 11/1152 vom 11.11.1987) für ein Akteneinsichtsrecht in Umweltakten.

(2) Das berechtigte Interesse einzelner Personen kann noch weiter gehen als das der Allgemeinheit. Den Personen, die unmittelbar und persönlich den gesundheitsgefährlichen Wirkungen von PER aus Chemischen Reinigungen ausgesetzt sind oder waren, also z.B. Arbeitnehmern in den Reinigungen, Bewohnern der Wohnungen in der Nachbarschaft, Geschäftsinhabern und Angestellten in benachbarten Läden, Kunden der Reinigungen und umliegenden Geschäfte, darf genaue Auskunft über die sie betreffenden Meßwerte und den Verursacher nicht vorenthalten werden. Soweit diese Personen selbst Beteiligte im Sinne von § 13 VwVerfG sind, haben sie aufgrund von § 29 VwVerfG einen (Rechts-) Anspruch auf Offenbarung durch Akteneinsicht. Aber auch wenn sie nicht Beteiligte in den Verwaltungsverfahren gegen eine bestimmte Reinigung sind und deshalb keinen auf einer speziellen Gesetzesnorm beruhenden Anspruch auf Offenbarung haben, ist die Verwaltung gehalten zu prüfen, ob nicht ihnen gegenüber gleichwohl eine Offenbarungsbefugnis besteht. Im Rahmen dieser Prüfung muß berücksichtigt werden, daß das Anliegen persönlich und physisch betroffener Auskunftssuchender auf dem grundgesetzlich geschützten Recht auf Leben, Gesundheit und körperliche Unversehrtheit beruht, dem gegenüber der Anspruch auf Schutz des eingerichteten Gewerbebetriebes zurücktreten muß. Wenn nicht gesundheitliche Belange, son-

dern Schadensersatzansprüche — etwa der Vermieter für Mietverluste oder der Lebensmittelhändler für unverkäuflich gewordene Ware — als berechtigtes Interesse von Auskunftsbegehrenden geltend gemacht werden, sind Auskunftsinteresse der Geschädigten und Geheimhaltungsinteresse der Betroffenen grundsätzlich als gleichrangig zu bewerten. Soweit die Offenbarung von Meßergebnissen allerdings notwendig ist, um die Erfolgsaussicht eines Prozesses abschätzen zu können, halte ich die Offenbarung aber auch für befugt.

Nach allem bleibt festzustellen:

Eine allgemeine Veröffentlichung der Meßergebnisse in firmen- oder personenbezogener Form ist mit § 30 VwVerfG nicht in Einklang zu bringen, wohl aber eine solche ohne Namens- und Adressenangabe sowie eine einzelfallbezogene, auf die jeweils verursachende Reinigung und den direkt betroffenen Personenkreis beschränkte zweckgebundene Offenbarung auf Antrag.

4.7.2 Erlaß von Regelungen zur Durchführung des Datenschutzes im Bereich der Gesundheits- und Umweltämter

Der unter 4.7.1 geschilderte "PER-Fall", zu dem ich mehrere Anfragen aus verschiedenen Bereichen des öffentlichen Lebens erhielt, veranlaßte mich im Sommer 1988, die Umweltbehörde und das Senatsamt für Bezirksangelegenheiten über meine Stellungnahme zu informieren. Gleichzeitig bat ich um Mitteilung der dortigen Auffassung zu der Frage, wer für den Erlaß von Regelungen zur Durchführung des Datenschutzes im Bereich der Gesundheits- und Umweltämter zuständig sei. Ein Bedarf für solche Regelungen (einschließlich von Weisungen zur Behandlung von Auskunftsersuchen) ist m.E. offenkundig. In anderen datenschutzrelevanten Bereichen liegen solche Regelungen inzwischen auch vor, so z.B. für den Bereich Soziales, Jugend, Wohngeld (DV der Behörde für Arbeit, Jugend und Soziales 050.30-5-2 "Schutz der Sozialdaten gem. § 35 SGB I und §§ 67 — 78 SGB X").

Das Senatsamt für Bezirksangelegenheiten hält sich für unzuständig, weil der Erlaß von Regelungen zum Datenschutz zum Bereich der Fachaufsicht und nicht zum Bereich der Bezirksaufsicht gehöre. Die Umweltbehörde hat sich noch nicht schriftlich geäußert. Aus meiner Sicht ist die Zuständigkeitsfrage zweitrangig. Wichtig erscheint mir, daß überhaupt Regelungen für die Durchsetzung des Datenschutzes in den Gesundheits- und Umweltämtern erlassen werden. Eine "allgemeine Auskunftssperre" zu praktizieren aus Furcht vor Verstößen gegen Datenschutzbestimmungen, ist keine angemessene Lösung für das Problem, das sich aus dem Spannungsverhältnis zwischen Geheimhaltungsinteresse und Auskunftsinteresse ergibt.

4.8 Bauwesen

4.8.1 Wohnraumdatei

An der automatisierten Wohnraumdatei habe ich seit ihrem Bestehen Kritik geübt (1. TB Nr. 6.4, 2. TB Nr. 3.6, 3. TB Nr. 3.4.2, 4. TB Nr. 4.5.2, 5. TB Nr. 5.5.3). Mittlerweile halte ich den Zeitpunkt für gekommen, daß die Baubehörde das Provisorium, welches durch die Option auf die Einführung der Fehlbelegungsabgabe in Hamburg entstanden ist, beendet und für die Wohnraumdatei ein Verfahren und einen Datenbestand schafft, der ausschließlich der Aufgabenerfüllung nach dem Wohnungsbindungsgesetz (WoBindG) dient. Das Verfahren Wohnraumdatei läßt sich in der gegenwärtigen Form m.E. nicht länger vertreten.

Im Jahre 1986 hatte sich die Baubehörde endlich bereitgefunden einzuräumen, daß ihre Auffassung zur Wohnraumdatei nicht haltbar war. Da danach feststand, daß die Wohnraumdatei nur auf der Grundlage des WoBindG und nur mit dem zur Aufgabenerfüllung nach diesem Gesetz erforderlichen Datenumfang rechtlich zulässig ist, hatte ich die Baubehörde gebeten, a) die Löschung unzulässig gespeicherter Daten sowie b) — in angemessener Zeit — die Bereinigung des Verfahrens vorzunehmen.

a) Löschung unzulässig gespeicherter Daten

Im Juni 1987 teilte mir die Baubehörde auf Anfrage mit, inzwischen seien im Datenbestand alle Angaben in den Feldern "Anzahl der Familienangehörigen", "Staatsangehörigkeit" und "Geschlecht" (zur Auswahl der passenden Anrede Herr/Frau) gelöscht und die betreffenden Felder gesperrt. Im Feld "Geburtsdatum" seien die Angaben zu Geburtstag und -monat gelöscht, und in Zukunft würden diese Teile des Feldes "Geburtsdatum" mit den fiktiven Angaben "01.01" gespeichert.

Zur Überprüfung ließ ich mir die ersten zweihundert Datensätze aus der Wohnraumdatei ausdrucken. Ich habe festgestellt, daß in zwanzig Fällen in den Feldern, die für die Speicherung des Namens eines Untermieters vorgesehen sind, Namen enthalten waren, obwohl es sich bei den betreffenden Personen offenbar nicht um Untermieter handelte, denn in dem Feld "untervermietete Fläche" waren Nullen gespeichert. Den Vornamen war jeweils ein "P." vorangestellt. Ich hatte Zweifel an der Rechtmäßigkeit und der Plausibilität dieser Datenspeicherung (1). Weiter stellte ich drei Fälle (mit der "Änderungsart 10") fest, in denen noch das volle Geburtsdatum (mit Tag und Monat) der gespeicherten Personen erhalten war, während nähere Angaben zur Wohnung fehlten; es war nur die Straße und die Hausnummer vorhanden (2).

(1) Die Baubehörde hat auf mehrfache Nachfrage endlich im Juni 1988 mitgeteilt, bei den in den Untermieterfeldern unter Voranstellung des "P." gespeicherten Personen handele es sich nicht um Untermieter, sondern um Personen, die — nach einer in Hamburg üblichen Praxis — die Wohnung zusammen mit einer anderen unter Vorlage einer gemeinsamen § 5-Bescheinigung bezogen hätten und die daher selbst als Inhaber dieser Bescheinigung angesehen würden ("Partnerverhältnisse"). Diese Personen seien Berechtigte im Sinne des WoBindG. Im Falle eines Auszugs der anderen (als Hauptmieter gespeicherten) Person blieben diese Personen wohnberechtigt, obwohl sie nicht "haushaltszugehörige Familienangehörige" der ausgezogenen Person seien.

Nach dieser Erläuterung habe ich meine Bedenken gegen die Speicherung für die Zukunft zwar nicht aufrecht erhalten (s. dazu weiter unten). Für die Vergangenheit habe ich diese Speicherung jedoch gerügt. Die Baubehörde hat als fachlich zuständige Stelle für die automatisierte Wohnraumdatei nämlich eine Signieranweisung (DV) herausgegeben, nach der die Anwender (Einwohnerämter der Bezirke) zu verfahren haben. Die Signieranweisung, in der die Signierung von "Partnerverhältnissen" nicht vorgesehen ist, ist ein Teil der Verfahrensdokumentation, sie ist für die Anwender verbindlich. Zur ordnungsgemäßen Anwendung des Verfahrens Wohnraumdatei gehört die strikte Einhaltung der Signieranweisung durch die Anwender. Wenn die Anwender eigenmächtig Partnerschaftsverhältnisse in das Verfahren eingegeben haben, so stellt dies einen Verstoß gegen die Ordnungsmäßigkeit der Anwendung von Programmen, die zur Verarbeitung personenbezogener Daten eingesetzt werden, dar.

Um die zukünftige Nutzung der Felder, die eigentlich nur für Untermietverhältnisse vorgesehen waren, für Zwecke der Partnermietverhältnisse einwandfrei zu gestalten, forderte ich die Baubehörde auf, die Signieranweisung entsprechend zu ergänzen. Ggf. müßten die Einwohnerämter prüfen, ob ihre Signierungen zu den betreffenden Feldern, die sie in der Vergangenheit vorgenommen hätten, der neuen Signieranweisung entsprächen. Erforderlichenfalls müßten Signierungen berichtigt werden. Da die bisherige Behandlung dieser Fälle nicht ordnungsgemäß gewesen sei, müßten die erforderlichen Arbeiten unverzüglich eingeleitet werden.

Gleichzeitig wies ich nochmals darauf hin, daß Untermietverhältnisse in der Wohnraumdatei nur gespeichert sein/werden dürfen, wenn die untermietweise bewohnte Fläche mehr als die Hälfte der gesamten Wohnfläche beträgt. Wenn ein Untermieter signiert wird, muß auch im Feld "untervermietete Fläche" eine Signierung erfolgen, wobei der Wert in diesem Feld mehr als die Hälfte der Gesamtwohnfläche betragen muß.

Im November 1988 übersandte die Baubehörde mir einen Ausschnitt aus der geänderten Signieranweisung, die meinen Forderungen zur transparenten Signierung von Partnerverhältnissen Rechnung tragen sollte. Dem geänderten Text konnte ich jedoch nicht zustimmen, weil zum einen auf eine unzutreffende Rechtsgrundlage (AFWoG) für die Speicherung verwiesen wurde und zum anderen nach der Anweisung auch solche Untermietverhältnisse signiert werden sollten, bei denen weniger als die Hälfte der Wohnung untermietweise bewohnt wird.

Schließlich räumte auch die Baubehörde ein, daß die Speicherung von Untermietverhältnissen nur zulässig sei, wenn die untervermietete Fläche mehr als die Hälfte der Wohnfläche betrage. Sie habe die Einwohneramtsleiter auf einer Sitzung darauf hingewiesen, und die Richtigstellung der Signieranweisung sei veranlaßt. Ich habe Zweifel, daß im Datenbestand nur solche Untermietverhältnisse gespeichert sind, weil in der Signieranweisung bis jetzt etwas anderes stand. Wenn sich die Sachbearbeiter in den Wohnungsämtern nach der jahrelang geltenden Fassung der Signieranweisung gerichtet haben, ist die Vermutung geradezu zwingend, daß auch Untermietverhältnisse gespeichert sind, für die das WoBindG als Rechtsgrundlage nicht greift.

(2) Bei den oben erwähnten Fällen mit der "Änderungsart 10" handelte es sich um Fälle, die beim Aufbau der automatisierten Wohnraumdatei aus einem Datenbestand des Einwohnerwesens in den Datenbestand gelangt waren und seitdem nicht wieder "angestoßen" worden waren. Außer dem Namen des Mieters, seinem Geburtstag und der Anschrift (Straße, Hausnr.) waren keine weiteren Dateneingaben zu dem Fall erfolgt. Dies deutete darauf hin, daß die betreffende Wohnung der Wohnungsbindung nicht unterliegt und deshalb die Nacherfassung der Wohnungsdaten unterblieben ist, die sonst vom Wohnungssachbearbeiter anhand der die Wohnung betreffenden Karteikarte aus der alten manuellen Wohnraumkartei hätte vorgenommen werden müssen.

Bei diesen Fällen handelte es sich also um die Speicherung von Personen, auf die das WoBindG nicht anzuwenden ist, weil die von ihnen gemietete Wohnung nicht dem WoBindG unterliegt. Ich habe die unzulässige Speicherung im April 1988 ausdrücklich gerügt und die Löschung aller Fälle dieser Art in dem gesamten Datenbestand verlangt. Auf diese Weise kam es zur Löschung von 1509 Fällen.

b) Bereinigung des Verfahrens

Bei meinen Bemühungen um eine Bereinigung der Wohnraumdatei bin ich auf so viele Unzulänglichkeiten, Fehler und unzulässige Datenspeicherungen gestoßen, daß ich dringend davor warnen muß, das Verfahren in dieser Form weiter zu betreiben. Die konzeptionellen Mängel des Verfahrens halte ich für so gravierend, daß es nicht als ordnungsmäßig bezeichnet werden kann. Hinzu kommen Mängel im Bereich der Verfahrensanwendung, die der DV-Revisor des Senatsamtes für den Verwaltungsdienst bei seiner organisatorisch-technischen Prüfung im August 1988 festgestellt hat. Die gravierenden konzeptionellen Mängel des Verfahrens sehe ich in folgendem:

(1) Der Datensatz der Wohnraumdatei ist überfrachtet mit Datenfeldern, die nur dann erforderlich gewesen wären, wenn die Datei zur Erhebung der Fehlbelegungsabgabe genutzt worden wäre.

(2) Der Vordruck "Bestandsblatt" ist ebenfalls mit den nicht benötigten Feldern für die Fehlbelegungsabgabe belastet.

(3) Die Signieranweisung nebst einer Reihe von Anlagen ist völlig auf die Nutzung des Verfahrens für die Fehlbelegungsabgabe ausgerichtet. Eine Reduzierung der Signieranweisung auf den für die Wohnraumdatei erforderlichen Umfang ist bis heute unterblieben. Selbst wenn Anweisungen aktuell geändert werden müssen, wird so getan, als diene das Verfahren der Erhebung der Fehlbelegungsabgabe, denn es wird z.B. unterlassen, Hinweise auf eine unzutreffende Rechtsgrundlage zu eliminieren.

(4) Die ursprünglich auf die Fehlbelegungsabgabe ausgerichteten Programme sind für die Pflege der Wohnraumdatei unzweckmäßig. Wichtige automatisierte Kontrollen zur Gewährleistung formal und sachlich richtiger Dateneingaben fehlen. Diese Kontrollen waren in den Programmen für die Fehlbelegungsabgabe geplant, zu deren Erstellung es wegen der Entscheidung des Senats vom Oktober 1984 nicht mehr gekommen ist. Deshalb konnte es zu der nicht vorgesehenen, zweckfremden Nutzung der Untermietfelder kommen, ohne daß die fachlich verantwortliche Baubehörde oder die programmierende Stelle davon wußten. Bei einem systematisch geplanten und programmierten Verfahren Wohnraumdatei wäre so etwas nicht möglich gewesen, weil eine programmierte Kombinationskontrolle der relevanten Felder zu einem Fehler geführt hätte. Der Fehler hätte darin bestanden, daß bei einem Untermietverhältnis auch im Feld "untervermietete Fläche" ein Eintrag erfolgen müßte, was bei den Partnerverhältnissen nicht geschehen ist.

(5) Die einerseits unvollständigen, andererseits aber mit nicht erforderlichen Routinen belasteten Programme sind immer schwieriger zu pflegen. Hinzu kommt, daß das Statistische Landesamt die Pflege des Straßenbandes eingestellt hat, weil dieses durch die digitalisierte Stadtgrundkarte ersetzt wird. Der Aufwand für die Programmpflege steht nicht mehr in einem angemessenen Verhältnis zum Nutzen der Wohnraumdatei (s. dazu unten (7)).

(6) Beim Aufbau der Wohnraumdatei wurden im Hinblick auf die geplante Erhebung der Fehlbelegungsabgabe ab 1.1.1984, also im Hinblick auf den vermeintlichen Zeitdruck, Mängel des Datenmaterials in Kauf genommen, die aus heutiger Sicht nicht mehr vertretbar erscheinen. Zum Aufbau der Datei wurden Datenbestände benutzt, die bekanntermaßen Fälle enthielten, die nicht unter das Wohnungsbindungsgesetz fielen (und fallen). So waren in dem Datenbestand, der vom Einwohnerwesen zur Verfügung gestellt wurde, auch Wohnungen enthalten, die nicht unter das WoBindG fielen und die deshalb in der Wohnraumdatei nicht hätten gespeichert werden dürfen. Der Einwohnerdatenbestand weist nämlich (nur) Anschriften nach, unter denen sich Wohnungen befinden, die als öffentlich gefördert gelten.

Aus dem Kenntnis- und Planungsstand von 1983/84 schien die Tatsache der Übernahme fehlerhafter Fälle hinnehmbar, weil davon ausgegangen werden konnte, daß die Erhebungsaktion für die Fehlbelegungsabgabe (d.h. das Aufforderungsschreiben an alle in der Datei gespeicherten potentiellen "Fehlbeleger" und deren Erklärungen) zügig zu einer Berichtigung fehlerhafter Angaben und Bereinigung des Bestandes von nicht zu speichernden Fällen und damit zu einem einwandfreien Datenbestand führen würde. Seit Oktober 1984 steht aber fest, daß keine Rückkopplung mit den betroffenen Bürgern erfolgen wird, so daß es nicht "automatisch" zu einer Bereinigung des Datenbestandes kommt. Trotzdem hat die Baubehörde als fachlich verantwortliche Stelle von sich aus nichts unternommen, um den Wohnraumdatenbestand durch gezielte Maßnahmen zu berichtigen und zu bereinigen. Dies ist ein Verstoß gegen § 15 Abs. 1 HmbDSG (Pflicht zur Berichtigung von Amts wegen) und gegen § 15 Abs. 3 HmbDSG (Pflicht zur Löschung unzulässig gespeicherter oder nicht mehr erforderlicher Daten).

(7) Zur Notwendigkeit einer automatisierten Wohnraumdatei anstelle der manuellen Wohnraumkarteien in den Einwohnerämtern führte die Baubehörde in der Senatsdrucksache Nr. 1228 — verteilt am 6.12.1983 — folgendes aus:

"... Diese Arbeiten wurden begonnen, weil die manuell geführte Wohnraumkartei nach dem bisherigen Verfahren nicht auf dem jeweils neuesten Stand zu halten ist. ... Im Zuge der bisher durchgeführten Arbeiten ist deutlich geworden, daß die manuell geführte Kartei in erheblichem Umfang fehlerhafte Angaben enthielt. Nur eine fehlerfreie Fortschreibung entspricht den gesetzlichen Anforderungen, die das Wohnungsbindungsgesetz an die Wohnraumkartei stellt. Zudem erlaubt eine automatisierte Wohnraumkartei mit ihrem hohen Aktualitätsgrad vielfältige statistische Bestandsauswertungen. ... Nach erfolgter Umstellung wäre auch die genaue Anzahl der noch in der gesetzlichen Bindung befindlichen Sozialwohnungen ermittelt. ..."

Richtig ist die Aussage, nur eine fehlerfreie Fortschreibung der Wohnraumdatei entspreche den gesetzlichen Anforderungen. Daraus folgt, wenn man diesen Gedanken konsequent zu Ende denkt: Da die fehlerfreie Fortschreibung der Wohnraumdatei nicht gelungen ist, verstößt ihre Weiterführung gegen gesetzliche Bestimmungen.

Wenn in der Datei — zumindest bis vor wenigen Wochen — noch Wohnungen nachgewiesen wurden, die nicht dem WoBindG unterliegen, so können auch die Ziele "hoher Aktualitätsgrad" und "Feststellung der genauen Anzahl noch der Bindung unterliegender Wohnungen" nicht als erreicht angesehen werden. Gegenüber der manuellen Kartei hat die automatisierte Datei allerdings den Vorzug, daß sie für Auswertungen leicht genutzt werden kann. Dieser Vorteil ist aber keine Rechtfertigung für unzulässige Datenspeicherungen.

Die Baubehörde wendet sich gegen diese Beurteilung mit dem Einwand, die Entscheidung über die Einführung der Fehlbelegungsabgabe in Hamburg sei immer noch in der Schwebe. Wenn auch das Verfahren zugegebenermaßen überfrachtet sei und hinsichtlich des Hauptanteils, nämlich des Teils zur Erhebung der Fehlbelegungsabgabe, z.Z. nicht praktiziert werde, so verstoße dies doch nicht gegen Datenschutzbestimmungen, weil der praktizierte Teil des Verfahrens auf der Grundlage des WoBindG zulässig sei. Die Programme seien keinesfalls für Zwecke der Wohnraumdatei unbrauchbar, die Kontrollmechanismen seien ausreichend, die Datei habe einen hohen wohnungspolitischen Wert, der den Pflegeaufwand rechtfertige. Die Zusammenarbeit zwischen Baubehörde, Wohnungsbaukreditanstalt, Einwohnerzentralamt und Bezirken gewährleiste einen hohen Aktualisierungsgrad sowie die notwendige Bereinigung. Zur Bekräftigung verweist die Baubehörde dann auf die 1.509 Fälle, die kürzlich gelöscht worden sind.

Das ist nun allerdings ein ungeeignetes Argument, denn diese Fälle sind ja gerade trotz der angeblichen Aktualität und funktionierenden Kontrollmechanismen jahrelang im Bestand gespeichert gewesen. Es war nicht die Baubehörde und es waren nicht die "geeigneten Kontrollmechanismen", die zur Löschung führten, sondern meine Prüfung einer kleinen Stichprobe des Bestandes.

Deshalb kann ich auch der Behauptung der Baubehörde, sie komme den Verpflichtungen zur Berichtigung und Löschung aus § 15 Abs. 1 und 3 HmbDSG laufend nach, nicht uneingeschränkt zustimmen. Zwar werden Veränderungen bei den Mietern und den Wohnungen durch den Veränderungsdienst aus dem Einwohnerverfahren an die Bezirke übermittelt, und es mag auch so sein — was ich noch nicht geprüft habe —, daß die notwendigen Veränderungssignierungen von den Wohnungssachbearbeitern in das Verfahren Wohnraumdatei eingegeben werden. Gleichwohl haben meine Kontrollen des Datenbestandes unrichtige bzw. unzulässige Datenspeicherungen offenbart.

Deshalb halte ich daran fest, daß die fehlerfreie Fortschreibung der Wohnraumdatei nicht gelungen ist und aufgrund des für eine andere Verwaltungsaufgabe (Erhebung der Fehlbelegungsabgabe) konzipierten Verfahrens auch in Zukunft nicht gewährleistet werden kann.

Auch das Argument der Baubehörde, das Verfahren müsse — weil die Fehlbelegungsabgabe vielleicht irgendwann einmal doch noch eingeführt werde — schon aus ökonomischen Erwägungen wegen des Umfangs der bereits geleisteten Arbeiten erhalten bleiben, kann nicht überzeugen. Die Programmteile, die speziell für die Berechnung und Erhebung der Fehlbelegungsabgabe konzipiert sind, sind vor Jahren in unfertigem Zustand "stillgelegt" worden. Sie sind bei notwendigen Verfahrenspflegemaßnahmen nicht angepaßt worden. Ob die Fehlbelegungsabgabe, wenn sie denn einmal kommt, in derselben Weise berechnet wird, wie es seinerzeit zur Grundlage für die Programmierung gemacht wurde, ist äußerst fraglich. Für fraglich halte ich vor allem, ob die Entscheidung noch rechtzeitig vor dem Auslaufen der Bindungen getroffen wird.

4.8.2 Befragung im Harburger Binnenhafen

Die Behörde für Wirtschaft, Verkehr und Landwirtschaft — Strom und Hafenbau — und die Baubehörde — Landesplanungsamt — führten 1988 gemeinsam das Projekt

"Untersuchung der Entwicklungstendenzen älterer Gewerbestandorte am Beispiel Harburger Binnenhafen" durch. Die Durchführung der Untersuchung wurde an eine privatwirtschaftliche Auftragnehmerin vergeben. Die von der Auftragnehmerin zu erbringenden Leistungen wurden vertraglich festgelegt.

Ein wesentlicher Teil des Untersuchungsauftrags bestand darin, betriebliche Bestimmungsgrößen für Standortbezogenheit und Entwicklungsaussichten, d.h. Informationen und Daten über Betriebsstruktur, Standortverbundenheit und Zukunftsperspektiven von den ansässigen Betrieben direkt zu erheben. In dem dafür entwickelten Fragebogen waren unter vielen anderen auch folgende Fragen enthalten:

Wie hoch war Ihr Umsatz 1986?

Wie hoch war die von Ihnen 1986 gezahlte Bruttolohn- und Gehaltssumme?

Welche Höhe hatten Ihre Investitionsausgaben in den Jahren 1980-1986?

Neben der Fragebogenerhebung wurden Interviews durchgeführt, die auf Tonband aufgenommen wurden. Das Ergebnis der Untersuchung, die in mehreren Stufen ablief (Bestandsaufnahme der Standortsituation, Befragung der ansässigen Betriebe, wissenschaftliche Analyse der Daten und Ermittlung der standortspezifischen Entwicklungstendenzen), war von der Auftragnehmerin zu dokumentieren und den Auftraggebern in Form von Zwischenberichten und einem Schlußbericht zu übergeben.

Ich wurde so früh von der Baubehörde beteiligt, daß alle datenschutzrechtlichen Belange bei diesem Projekt berücksichtigt werden konnten. So war von Anfang an klar, daß diese Befragung nur auf freiwilliger Basis durchgeführt werden konnte, weil es keine bereichsspezifische Vorschrift gibt, die eine derartige Befragung zum Gegenstand hat. Deshalb wurde mit Pressemitteilungen und Informationsschreiben an die betroffenen Betriebe umfangreiche Motivierungsarbeit geleistet. Die klare Darstellung von Gegenstand, Inhalt und Umfang der geplanten Datenverarbeitung diente nicht nur der Erhöhung der Mitwirkungsbereitschaft der angesprochenen Kreise, sondern war gesetzlich geforderte Voraussetzung für die Zulässigkeit der Datenverarbeitung mit Einwilligung (§ 5 Abs. 1 Nr. 2 und Abs. 2 HmbDSG). Zu der großen Akzeptanz dieser Befragung hat ohne Zweifel auch beigetragen, wie die Verwendung der Daten geregelt war. Über die geplante Verwendung wurden die Betroffenen — wie es § 5 Abs. 2 Satz 2 HmbDSG verlangt — vor der Befragung informiert:

"Ihre Angaben werden vertraulich behandelt und nur für den genannten Zweck verwendet. Die Fragebögen werden nach ihrer Auswertung vernichtet. Die Dateien werden nach Abschluß der Untersuchung Ende 1988 gelöscht. Jeder Interviewer ist auf das Datengeheimnis verpflichtet worden. Die Erhebung ist mit dem Hamburgischen Datenschutzbeauftragten abgestimmt worden und unterliegt seiner Kontrolle." Schließlich wurde auch auf dem Fragebogen selbst unübersehbar auf die Freiwilligkeit der Mitwirkung hingewiesen.

Überrascht war ich dann allerdings, daß zwischen Auftraggebern und Auftragnehmerin nach Durchführung der Befragung eine Meinungsverschiedenheit darüber entstand, ob die Erhebungsunterlagen, d.h. die ausgefüllten Fragenbogen von der Auftragnehmerin an die Auftraggeber herauszugeben seien. Die Auftragnehmerin verweigerte die Herausgabe unter Hinweis darauf, daß sie sich den Befragten gegenüber zur vertraulichen Behandlung verpflichtet hatte. Die Auftraggeber begründeten ihren Herausgabewunsch damit, ihnen genüge nicht die Information, daß z.B. 10 % der am Standort ansässigen Unternehmen eine Erweiterung planten. Sie wollten Genaueres wissen und die betreffenden Unternehmen ansprechen können, um deren Wünsche auch umsetzen zu können.

Die datenschutzrechtliche Antwort auf diese Streitfrage mußte eindeutig ausfallen: Auf freiwilliger Basis erhobene Daten dürfen nur für den Zweck/die Zwecke verwendet werden, die den Befragten gegenüber vor Erteilung der Einwilligung genannt worden sind. Die Einwilligung umfaßt nur die Datenverwendung, in die ausdrücklich eingewilligt wurde. In eine Übermittlung von Einzelfalldaten an die Auftraggeber war nicht eingewil-

ligt worden. Den Befragten war vertrauliche Behandlung ihrer Angaben zugesichert worden. Sie hatten nur der Übermittlung von Ergebnisdaten — aggregierten, anonymisierten Daten — an die Auftraggeber zugestimmt. Daten, die im Rahmen einer einem bestimmten Zweck dienenden Erhebung angegeben worden sind, dürfen auch dann nicht für den Verwaltungsvollzug weiterbenutzt werden, wenn Auftraggeber der Erhebung und für den Verwaltungsvollzug zuständige Stelle — wie hier — identisch sind.

Ich habe den Beteiligten vorgeschlagen, die Erkenntnisse aus den Gutachten zu nutzen und zeitnah zu der Erhebung "nachzufassen". Damit meine ich, die Behörden sollten das bei den Beteiligten durch die Untersuchung geweckte Interesse nutzen und im Zusammenhang mit der öffentlichen Information über das Ergebnis der Untersuchung die betroffenen Kreise auffordern, ihre bei der Befragung geäußerten Wünsche nunmehr an die zuständigen Stellen heranzutragen, damit diese Wünsche nun auch im Verwaltungsvollzug berücksichtigt werden können.

4.9 Steuerwesen

4.9.1 Fortdauer bzw. Erledigung alter Probleme

Im Berichtsjahr 1988 konnte nur eines der Probleme im Bereich der Steuerverwaltung, über die ich in meinem 6. Tätigkeitsbericht (4.9, S. 74 ff.) berichtet habe, erledigt werden.

Zur Erinnerung: Die entschiedene Kritik der Datenschutzbeauftragten des Bundes und der Länder an der im Finanzbereich geübten Praxis, in einer Vielzahl von Fällen regelmäßig Kontrollmitteilungen ohne ausreichende Rechtsgrundlage auszutauschen (§ 111 AO 1977 — Amtshilfe — war für regelmäßige, nicht auf den Einzelfall beschränkte Informationsflüsse nicht tragfähig), hatte im Rahmen des Steuerbereinigungsgesetzes 1986 zur Einführung des § 93a AO geführt. Hiernach werden nur noch solche Mitteilungen zulässig sein, die aufgrund einer allgemeinen, durch Rechtsverordnung näher bestimmten Mitteilungspflicht erfolgen. In § 93a AO werden die Tatbestände genannt, für die mit der Rechtsordnung allgemeine Mitteilungspflichten angeordnet werden können. Da bis heute die Verordnung zu § 93a AO ("Kontrollmitteilungsverordnung") nicht erlassen ist, was bedeutet, daß immer noch für keinen einzigen Tatbestand regelmäßige Kontrollmitteilungen durch Rechtsverordnung angeordnet sind, stehen wir faktisch nicht besser da als vor Einführung des § 93a AO:

Der Austausch von regelmäßigen Kontrollmitteilungen im Bereich der AO erfolgt auch heute noch ohne ausreichende Rechtsgrundlage. Wer angenommen hatte, der weitere Austausch von Kontrollmitteilungen könne im Hinblick auf den unmittelbar nach Erlaß des § 93a AO folgenden Erlaß der Rechtsverordnung hingenommen werden, sieht sich enttäuscht.

Die in Nr. 5.2 der Anlagen zu den Verwaltungsvorschriften zu §§ 23 und 44 LHO vorgeschriebenen Kontrollmitteilungen ließen sich — wie berichtet — mit § 93a AO nicht in Einklang bringen. Die Finanzbehörde hatte zugesagt, die betreffende Regelung bei der ohnehin gerade anstehenden Änderung der Verwaltungsvorschrift zu streichen (s. 6. TB, S. 76). Dies ist nun — kurz vor dem Druck dieses Berichts — erfolgt, wie ich dem Amtlichen Anzeiger vom 9. November 1988, Seiten 2079 ff. (2080) entnommen habe.

Auch die Steuerdaten-Abrufverordnung ist noch nicht erlassen worden. Im Berichtsjahr wurde die Frage weiter diskutiert, in welchem Umfang zur nachträglichen Kontrolle der Berechtigung von Datenabrufen automatische Protokollierungen erforderlich sind (s. 6. TB, S. 74). Ebenfalls noch nicht erledigt ist der Streit über die Möglichkeit, für die Amtsträger der obersten Finanzbehörden und der Oberfinanzdirektionen automatisierte Abrufverfahren einzurichten. Die Einführung solcher Abrufverfahren bedeutet, daß bei den Oberfinanzdirektionen, den obersten Finanzbehörden der Länder und beim Bundesminister der Finanzen zentrale Abrufmöglichkeiten geschaffen werden können, die diesen Behörden einen unmittelbaren automatisierten Zugriff auf Steuerdaten der Finanzämter ihres Zuständigkeitsbereichs ermöglichen. Dies ist zur Aufgabenerfüllung

— wie im 6. TB ausgeführt — nicht erforderlich. Die Datenschutzbeauftragten des Bundes und der Länder haben deswegen die Streichung dieser Möglichkeit gefordert.

4.9.2 Änderungen des § 31 der Abgabenordnung (AO)

Seit Jahren wird nach einer datenschutzrechtlich einwandfreien Lösung für ein Problem aus dem Bereich der Bezirksverwaltung gesucht, auf das mich das Senatsamt für Bezirksangelegenheiten im Dezember 1985 aufmerksam gemacht hat. (In den Kommunen anderer Bundesländer stellt sich das Problem in gleicher Weise, wie die bundesweite Erörterung gezeigt hat.)

Im Rahmen der Erhebung von Sielbau- und Wegebaubeiträgen benötigen die Abgabenämter die Anschriften der beitragspflichtigen Grundeigentümer und Erbbauberechtigten. Dazu übermittelt die Baubehörde nach Abschluß der entsprechenden Baumaßnahmen den Abgabenämtern Computerlisten mit den Namen und Anschriften der Abgabepflichtigen. Die Angaben in den Listen stimmen mit den Anschriftenlisten der Hamburger Feuerkasse überein. In zahlreichen Fällen sind die Anschriften jedoch nicht mehr aktuell, die Abgabenbescheide können nicht zugestellt werden. Die Sachbearbeiter in den Abgabenämtern versuchten in solchen Fällen, vom Finanzamt für Verkehrssteuern und Grundbesitz die neuen Anschriften zu erfragen, da diese Dienststelle über stets aktuelle Unterlagen verfügt. Nachdem in der Vergangenheit solche Fragen offenbar beantwortet worden waren, verweigerte das Finanzamt für Verkehrssteuern und Grundbesitz ab 1985 dies jedoch unter Hinweis auf das Steuergeheimnis nach § 30 AO.

Ich habe dem Senatsamt für Bezirksangelegenheiten seinerzeit mitteilen müssen, bei der gegenwärtigen Rechtslage sei die Übermittlung von Namen und Anschriften der Grundstückseigentümer und Erbbauberechtigten aus der Grundsteuererhebung an die Abgabenämter nicht zulässig. Die Übermittlung von Daten aus dem Besteuerungsverfahren an Dritte sei bereichsspezifisch und abschließend in § 30 AO geregelt. Danach sei die Übermittlung nicht zulässig. Die §§ 31 und 31a AO, die Ausnahmen von § 30 AO zum Gegenstand hätten, seien für den Fall der Abgabenämter nicht einschlägig. Abschließend wies ich darauf hin, daß ich mir eine Lösung derart vorstellen könnte, daß bei einer Novellierung der AO in § 31 auch die Übermittlung der Daten "Grundstückseigentümer" (Name und Anschrift) und "Grundstücksbezeichnung" an die Abgabenämter zum Zwecke der Erhebung von Wege- und Sielbaubeiträgen zugelassen werden könnte. Die Finanzbehörde hielt meinen Vorschlag seinerzeit auch mittelfristig nicht für realisierbar.

Auf Drängen der Abgabenämter und der Datenschutzbeauftragten befaßten sich der Bundesminister der Finanzen und die Finanzminister/-senatoren der Länder im Jahre 1987 mit dem Problem. Sie kamen zu dem Ergebnis, die bestehenden gesetzlichen Regelungen ließen auch eine andere als die bisher vertretene Auslegung zu. Nach § 1 Abs. 2 Nr. 1 AO gelte § 30 AO für die Realsteuern entsprechend. Im Rahmen der entsprechenden Anwendung der AO durch die Gemeinde seien die Wörter "Verwaltungsverfahren in Steuersachen" in § 30 Abs. 2 Nr. 1a AO als "Verwaltungsverfahren in Abgabensachen" (kommunale Steuern, Gebühren und Beiträge) zu lesen. Damit könnten die für die Verwaltung der Gebühren und Beiträge notwendigen Informationen gem. § 30 Abs. 4 Nr. 1 AO aus dem Datenbestand der Grundsteuer entnommen werden. Aufgrund dieser Auslegung stimmte die Finanzbehörde in Hamburg der Übermittlung von Anschriften der Grundeigentümer und Erbbauberechtigten an die Abgabenämter wieder zu.

Die Datenschutzbeauftragten können der Auffassung der obersten Finanzbehörden des Bundes und der Länder nicht folgen. Nach § 1 Abs. 2 AO sind zwar die Vorschriften der AO für Realsteuern entsprechend anwendbar, aber § 3 Abs. 2 AO nennt als Realsteuern nur die Grundsteuer und die Gewerbesteuer. Abgaben wie Wege- und Sielbaubeiträge sind keine Realsteuern. Inzwischen legte der Bundesminister der Finanzen den Entwurf eines Abs. 3 zu § 31 AO vor, der m.E. über das angestrebte Ziel weit hinausgeht und gegen den ich erhebliche Bedenken habe. Danach sollen die Gemeinden

berechtigt sein, die nach § 30 geschützten Namen und Anschriften von Grundstückseigentümern, die bei der Verwaltung der Grundsteuer bekanntgeworden sind, zur Verwaltung anderer Aufgaben sowie zur Erfüllung sonstiger hoheitlicher Aufgaben zu verwenden oder den hierfür zuständigen Behörden oder Körperschaften des öffentlichen Rechts mitzuteilen. M.E. sollte nur die Übermittlung an die Abgabenämter zum Zwecke der Feststellung der Schuldner von Wege- und Sielbaubeiträgen erlaubt werden. Dieser Zweck hat noch eine gewisse Nähe zum Steuererhebungsverfahren im Zusammenhang mit dem Eigentum am Grund und Boden, so daß eine Durchbrechung des Steuergeheimnisses noch verhältnismäßig erscheint. Grundsätzlich sollten die im Steuerverfahren erhobenen Daten aber nicht für andere Zwecke der Verwaltung (— die im übrigen in dem Entwurf des Bundesministers der Finanzen nicht klar und im einzelnen benannt sind —) zur Verfügung stehen.

Im übrigen halte ich es für fragwürdig, einem Problem, das nicht aus dem Steuerbereich stammt, mit dem Steuerrecht zu begegnen. Offensichtlich haben etliche kommunale Stellen erhebliche Schwierigkeiten mit der Ermittlung von aktuellen Grundstückseigentümerangaben. Diesem Problem kann aber m.E. nicht dadurch angemessen begegnet werden, daß das Steuergeheimnis — ein Eckpfeiler unseres Steuerrechts — verwässert wird. Vielmehr muß nach einer Lösung gesucht werden, die es der für den Nachweis des Eigentums am Grund und Boden gesetzlich zuständigen Stelle, nämlich dem Grundbuchamt, ermöglicht, diese Aufgabe zu erfüllen.

4.9.3 Auskunftsersuchen an Arbeitgeber zum Nachweis angeblicher Bewerbungskosten

Eine Steuerpflichtige hat sich über die Art und Weise bei mir beschwert, in der das für sie zuständige Finanzamt von der nach § 93 AO bestehenden Möglichkeit, Dritte zu befragen, Gebrauch gemacht hat. Die Steuerpflichtige hatte in ihrer Einkommensteuererklärung Bewerbungskosten geltend gemacht, aber nicht belegt. Die zuständige Sachbearbeiterin im Finanzamt hatte bei dieser Sachlage die Personalabteilung des Arbeitgebers der Steuerpflichtigen telefonisch um Auskunft gebeten, ob diese sich in einem gekündigten oder ungekündigten Arbeitsverhältnis befände. Die Steuerpflichtige war der Meinung, die Anfrage bei ihrem Arbeitgeber stelle eine schwerwiegende Amtspflichtverletzung dar. Ihre Dienstaufsichtsbeschwerde wurde von der Oberfinanzdirektion zurückgewiesen. Zur Begründung führte die OFD aus, bei der Bearbeitung der Einkommensteuererklärung sei die erforderliche Sorgfalt geübt worden. Die Sachbearbeiterin habe sich bemüht, zugunsten der Steuerpflichtigen Ermittlungen durchzuführen, um eine Glaubhaftmachung der geltend gemachten Werbungskosten zu erreichen. Weder das Steuergeheimnis noch das Bundesdatenschutzgesetz seien verletzt worden, weil in der nach § 93 AO grundsätzlich zulässigen Befragung des Arbeitgebers keinerlei Angaben über den Grund gemacht worden seien.

Diese Ausführungen halten einer Nachprüfung nicht stand. Zur Beurteilung der Frage, ob mit der Anfrage an den Arbeitgeber gegen § 30 AO verstoßen worden ist, kam es auf § 93 AO nicht an. Diese Vorschrift regelt die Auskunftspflicht eines Dritten, den ein Finanzamt nach Verhältnissen eines Steuerpflichtigen befragt. Die Petentin hatte sich aber nicht darüber beschwert, daß der Arbeitgeber die Frage beantwortet hatte, sondern darüber, daß das Finanzamt einen Dritten befragt hatte, was sie in ihrem Fall für unverhältnismäßig hielt. Zur Beurteilung dieser Maßnahme ist § 88 AO heranzuziehen. Danach hat zwar die Finanzbehörde Art und Umfang der Ermittlungen zu bestimmen, dabei hat sie jedoch die Grundsätze der Verhältnismäßigkeit, der Zumutbarkeit und der Zweckmäßigkeit zu beachten. Wo die amtliche Ermittlungspflicht ihre Grenzen hat, bestimmt sich nicht zuletzt auch nach der Art und dem Ziel des durchzuführenden Verwaltungsverfahrens. Begünstigende Verwaltungsakte, insbesondere solche, auf deren Gewährung kein Rechtsanspruch besteht und die üblicherweise auf Antrag gewährt werden, bedingen primär eine ausreichende Darlegung des maßgebenden Sachverhalts durch den begünstigten Beteiligten.

Im konkreten Fall hätte also

— der Grundsatz der Zumutbarkeit es der Sachbearbeiterin im Finanzamt erlaubt, auf eigenes Suchen nach Belegen für das Entstehen von Bewerbungskosten zu ver-

zichten und statt dessen die Steuerpflichtige zur Vorlage von geeigneten Belegen aufzufordern mit dem Hinweis, daß sonst die betreffenden Aufwendungen nicht anerkannt werden können;

— der Grundsatz der Verhältnismäßigkeit die Sachbearbeiterin davon abhalten sollen, beim Arbeitgeber der Steuerpflichtigen Erkundigungen einzuholen, weil immerhin die Gefahr bestand, daß die befragte Person aus der finanzamtlichen Anfrage zutreffende oder auch unzutreffende Schlüsse ziehen würde, wenn nicht gar die Gefahr, daß bei Gelegenheit des Gesprächs dem Steuergeheimnis unterliegende Daten (versehentlich) preisgegeben würden;

— der Grundsatz der Zweckmäßigkeit die Sachbearbeiterin davon abhalten müssen, die Anfrage an den Arbeitgeber zu richten, weil die Anfrage ungeeignet war, das Entstehen der Bewerbungskosten zu belegen oder zu widerlegen: Bewerbungen werden nicht nur geschrieben, wenn der Arbeitgeber dem Beschäftigten gekündigt hat. Wer sich beruflich verändern und/oder verbessern möchte, bewirbt sich durchaus auch aus ungekündigter Stellung heraus bei anderen Arbeitgebern und wird dies, jedenfalls solange er keine Zusage vom neuen Arbeitgeber hat, auch nicht seinem derzeitigen Arbeitgeber erzählen. Solche Bewerbungen können auch ergebnislos verlaufen, so daß der Betreffende auch noch nach Jahren beim ursprünglichen Arbeitgeber beschäftigt ist. Auch Kosten ergebnisloser Bewerbungen sind steuerlich absetzbar. Es ist daher unerfindlich, in welcher Weise die Sachbearbeiterin das Ergebnis der Anfrage verwerten zu können glaubte. Ungeeignete Maßnahmen können aber niemals zweckmäßig sein.

Ich habe daher empfohlen, in Fällen, in denen es um den Nachweis von Tatsachen geht, die der Steuerpflichtige zur Minderung seiner Steuerschuld geltend macht, vorrangig den Steuerpflichtigen zum Nachweis dieser Tatsachen aufzufordern. Kann oder will der Steuerpflichtige den Nachweis nicht erbringen, so sollte er auf die Möglichkeit hingewiesen werden, zur Vermeidung der Ablehnung der beantragten steuerlichen Vergünstigung Dritte zu benennen, bei denen die Finanzbehörde gem. § 93 AO Auskünfte einholen kann. Ist er mit der Befragung Dritter nicht einverstanden, so wäre die entsprechende steuerliche Berücksichtigung zu versagen. Ein solches Vorgehen scheint mir die Grundsätze der Verhältnismäßigkeit, Zumutbarkeit und Zweckmäßigkeit zu gewährleisten.

4.9.4 Innenrevision im Bereich der OFD Hamburg und Bestimmungen über das Zeichnungsrecht in den Finanzämtern

Im Laufe des Berichtsjahres hatte ich mich mit der Innenrevision im Bereich der OFD zu befassen. Daten aus dem automatisierten Personaldatensystem der Personalstelle in der OFD waren der Innenrevision zur Verfügung gestellt worden. Die Datenübermittlung diente der Durchführung von Kontrollen hinsichtlich der Veranlagung derjenigen Mitarbeiter der Finanzämter, die im selben Bezirk wohnen, in dem sie arbeiten. Überprüft werden sollte die Einhaltung der Zeichnungsrechtsbestimmungen (dazu weiter unten mehr).

Die Übermittlung von Daten aus dem Personaldatensystem an die Innenrevision war datenschutzrechtlich bedenklich, weil die Einrichtung des automatisierten Personaldatensystems auf einer Dienstvereinbarung (vom 7.8.1986) zwischen der OFD und dem Personalrat der OFD beruht. Wesentlicher Bestandteil dieser Dienstvereinbarung ist eine abschließende Aufzählung der zulässigen Nutzungen des Datenbestandes, und die Nutzung für Zwecke der Innenrevision war in dieser Aufzählung nicht enthalten. Nach der Dienstvereinbarung sind weitere Verwendungen des Datenbestandes nur nach Vereinbarung mit der Personalvertretung zulässig.

Bei Ausdruck der Namensliste für die Innenrevision ging die Personalstelle der OFD davon aus, dies kollidiere nicht mit der Dienstvereinbarung. Der Personalrat wurde daher nicht über die Übermittlung der Namensliste informiert, wohl aber über die Erteilung der Abfragemöglichkeit für die Innenrevision bezüglich der Datei mit den Steuer-

konten (INFES). Noch während der laufenden Prüfungen rügte der Personalrat die Nutzung der Personaldaten für Zwecke der Innenrevision. Die daran anschließende (erregte) Diskussion im Bereich der Steuerverwaltung führte im Ergebnis zum Einvernehmen zwischen den Parteien der Betriebsvereinbarung darüber, daß jede Weitergabe von Daten über die in der Betriebsvereinbarung getroffene Regelung hinaus der vorherigen Erörterung mit dem Personalrat bedarf. Diesem Ergebnis ist zuzustimmen.

Inhalt der Prüfung der Innenrevision war in diesem Fall, wie oben schon erwähnt, die Einhaltung der Zeichnungsrechtsbestimmungen. In Hamburg sind aufgrund § 23 Abs. 1 Nr. 4 der bundeseinheitlich geltenden Geschäftsordnung für die Finanzämter (FAGO) Bestimmungen über das Zeichnungsrecht in den Finanzämtern erlassen worden. Darin sind in Abschnitt A 2 Nr. 8 der Zeichnungsvorbehalt der Vorsteher für Steuerangelegenheiten von Amtsangehörigen und in Abschnitt A 3 Nr. 21 der Zeichnungsvorbehalt der Sachgebietsleiter für Steuersachen von Angehörigen der Steuerverwaltung, die nicht Angehörige des Finanzamtes sind, geregelt.

Von betroffenen Angehörigen des Finanzamtes wird dies kritisiert, weil dadurch regelmäßig ihre Vorgesetzten über ihre steuerlichen Belange umfassend informiert werden. Sie sehen darin eine unverhältnismäßige Beeinträchtigung ihres informationellen Selbstbestimmungsrechts. Aus der Überlegung, daß im Bereich der Steuerverfahren insbesondere für die Angehörigen der Steuerverwaltung wegen ihrer einschlägigen Fachkenntnisse und der Kenntnisse der Interna Manipulationsmöglichkeiten nicht von der Hand zu weisen sind, erscheinen mir interne, speziell auf die Mitarbeiter gerichtete Kontrollen indessen erforderlich. Ich habe daher keine grundsätzlichen Bedenken gegen Zeichnungsvorbehalte.

Die Frage ist allerdings, ob der derzeitige Umfang — auch im Hinblick auf die zusätzlichen Kontrollen durch die Innenrevision — noch verhältnismäßig ist.

4.9.5 Übermittlung von Lohnsteuerkarten an kirchliches Rechenzentrum

In Hamburg werden die Lohnsteuerkarten aus den Jahren, für die nach dem Zerlegungsgesetz und dem Gesetz über Steuerstatistiken (Bundesgesetze) die Lohnsteuerzerlegung durchgeführt und Steuerstatistiken aufgestellt werden, nach Auswertung durch das Statistische Landesamt in Hamburg an das Rechenzentrum Nordelbien-Berlin (RNB) weitergeleitet. Dies ist zuletzt mit den Lohnsteuerkarten aus 1983 so geschehen.

Das RNB ist eine Einrichtung der Nordelbischen Evangelisch-Lutherischen Kirche, die für unterschiedliche Auftraggeber (Kirchen, kirchliche Einrichtungen in privatrechtlicher Organisationsform u.a.) Datenverarbeitung betreibt. Es wertet die Lohnsteuerkarten für die Evangelische und die Römisch-katholische Kirche in Norddeutschland (Hamburg, Bremen, Berlin, Schleswig-Holstein) aus. Die Auswertung wird durch Personal des RNB in einer einheitlichen Aktion, d.h. nicht getrennt nach Steuerkarten von Protestanten bzw. Katholiken, durchgeführt. Auch Lohnsteuerkarten ohne Kirchensteuermerkmal wurden bisher an das RNB übermittelt. Nach der Auswertung der Lohnsteuerkarten im RNB werden sie vernichtet.

Die Evangelische Kirche in Deutschland hat diverse Gesetze und Verordnungen zum kirchlichen Datenschutz erlassen, so daß Datenübermittlungen von öffentlichen Stellen an die Evangelische Kirche nach § 10 Abs. 3 HmbDSG erlaubt sein könnten. Im zu untersuchenden Fall handelt es sich aber um die Übermittlung von dem Steuergeheimnis unterliegenden Daten, für die mit §§ 30, 31 AO eine bereichsspezifische Regelung vorliegt, so daß für die Anwendung der Generalklausel im HmbDSG kein Raum ist. Gem. § 31 Abs. 1 AO sind die Finanzbehörden berechtigt, Besteuerungsgrundlagen, Steuermeßbeträge und Steuerbeträge an Religionsgemeinschaften, die Körperschaften des öffentlichen Rechts sind, mitzuteilen zur Festsetzung solcher Abgaben, die an diese Besteuerungsgrundlagen, Steuermeßbeträge oder Steuerbeträge anknüpfen.

In Hamburg werden die Kirchensteuern der Evangelisch-Lutherischen Kirche und der Römisch-katholischen Kirche durch die staatlichen Behörden verwaltet. Grundlage dafür sind § 10 des (hamburgischen) Kirchensteuergesetzes in Verbindung mit der Verordnung über die Verwaltung von Kirchensteuern durch staatliche Behörden in der Freien und Hansestadt Hamburg. Die staatlichen Behörden setzen die Kirchensteuern fest und erheben sie. Eine Übermittlung der Lohnsteuerkarten an die Kirchen scheint deshalb nicht erforderlich, denn die Kirchen benötigen die Angaben aus den Karten nicht zur Festsetzung der Kirchensteuern. Insbesondere sind die Lohnsteuerkarten ohne Kirchensteuermerkmal zur Festsetzung von Kirchensteuern nicht erforderlich. Aber es sind auch die Karten der protestantischen Steuerpflichtigen für die Römisch-katholische Kirche ohne Belang und die Karten der Katholiken entsprechend für die Evangelische Kirche (gemeinsame Auswertung sämtlicher Karten durch das RNB!). Schließlich enthalten die Lohnsteuerkarten Daten, die für die Verwaltung der Kirchensteuern nicht benötigt werden, wie z.B. Freibeträge, Arbeitnehmersparzulagen u.a.

Die Vertreter der Kirche machen geltend, zur Festsetzung der ihnen zustehenden Abgaben gehöre es nicht nur, den Steuerschuldner, den Steuerbetrag und die Religionsgemeinschaft im Groben (evangelisch oder katholisch) festzustellen, was in der Tat durch die staatlichen Behörden in Hamburg geschehe. Vielmehr gehöre zur Festsetzung auch die Ermittlung des richtigen Steuergläubigers, nämlich der Kirchengemeinde, der der Steuerpflichtige angehöre. Wegen der Regelung, daß Arbeitgeber die gesamten einbehaltenen Kirchensteuern ihrer Arbeitnehmer an das Arbeitsstättenfinanzamt abzuführen hätten, während die Steuern im einzelnen der jeweiligen Kirche gebührten, der die Steuerpflichtigen an ihrem Wohnort angehörten, müßten die Kirchen ein Zerlegungsverfahren entsprechend dem Zerlegungsverfahren der staatlichen Lohnsteuer durchführen.

Ich habe Zweifel, ob der Festsetzungszweck in § 31 AO so ausgelegt werden kann. Jedenfalls sollte, wenn der Zweck des § 31 AO so weit geht, eine Klarstellung (... zur Festsetzung und Zerlegung solcher Angaben ...) im Gesetz erfolgen.

Die Vertreter der Kirche berufen sich zur Rechtfertigung der Übermittlung der Lohnsteuerkarten außer auf § 31 AO auch auf §§ 7 und 8 des (hamburgischen) Kirchengesetzes, die wie folgt lauten:

§ 7 Die staatlichen Behörden erteilen den steuerberechtigten Körperschaften Auskunft über die Daten, derer sie zur Durchführung der Besteuerung und der Feststellung ihrer Anteile bedürfen.

§ 8 Die Kirchensteuern werden von den steuerberechtigten Körperschaften verwaltet, soweit die Verwaltung nicht den staatlichen Behörden übertragen worden ist.

Nach § 7 hätten die staatlichen Behörden den Kirchen die Angaben mitzuteilen, derer diese zur Feststellung ihrer Anteile bedürften. Zwar sei in Hamburg "die Verwaltung" der Kirchensteuern den staatlichen Behörden übertragen, doch erstrecke sich die Übertragung nicht auf den auch zur Verwaltung der Kirchensteuer gehörenden Vorgang der Feststellung der Anteile der einzelnen Kirchen am Kirchensteueraufkommen ("Zerlegung"). Die Zerlegung müßten die Kirchen in eigener Regie durchführen. Da die staatlichen Behörden keine Zusammenstellung der für die Zerlegung eigentlich nur erforderlichen Daten (Lohnsteuerbetrag, Kirchensteuerbetrag, Arbeitsstättenfinanzamt, Wohnort des Steuerpflichtigen, Religionsgemeinschaft) zur Verfügung stellten, seien die Kirchen auf die Übersendung der Lohnsteuerkarten mit Kirchensteuermerkmal angewiesen.

Die Finanzbehörde hat keine Bedenken gegen die Übermittlung der Lohnsteuerkarten. Immerhin hat sie sich im Februar 1988 beim Bundesminister der Finanzen dafür eingesetzt, eine Klarstellung im Gesetz herbeizuführen, indem in § 31 Abs. 1 AO die Datenübermittlung an die Kirchen zur Festsetzung und Zerlegung von Kirchensteuern zugelassen wird. Sie hält es z.Z. nicht für durchführbar, daß die staatlichen Behörden den Kirchen einen zur Zerlegung geeigneten und auf den erforderlichen Datenumfang beschränkten Datenbestand zur Verfügung stellen.

Damit stellte sich die Frage, ob die Übersendung der Lohnsteuerkarten an die Kirchen weiter hingenommen werden kann, obwohl damit mehr Daten als erforderlich übermittelt werden. Ich habe zunächst vorgeschlagen, in Zukunft die Übersendung von Lohnsteuerkarten ohne Kirchensteuermerkmal an die Kirchen zu unterlassen. Außerdem habe ich die Kirche darum gebeten, mir mitzuteilen, welche organisatorischen Maßnahmen im Rechenzentrum sie getroffen hat, um zu gewährleisten, daß

— die Evangelische Kirche und die Römisch-katholische Kirche jeweils nur Daten ihrer eigenen Steuerpflichtigen erhalten,

— nur jeweils die Daten aus den Lohnsteuerkarten entnommen und weiterverwendet werden, die zur Kirchenlohnsteuerzerlegung erforderlich sind,

— die Lohnsteuerkarten nach Auswertung in diesem Sinne unverzüglich ordnungsgemäß vernichtet werden.

Ich habe betont, die Möglichkeit, die Übermittlung nicht erforderlicher Daten als noch vertretbar hinnehmen zu können, weil diese untrennbar mit den Lohnsteuerkarten verbunden sind, sei abhängig von den ausgleichenden Wirkungen geeigneter organisatorischer Maßnahmen gegen mißbräuchliche Verwendung.

Mitte November 1988 teilten mir die Finanzbehörde und die Kirche — vorerst nur telefonisch — mit, daß inzwischen an einem Verfahren gearbeitet werde, mit dem aus dem automatisierten Datenbestand der Finanzbehörde ein Datenbestand abgesplittet werde, der den Kirchen die für die Zerlegung erforderlichen Daten liefert. Damit werde die Übermittlung der Lohnsteuerkarten überflüssig. Die genaue Verfahrensbeschreibung soll mir demnächst übersandt werden. Ich gehe nach dieser Vorabinformation davon aus, daß in Zukunft nur folgende Daten von der Finanzbehörde an das RNB übermittelt werden:

— Amtlicher Gemeindeschlüssel

— Religionsschlüssel
für Antragsteller (Arbeitnehmer)
für Ehegatten

— Veranlagungsjahr

— Berichtigungsschlüssel

— einbehaltene Jahreskirchenlohnsteuer

— verbleibende Kirchenlohnsteuer

Eine abschließende Bewertung muß der Prüfung der noch ausstehenden schriftlichen Beschreibung des neuen Verfahrens vorbehalten bleiben.

4.10 Einwohnerwesen

4.10.1 Ausländerzentralregister

Die zuletzt in meinem 5. Tätigkeitsbericht (5.7.5, S. 65) erwähnten Überlegungen des Bundesministers des Innern zu einer Neukonzeption des Ausländerzentralregisters (AZR) wurden im Berichtsjahr soweit konkretisiert, daß er im Juli 1988 den Referentenentwurf eines Gesetzes über das Ausländerzentralregister (AZR-Gesetz) vorlegen konnte. Der Bundesbeauftragte für den Datenschutz hat die bisherigen Vorarbeiten an dem Gesetzentwurf in der Arbeitsgruppe "Neukonzeption des Ausländerzentralregisters" begleitet. Parallel dazu haben die Datenschutzbeauftragten des Bundes und der Länder einen Arbeitskreis "Ausländerzentralregister" eingerichtet und sich dort mit den Datenschutzproblemen beschäftigt, die mit einem solchen Gesetzesvorhaben verbunden sind.

Die Bemühungen um eine gesetzliche Regelung, die den Anforderungen des Volkszählungsurteils des Bundesverfassungsgerichts entspricht, werden von mir grundsätzlich begrüßt; mittlerweile ist es überfällig, die Arbeit des AZR auf eine tragfähige

gesetzliche Grundlage zu stellen. Leider bleibt jedoch der Gesetzentwurf in einer Reihe von Punkten hinter den Forderungen der Datenschutzbeauftragten nach Normenklarheit, Bestimmtheit der Zweckbindung und Verhältnismäßigkeit zurück:

— Das AZR soll nicht nur für die eigentlichen Aufgabenzwecke der Ausländer- bzw. Asylbehörden zur Verfügung stehen, sondern in gleicher Weise auch sonstige öffentliche Stellen — z.B. Sicherheitsbehörden — unterstützen. Eine solche Unterstützung anderer Behörden kann jedoch nicht allein in einem Registergesetz geregelt werden. Vielmehr bedarf es ergänzender spezialgesetzlicher Regelungen, die durch Novellierungen des Ausländergesetzes, des Staatsangehörigkeitsrechts, der StPO und des Polizeirechts geschaffen werden müssen, damit der Betroffene das Ausmaß des Eingriffs in sein Recht auf informationelle Selbstbestimmung einschätzen kann. Solange jedenfalls solche spezialgesetzlichen Regelungen nicht existieren, sind die Speicherungen und Übermittlungen aus dem AZR in dem Umfang, in dem sie praktiziert werden bzw. in dem Gesetzentwurf vorgesehen sind, problematisch; auch unter Berücksichtigung des Übergangsbonus sind sie teilweise unzulässig.

— Es ist zu befürchten, daß das AZR in der Praxis alsbald zu einem bundesweiten zentralen Melderegister für Ausländer zweckentfremdet wird, weil der Gesetzentwurf die Nutzungszwecke des AZR nicht hinreichend präzise festlegt. Dies wäre allerdings schlichtweg unvereinbar mit den bewußt dezentral gegliederten Auskunftsverfahren des Meldewesens. Ich darf nur daran erinnern, daß nicht zuletzt wegen durchgreifender verfassungsrechtlicher Bedenken im Verlauf der Beratungen über das Melderechtsrahmengesetz auf ein zentrales Bundeseinwohnermelderegister, ja sogar auf Landesadreßregister verzichtet wurde. Es ist nicht nachvollziehbar, aus welchen Gründen diese Bedenken nicht für Ausländer gelten sollten.

— Im Gesetzentwurf bleibt die Sperrung und Löschung von Daten im AZR weitgehend ungeregelt. Aus datenschutzrechtlichen Gründen kann aber auf Regelungen zur systematischen wie einzelfallbezogenen Datensperrung und -löschung nicht verzichtet werden, da es sich hierbei — wie das Bundesverfassungsgericht zum Volkszählungsurteil ausgeführt hat — um wesentliche verfahrensrechtliche Vorkehrungen zum Schutz des informationellen Selbstbestimmungsrechts handelt.

— Der Entwurf enthält nur an wenigen Stellen Protokollierungsregelungen — und dies auch nur in unzulänglicher Weise. Hierauf kann aber gerade wegen der beabsichtigten Abrufe im automatisierten Verfahren nicht verzichtet werden. Auch ist nicht ausgeschlossen, daß die Protokolldaten wiederum zweckentfremdet werden können und mithin das informationelle Selbstbestimmungsrecht der Betroffenen neuen Gefährdungen ausgesetzt wird. Deshalb muß festgelegt werden, daß Protokolldaten lediglich zur Kontrolle der Zulässigkeit der Datenverarbeitung verwendet werden dürfen, wie dies beispielsweise in den ZEVIS-Regelungen erfolgt ist.

— Der geplante Datensatz sieht u.a. vor, auch das Datum "Einreisebedenken" abzuspeichern. Damit sollen belastende Vorgänge aus dem Umfeld des Ausländers erfaßt werden, die noch keine ausländerrechtlichen Maßnahmen ausgelöst haben. Es sollen also nicht nur Informationen, die das Ergebnis eines Verwaltungsverfahrens sind, sondern auch unpräzise Angaben über ein vermutetes (Fehl-) Verhalten des Ausländers gespeichert werden. Es liegt auf der Hand, daß damit besondere Probleme verbunden sind. So kann ich mir vorstellen, daß bestimmte Erkenntnisse von einer Ausländerbehörde als "Einreisebedenken" gewertet werden, während eine andere Ausländerbehörde zu einem anderen Ergebnis kommt. Ein solches "weiches" Datum ist deshalb in einem Auskunftsregister fehl am Platze, solange nicht zumindest durch eine Rechtsverordnung präzise umschrieben wird, welche Tatbestände unter diese Angabe fallen. Außerdem muß sichergestellt werden, daß allein aufgrund der Registerauskunft keine negativen Entscheidungen getroffen werden dürfen.

— Es ist beabsichtigt, den INPOL-Fahndungsbestand in das AZR zu übernehmen. Hiergegen habe ich Bedenken, weil damit das AZR faktisch die Funktion eines weiteren polizeilichen Informationssystems erhält. Dies ist mir unverständlich, weil die Stellen mit Fahndungsaufgaben ohnehin schon auf INPOL zugreifen können. Für die Stellen, die an der Fahndung nicht beteiligt sind, sind die von ihnen zu treffenden Entscheidungen zunächst jedenfalls nicht von Gesetzes wegen davon abhängig, ob ein Ausländer zur Fahndung oder Aufenthaltsermittlung ausgeschrieben ist. Sollte eine solche Kenntnis im Einzelfall erforderlich sein, könnte sie von der entscheidenden Behörde im Nachhinein beschafft werden. Die Polizei könnte die Informationen, die sie zur Erfüllung ihrer Aufgaben benötigt, z.B. durch einen regelmäßigen Datenabgleich zwischen den polizeilichen Informationssystemen und dem AZR erhalten. Somit sind zwingende Gründe für eine Übernahme des INPOL-Fahndungsbestandes in das AZR nicht ersichtlich.

Daneben habe ich in meiner Stellungnahme zum Entwurf eines AZR-Gesetzes die Behörde für Inneres auf eine Reihe von Unzulänglichkeiten einzelner Bestimmungen hingewiesen, auf deren Darstellung ich hier aus Platzgründen verzichten möchte. Es handelt sich dabei im einzelnen um Hinweise

— zum Umfang der Daten, die im Register gespeichert werden dürfen,

— zur Speicherung von Aussiedlern und Vertriebenen,

— zur Speicherung von EG-Angehörigen,

— zur Datenübermittlung an das Register,

— zur Datenübermittlung vom AZR an Ausländerbehörden und sonstige öffentliche Stellen,

— zum Abruf im automatisierten Verfahren,

— zur Statistik,

— zur Auskunftserteilung an nicht-öffentliche Stellen, die humanitäre oder soziale Aufgaben wahrnehmen, an Behörden anderer Staaten, an natürliche Personen und juristische Personen des öffentlichen Rechts und an den Betroffenen.

Ich habe Zweifel, ob es gelingen wird, noch im Laufe der jetzigen Wahlperiode des Bundestages ein AZR-Gesetz zu verabschieden, das den modernen datenschutzrechtlichen Anforderungen entspricht. Sofern dies nicht gelingen sollte, hätte ich Bedenken, daß der gegenwärtige Betrieb des AZR mit all seinen Funktionen über diese Wahlperiode des Bundestages hinaus weiterbetrieben wird.

4.10.2 Personenstandswesen

Unter Federführung des Bundesministers des Innern sind mittlerweile die Beratungen und Vorarbeiten für ein Fünftes Gesetz zur Änderung und Ergänzung des Personenstandsgesetzes angelaufen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich in einem Beschluß vom 15. März 1988 hierzu geäußert und insbesondere die Absicht,

— die Mitteilungspflichten des Standesbeamten gesetzlich zu verankern,

— die Einsicht in die Personenstandsbücher und die Erteilung von Auskünften und Urkunden präziser zu regeln, insbesondere eigenständige Vorschriften über die Auskunft bzw. Einsicht für Zwecke wissenschaftlicher Forschung zu schaffen,

— das öffentliche Aufgebot wegfallen zu lassen,

positiv bewertet.

Der im Juli 1988 vorgelegte Vorentwurf enthält in mehreren Punkten datenschutzrechtliche Verbesserungen gegenüber früheren Fassungen. Trotzdem gibt es noch Defizite, die bis zur endgültigen Fassung des Änderungsgesetzes abgebaut sein sollten.

So sollte auf die Eintragung des Berufs in Personenstandsbüchern verzichtet werden, weil dies für die Beurkundung nicht erforderlich ist und für Identifizierungszwecke genügend andere Merkmale zur Verfügung stehen. Eine solche Angabe ist wegen ihrer begrifflichen Ungenauigkeit für die Identifizierung auch nicht geeignet. Es bleibt nämlich weitgehend dem Betroffenen überlassen, ob er seinen erlernten oder ausgeübten Beruf angibt und welche Bezeichnung er dafür wählt (z.B. Beamter, Jurist, Verwaltungsjurist, Regierungsrat, Referent), während die übrigen Eintragungen in die Personenstandsbücher präzise geregelt sind. Die bessere Aussagefähigkeit der Bücher für die spätere historische Forschung reicht als Begründung für die Erhebung des Berufs nach meiner Auffassung nicht aus.

Die Berechtigung von Behörden und bestimmten öffentlichen Stellen, Auskunft aus einem und Einsicht in einen Personenstandseintrag sowie Erteilung von Personenstandsurkunden zu verlangen, sollte in einer gesonderten Vorschrift bereichsspezifisch geregelt werden. Eine "Durchsicht dieser Bücher", wie sie bislang § 61 Personenstandsgesetz vorsieht, dürfte künftig weder Behörden und bestimmten öffentlichen Stellen noch anderen Personen erlaubt sein. Es muß im übrigen sichergestellt werden, daß die Gewährung von Auskunft und Einsicht nicht routinemäßig, sondern nur auf Ersuchen im Einzelfall erfolgt, wobei ein Direktzugriff auf Personenstandseintragungen dementsprechend auszuschließen ist.

Aus meiner Sicht muß außerdem die Gewährung von Informationen an Behörden und bestimmte sonstige Stellen an die gleichzeitige Benachrichtigung des Betroffenen gebunden werden.

Es ist auch erforderlich, die Weitergabe von personenstandsrechtlichen Daten zum Zweck der wissenschaftlichen Forschung durch gesetzliche Vorschriften bereichsspezifisch zu regeln. Dabei sollte das Prinzip der Gewährung von Auskunft und Einsicht nur mit Einwilligung der Betroffenen als Regelfall an den Anfang gestellt werden. Daran anschließend sollte als Ausnahme vorgesehen werden, daß es der Einwilligung dann nicht bedarf, wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens das Geheimhaltungsinteresse des Betroffenen erheblich überwiegt, die Einholung der Einwilligung nicht möglich ist und der Zweck des Forschungsvorhabens auf andere Weise nicht erreicht werden kann.

Auf jeden Fall bedarf es aber einer gesetzlichen Bindung der gewährten Informationen an den Zweck eines im Auskunftsersuchen zu bestimmenden Forschungsvorhabens. Die Konkretisierung ist unerläßlich, weil nur bei möglichst konkreter Bestimmung des Forschungsprojektes eine rechtsverbindliche Einwilligung zustandekommen kann und weil die erforderliche Güterabwägung im Falle der subsidiär zulässigen Datenweitergabe auf gesetzlicher Grundlage ebenfalls eine genauere Kenntnis erfordert.

Das Verhältnis der Vorschriften zugunsten wissenschaftlicher Forschung zu Vorschriften, die der — privaten — Ahnenforschung entgegenkommen sollen, bedarf — besonders mit Blick auf erhebliche Abgrenzungsprobleme in der Praxis — näherer Präzisierung.

Ebenfalls für die Praxis von Bedeutung sind die Orts- und Zeitangaben in Urkunden, insbesondere in Sterbeurkunden. Solche Urkunden dürfen Dritten keinen Anlaß zu Spekulationen über die näheren Umstände des Todes geben.

Neben den Vorschriften über Informationsgewährung auf Ersuchen bedarf es präziser Rechtsgrundlagen für die Mitteilungspflichten des Standesbeamten, denen ein Ersuchen nicht vorausgeht. Die als Mitteilungsempfänger vorgesehenen Behörden und Stellen sollten im Gesetz abschließend genannt, der Umfang der Mitteilungsinhalte beschrieben und klargestellt werden, daß die Mitteilung der Angaben nur zu einem bestimmten Verwendungszweck erfolgt, der in der Zuständigkeit der Empfängerbehörde bzw. -stelle liegt und gesetzlich bestimmt ist. Außerdem ist festzulegen, daß es für den etwaigen Einsatz automatischer Datenverarbeitung zur Erfüllung der Mitteilungspflichten verordnungsmäßiger Regelungen bedarf.

Schließlich muß sichergestellt werden, daß bei einer Inkognito-Adoption Minderjähriger vom Standesbeamten kein Informationsweg zur Meldebehörde der bisherigen Verwandten führt, weil eine Mitteilungspflicht des Standesbeamten an die für den Wohnort der leiblichen Eltern zuständige Meldebehörde mit dem Offenbarungsverbot des § 1758 BGB nicht vereinbar ist. An welche Meldebehörde die Mitteilung über die Geburt zu richten ist, bedarf auch in den Fällen näherer Konkretisierung, in denen sich schon kurz nach der Geburt Anhaltspunkte dafür ergeben, daß das Kind für eine Adoptionsvermittlung in Betracht kommt, es also nicht in die Hauptwohnung der leiblichen Eltern bzw. Mutter aufgenommen, sondern in Adoptionspflege gegeben wird. Mit Rücksicht auf die Bestimmung des § 1747 Abs. 3 Satz 1 BGB, wonach die Einwilligung der Eltern bzw. der Mutter eines nicht-ehelichen Kindes in eine Adoption erst erteilt werden kann, wenn das Kind acht Wochen alt ist, sollte im Falle des Vorliegens derartiger Anhaltspunkte zunächst von einer Mitteilung an die für die Hauptwohnung der Eltern bzw. der Mutter eines nicht-ehelichen Kindes zuständige Meldebehörde abgesehen werden. Die Meldung an die zuständige Meldebehörde sollte dann erfolgen, wenn feststeht, ob und ggf. zu wem das Kind in Adoptionspflege gegeben wird.

4.10.3 Online-Anschluß der Polizei an das Melderegister

Nach § 31 Abs. 4 Hamburgisches Meldegesetz (HmbMG) dürfen an hamburgische Polizeidienststellen bestimmte Daten aus dem Melderegister durch automatisierten Abruf übermittelt werden. Dabei darf der Polizei der Abruf nur unter Verwendung des Namens oder von Namensteilen ermöglicht werden. Ein Abruf von Daten aller Einwohner, die unter einer bestimmten Anschrift gemeldet sind, ist nach dem Gesetz nur zulässig, wenn die Identität nicht auf andere Weise festgestellt werden kann.

Bisher ist ein online-Anschluß der Polizei an das Melderegister noch nicht verwirklicht worden. Allerdings habe ich von der Behörde für Inneres erfahren, daß die technischen Möglichkeiten für einen Direktzugriff der Polizei auf das Melderegister im automatisierten Verfahren im Laufe des Jahres 1989 geschaffen werden sollen. Derzeit wird daran gedacht, die vorhandenen POLAS-Bildschirme zu nutzen.

Seit der Einführung der Automation im Meldewesen, über die ich zuletzt in meinem 5. Tätigkeitsbericht (5.7.1, S. 60) berichtet habe, ist die frühere "Schlüssellösung" für die Polizei entfallen. Auskünfte aus dem Melderegister müssen deshalb gegenwärtig von der Polizei außerhalb der üblichen Dienstzeit über den telefonischen Bereitschaftsdienst des Einwohner-Zentralamtes eingeholt werden. Da ein solches Verfahren zu längeren Wartezeiten führen kann, wird aus polizeilicher Sicht ein online-Anschluß an das Melderegister immer drängender.

Ich muß an dieser Stelle allerdings darauf hinweisen, daß durch eine solche neue Technik auch zusätzliche Gefahren für den Bürger entstehen können (vgl. meine Ausführungen zur online-Übermittlung im 4. TB, 3.2, S. 11), da auch wirksame Zugriffssicherungen durch die dazu autorisierten Personen außer Kraft gesetzt werden können. Ich will niemandem derartige Absichten unterstellen. Dennoch darf nicht übersehen werden, daß damit der Polizei eine Technik an die Hand gegeben wird, die dem Grunde nach derartige Mißbräuche ermöglicht.

Umso wichtiger ist es, daß der Senat durch Rechtsverordnung regelt, welche technischen und organisatorischen Maßnahmen zur Sicherung gegen Mißbrauch getroffen werden sollten und wie die Zulässigkeit der Abrufe kontrolliert werden soll. Bisher ist mir nicht bekannt geworden, daß an einer solchen Rechtsverordnung gearbeitet wird.

Ich werde meine Zustimmung zu dem online-Anschluß u.a. erst dann erteilen können, wenn diese Rechtsverordnung auch tatsächlich vorliegt. Solange dies nicht der Fall ist, muß die Polizei in der bisherigen Weise weiter verfahren.

4.10.4 Novellierung des Melderechtsrahmengesetzes

Das Melderechtsrahmengesetz (MRRG) ist seit mehr als acht Jahren in Kraft und hat sich in dieser Zeit grundsätzlich bewährt. Allerdings hat sich mittlerweile ein Ände-

rungsbedarf gezeigt, der nicht zuletzt eine Konsequenz des Volkszählungsurteils des Bundesverfassungsgerichts ist. Die Datenschutzbeauftragten des Bundes und der Länder hatten bereits in einem Konferenzbeschluß vom 27./28. März 1984 darauf hingewiesen, daß das MRRG an die verfassungsrechtlichen Anforderungen angepaßt werden müßte. Sie hatten vor allem davor gewarnt, daß das Meldewesen die Funktion einer potentiell unbegrenzten Informationssammlung oder -bereitstellung übernimmt. Die damals gegebenen Hinweise gelten unverändert fort.

Der Bundesminister des Innern hat im November 1988 den Entwurf eines Gesetzes zur Änderung des MRRG den Innenverwaltungen der Länder zur Stellungnahme vorgelegt mit der Absicht, diesen Entwurf kurzfristig in das Bundeskabinett einzubringen. Gegenüber der Behörde für Inneres habe ich mich zur bevorstehenden Novellierung des MRRG geäußert und dabei im wesentlichen auf folgendes hingewiesen:

— In einer gutachterlichen Äußerung zu verfassungsrechtlichen Fragen des Entwurfs eines Meldegesetzes für das Land Berlin hatte Professor Dr. Benda im Jahre 1984 bezweifelt, daß die Regelungen zur Hotel- und Krankenhausmeldepflicht (§ 16 Abs. 2 und 3 MRRG) und die entsprechenden Bestimmungen in den Landesmeldegesetzen verfassungskonform sind. Das MRRG schreibt nämlich vor, daß Personen, die in einem Hotel oder einer Pension übernachten, handschriftlich Meldevordrucke auszufüllen und zu unterschreiben haben. Die Leiter solcher Beherbergungseinrichtungen haben "die ausgefüllten Meldevordrucke nach Maßgabe des Landesrechts für die zuständige Behörde bereitzuhalten oder dieser zu übermitteln". Als "zuständige Behörde" gelten in den Ländern die jeweiligen Landespolizeidienststellen.

  Desgleichen müssen bestimmte Daten über Personen, die in Krankenhäusern, Pflegeheimen oder ähnlichen Einrichtungen aufgenommen worden sind, vom Leiter dieser Einrichtungen in ein Verzeichnis eingetragen werden, das ebenfalls für die Landespolizeidienststellen bereitzuhalten ist.

  Ich teile die von Benda geäußerten verfassungsrechtlichen Zweifel, ob die mit der Hotel- und Krankenhausmeldepflicht verbundene zwangsweise Erhebung und Weitergabe personenbezogener Daten an die Polizei im überwiegenden Allgemeininteresse erforderlich ist. Deshalb habe ich sowohl in meinem 3. Tätigkeitsbericht (3.7.1.5, S. 53) als auch im Verlauf der Beratungen eines Gesetzentwurfs zur Änderung des Hamburgischen Meldegesetzes (HmbMG) im Jahre 1985 auf die Problematik hingewiesen und im Ergebnis die Streichung von Hotel- und Krankenhausmeldepflicht empfohlen. Weil die Länder durch das MRRG gebunden sind, habe ich letztlich — mit gewissen Einschränkungen — der jetzigen Fassung des § 27 HmbMG zugestimmt. Bei der nunmehr anstehenden Novellierung des MRRG besteht jedoch die Möglichkeit, die vorhandenen verfassungsrechtlichen Probleme zu lösen. Ein solcher Lösungsansatz ist allerdings mit dem Gesetzentwurf nicht vorgelegt worden. Vielmehr soll es im wesentlichen bei der bisherigen Praxis verbleiben.

  Ich erachte es jedenfalls für angemessen, die Diskussion über die Hotel- und Krankenhausmeldepflicht noch einmal bundesweit zu führen. Dabei würde sicherlich deutlich werden, daß die Vorschrift des § 16 Abs. 3 MRRG (Krankenhaus-Meldepflicht) noch weniger im überwiegenden Allgemeininteresse liegt als die Bestimmung des § 16 Abs. 2 MRRG (Hotel-Meldepflicht), zumal die von den Krankenhäusern geführten Verzeichnisse so gut wie nie für die polizeiliche Tätigkeit benötigt werden. Deshalb scheint mir ein Verzicht auf die Krankenhausmeldepflicht unbedingt erforderlich zu sein, während über die grundsätzliche Notwendigkeit einer Hotelmeldepflicht noch eingehender diskutiert werden sollte.

— Nach § 18 Abs. 1 MRRG darf die Meldebehörde an andere Behörden oder sonstige öffentliche Stellen unter bestimmten Voraussetzungen eine Reihe von Daten weitergeben, u.a. auch das Datum "Übermittlungssperre". Eine solche Übermittlungssperre wird von der Meldebehörde eingerichtet, wenn ein Bürger glaubhaft machen

kann, daß ihm oder einer anderen Person durch die Weitergabe seiner Daten eine Gefahr für Leben, Gesundheit, persönliche Freiheit o.ä. schutzwürdige Belange erwachsen können (§ 21 Abs. 5 MRRG).

Ich vertrete die Auffassung, daß das Merkmal "Übermittlungssperre" als akzessorisches, d.h. nicht eigenständiges Datum auch dann weitergegeben werden muß, wenn dies nicht ausdrücklich in der Rechtsvorschrift, die eine Übermittlung der sonstigen Daten anordnet, vorgeschrieben ist. Die Meldebehörde hat nämlich grundsätzlich dafür Sorge zu tragen, daß die Art und Weise, in der sie Daten übermittelt, nicht die Gefahr einer Persönlichkeitsverletzung eröffnet. Dies kann am besten durch die regelmäßige Weitergabe einer Übermittlungssperre erfolgen. Allerdings verkenne ich nicht, daß in bestimmten Fällen die Mitteilung der Übermittlungssperre keinen zusätzlichen Schutz des Betroffenen bewirkt, sondern sogar im Einzelfall zu einer Beeinträchtigung schutzwürdiger Belange führen könnte. Deshalb sollte § 18 MRRG neben der grundsätzlichen Verpflichtung zur Weitergabe des Datums "Übermittlungssperre" eine Ausnahmeregelung enthalten, die es zuläßt, unter genau umrissenen Bedingungen auf eine Mitübermittlung der Sperre zu verzichten.

4.11 Polizei

Seit meinem ersten Tätigkeitsbericht habe ich darauf hingewiesen, daß die Schaffung bereichsspezifischer gesetzlicher Grundlagen für die Datenverarbeitung der Polizei ein dringendes Anliegen nicht nur für den Datenschutz, sondern auch für die Polizei ist. Nachdem einige Gerichte dem Begehren von Bürgern auf Löschung ihrer in polizeilichen Informationssystemen gespeicherten Daten stattgegeben hatten, habe ich in den letzten beiden Tätigkeitsberichten (5. TB, 5.8 und 6. TB, 4.11) darauf aufmerksam gemacht, wie sich die Situation ständig zuspitzt und unter welchen Druck die parlamentarischen Gremien geraten werden, wenn nicht bald entsprechende Gesetzentwürfe zur Diskussion gestellt werden. Nach meinen ausführlichen Darstellungen in den letzten Tätigkeitsberichten (a.a.O.) läßt sich die Lage kurz wie folgt zusammenfassen: Grundrechtseingriffe ohne gesetzliche Grundlage sind nach der Rechtsprechung des Bundesverfassungsgerichts für eine Übergangszeit zulässig, um dem Gesetzgeber Gelegenheit zu geben, die Gesetzgebungslücke zu beseitigen. Während der Übergangszeit reduzieren sich die Befugnisse auf das, was für die Aufrechterhaltung der Funktionsfähigkeit staatlicher Einrichtungen unerläßlich ist. Übergangsfristen sind ihrer Natur nach nicht unbegrenzt. Sie können nach der Verfassungsrechtsprechung dann nicht mehr anerkannt werden, wenn der Gesetzgeber eine Neuregelung ungebührlich verzögert. In Anbetracht des seit dem Volkszählungsurteil des Bundesverfassungsgerichts verstrichenen Zeitraums dürfte die Übergangszeit in Hamburg spätestens mit Ablauf der derzeitigen Legislaturperiode enden.

Vor diesem Hintergrund sind in Berlin, Niedersachsen, Hessen, Bayern, Nordrhein-Westfalen und im Saarland Entwürfe für die Novellierung der Polizeigesetze erarbeitet worden. Auch der Bund will sich bemühen, durch einen nunmehr vorgelegten Entwurf für ein neues BKA-Gesetz, den Anforderungen des Bundesverfassungsgerichts an die Datenverarbeitung auch für die Polizei gerecht zu werden, soweit dies in seiner Gesetzgebungskompetenz liegt. Aus Hamburg läßt sich über solche Fortschritte leider immer noch nicht berichten. Der Innensenator hat lediglich erklärt, auch er halte ein neues Polizeirecht für dringend erforderlich. Ich muß allerdings in Anbetracht der Tatsache, daß die Legislaturperiode schon zur Hälfte abgelaufen ist, fragen, wie dieses schwierige — und wahrscheinlich auch kontroverse — Gesetzesvorhaben noch abgeschlossen werden soll, wenn nicht sehr bald ein entsprechender Entwurf vorgelegt wird.

4.11.1 Anforderungen an ein neues Polizeirecht

An den bis in das Jahr 1986 geführten Diskussionen um ein neues Polizeirecht habe ich mich auf der Grundlage der bis dahin vorliegenden Entwürfe für ein einheitliches Polizeigesetz (Musterentwurf) und für ein novelliertes hamburgisches SOG ständig beteiligt und darüber in meinen Tätigkeitsberichten Auskunft gegeben. Diese Diskus-

sionsbeiträge halte ich inhaltlich aufrecht, auch wenn die Regelungsversuche, auf die sie sich beziehen, nicht mehr aktuell sind und noch nicht abzusehen ist, wie ein neuer Gesetzentwurf aussehen wird. In Erwartung eines solchen Entwurfes will ich jedoch — teilweise über meine bisherigen Stellungnahmen hinaus — auf die folgenden, besonders kritischen Regelungsbereiche aufmerksam machen.

— Es liegt im Interesse des Vertrauens der Bürger in staatliche Institutionen und insbesondere in die Polizei, daß deren Arbeit grundsätzlich offen erfolgen und transparent sein muß. Der Einzelne muß erkennen können, wann er polizeiliches Handeln auslöst und wann seine Daten Eingang in polizeiliche Akten und Informationssysteme finden.

  Die heimliche Datenerhebung muß eindeutig Ausnahme bleiben.

  So sollte die Datenerhebung bei Dritten — sofern sie nicht ausnahmsweise im Interesse des Betroffenen liegt — nur zugelassen werden, wenn die Erfüllung polizeilicher Aufgaben ansonsten unmöglich ist.

  Der Einsatz spezieller polizeilicher Methoden zur heimlichen Datenerhebung wie V-Leute, verdeckte Ermittler, versteckte Ton- und Bildaufzeichnungsgeräte, Observationen, polizeiliche Beobachtung sowie Rasterfahndung darf — soweit diese Mittel im präventiven Bereich überhaupt in Betracht kommen — nur dann zugelassen werden, wenn tatsächliche Anhaltspunkte die Annahme begründen, daß dies zur Verhinderung erheblicher, im Gesetz klar umrissener Straftaten erforderlich ist. Sollte etwa an den Straftatenkatalog des § 100a StPO angeknüpft werden, bedürfte dieser angesichts seines Umfangs (über 80 Straftaten) vor der Übernahme in das Polizeirecht einer kritischen Überprüfung.

  Jede spezielle Datenerhebungsmethode ist gesondert zu regeln. Die Datenerhebung aus Wohnungen darf z.B. nur bei gegenwärtiger Gefahr für Leben und Gesundheit einer Person zugelassen werden. Die Grenzen der Befugnisse verdeckter Ermittler sind gesetzlich festzulegen. Alle heimlichen Datenerhebungen mit speziellen Erhebungsmethoden sind der richterlichen Anordnungsbefugnis vorzubehalten. Nur bei Gefahr im Verzuge können Ausnahmen zugelassen werden. Schließlich müssen die Betroffenen von der heimlichen Datenerhebung informiert werden, sobald dies ohne Gefährdung des Zwecks der Maßnahme geschehen kann.

— Die Berücksichtigung des informationellen Selbstbestimmungsrechts im Polizeirecht bedeutet, daß die Bedingungen der automatisierten Datenverarbeitung bei der Polizei unter angemessener Berücksichtigung der Gefahren für die schutzwürdigen Belange der Betroffenen gesetzlich festgelegt werden. Dazu gehört u.a. die Regelung, daß der Abruf von Daten auf die zuständigen Bediensteten zu beschränken ist, ebenso wie die Forderungen, daß durch automatisierte Verarbeitung keine unangemessene Verkürzung oder Verzerrung von Sachverhalten entstehen dürfen und daß die Herkunft und Richtigkeit der Informationen in Akten oder anderen Unterlagen nachweisbar sein muß.

  Daneben ist die vielfach erhobene Forderung zu realisieren, daß Daten über Kinder nur dann automatisiert gespeichert werden dürfen, wenn sie wiederholt erhebliche strafbare Handlungen begangen haben.

  Die Speicherung personengebundener Hinweise und Daten über äußere Merkmale muß auf die Fälle beschränkt werden, in denen dies zur Gefahrenabwehr und vorbeugenden Straftatenbekämpfung unerläßlich ist.

  Für welche Aufgaben und in welchem Umfang sich die Polizei an von Bund und Ländern gemeinsam geführten Dateien beteiligen darf, ist gesetzlich zu regeln.

— Im Gegensatz zur ständigen Praxis ist zu fordern, daß neu erhobene Daten in bereits vorhandenen Datenbeständen der Polizei nur abgefragt werden dürfen, wenn dies sowohl vom Zweck der Erhebung als auch vom Zweck der Speicherung

erfaßt wird. Ein Abgleich von Daten eines Störers kann danach nur insoweit zulässig sein, als dies zur Abwehr der Gefahr, die er verursacht hat, erforderlich ist. Der Abgleich von Daten sonstiger Personen muß auf die Fälle beschränkt werden, in denen sie auf gesetzlicher Grundlage in Anspruch genommen werden dürfen. Der Abgleich personenbezogener Daten mit dem Fahndungsbestand kann nur dann zulässig sein, wenn die gesetzlichen Voraussetzungen für eine Personenkontrolle vorliegen. Schließlich ist in den Polizeigesetzen zu regeln, ob und ggf. unter welchen Voraussetzungen die Polizei — über Einzelanfragen hinaus — ihren Datenbestand mit öffentlichen Registern (AZR, Melderegister, ZEVIS) abgleichen darf.

— Polizeibehörden erheben und speichern Daten zu den verschiedensten Zwecken. Neben den Daten, die für Strafverfolgungszwecke und zur Gefahrenabwehr erforderlich sind, gibt es Datensammlungen, die der Vorgangsverwaltung, Dokumentations-, Beweis- oder Ausbildungszwecken dienen. Diese Datensammlungen müssen grundsätzlich zur Gewährleistung der Zweckbindung voneinander abgeschottet werden. Im übrigen hat der Gesetzgeber festzulegen, für welche eng begrenzten Ausnahmen Daten aus verschiedenen Sammlungen sowie Daten, die der Polizei bei anderen Stellen zur Verfügung stehen (Ausländerzentralregister, Melderegister, Zentrales Verkehrsinformationssystem), zusammengeführt werden dürfen.

— Die Übernahme der in Strafermittlungsverfahren gewonnenen Informationen in Unterlagen und Dateien zur Gefahrenabwehr und zur vorbeugenden Bekämpfung von Straftaten ist nur bei Verdacht enumerativ aufzuführender Straftaten und einer verantwortbaren Prognose, daß nach Schwere, Art und Ausführung der Tat oder aufgrund der Persönlichkeit des Täters die Gefahr der Begehung weiterer erheblicher Straftaten besteht und die Daten für zukünftige Ermittlungen geeignet und erforderlich sind. Für bestimmte Straftaten, die gesetzlich zu benennen sind, ist das wohl von vornherein auszuschließen. Die Prognoseentscheidung ist aktenkundig zu machen. Die Übernahme von Daten aus Strafverfahren, die mangels hinreichenden Tatverdachts oder wegen geringer Schuld des Betroffenen eingestellt oder sonst beendet wurden oder in denen die Anklageerhebung mangels öffentlichen Interesses an der Strafverfolgung abgelehnt wurde, ist zu untersagen. Der Gesetzgeber hat die Polizei gesetzlich zu verpflichten, sich — sofern die Staatsanwaltschaften nicht selbst berichten — über den Ausgang von Strafverfahren zu informieren, damit eine Überprüfung des Datenbestandes vorgenommen werden kann.

— Dem heutigen Verständnis erweiterter polizeilicher Aufgaben entsprechend werden in der polizeilichen Praxis immer mehr Daten solcher Personen erhoben und gespeichert, die selbst nicht als Beschuldigte, Verdächtige oder Störer in Betracht kommen. Anzeigende, Zeugen, Hinweisgeber, Kontakt- und Begleitpersonen, Geschädigte und Gefährdete müssen mit der Speicherung ihrer Daten rechnen. Der Gesetzgeber wird zu entscheiden haben, welche dieser Daten unter welchen Voraussetzungen automatisiert verarbeitet werden dürfen. Dies sollte für Daten von Anzeigenden, Zeugen und Hinweisgebern im Gefahrenabwehrbereich die Ausnahme bleiben. Darüber hinaus sollte die Speicherung der Daten von Geschädigten nach Abschluß eines Strafermittlungsverfahrens sowie von Gefährdeten in polizeilichen Informationssystemen nur mit Zustimmung der Betroffenen zugelassen werden. Die Zulässigkeit der automatisierten Verarbeitung der Daten von Kontakt- und Begleitpersonen muß an die Verhinderung von erheblichen — im Gesetz aufzuzählenden — Straftaten geknüpft werden.

— Die Rechtsbindung der polizeilichen Datenverarbeitung darf nicht dadurch unterlaufen werden, daß von den Betroffenen eine Einwilligung eingeholt wird. Auch mit Einwilligung ist die Verarbeitung personenbezogener Daten durch die Polizei nur dann gerechtfertigt, wenn die Informationen zur Aufgabenerfüllung erforderlich sind und der Rahmen der durch Gesetz vorgegebenen Aufgabenstellung der Polizei nicht verlassen wird. Durch Gesetz ist nicht nur die Verwendung der mit Einwilligung erhobenen Daten festzulegen, sondern auch Form und Inhalt der gebotenen Aufklärung der Betroffenen. Darüber hinaus ist die Polizei zu verpflichten, Hinweise auf Rechtsgrundlagen und auf die Freiwilligkeit der Auskunft aktenkundig zu machen.

— Eines der Kernstücke unserer demokratischen Rechtsordnung ist das Recht der Bürger, sich zu versammeln und ihrer politischen Meinung Ausdruck zu verleihen. Die Bedeutung dieses Rechts muß der Datenerhebung durch die Polizei bei öffentlichen Versammlungen Grenzen setzen. Darauf hat das Bundesverfassungsgericht mehrfach hingewiesen. Deshalb ist zu fordern, daß die Datenerhebung bei oder im Zusammenhang mit öffentlichen Versammlungen nur bei Vorliegen konkreter Gefahren der Begehung von Straftaten zugelassen wird. Etwaige Bild- oder Tonaufzeichnungen sind unverzüglich nach der Versammlung zu vernichten, gespeicherte Daten zu löschen, soweit sie nicht für die Verfolgung von Straftaten benötigt werden. Eine Verwendung für andere Zwecke — auch Dokumentations-, Schulungs- oder wissenschaftliche Zwecke — ist auszuschließen.

— Geradezu unübersehbar ist inzwischen die zur Verfügung stehende Datenerhebungs- und Datenverarbeitungstechnik. Der Einsatz von Videogeräten (etwa für Sicherungs-, Verkehrslenkungs- und Überwachungsmaßnahmen), Tonaufnahmegeräten und Richtmikrophonen bedarf ebenso der rechtlichen Fundierung wie etwa die Verwendung von dezentralen Datenverarbeitungsanlagen, gegen deren Verwendung für kriminalpolizeiliche Zwecke und zur vorbeugenden Straftatenbekämpfung wegen des hohen Risikos bei der Datensicherheit erhebliche Bedenken bestehen. Sie sollten lediglich für die Vorgangsverwaltung, die Textverarbeitung und die nicht polizeispezifische Bürokommunikation zugelassen werden.

4.11.2 Einsatz von Personalcomputern

Unabhängig von meinen zuletzt beschriebenen Erwartungen an den hamburgischen Gesetzgeber habe ich im Berichtsjahr dem Einsatz von Personalcomputern auch zu kriminalpolizeilichen Zwecken zugestimmt, weil die Behörde für Inneres und die Polizei darauf hingewiesen haben, daß dies nur für einen Übergangszeitraum bis zur Umstellung der Großrechneranlage auf ein neues Betriebssystem erforderlich ist, und gleichzeitig zugesichert haben, ein den besonderen Risiken entsprechendes Sicherungskonzept in Abstimmung mit dem Datenschutzbeauftragten in die Praxis umzusetzen (vgl. 6. TB, 4.11.2). Dieses Sicherungskonzept ist inzwischen entwickelt und durch Verfügung des Polizeipräsidenten im Januar 1988 als verbindliche Regelung für den Einsatz von PC's bei der Polizei in Kraft gesetzt worden. Das Sicherungskonzept enthält detaillierte Regelungen zur Verfahrensfreigabe, zur Verfahrenskontrolle, zu den Aufgaben des Dienststellenleiters und den zu treffenden Sicherungsmaßnahmen. Ferner ist eine Verfahrensdokumentation verbindlich vorgeschrieben.

In dem Sicherheitskonzept ist darüber hinaus vorgesehen, daß den anwendenden Stellen ausschließlich Laufzeitverfahren mit einer geschlossenen Benutzeroberfläche (Bedienerführung) ohne Entwicklungswerkzeuge zu übergeben sind. Damit soll die Funktionstrennung zwischen programmierender Stelle und fachlich zuständiger Stelle — ein fundamentales Datenschutzprinzip — sichergestellt werden, da dann ein Datenmißbrauch die Zusammenarbeit von zwei verschiedenen Stellen voraussetzen würde.

Die Kooperationsbereitschaft der beteiligten Stellen in diesem Fall möchte ich besonders herausstellen. Mir scheint, daß auf diesem Weg ein vertretbarer Ausgleich der verschiedenen Interessen gelungen ist. Wenn die Verfügung des Polizeipräsidenten strikt eingehalten wird, dürften die von mir geplanten Kontrollen der dezentralen Datenverarbeitung keine gravierenden Mängel mehr ergeben.

4.11.3 Bildaufzeichnungen durch Polizei und Verfassungsschutz

Gegen Ende des Berichtsjahres habe ich mich um einen Überblick darüber bemüht, welche Möglichkeiten der Polizei und dem Verfassungsschutz derzeit zur Verfügung stehen, um offen oder heimlich personenbezogene Bilder aufzuzeichnen und zu speichern. Diese Bemühungen werde ich fortsetzen, zumal die Entwicklung insbesondere der Videotechnik ein Niveau erreicht hat, das eine inhaltliche Auswertung der aufgezeichneten Bilder und den Abgleich der so gewonnenen Informationen mit vorhandenen Datenbeständen in naher Zukunft ermöglicht. Dies vor allem macht es nach mei-

ner Auffassung dringend erforderlich, daß die jeweiligen Gesetzgeber im Rahmen ihrer Gesetzgebungskompetenz Zulässigkeit und Umfang von Bildaufzeichnung und -verwertung regeln, worauf ich schon an verschiedenen Stellen dieses Berichts hingewiesen habe.

4.11.4 Polizeieinsatzzentrale

Für die Polizeieinsatzzentrale ist ein neues leistungsfähiges und flexibles automatisiertes Informationssystem geplant, das unter der Bezeichnung "Hamburgisches Einsatzleitsystem Polizei (HELP)" arbeiten soll. Auch wenn das HELP in erster Linie der Einsatzlenkung dient und kein personenbezogenes Auskunftssystem ist, werden darin doch in großem Umfang personenbezogene Daten gespeichert. Die Organisation von HELP als Datenbank gestattet es, die gespeicherten Daten vielfältig miteinander zu verknüpfen und variabel auszuwerten.

4.11.4.1 Beschreibung von HELP

Für die Datei wurde mir im Berichtsjahr der Entwurf einer Errichtungsanordnung übersandt. Danach sollen nicht nur die Daten von Anzeigenden, Anrufern, Hinweisgebern, Veranstaltern, Anmeldern und Leitern polizeilich relevanter Veranstaltungen, sondern u.a. auch die von gefährdeten, vermißten und gesuchten Personen sowie von Polizeibeamten in ihren verschiedenen Funktionen gespeichert werden. Die in der Errichtungsanordnung aufgeführten "Personaldaten" (z.B. Name, Vorname, Anschrift, Telefon, Staatsangehörigkeit, Beruf, Titel usw.) können mit den übrigen Institutions-, Objekt-, Sach- und Einsatzdaten komfortabel verknüpft werden. Dadurch werden alle in HELP gespeicherten Daten — auch die Dateiabschnitte, die für sich genommen keinen Personenbezug aufweisen — zu personenbezogenen Daten i.S.v. § 4 Abs. 1 HmbDSG.

Ein besonderes Problem stellen die vorgesehenen "Freitext (FT)- felder" dar, die sich einer datenschutzrechtlichen Bewertung weitgehend entziehen. Während bei definierten Datenfeldern der Feldinhalt im Hinblick auf seine Form und Aussagekraft weitgehend vorgegeben ist, steht es bei den Freitextfeldern im Belieben des Anwenders, welche Eintragungen er vornimmt. Auch wenn eine gezielte Auswertung der FT-Felder bei HELP z.Z. nicht vorgesehen ist, kann auf die Inhalte dieser Felder über andere Suchkriterien (z.B. Einsatznummer) zugegriffen werden.

Das Datenbanksystem HELP dient neben der aktuellen Vorbereitung, Führung, Bearbeitung, Abwicklung und Auswertung von Einsätzen auch Zwecken der langfristigen Dokumentation. Der Entwurf der Errichtungsanordnung sieht vor, daß die Daten, die für den laufenden Betrieb nicht mehr erforderlich sind oder für die die Erfassungsvoraussetzungen entfallen, auszusondern bzw. zu löschen sind. Ausgesonderte Daten sind danach

— dem unmittelbaren, aktuellen Zugriff entzogen,

— aus Gründen der Dokumentation polizeilichen Handelns und Einsatzauswertung auf Langzeitspeicher zu übernehmen und nach Ablauf der Speicherfrist zu löschen.

Personenbezogene Daten sollen grundsätzlich eine Woche nach Eintrag oder Abschluß des Ereignisses, Einsatzes oder Vorganges ausgesondert werden. Die Speicherungsdauer ausgesonderter Daten auf Langzeitspeichern beträgt ein Jahr nach Aussonderung. Die Aussonderung der Daten soll in einem zweistufigen Verfahren erfolgen. Die ausgesonderten Daten werden automatisiert in sog. backup-Dateien überspielt. Die backup-Dateien sind zwar nicht auf denselben Magnetplatten wie die aktuellen Dateien gespeichert, werden aber genauso wie diese vom Datenbank-Managementsystem verwaltet. Erst wenn die für backup-Zwecke genutzten Magnetplatten die Speicherung weiterer Daten aus Kapazitätsgründen nicht mehr ermöglichen, werden Teile des backup-Datenbestandes auf Magnetband überspielt und dort bis zum Ablauf der Speicherfrist (ein Jahr nach Aussonderung aus dem aktuellen Datenbestand) gespeichert.

In der Errichtungsanordnung werden die durch das Datenbanksystem verwalteten backup-Dateien nicht gesondert aufgeführt, obwohl sie Bestandteil von HELP sind — zwar nicht inhaltsgleich, wohl aber strukturgleich zu bestimmten aktuellen Dateiabschnitten. Auf die in Plattendateien gespeicherten backup-Daten kann mit denselben Funktionen zugegriffen werden wie auf den aktuellen Datenbestand. Es ist also auch die Verwendung der flexiblen Abfragesprachen für dateiabschnittsweise oder dateiabschnittsübergreifende Auswertungen möglich. Darüber hinaus kann mit verschiedenen vorgefertigten Programmen auf die Datenbestände zugegriffen werden. Der Führungs- und Lagedienst der Polizei wird nach den Planungen auch bezogen auf die für Dokumentationszwecke gespeicherten backup-Daten ein umfassendes Zugriffs- und Auswertungsrecht haben.

An HELP werden die verschiedensten polizeilichen Dienststellen angeschlossen. Dafür soll ein sehr differenziertes System der Vergabe und Überprüfung von Zugriffsberechtigungen eingerichtet werden:

— Zugriffsberechtigungen nach Dateiabschnitten für die an HELP angeschlossenen Dienststellen,

— Verfügbarkeit von HELP-Kommandos (sowohl DISQUEL als auch programmierte Zugriffe) nach Funktionsgruppen innerhalb der Dienststellen,

— Zugriffsberechtigungen für die Abfragesprache DISQUEL nach Funktionsgruppen innerhalb der Dienststellen, differenziert nach Zugriffsarten (Lesen, Ändern, Hinzufügen, Löschen) und nach der Berechtigung, auf mit Sperrvermerk versehene Sätze zuzugreifen.

Die Zugriffsberechtigten werden nicht nur über zwei flexible Abfragesprachen, sondern darüber hinaus über eine große Anzahl vorprogrammierter Funktionen (Prozesse), die häufig auch auf mehrere Dateiabschnitte zugleich zugreifen (z.B. Hinzufügen von Datensätzen, Listendruck anstoßen usw.), verfügen.

Eine Protokollierung ist lediglich für schreibende und ändernde Zugriffe vorgesehen. Lesende Zugriffe (hierunter fallen auch differenzierte dateiübergreifende Auswertungen) sollen nicht technisch protokolliert werden. Dies wird damit begründet, daß bei Protokollierung lesender Zugriffe die Performance des Systems (Leistungsfähigkeit, insbesondere Antwortzeitverhalten) sich verschlechtern würde.

Das System soll eine POLAS/INPOL-Schnittstelle erhalten, die nach Auskunft der Polizei lediglich zur Kommunikation mit dem POLAS-System vom HELP-Arbeitsplatz aus dient. Die POLAS-Daten werden nicht auf automatisierte Weise in den HELP-Datenbestand eingespielt. Es soll weder eine programmunterstützte Überspielung der POLAS-Daten in den HELP-Datenbestand noch eine sonstige technische Unterstützung, etwa in Form einer entsprechend programmierten Funktionstaste geben. Die einzige Möglichkeit, daß POLAS-Daten in HELP-Datensätze übernommen werden, besteht nach Auskunft der Polizei darin, daß die Daten nochmals manuell vom entsprechenden Beamten in das Freitextfeld im HELP-Datensatz eingegeben würden. Schnittstellen zu weiteren Systemen sind nach Auskunft der Bfl nicht geplant.

4.11.4.2 Bewertung von HELP

Wie in allen bisherigen Verfahren, werden für die rechtliche Fundierung auch von HELP die §§ 163 StPO, 3 SOG und 53 OWiG genannt, obwohl sämtlichen Beteiligten klar ist, daß es sich dabei nicht um tragfähige Rechtsgrundlagen für die beabsichtigten Eingriffe in das informationelle Selbstbestimmungsrecht der Betroffenen handelt.

Auch die Rechtsprechung des Bundesverfassungsgerichts zu Grundrechtseingriffen ohne gesetzliche Grundlage während einer Übergangszeit (vgl. 4.11) kann für die Einführung eines so umfassenden Systems wie HELP in der bisher vorgesehenen Form nicht herangezogen werden. Diese verlangt nämlich, daß Grundrechtseingriffe in der Übergangszeit auf das zu beschränken sind, was für die Aufrechterhaltung der Funktionsfähigkeit staatlicher Institutionen unerläßlich ist. Eine überzeugende Begründung

dafür, daß das Gesamtsystem i.S.d. vorstehenden Rechtsprechung unerläßlich ist, liegt mir bisher nicht vor. Ohne sie wird mir eine Zustimmung zu HELP unmöglich gemacht.

Beim gegenwärtigen Stand der Verfahrensentwicklung sind darüber hinaus aus datenschutzrechtlicher Sicht schon jetzt folgende Forderungen zu erheben:

— Die Speicherung personenbezogener Daten ist auf einen unverzichtbaren Umfang zu reduzieren. Dies bedeutet im einzelnen:

  Die Daten von Anrufern u.ä. dürfen nur in den aktiven Datenbestand genommen werden und sind nach Abschluß des Einsatzes zu löschen. Dies gilt ebenso für die Daten von Veranstaltern u.ä.

  Die Daten von Gefährdeten und Funktionsträgern dürfen nur mit Zustimmung der Betroffenen, und zwar ausschließlich im aktiven Bestand gespeichert werden. Sie sind nach Wegfall der Voraussetzungen zu löschen. Zur Bestandspflege sind Prüfungs- bzw. Aussonderungstermine zu notieren.

— Wie schon jetzt, sind Fahndungsnotizen nach Erledigung der Fahndung zu löschen. Es ist sicherzustellen, daß statistische Auswertungen nur ohne Personenbezug stattfinden können.

  Auch die Daten von Polizeibeamten dürfen grundsätzlich nur mit deren Zustimmung gespeichert werden. Auf die besonderen Rechte der Personalräte wird in diesem Zusammenhang hingewiesen. Zur Bestandspflege sind Prüffristen zu notieren.

— Besondere datenschutzrechtliche Anforderungen sind an den Langzeitspeicher (LZS) zu stellen. Nach dem Entwurf der Errichtungsanordnung soll der Langzeitspeicher der Dokumentation gespeicherter Daten und der Einsatzauswertung dienen. Es muß daher geprüft werden, ob für diese Aufgaben sämtliche im Rahmen von HELP anfallenden Daten, insbesondere Daten mit Personenbezug, unterschiedslos in den LZS übernommen werden müssen. Die Notwendigkeit der laufenden Speicherung ist aus meiner Sicht zu verneinen für die Anrufer usw. sowie für gefährdete Personen.

  Die Polizei hat nach § 8 Abs. 1 HmbDSG die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um die Beachtung des Verarbeitungs- und Nutzungsverbotes sicherzustellen. Das vorgesehene Verfahren entspricht dieser Anforderung noch nicht, da der Führungs- und Lagedienst ein umfassendes Zugriffsrecht auch auf den Langzeitspeicher hat.

— Die für Dokumentationszwecke gespeicherten Daten sind aus dem aktuellen Datenbestand wirksam auszusondern. Sie sind als gesperrte Daten i.S.v. § 15 Abs. 2 HmbDSG anzusehen. Sie dürfen nicht mehr verarbeitet oder genutzt werden.

  Die Dokumentation polizeilichen Handelns muß auch organisatorisch von der aktuellen Einsatzsteuerung abgekapselt werden. Es bietet sich an, hierfür eine gesonderte Dokumentationsstelle einzurichten.

— Das Datenbanksystem HELP orientiert sich vollständig an den Erfordernissen der Einsatzlenkung. So wird — um möglichst kurze Reaktionszeiten zu erreichen — auf eine Protokollierung von Abfragen verzichtet. Die Notwendigkeit des Einsatzes flexibler Abfragesprachen wird damit begründet, daß eine auf den Einzelfall bezogene Programmierung zu aufwendig und unflexibel wäre und sich mit den Aufgaben der polizeilichen Einsatzlenkung nicht vereinbaren ließe.

  Die Langzeitspeicherung und die Auswertung von Daten für Dokumentationszwecke finden jedoch unter gänzlich anderen Rahmenbedingungen statt: Die Auswertungen dürften weder zeitkritisch sein noch unter dem Druck ständig variierender Auswertungswünsche stehen. Demgegenüber ist der LZS wegen seines Umfangs und der Speicherdauer datenschutzrechtlich weit bedeutsamer als der aktuelle Kurzzeitspeicher. Deshalb sollte beim LZS auf den Einsatz flexibler Abfragesprachen ver-

zichtet werden. Damit geprüft werden kann, ob auf den LZS nur bei Vorliegen der gesetzlichen Voraussetzungen des § 15 Abs. 2 Satz 4 HmbDSG zugegriffen wird, müssen hier alle lesenden Zugriffe protokolliert werden.

Da die Entwicklungsarbeiten für HELP noch nicht abgeschlossen sind, erwarte ich, daß diesen wichtigen datenschutzrechtlichen Bedenken noch Rechnung getragen wird. Eine Stellungnahme der Behörde für Inneres lag mir bei Redaktionsschluß zu diesem Bericht noch nicht vor.

4.11.5 Datenverarbeitung beim polizeilichen Staatsschutz

4.11.5.1 Bisherige Konsequenzen aus der Datenschutzkontrolle bei der Fachdirektion 7

In meinem letzten Tätigkeitsbericht (6. TB, 4.11.3.1) habe ich ausführlich über eine datenschutzrechtliche Prüfung bei der Staatsschutzabteilung der hamburgischen Polizei (FD 7) berichtet. Bei der Prüfung hatte ich festgestellt, daß die — die Speicherung einschränkenden — Regelungen der Bedienungsvorschriften häufig nicht beachtet worden waren. Außerdem habe ich die von den Datenschutzbeauftragten schon vor der Einführung von APIS vorgebrachte Kritik bestätigt gefunden, daß die Errichtungsanordnung für die von den polizeilichen Staatsschutzdienststellen des Bundes und der Länder betriebene Verbunddatei "PIOS-Innere Sicherheit (APIS)" den Sachbearbeitern vor Ort keine klaren Hinweise zur Entscheidung, ob ein Sachverhalt zu speichern ist, an die Hand gibt. So bestand und besteht die Gefahr, daß statt Erkenntnissen über polizeilich relevante Sachverhalte, die sich gegen die freiheitlich demokratische Grundordnung, den Bestand und die Sicherheit des Bundes oder der Länder und gegen die Amtsführung von Mitgliedern verfassungsgemäßer Organe richten, auch solche Handlungen in die Datei Eingang fanden und finden können, die nur ganz allgemein im Zusammenhang mit politischen Themen stehen. Ich habe diese Kritik mit einer Reihe von Beispielen belegt. Sie ist Mitte des vergangenen Jahres vom Leiter des hamburgischen Landesamtes für Verfassungsschutz in einem Aufsatz für eine juristische Fachzeitschrift bestätigt worden.

Inzwischen kann ich berichten, daß sämtliche in meinem letzten Tätigkeitsbericht herausgestellten Einzelfälle in APIS gelöscht sind.

Eine endgültige Stellungnahme zu meinem Prüfbericht, den ich der Behörde für Inneres und der Polizei immerhin im November 1987 übersandt habe, lag mir bei Abschluß dieses Berichts dagegen immer noch nicht vor. Diese Stellungnahme sollte insbesondere auf folgende Fragen eingehen:

— Entsprachen die bisherige Speicherungspraxis, die Vergabe der Prüffristen (speziell für Fälle von geringer Bedeutung) und die Überprüfungskriterien
  - dem vorgesehenen Zweck des APIS-Systems?
  - dem Wortlaut der APIS-Errichtungsanordnung?
  - den Weisungen der Behörde im Zusammenhang mit der Errichtungsanordnung?
  - den kriminalpolizeilichen Erfordernissen?

— Bestehen Differenzen zwischen den kriminalpolizeilichen Erfordernissen und dem Wortlaut der APIS-Errichtungsanordnung sowie den Weisungen der Behörde?

— In welchen Fällen sind Doppelspeicherungen in POLAS und APIS erforderlich bzw. in welchen Fällen ist eine POLAS-Speicherung ausreichend?

Statt einer Stellungnahme hat der Polizeipräsident in der Sitzung des Rechtsausschusses vom 12. September 1988, in der mein 6. Tätigkeitsbericht beraten wurde, vorgetragen, daß Hamburg auf Bundesebene eine Initiative ergriffen habe, die bestehenden Richtlinien zu APIS im einengenden Sinne zu konkretisieren. Unabhängig vom Ergebnis dieser Beratung werde der Hamburger APIS-Bestand schon jetzt anhand der eigenen restriktiven Vorstellungen überprüft. Das habe bisher dazu geführt, daß 35 % (etwa 430 Datensätze) der Speicherungen von Beschuldigten und Verdächtigen gelöscht worden seien.

Diese Information kam für mich völlig überraschend. Leider ließ sie mich im unklaren darüber,

— welche neuen Kriterien nun an die APIS-Speicherungen angelegt werden,

— unter welchen Voraussetzungen die Restspeicherungen bei den Beschuldigten und Verdächtigen aufrecht erhalten werden,

— welche Kriterien die gelöschten Datensätze nicht erfüllten.

Hierüber habe ich mit Schreiben vom 15. September 1988 um Aufklärung gebeten.

Aber auch diese Anfrage war bis Redaktionsschluß nicht beantwortet. Nunmehr habe ich der Behörde für Inneres eine letzte Frist bis zum 31.12.1988 gesetzt.

4.11.5.2 Speicherung von Volkszählungsgegnern

In meinem letzten Tätigkeitsbericht (4.11.3.2) hatte ich berichtet, daß von den ursprünglich im Zusammenhang mit der Volkszählung 1987 in APIS gespeicherten 110 Personendatensätzen 56 gelöscht waren, davon 51, die nur deshalb gespeichert waren, weil die Betroffenen Volkszählungsunterlagen beschädigt oder dazu aufgerufen hatten. Ich hatte angekündigt, die verbliebenen 54 Datensätze auf ihre Vereinbarkeit mit der Errichtungsanordnung für APIS zu überprüfen. Dies ist inzwischen geschehen. Danach ergibt sich folgendes Bild.

Die weit überwiegende Anzahl dieser Datensätze (33) betrifft Sachverhalte, in denen ein Straftäter nicht zu ermitteln war, so daß hier lediglich die Daten der geschädigten Personen gespeichert sind. Auf Anfrage hat mir die Behörde für Inneres dazu mitgeteilt, daß die Daten aus Unbekannt-Sachen so lange gespeichert bleiben müßten, wie die Verfolgungsverjährung (§ 78 StGB) noch nicht abgelaufen ist. Dies halte ich für ein sachgemäßes Kriterium. Es setzt aber voraus, daß entsprechend der differenzierten Verjährungsfristen auch differenzierte Löschungsfristen notiert werden. Dies ist bisher nicht geschehen. Darüber hinaus ist auch bei Unbekannt-Sachen zu prüfen, ob ein Sachverhalt vorliegt, der eine Speicherung in APIS rechtfertigt. Dies dürfte für die meisten der von mir überprüften Sachverhalte nicht zutreffen. Insoweit ist jedoch die Prüfung der Behörde für Inneres noch nicht abgeschlossen.

Von den übrigen Datensätzen sind inzwischen weitere vier im Hinblick auf meine Prüfungsbemerkungen gelöscht worden. Für weitere Fälle wurde im September 1988 eine Prüfung zugesagt, die aber offensichtlich immer noch nicht abgeschlossen ist.

4.11.6 Löschung von Daten über Suizidversuche

Bekanntlich hatte der Senat im Januar 1986 beschlossen, auf die Speicherung von Suizidversuchen in polizeilichen Informationssystemen in Zukunft zu verzichten und die zur Zeit noch gespeicherten Hinweise zu löschen. Da diese Daten nach Aussage der Behörde für Inneres nicht gesondert abrufbar sind, führt die Polizei die Löschung nur bei Gelegenheit eines Zugriffs aus anderem Grund auf einen entsprechenden Datensatz durch. So wird seit Mai 1986 verfahren. Eine Überprüfung im August des Berichtsjahres hat ergeben, daß bis zum 31. Juli 1988 der personengebundene Hinweis "Freitodgefahr" in 12.532 (!) Fällen in POLAS-Datensätzen und den dazugehörenden Kriminalakten bei Gelegenheit des Zugriffs gelöscht wurden. Ich werde die Löschungen weiter überwachen.

Es bleibt in diesem Zusammenhang darauf hinzuweisen, daß der Arbeitskreis II der Innenministerkonferenz im September 1988 beschlossen hat, den Hinweis "Freitodgefahr" weiter zu verwenden. Die hamburgische Praxis wird davon jedoch nicht berührt.

4.11.7 Polizei in der Zentralambulanz für Betrunkene (ZAB)

Im Mai 1986 hatte ich die ZAB einer datenschutzrechtlichen Kontrolle unterzogen. Eine zentrale Rüge aufgrund dieser Kontrolle war, daß von sämtlichen Patienten der ZAB Identifizierungsdaten erhoben und mit polizeilichen Informationssystemen abgegli-

chen wurden. Dies wurde durch einen Polizeiposten gewährleistet, der in der ZAB ständig Dienst verrichtete. Nunmehr hat die Behörde für Inneres mitgeteilt, daß der Polizeiposten in der ZAB zum 1. Oktober 1988 aufgelöst wurde. Ich werde zu gegebener Zeit noch einmal überprüfen, ob nunmehr der Patientendatenschutz in der ZAB gewährleistet ist.

4.12 Novellierung des Bundesverfassungsschutzes

Gegen Ende des Berichtsjahres hat die Bundesregierung Entwürfe für ein Bundesverfassungsschutzgesetz (BVerfSchG), ein MAD-Gesetz (MAD-G) und ein BND-Gesetz (BND-G) beschlossen. Diese Gesetze sind auch für Hamburg von Bedeutung, weil mit ihnen auch die Informationsbeziehungen von Bundes- und Landesbehörden, teilweise darüber hinaus von Landesbehörden untereinander geregelt werden sollen.

Mit den vorgelegten Entwürfen sollen die nach der Rechtsprechung des Bundesverfassungsgerichts erforderlichen bereichsspezifischen Rechtsgrundlagen für die Informationsverarbeitung der Sicherheitsbehörden geschaffen werden. So dringend die Beseitigung der bestehenden Regelungsdefizite auch ist, müssen sich neue Gesetze gerade im Sicherheitsbereich in besonderem Maße daran messen lassen, daß den Bürgern keine unverhältnismäßigen Eingriffe in ihre Freiheitsrechte zugemutet werden. So hat es das Bundesverfassungsgericht als eine elementare Funktionsbedingung des auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens bezeichnet, daß der einzelne die Entscheidungsfreiheit darüber behält, welche Handlungen er vornehmen oder unterlassen will. "Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Informationen dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten" (BVerfGE 65, 1/42 f.). Diesen Vorgaben werden auch die nunmehr vorgelegten Entwürfe nicht gerecht.

Auch der neueste Entwurf zur Novellierung des Bundesverfassungsschutzgesetzes verfolgt deutlich das Ziel, die bisherige Praxis der Datenverarbeitung beim Verfassungsschutz und des Datenaustausches mit anderen Behörden festzuschreiben oder gar auszuweiten, soweit es — vorgeblichen — Sicherheitsinteressen dienen könnte. Der Entwurf hält überwiegend daran fest, daß bei der Erfüllung der Aufgaben des Bundesamtes für Verfassungsschutz die vom Bundesverfassungsgericht geforderte Zweckbindung nicht gelten soll. Der von dem früheren Regierungsentwurf (1986) unternommene Versuch, einige Befugnisse des Verfassungsschutzes auf die Bereiche Spionage und Terrorismus zu beschränken, wird weitgehend wieder aufgegeben. Auch verzichtet der Entwurf auf eingrenzende Regelungen für Datenerhebung und Datenübermittlung des Bundesgrenzschutzes im Zusammenhang mit Amtshilfeersuchen der Nachrichtendienste. Würde der von der Bundesregierung vorgelegte Entwurf Gesetz, würde der Bürger weiterhin nicht wissen können, wer was wann und bei welcher Gelegenheit über ihn in Erfahrung gebracht hat.

4.12.1 Informationsverarbeitung

Da sich der zulässige Umfang der Informationsverarbeitung maßgeblich nach den Aufgaben der datenverarbeitenden Stelle bemißt, bedarf es einer abschließenden, möglichst genauen gesetzlichen Beschreibung dieser Aufgaben. Die im Entwurf verwendeten Begriffe, wie etwa "Bestrebungen gegen die freiheitlich-demokratische Grundordnung" oder "Gefährdung auswärtiger Belange" bleiben indessen hinter den Anforderungen, die an die Normenklarheit einer Vorschrift zu stellen sind, weit zurück. Für den einzelnen ist weiterhin nicht erkennbar, wann er die Schwelle von der Ausübung der

Grundrechte zur verfassungsfeindlichen Bestrebung überschreitet. Insbesondere bleibt unklar

— welchen Grad an organisatorischer Verfestigung Gruppierungen erreicht haben müssen, damit eine "Bestrebung" vorliegt und ob auch solche "Bestrebungen" beobachtet werden, die erkennbar nicht gegen die freiheitlich demokratische Grundordnung gerichtet sind, an denen aber Personen beteiligt sind, die an anderen gegen diese Grundordnung gerichteten Bestrebungen mitwirken;

— ob und ggf. in welchem Umfang Informationen über demokratische Organisationen gesammelt und gespeichert werden dürfen, die Gegenstand extremistischer Beeinflussung(sversuche) sind;

— ob die Beobachtung von nicht organisierten Einzelpersonen grundsätzlich ausgeschlossen ist bzw. wann, unter welchen Voraussetzungen und in welchen Grenzen sie zulässig sein soll.

Bei einer derartig vagen Umschreibung der Aufgaben wäre es umso notwendiger, die Voraussetzungen für die Erhebung, Speicherung und sonstige Verwendung personenbezogener Daten je nach dem, welche seiner ganz unterschiedlichen Aufgaben (Extremismusbeobachung, Spionageabwehr, Mitwirkung an Sicherheitsüberprüfungen etc.) der Verfassungsschutz wahrnimmt, differenziert, präzise und für den Bürger transparent zu regeln. Auch dies ist aber nicht der Fall. Ich vermisse insbesondere Regelungen darüber, ob und ggf. in welchem Umfang, für welche Zwecke und mit welchen Speicherungsfristen Daten über Unverdächtige und unbeteiligte Personen erhoben und gespeichert werden dürfen.

Darüber hinaus wird die Informationsverarbeitung des Verfassungsschutzes nicht wirklich bereichsspezifisch geregelt. Da der Entwurf nicht nach verschiedenen Aufgabengebieten des Verfassungsschutzes differenziert, wird dem Verfassungsschutz vielmehr eine Art Generalbefugnis erteilt. Es müßte demnach sehr viel klarer geregelt werden, unter welchen Voraussetzungen welche Arten von Dateien eingerichtet werden dürfen und in welchen Zusammenhängen welche Textzusätze gespeichert werden dürfen. Es müßte sichergestellt werden, daß in den Dateien die für die Bewertung und Überprüfung von Textzusätzen maßgeblichen Unterlagen angegeben werden. Schließlich sollte klargestellt werden, daß in Textdateien nur Daten über solche Personen gespeichert werden dürfen, die selbst im Verdacht stehen, eine der im Gesetzentwurf aufgezählten Straftaten zu planen, zu begehen oder begangen zu haben.

Auch der neue Entwurf regelt lediglich die Speicherung personenbezogener Daten in Dateien, obwohl die Fortschritte der Informationsverarbeitung es immer leichter möglich machen, auch komplexe Datensammlungen — bestehend aus Akten, Dateien und anderen Unterlagen — gezielt mit Hilfe automatischer Verfahren zu erschließen.

Die für das BfV vorgesehene Befugnis, automatisiert oder herkömmlich geführte "amtliche Register", d.h. alle derartigen Register, einzusehen, wenn die Informationen nicht aus allgemein zugänglichen Quellen oder nur mit unverhältnismäßigem Aufwand oder nur durch eine den Betroffenen stärker belastende Maßnahme erhoben werden können, ist in diesem Umfang nicht hinnehmbar. Dies würde bedeuten, daß das BfV selbst für Zwecke der Extremismusbeobachtung eine Art "Rasterfahndung" in Form der Durchsicht aller amtlich geführten Register betreiben könnte.

Weiterhin nicht hinreichend beachtet wird der Grundsatz, daß die Verwendung von personenbezogenen Daten grundsätzlich auf den Zweck beschränkt ist, für den sie erhoben werden (Zweckbindungsgebot). So darf jede Behörde oder öffentliche Stelle grundsätzlich dem BfV alle Daten übermitteln, wenn nach ihrer Auffassung tatsächliche Anhaltspunkte dafür bestehen, daß die Übermittlung für die Erfüllung der Aufgaben des BfV erforderlich ist und sie entgegenstehende Übermittlungsverbote nicht zu erkennen vermag. Innerhalb des BfV darf jede Information unabhängig von ihrer Herkunft für jede Aufgabe verwendet werden. Das BfV darf grundsätzlich alle Informationen an andere Behörden, ja selbst an private Stellen übermitteln. Die nunmehr vorge-

sehenen Übermittlungsverbote reichen vor allem deshalb nicht aus, weil das BfV nicht ausdrücklich verpflichtet wird, entgegenstehende schutzwürdige Belange zu ermitteln.

Weiter fehlen befriedigende Löschungsregelungen. Abgesehen davon, daß die Löschung von Daten in Akten nicht einmal erwähnt wird, ist zu fordern, daß schon im Gesetz Regelfristen für die Überprüfung und Löschung der verarbeiteten Daten festzulegen sind. Dabei muß zwischen den einzelnen Aufgabenbereichen unterschieden werden.

4.12.2 Nachrichtendienstliche Mittel

Der Versuch, bei der Regelung des Einsatzes von nachrichtendienstlichen Mitteln mehr Präzision zu schaffen, ist im Ansatz stecken geblieben. Unklar ist insbesondere, welche rechtlichen Grenzen dem Einsatz nachrichtendienstlicher Mittel gesetzt sind. Vorgänge in der jüngsten Zeit lassen es geboten erscheinen klarzustellen, daß der Einsatz nachrichtendienstlicher Mittel Verstöße gegen Straftatbestände auf keinen Fall rechtfertigt, wenn Rechte Privater tangiert werden.

Auch fehlt bislang die Klarstellung, daß sich der Einsatz nachrichtendienstlicher Mittel grundsätzlich nur gegen denjenigen richten darf, der selbst in Verdacht steht, die vom Verfassungsschutz beobachteten Bestrebungen oder Tätigkeiten auszuüben. Soweit beim Einsatz nachrichtendienstlicher Mittel Informationen über andere Personen anfallen, sollte entsprechend dem G-10-Gesetz ein Verwertungsverbot statuiert werden.

Ferner sollten beim Einsatz nachrichtendienstlicher Mittel zum Schutz des Betroffenen — über die jetzt vorgesehene Unterrichtung der Kommission nach § 9 Abs. 2 G-10-Gesetz hinaus — zusätzliche Schutzvorkehrungen eingebaut werden. Um dem Betroffenen die Möglichkeit zu geben, sich gegen eine mögliche Verletzung seiner Rechte zur Wehr zu setzen, ist er — jedenfalls bei schweren Eingriffen — über den Einsatz nachrichtendienstlicher Mittel zu informieren, sobald eine Gefährdung des Zwecks der Maßnahme ausgeschlossen werden kann. Auch muß die Kontrolle durch die unabhängigen Datenschutzbeauftragten gewährleistet sein.

4.12.3 Trennungsgebot

Das Vorhaben, den Austausch von Informationen in einem eigenen Gesetz — ursprünglich Zusammenarbeitsgesetz (ZAG), dann Verfassungsschutzmitteilungsgesetz (VerfSchMiG) genannt — zu regeln, hat der Bundesinnenminister nunmehr aufgegeben und die vorgesehenen Regelungen in das BVerfSchG integriert. Inhaltliche Änderungen, die der bisher vorgebrachten Kritik Rechnung tragen, sind leider kaum feststellbar. Auch der jetzt vorgelegte Entwurf zieht nicht die gebotenen Konsequenzen aus dem Trennungsgebot für Polizei und Verfassungsschutz, das als eine der Konsequenzen aus demokratiefeindlicher Machtzusammenballung im NS-Staat in unsere Rechtsordnung eingeführt wurde. Ziel dieses aus dem Rechtsstaatsprinzip zwingend abzuleitenden Trennungsgebotes ist nicht nur die rein organisatorische Schaffung zweier unterschiedlicher Behörden für Aufgaben der Polizei und des Verfassungsschutzes. Seine materiell-inhaltliche Bedeutung besteht im Zeitalter der automatisierten Datenverarbeitung vielmehr auch darin, daß durch die Verteilung polizeilicher Befugnisse auf die eine und nachrichtendienstlicher Befugnisse auf die andere der beiden Behörden auch eine Bündelung der mit diesen unterschiedlichen Befugnissen gewonnenen Informationen vermieden werden soll.

Dieses Ziel wird von den in Aussicht genommenen Übermittlungsvorschriften verfehlt. Der Austausch der jeweils mit spezifischen Befugnisnormen gewonnenen Informationen führt dazu, daß das Trennungsgebot von einem Prinzip der Machthemmung zu einem Instrument möglichst effektiver Arbeitsteilung degeneriert. Der Entwurf verpflichtet nicht einmal den Datenempfänger, die übermittelten Daten nur für den Zweck zu verwenden, zu dem sie ihm übermittelt worden sind, und er läßt auch die Weiterübermittlung von Daten über mehrere Stationen zu, ohne daß es auf den Zweck der jeweiligen Übermittlungen ankäme. Würde der jetzige Entwurf Gesetz, bliebe es dabei,

daß sich Nachrichtendienste und Polizeien des Bundes und der Länder in Angelegenheiten des Staats- und Verfassungsschutzes beim Informationsaustausch wie Abteilungen ein und derselben Behörde verhalten könnten.

Informationen, die im Rahmen von Telefonüberwachungsmaßnahmen gewonnen werden, sollen jetzt nur noch unter Einschränkungen an das BfV übermittelt und von diesem verwertet werden dürfen. Ergänzend müßte sichergestellt werden, daß die verfahrensrechtlichen Sicherungen sowie die Benachrichtigungspflicht nach der StPO nicht unterlaufen werden. Aber auch für Daten, die die Polizei bei Hausdurchsuchungen oder durch den Einsatz von V-Leuten, verdeckten Ermittlern oder technischen Geräten, durch polizeiliche Beobachtung oder längerfristige Observationen gewonnen hat, müssen einschränkende Verwertungsregelungen geschaffen werden. Weiter ist klarzustellen, daß es nicht Aufgabe der Polizei sein kann, "Zufallsfunde" zu sammeln und weiterzugeben, die ihr bei Gelegenheit der Erfüllung ihrer Aufgaben bekannt werden, ohne für ihre eigentliche Aufgabenerfüllung erforderlich zu sein. Die Amtshilfe der Grenzpolizeien für den Verfassungsschutz muß einschränkend geregelt werden.

Angesichts einer polizeilichen Praxis, die immer mehr dazu übergegangen ist, Daten auch über "andere Personen" als nur Verdächtige und Beschuldigte zu sammeln, ist sicherzustellen, daß die Nachrichtendienste nur unter besonderen Einschränkungen an polizeilichen Vorfeldermittlungen partizipieren können.

Für die Einrichtung von automatisierten Direktabrufverfahren zwischen Polizeibehörden und Nachrichtendiensten ist ein Bedürfnis nicht dargelegt. Wegen der damit verbundenen massiven Durchbrechung des Trennungsgebotes muß die entsprechende Erlaubnis ersatzlos gestrichen werden.

4.12.4 Auskunft

Schließlich sollte die Behandlung von Auskunftsersuchen der Bürger bereichsspezifisch im Bundesverfassungsschutzgesetz und nicht — wie bisher — im Bundesdatenschutzgesetz geregelt werden. Eine schematische Ablehnung solcher Ersuchen — auch wenn keine Ausforschungsgefahr besteht — ist rechtsstaatlich nicht zu vertreten. Stattdessen muß der Gesetzgeber eine differenzierte Regelung schaffen.

Die Auskunft ist in aller Regel zu erteilen, wenn die Speicherung nur auf einer Sicherheitsüberprüfung beruht. Im übrigen bedarf es einer Abwägung im Einzelfall. Bei einer Auskunftsverweigerung sind die Gründe im einzelnen zu dokumentieren. Die Bearbeitung von Auskunftsersuchen muß getrennt von anderen Informationssammlungen erfolgen. Die Tatsache der Antragstellung darf nicht zum Nachteil der Betroffenen verwertet werden.

4.13 Justiz

4.13.1 Stand der Gesetzgebung

Auch für die Justizverwaltung, für die Gerichte und die Staatsanwaltschaft, aber auch für weite Teile des Strafvollzugs stellt sich immer drängender das Problem der gesetzlichen Grundlagen für die Eingriffe in das informationelle Selbstbestimmungsrecht der Betroffenen. So hat — um ein Beispiel zu nennen — das Oberlandesgericht Frankfurt im Juli 1988 entschieden, daß für die Führung der Zentralen Namenskarteien der Staatsanwaltschaften (in Hamburg: Zentralkartei) gesetzliche Grundlagen erforderlich sind, die derzeit nicht bestehen. Diese Karteien dürften zwar für eine Übergangsfrist (vgl. dazu 4.11.1) weiter betrieben werden. Die Übergangsfrist laufe jedoch mit dem Ende der laufenden Legislaturperiode für den Bundestag, mithin 1990, aus.

Um so erstaunlicher ist, mit wie wenig Nachdruck die notwendigen Gesetzesvorhaben betrieben werden. Über einige aktuelle Vorhaben hatte ich im letzten Tätigkeitsbericht (6. TB, 4.13.1 — 4.13.2, 4.14.1.1 — 4.14.1.3) ausführlich berichtet. Es ist mir leider nicht möglich, nunmehr nach Ablauf eines weiteren Jahres von erkennbaren Fortschritten zu berichten. Es werden zwar hin und wieder neue Diskussionsergebnisse vorgelegt; von

einer an sich erforderlichen zügigen Gesetzgebungsarbeit kann jedoch keine Rede sein. Bei dieser Sachlage versage ich es mir, nochmals auf Einzelheiten einzugehen, die überwiegend nur Wiederholungen früherer Berichte sein könnten.

4.13.2 Technikeinsatz

Im Gegensatz zu den fehlenden Rechtsgrundlagen stehen die Bemühungen, in den verschiedenen Bereichen der Justiz verstärkt die Möglichkeiten der automatisierten Datenverarbeitung zu nutzen. Bis zum Ende des Berichtsjahres waren bei den Gerichten der Finanz-, der Verwaltungs- und der ordentlichen Gerichtsbarkeit nach den Planungen der Justizbehörde 54 dezentrale Datenverarbeitungsanlagen im Einsatz. Dabei stößt die Technik in einen Bereich vor, in dem die potentiellen Anwender bisher nur unzureichend auf sie vorbereitet wurden. Die bisher geführten Gespräche und eine Prüfung beim Verwaltungsgericht (s. 4.13.1.2) haben gezeigt, daß seitens der Justizbehörde noch sehr viel Aufwand erforderlich ist, um auf Dauer eine ordnungsgemäße Datenverarbeitung zu gewährleisten.

Aus der Sicht des Datenschutzbeauftragten muß der Einsatz von Datenverarbeitungstechnik bei den Gerichten danach unterschieden werden, ob sie Verwaltungszwecken dienen oder direkt im Rahmen der Rechtsprechungstätigkeit der Richter nutzbar gemacht werden soll. Letztere Anwendung unterliegt gem. § 20 Abs. 2 HmbDSG nicht der Kontrolle durch den HmbDSB. Dies bedeutet jedoch nicht, daß die Richter bei ihrer Datenverarbeitungstätigkeit nicht die rechtlichen Vorgaben des Grundgesetzes und des Hamburgischen Datenschutzgesetzes zu beachten hätten, wie noch auszuführen sein wird.

4.13.2.1 Datenverarbeitung in den Verwaltungen des Landgerichts und des Amtsgerichts

Im November habe ich mit dem Landgericht, dem Amtsgericht und der Justizbehörde ein erstes Gespräch über die bei diesen Gerichten schon vorhandene und geplante Technikunterstützung der Gerichtsverwaltungstätigkeit geführt. Dabei hat sich gezeigt, daß die automatisierte Datenverarbeitung in der Gerichtsverwaltung vielfältige Anwendung finden kann. Das beginnt bei der Führung der Geschäftsverteilungspläne und geht über Eingangs- und Erledigungsstatistiken bis hin zu Raumbelegungsplänen. Aber auch Anwaltsverzeichnisse und Schöffenlisten können automatisiert geführt werden. Dabei können sich die Gerichte zum Teil auf ältere — für die konventionelle Datenverarbeitung gedachte — Rechtsvorschriften stützen (vgl. etwa §§ 21e Abs. 6, 44 GVG, § 31 BRAO); sie müssen allerdings zumindest durch verbindliche Verwaltungsvorschriften, die den Besonderheiten und Gefahren der automatisierten Verarbeitung Rechnung tragen, ergänzt werden. Darüber hinaus sollten die Betroffenen in geeigneter Form informiert werden, wenn eine Umstellung von konventioneller in automatisierte Datenverarbeitung erfolgt, es sei denn, eine Datenverarbeitung ist ohnehin nur mit ihrer Einwilligung zulässig. Soweit persönliche Daten der Bediensteten verarbeitet werden sollen, wird noch zu klären sein, wie durch besondere Schutzmaßnahmen unzulässige Zweckdurchbrechungen verhindert werden können. Ich möchte an dieser Stelle hervorheben, daß sich die Verantwortlichen beider Gerichte nach meinem Eindruck den Problemen des Datenschutzes offen und sensibel widmen, so daß zu erwarten ist, daß in diesem Bereich ein angemessener Ausgleich zwischen den Bedürfnissen der Verwaltung und den schutzwürdigen Belangen der Betroffenen gelingt.

4.13.2.2 Prüfung der Datenverarbeitung beim Verwaltungsgericht

Im Oktober 1987 hat mich die Justizbehörde davon in Kenntnis gesetzt, daß zur rationelleren Eingangs- und Verfahrensbearbeitung von Verfahren nach § 80 VwGO im Zusammenhang von Heranziehungsbescheiden des Statistischen Landesamtes nach dem Volkszählungsgesetz der Einsatz eines PC-Mehrplatzsystems Siemens MX 2 mit 4 Bildschirmen sowie der Aufbau einer Personen- und Verfahrensdatei geplant sei. Nach meiner vorläufigen Stellungnahme und Hinweisen auf die zu treffenden Datensicherungsmaßnahmen teilte die Justizbehörde Mitte Juni 1988 mit, daß die vorerwähnte

Technik nunmehr zu dem angegebenen Zweck eingesetzt werde. Diesem Schreiben war eine Dienstanweisung des Verwaltungsgerichts beigefügt, in der die nach § 16 HmbDSG getroffenen organisatorischen und technischen Maßnahmen zur Sicherstellung des Datenschutzes festgelegt waren. In den Kernaussagen, die mit meinen Forderungen übereinstimmten, heißt es in dieser Verfügung:

— Es werden nur Programme verwendet, die von der Justizbehörde entwickelt und nach gemeinsamer Prüfung mit dem Verwaltungsgericht freigegeben worden sind.

— Über die beweglichen Datenträger ist ein Bestandsverzeichnis zu führen. Das Einbringen von nicht protokollierten Datenträgern ist verboten.

— Die Benutzer haben nur über differenzierte Benutzeridentifikationen und eigenes Paßwort Zugang zum System. Für die Vergabe sind die Systembetreuer verantwortlich. Paßworte dürfen an andere Personen oder Benutzer nicht weitergegeben werden.

— Der Datenaustausch oder die Übermittlung der für die Abwicklung der Volkszählungsverfahren gespeicherten Daten zu anderen Verfahren oder Behörden ist verboten.

Etwa zeitgleich mit dem Schreiben der Justizbehörde erhielt ich die Eingabe eines Bürgers, der sich mit einem Antrag beim Verwaltungsgericht gegen Maßnahmen des Statistischen Landesamtes zur Erzwingung der Angaben zur Volkszählung gewandt hatte und dem kurz darauf eine ablehnende Entscheidung des Gerichts förmlich zugestellt worden war. Da sich der Petent die Abgabe des Volkszählungsbogens vom Statistischen Landesamt hatte schriftlich quittieren lassen und diese Quittung auch seinem Antrag beim Gericht beigefügt hatte, bat er das Gericht um Aufklärung. Dieses teilte ihm mit, eine Überprüfung habe ergeben, daß die zuständige Kammer die zugestellte Entscheidung weder getroffen habe noch treffen werde. Sie sei irrtümlich durch die Datenverarbeitungsanlage ausgedruckt worden.

Dieser Vorgang war für mich Anlaß, die Datenverarbeitung beim Verwaltungsgericht einer datenschutzrechtlichen Kontrolle zu unterziehen. Immerhin war die "ergangene" Entscheidung durch nichts als "Nicht-Entscheidung" zu erkennen. Sie war darüber hinaus förmlich durch Postzustellungsurkunde dem Petenten zugestellt worden. Zwar konnte der Vorgang durch die anschließende Prüfung nicht vollständig aufgeklärt werden — möglicherweise lag ein Bedienungsfehler vor, nicht auszuschließen ist aber auch, daß es sich um einen Organisationsmangel handelte. Gleichwohl mußte ich nicht nur erhebliche Mängel bei der Datenverarbeitung des Gerichts feststellen, sonderen auch zur Kenntnis nehmen, daß mir eine andere Technik gemeldet worden war, als tatsächlich eingesetzt wurde — nämlich ein Abteilungsrechner des Typs MX-500/20 mit 6 Arbeitsplätzen.

Zu den wichtigsten Mängeln im einzelnen:

— Entgegen der Festschreibung in der Dienstanweisung wurden nicht von der Justizbehörde entwickelte und freigegebene Programme verwendet. Programmierungsarbeiten wurden auch vom Gericht vorgenommen, weil — so das Verwaltungsgericht — die vorgegebenen Programme teilweise nicht funktionierten. Durch diese Art der Vorgehensweise waren schon die Grundvoraussetzungen für eine ordnungsgemäße Datenverarbeitung nicht gegeben.

— Während der Prüfung war es möglich, unter einer Kennung, deren genaue Bedeutung dem Systemverantwortlichen gar nicht bekannt war, in das System einzudringen und sogar die Berechtigung zur Ausführung von Betriebssystemkommandos zu erlangen. Dies stellt eine erhebliche Schwachstelle dar, denn die datenverarbeitenden Stellen haben bei der technischen Datensicherung vor allem darauf hinzuwirken, daß die gespeicherten Daten nicht durch Unbefugte genutzt oder verändert werden können.

— Im Bestand der beweglichen Datenträger fanden sich nicht registrierte Disketten und Magnetbandkassetten. Obwohl sich kein Anhaltspunkt dafür ergeben hat, daß

ein Datenmißbrauch vorgekommen oder beabsichtigt war, ist der Sachverhalt doch gravierend.

Das aus datenschutzrechtlicher Sicht bedeutendste Risiko beim Einsatz von Personalcomputern ist der Datenbestand auf beweglichen Datenträgern. Praktisch unbemerkt können große Datenmengen vom Arbeitsplatz entfernt und in sehr kurzer Zeit anderweitig kopiert werden, wenn dem nicht durch ein möglichst dichtes Datensicherungskonzept entgegengewirkt wird. Dazu gehört nicht nur eine ständige Aufsicht über die registrierten Datenträger, sondern auch die Einhaltung und Überwachung des Verbots, nicht registrierte Datenträger in die Arbeitsabläufe einzubringen.

Nachdem ich dem Verwaltungsgericht und der Justizbehörde meinen Prüfbericht übersandt und darauf hingewiesen hatte, daß wegen der Art der Mängel auch eine förmliche Beanstandung gem. § 21 HmbDSG erwogen werden müßte, wurde ich von der Reaktion völlig überrascht. Mir wurde vorgeworfen, meine datenschutzrechtliche Bewertung sei überzogen, man habe Mühe, sachliche Gründe für die Ankündigung einer förmlichen Beanstandung zu sehen und in meinem Bericht sei selbst ausgeführt, die festgestellten Mängel ließen sich dadurch vermeiden, daß sich die Justizbehörde und das Verwaltungsgericht an die selbst gegebenen Regeln hielten. Eine solche Stellungnahme kann ich nur als Ausdruck eines mangelnden Datenschutzbewußtseins werten. Natürlich lassen sich Verstöße durch Einhaltung der Regeln vermeiden, aber es liegt nicht im Ermessen der datenverarbeitenden Stellen, sie zu beachten oder nicht, nur weil es — nach Abstimmung mit dem Datenschutzbeauftragten — selbst gegebene sind. Dienstanweisungen und andere Verwaltungsvorschriften haben im Innenverhältnis die gleiche Funktion wie Gesetze im Außenverhältnis. Sie sind zu beachten und dies vor allem dann, wenn sie dem Schutz von Grundrechten dienen.

Ich habe deshalb den Justizsenator gebeten, durch geeignete Maßnahmen sicherzustellen, daß Datenschutzvorschriften vom Verwaltungsgericht in Zukunft besser beachtet werden. Von einer Beanstandung gegenüber dem Senat habe ich Abstand genommen, weil die beteiligten Stellen zugesichert haben, die bisher festgestellten Mängel zu beseitigen.

4.13.2.3 Personalcomputer für Richter

Soweit ich an Gesprächen beteiligt war, die die Benutzung von Personalcomputern durch Richter zum Gegenstand hatten, ging es ausschließlich um die Feststellung der Justizbehörde und der Gerichtsverwaltungen, diese Datenverarbeitungsanlagen unterlägen nicht der Kontrolle durch den Hamburgischen Datenschutzbeauftragten und der Einsatz privater PC's dürfe wegen der richterlichen Unabhängigkeit nicht eingeschränkt oder gar verboten werden.

Ob die Reduzierung der Diskussion auf diese Fragestellung dem Thema angemessen ist, müssen die Betroffenen selbst entscheiden. So hielte ich es durchaus für erörterungsbedürftig, ob nicht der richterlichen Unabhängigkeit langfristig durch die vom massenhaften Einsatz automatisierter Datenverarbeitung erzwungene Standardisierung auch richterlicher Entscheidungen eine wirkliche Gefahr droht und durch welche Maßnahmen dem möglicherweise begegnet werden könnte.

Die vorerwähnte Feststellung halte ich darüber hinaus in dieser Allgemeinheit nicht für zutreffend. Gem. § 20 Abs. 1 HmbDSG unterliegen die Gerichte der datenschutzrechtlichen Kontrolle dann, wenn sie in Verwaltungsangelegenheiten tätig werden. Der Hamburgische Datenschutzbeauftragte hat mithin zu überprüfen, ob auf den "Richter-PC's" nicht auch Verwaltungsaufgaben erledigt werden. Ist dies der Fall, gelten die normalen Kontrollmaßstäbe.

Auch die Einschätzung, die Nutzung privater PC's durch Richter für dienstliche Zwecke könne wegen der richterlichen Unabhängigkeit nicht untersagt oder unter einen Genehmigungsvorbehalt gestellt werden, hat mich bisher noch nicht überzeugt. Dies bedarf aus meiner Sicht noch weiterer Erörterungen.

Erforderlich dagegen dürfte sein, den Richtern die Verarbeitung von Verwaltungsdaten auf privaten PC's zu untersagen.

Im übrigen ist darauf hinzuweisen, daß unabhängig von einer Datenschutzkontrolle selbstverständlich auch die Richter den Anforderungen an eine Datenverarbeitung, wie sie sich nach der Rechtsprechung des Bundesverfassungsgerichts aus dem Grundrecht auf informationelle Selbstbestimmung (vgl. BVerfGE Bd. 65, S. 1 ff.) ergeben, gerecht werden müssen. Dies bedeutet u.a., daß die Erhebung und Speicherung von personenbezogenen Daten nur auf der Grundlage bereichsspezifischer, normenklarer und dem Grundsatz der Verhältnismäßigkeit genügender gesetzlicher Grundlagen im überwiegenden Allgemeininteresse zulässig ist. Insoweit werden die Gerichte auch zu prüfen haben, welche Maßnahmen nicht zuletzt aus Gründen der Fürsorgepflicht geboten sind, um die potentiellen Anwender mit den rechtlichen Rahmenbedingungen der Datenverarbeitung sowie den erforderlichen Sicherheitsmaßnahmen vertraut zu machen.

4.13.3 Telefonüberwachung gem. § 100a StPO

Erstmalig in der Berichterstattung der Tageszeitung "Die Welt" vom 23.12.1987 wurde darüber berichtet, daß im Zuge strafrechtlicher Ermittlungen an einigen Tagen im November 1987 verschiedene Telefongespräche im Bereich der St. Pauli-Hafenstraße abgehört und aufgezeichnet wurden. In der Folgezeit wendeten sich insgesamt 39 Personen an mich mit der Bitte zu überprüfen, ob sie selbst Betroffene dieser Maßnahmen gewesen sind und ob ggf. dieser Eingriff in ihr informationelles Selbstbestimmungsrecht gesetzmäßig vollzogen wurde. Einer der Petenten teilte mit, ihm habe ein Redakteur des NDR erzählt, die Tatsache, daß er Betroffener der Telefonabhöraktion gewesen sei, habe dieser von einem Bürgerschaftsabgeordneten der CDU erfahren. Es bestand demnach Anlaß, neben der Beantwortung der gestellten Fragen auch zu überprüfen, ob bei der weiteren Verarbeitung der erhobenen Daten die notwendigen Sicherungsmaßnahmen gegen mißbräuchliche Verwendung getroffen worden waren.

Die von mir beabsichtigte umfassende Prüfung wurde durch Entscheidungen der Staatsanwaltschaft und der Justizbehörde zunächst verhindert. Nachdem die Staatsanwaltschaft in der ersten Phase meine Kontrollkompetenz generell bestritt, war nach längeren Erörterungen die Justizbehörde dann bereit, mich wenigstens prüfen zu lassen,

— inwieweit die äußere Datensicherheit für die bestehenden Unterlagen gewährleistet sei,

— ob entgegen der Auffassung der Staatsanwaltschaft und der Justizbehörde personenbezogene Daten dateimäßig verarbeitet worden seien (Tonbandprotokolle).

Darüber hinaus sollte mir die Staatsanwaltschaft mitteilen, welche öffentlichen Telefonanschlüsse überwacht wurden und inwieweit die Personen, die sich an mich gewendet hatten, von Abhörmaßnahmen betroffen waren. Doch auch diese — im Januar 1988 begonnene — Prüfung wurde massiv behindert:

— Da die Tatsache der Telefonüberwachung an die Öffentlichkeit gedrungen war und ich Hinweise erhalten hatte, daß sogar einzelne Protokollabschriften unzulässig weitergegeben worden sein sollen, habe ich von Anfang an deutlich gemacht, daß den Fragen der äußeren Datensicherung besondere Bedeutung zukommt. Zu diesem Komplex habe ich deshalb der Polizei im Beisein der Staatsanwaltschaft Fragen gestellt, die sich auf den Weg vom Entstehen der Tonbandaufnahmen und der Herstellung der Tonbandprotokolle bis zu ihrem Aufbewahrungsort bezogen. Insbesondere ging es um die Frage, wieviele Personen aus welchen Dienststellen an den Maßnahmen beteiligt waren und welche Sicherungsvorkehrungen gegen mißbräuchliche Verwendung und unzulässige Weitergabe getroffen worden waren. Die Beantwortung dieser Fragen nahm einige Wochen in Anspruch.

— Soweit ich nach Auffassung der Justizbehörde sollte prüfen dürfen, ob die Tonbandprotokollabschriften eine Datei i.S.d. Hamburgischen Datenschutzgesetzes darstellen, wurde auch diese Prüfung in entscheidenden Punkten verweigert. Die Justizbehörde hatte ausgeführt:

> "Dies kann durch Vorlage von bei der Telefonüberwachung generell verwandten Formularen — evtl. fingiert ausgefüllt — ohne Einsichtnahme in die konkreten Akten erfolgen. Die aktenmäßige Behandlung der Formulare im anhängigen Verfahren ist zu erläutern. Die entstandenen Unterlagen sind so vorzuweisen, daß ohne Kenntnisnahme vom konkreten Inhalt der Aufzeichnungen festgestellt werden kann, ob die Sammlung unter Verwendung der Formulare erstellt worden ist und sich darauf beschränkt."

Entgegen dieser Zusicherung war die Staatsanwaltschaft nur bereit, mir ein Formular zu übergeben und zu versichern, daß nur dieses Formular verwendet worden sei. Selbst ein Prüfungsverfahren, das eine Kenntnisnahme des konkreten Inhalts der Protokolle mit Sicherheit ausschloß (Einsichtnahme aus 2 1/2 m Abstand in die auf den Kopf gestellten Protokolle) wurde von der Staatsanwaltschaft strikt verweigert.

Gleichwohl hatte die rechtliche Prüfung des Sachverhalts, der mir bis dahin bekannt geworden war, ergeben, daß von der Polizei und der Staatsanwaltschaft personenbezogene Daten dateimäßig verarbeitet wurden. Unter einer Datei ist nach der Legaldefinition des § 4 Abs. 4 Nr. 3 HmbDSG eine gleichartig aufgebaute Sammlung von Daten zu verstehen, die nach bestimmten Merkmalen erfaßt und geordnet, nach anderen bestimmten Merkmalen umgeordnet und ausgewertet werden kann. Meine Prüfung hatte ergeben, daß diese Voraussetzungen für die Sammlungen der Protokollabschriften sämtlich vorlagen und daß ich deshalb selbst nach Auffassung der Justizbehörde zu einer umfassenden Prüfung berechtigt sein müßte. Dies habe ich der Justizbehörde noch am 18. Januar 1988 schriftlich dargelegt.

Nunmehr teilte mir die Justizbehörde mit, zwar sei nicht zu bestreiten, daß die Sammlung der Protokolle alle Merkmale einer Datei trage; es handele sich dabei aber gleichwohl um eine Akte, weil "nach der dienstlichen Erklärung des zuständigen Staatsanwalts nicht davon auszugehen" sei, "daß von der — allgemein gegebenen — Umordnungs- und Auswertungsmöglichkeit auch tatsächlich Gebrauch gemacht" werde. Es bestehe auch keine Veranlassung, am zutreffenden Gehalt dieser Erklärung zu zweifeln. Der zuständige Staatsanwalt habe zugleich darauf hingewiesen, daß er auch bei früheren Telefonüberwachungsmaßnahmen die Umordnungs- und Auswertungsmöglichkeiten nicht genutzt habe. Es entspreche "der Natur der Sache", daß bei der Bewertung, ob eine Datei oder eine Akte vorliege, allein auf den Willen des Bearbeiters abzustellen sei, der in fachlicher Verantwortung diejenige Bearbeitungsform wähle, die seinem Arbeitsstil und dem fachlichen Ziel am ehesten entspreche. Diese Auffassung wurde bis heute nicht aufgegeben. Auch der bisher vorliegende Entwurf für ein neues Hamburgisches Datenschutzgesetz läßt die Möglichkeit einer solchen Interpretation zu.

Da die Justizbehörde der Auffassung war, für eine Datenverarbeitung in Akten fehle mir die Kontrollkompetenz, habe ich diese Beschränkung meiner Befugnisse gegenüber dem Senat am 1. Februar 1988 gem. § 21 HmbDSG beanstandet und für den Fall, daß der Senat entgegen seiner Stellungnahme zu meinem zweiten Tätigkeitsbericht (Bürgerschafts-Drs. 11/2573, S. 7) der Auffassung der Justizbehörde folgen sollte, vorsorglich die Feststellung beanstandet, daß eine Datei nicht vorliege.

Die von mir insoweit erbetene Stellungnahme des Senats brauchte jedoch nicht mehr abgegeben zu werden, weil nunmehr eine überraschende Wendung eintrat.

Im Verlaufe der Diskussion um meine Kontrollkompetenz hinsichtlich der Verarbeitung der bei den Telefonüberwachungsmaßnahmen gewonnenen Daten hatte die Staatsanwaltschaft bei dem Landgericht Hamburg ausdrücklich betont, daß "weder ein automatisiertes Verfahren zur Verwertung des Inhalts der Protokolle eingerichtet und einsatzbereit sei noch die benötigten Daten in den Protokollen in maschinenlesbarer Form vorlägen." Dies hatte die Polizei bestätigt.

Unmittelbar nachdem ich meine Beanstandung vom 1. Februar 1988 der Senatskanzlei übergeben hatte, bekam ich Hinweise, daß bei der Fachdirektion 7 (FD 7) der Polizei Telefonüberwachungsdaten auf einem Personalcomputer verarbeitet würden. Eine sofort von mir eingeleitete Prüfung ergab folgendes:

— Ein bei der FD 7 eingesetzter PC war von der Justizbehörde für die Staatsanwaltschaft etwa Mitte 1987 beschafft, jedoch unmittelbar an die FD 7 ausgeliefert worden.

— Mit dem auf dem Gerät eingesetzten Softwarepaket wurden diverse personenbezogene Daten — wenn auch nicht Gesprächsinhalte — verarbeitet.

— Unzweifelhaft lag eine Datei i.S.d. Hamburgischen Datenschutzgesetzes vor, die für die verschiedensten Zwecke im Rahmen von Telefonüberwachungsmaßnahmen eingesetzt wurde.

— Für die Datei lag weder eine erforderliche Dateimeldung vor, noch war für die eingesetzte Technik das zwischenzeitlich vom Polizeipräsidenten vorgeschriebene Sicherheitskonzept (vgl. 4.11.2) verwirklicht.

Das Verschweigen dieser Datei habe ich gegenüber dem Senat am 4. Februar 1988 gesondert beanstandet. Erst jetzt gab der Justizsenator die Prüfung frei und bedauerte, daß mir objektiv eine unrichtige Auskunft erteilt und ich in der Erfüllung meiner Aufgaben behindert worden war. Dem schloß sich der Senat später an.

Die von mir nunmehr durchgeführte Prüfung ergab im einzelnen über die bis dahin getroffenen Feststellungen hinaus folgendes:

— Vom 15.—20.11.1987 sind im Bereich der St. Pauli-Hafenstraße insgesamt sechs Telefonanschlüsse (davon zwei öffentliche Telefonzellen) auf der Grundlage der §§ 100a, 100b StPO überwacht worden. Sämtliche von diesen Anschlüssen geführten Telefongespräche (mehrere hundert) wurden auf Tonbänder aufgezeichnet; von den meisten wurden schriftliche Protokolle angefertigt.

— Grundlage für die Anordnung der Maßnahmen war der Verdacht der Staatsanwaltschaft gegen unbekannte Personen, in der Hafenstraße solle eine kriminelle Vereinigung gebildet werden oder habe sich schon gebildet (§ 129 StGB), die Verabredungen zur Regelung von Straftaten treffen wolle. Da die Staatsanwaltschaft am Abend des 14.11.1987 Gefahr im Verzuge angenommen hat, beruhten die Überwachungsmaßnahmen zunächst nicht auf gerichtlichen, sondern auf ihren eigenen Anordnungen. Um eine gerichtliche Entscheidung hat sich die Staatsanwaltschaft zu diesem Zeitpunkt nicht bemüht. Erst am 16.11.1987 wurde eine gerichtliche Entscheidung für die Fortführung der Maßnahmen beantragt; diese erging am 17.11.1987. Gefahr im Verzuge i.S.v. § 100b StPO darf nach allgemeiner Auffassung nur dann angenommen werden, wenn der Verlust von Beweismitteln durch die Verzögerung zu besorgen ist, die mit der Einholung einer richterlichen Anordnung entsteht. Vor diesem Hintergrund ist die staatsanwaltschaftliche Entscheidung nur schwer nachvollziehbar, da beim Amtsgericht Hamburg ein durchgehender richterlicher Eil- und Bereitschaftsdienst besteht und klar war, daß die technischen Voraussetzungen für die Überwachung erst am nächsten Tag geschaffen werden konnten.

— Für Polizei und Staatsanwaltschaft mußte relativ schnell nach Abschluß der Maßnahmen klar sein, daß praktisch keines der aufgezeichneten Gespräche den ursprünglich angenommenen Verdacht bestätigte und deshalb auch nicht für die Strafverfolgung verwertbar war. Für diesen Fall ordnet § 100b Abs. 5 StPO die alsbaldige Vernichtung an. Für Gespräche, die mit der beabsichtigten Strafverfolgung unter keinem Gesichtspunkt beachtlich sind, wird von der Fachliteratur sogar die sofortige Vernichtung der entsprechenden Unterlagen gefordert. Aufzeichnungen über solche Gespräche fallen gerade bei der Überwachung von Telefonzellen besonders häufig an. Hätte die Staatsanwaltschaft diese Schutzvorschrift hinreichend beachtet, hätten am 23.12.1987, als durch Indiskretionen die Überwachungsmaßnahmen der Öffentlichkeit bekannt wurden, Unterlagen nicht mehr vorhanden sein dürfen.

— Nach § 101 Abs. 1 StPO sind alle Beteiligten von der Überwachung ihrer Gespräche zu benachrichtigen, sobald dies ohne Gefährdung des Untersuchungszwecks geschehen kann. Damit soll das rechtliche Gehör der Betroffenen sichergestellt werden. Einige Personen hatte die Staatsanwaltschaft Ende Januar 1988 informiert. Die Kontrolle ergab, daß weitere Personen, die ohne größeren Aufwand als Gesprächsteilnehmer zu identifizieren waren, nicht benachrichtigt wurden. Darunter fanden sich auch zwei Personen, die sich mit einer Eingabe an mich gewandt hatten und deren Beteiligung an überwachten Gesprächen die Staatsanwaltschaft zuvor mir gegenüber verneint hatte.

— Darüber hinaus hat der vorliegende Fall exemplarisch gezeigt, daß die Vorschriften des § 100a StPO dringend einer gesetzgeberischen Überarbeitung und Straffung bedürfen, damit die Grundrechtseingriffe auf das Unumgängliche beschränkt werden. So ist erneut deutlich geworden, daß der über 80 Straftaten umfassende Katalog des § 100a StPO viel zu umfangreich ist. Vor allem wirken so weitgefaßte Tatbestände wie § 129 StGB (Bildung und Unterstützung einer kriminellen Vereinigung) wie eine Einladung zur exzessiven Anwendung dieser Maßnahmen, von denen wegen ihres grundrechtsbeschränkenden Charakters nur zurückhaltend Gebrauch gemacht werden darf. Weiter ist deutlich geworden, daß § 100a StPO auch in seinen einzelnen Voraussetzungen von der Rechtsprechung und im Anschluß daran von der Praxis sehr großzügig ausgelegt wird. Immerhin wurden im Verlauf der hier beschriebenen Überwachungsmaßnahmen mehrere hundert Telefongespräche von ausschließlich unverdächtigen Bürgern abgehört, was spätestens nach einigen Stunden erkennbar war und — soweit öffentliche Telefonzellen abgehört wurden — von vornherein in Kauf genommen wurde.

— Verstärkt werden müßte auch die richterliche Verantwortung für die Überwachungsmaßnahmen. Dazu sollte nicht nur eine ständige Kontrolle der Durchführung von angeordneten Maßnahmen, sondern auch das Recht der eigenständigen Beendigung und der Anordnung der Vernichtung von Unterlagen durch den Richter gehören.

  Die Intentionen des BMJ gehen in die entgegengesetzte Richtung. In einem vor einigen Tagen versandten Entwurf zur Novellierung der StPO wird der Richtervorbehalt erheblich aufgeweicht. Eine spätere Verwendung der durch eine TÜ-Maßnahme gewonnenen Daten etwa zu einem Datenabgleich, wie sie der Entwurf ausdrücklich zuläßt, ist von der ursprünglichen richterlichen Prüfung nicht umfaßt. Viel bedenklicher noch: Gestattet werden soll eine Nutzung der Daten auch für präventive Zwecke, und zwar zur Verhütung einer der zahlreichen Straftaten aus dem Katalog des § 100a StPO, und dies, obwohl die Polizeigesetze die Erhebung von Daten mittels Telefonüberwachung zu keinem Zweck gestatten.

— Nach Kenntnis meines Prüfberichts hat der Leitende Oberstaatsanwalt bei dem Landgericht Hamburg angeordnet, daß Tonbänder und Protokolle, die anläßlich von Telefonüberwachungsmaßnahmen angefertigt wurden, monatlich daraufhin zu überprüfen sind, ob sie vernichtet werden müssen. Eine Prüfung des Bestandes der noch vorhandenen Aufzeichnungen über ältere Telefonüberwachungsmaßnahmen hat bis August 1988 dazu geführt, daß Unterlagen aus etwa 80 Verfahren (über mehr als 120 Telefonanschlüsse) vernichtet werden mußten, weil das Gebot des § 100b Abs. 5 StPO (Unterlagen, die zur Strafverfolgung nicht mehr erforderlich sind, alsbald zu vernichten) offenbar nicht beachtet worden ist.

— Die Behörde für Inneres hat inzwischen die Telefonüberwachungsdatei zum Datenschutzregister gemeldet.

— Der Senat hatte schon im März in Beantwortung meiner Beanstandung vom 4.2.1988 darauf hingewiesen, daß die technische Sicherung des PC und die übrigen Maßnahmen des vom Polizeipräsidenten verfügten Sicherungskonzepts für den PC-Einsatz veranlaßt worden seien. Dies habe ich am 11.8.1988 überprüft. Dabei habe ich festgestellt, daß die Datenverarbeitung immer noch nicht ordnungsgemäß ist. Nachdem die von mir mündlich gerügten Mängel in der Abgangskontrolle (Verhinderung der unbefugten Entfernung von Datenträgern) kurzfristig beseitigt wurden, gibt es weiterhin Schwachstellen in der Organisation der Datenverarbeitung.

Die speichernden Stellen haben die innerbehördliche und innerbetriebliche Organisation so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle — Anlage zu § 8 Abs. 1 Satz 1 Nr. 10 HmbDSG). Der Polizeipräsident hat in der schon erwähnten Verfügung vom 29.1.1988 verbindliche Richtlinien zum Einsatz von Personalcomputern erlassen, um den Besonderheiten des Einsatzes dieser Geräte bei der Verarbeitung personenbezogener Daten gerecht zu werden. In dem Sicherheitskonzept ist vorgesehen, daß den anwendenden Stellen ausschließlich Laufzeitverfahren mit einer geschlossenen Benutzeroberfläche (Bedienerführung) ohne Entwicklungswerkzeuge zu übergeben sind. Damit soll die Funktionstrennung zwischen programmierender Stelle und fachlich zuständiger Stelle sichergestellt werden.

Das bei der Telefonüberwachung eingesetzte Verfahren genügt dieser Anforderung nicht, da das eingesetzte Softwarepaket nicht zwischen Benutzung und Entwicklung unterscheidet. Dadurch ist es dem Anwender möglich, ohne Beteiligung der programmierenden Stelle

— Dateien anzulegen und zu löschen,

— die Struktur bestehender Dateien zu verändern,

— sämtliche so angelegten bzw. veränderten Datenbestände flexibel auszuwerten.

Die in der Verfahrensbeschreibung vorgesehene Protokollierung beschränkt sich auf den Zugang zum System und zum Softwarepaket sowie auf die externe Sicherung von Dateien auf Disketten. Demgegenüber wird die Einrichtung, Löschung und Veränderung von Dateien und Daten nicht protokolliert. Eine nachgehende Kontrolle, welche Dateien zu welchem Zeitpunkt von der FD 7 gehalten und verarbeitet worden sind, ist unter diesen Umständen nicht möglich.

Die im Rahmen des derzeitigen Verfahrens vorgesehenen Sicherheitsmaßnahmen entsprechen vor allem wegen der unzureichenden Einhaltung des vorgeschriebenen Freigabeverfahrens nicht den Anforderungen, die an die Verarbeitung sensibler personenbezogener Daten zu richten sind. Das eingesetzte Softwarepaket ist unter Datensicherungsgesichtspunkten nicht zum Einsatz für diesen Zweck geeignet. Es gibt eine ganze Reihe von Softwareprodukten, mit denen sich die von der FD 7 bei der Verwaltung von TÜ-Maßnahmen anfallenden Aufgaben abwickeln lassen, die jedoch die beschriebenen Datenschutzmängel nicht aufweisen.

4.13.4 Erstellung eines zentralen privaten Handelsregisters

Ende 1987 ist bekannt geworden, daß ein privater Wirtschaftsinformationsdienst beabsichtigt, sämtliche Handelsregister in der Bundesrepublik auf Mikrofilm abzulichten, durch Einspeisung der Eintragsveröffentlichungen im Bundesanzeiger ständig zu aktualisieren und im Wege der Erteilung von Auskünften und Informationen unter Einsatz moderner Techniken kommerziell zu verwerten.

Vor dem Hintergrund der derzeitigen Gesetzeslage halte ich das Vorhaben nicht für zulässig und habe dies der Justizbehörde wie folgt erläutert: Das Handelsregister enthält personenbezogene Daten (vgl. z.B. § 29 HGB; § 39 GmbHG). Die Verfilmung des Registers durch eine private Gesellschaft stellt damit aus der Sicht der Registergerichte eine Verarbeitung personenbezogener Daten in Form der Datenübermittlung dar. Die Übermittlung personenbezogener Daten berührt das informationelle Selbstbestimmungsrecht der Betroffenen und bedarf deshalb einer hinreichenden Rechtsgrundlage (BVerfGE 65, 1).

Für die Übermittlung von Daten aus dem Handelsregister enthält § 9 HGB eine bereichsspezifische Regelung. Hiernach ist die Einsicht in das Register jedermann ohne Nachweis eines berechtigten Interesses gestattet (ferner werden alle Änderungen des Inhalts der Handelsregister regelmäßig im Bundesanzeiger veröffentlicht). Diese Vorschrift vermag eine Übermittlung des gesamten Datenbestandes im Wege der Verfilmung des Registers indessen nicht zu rechtfertigen. Die Abnahme des gesamten

Registerinhalts zur Gewinnung eines vermarktbaren Produkts kann begrifflich nicht mehr als "Einsicht" im Sinne von § 9 Abs. 1 HGB angesehen werden. Außerdem hat der Gesetzgeber in § 8 HGB zum Ausdruck gebracht, daß das Handelsregister dezentral von den Gerichten geführt werden soll. Die Errichtung eines zentralen privaten Nebenhandelsregisters entspräche deshalb auch nicht dem Willen des Gesetzgebers.

Die ins Auge gefaßten Datenübermittlungen zur Verfilmung der Handelsregister der Amtsgerichte durch eine Privatfirma sind damit mangels hinreichender Rechtsgrundlage auch aus datenschutzrechtlicher Sicht nicht zulässig.

Die Justizbehörde hat sich meinen Argumenten offensichtlich nicht verschlossen, denn sie hat den Antrag des Unternehmens abgelehnt. Dies scheint der neueren Praxis der meisten Landesjustizverwaltungen zu entsprechen. Gleichwohl hatte die Firma nach einer Mitteilung des Bundesjustizministers bis Oktober 1987 bereits bei 129 der ca. 440 Amtsgerichte die Zentralkarteien des Handelsregisters mikroverfilmt.

4.13.5 Gerichtsvollzieher

In immer stärkerem Maße wird auch die Arbeit der Gerichtsvollzieher durch den Einsatz automatisierter Datenverarbeitung unterstützt. Dies wurde schon 1986 durch eine Allgemeine Verfügung der Justizbehörde (AV Nr. 3/1986) zugelassen. Aus Anlaß der Änderung dieser Verfügung habe ich mich erstmals grundsätzlich mit dem Einsatz von ADV-Technik im Bürobetrieb der Gerichtsvollzieher auseinandergesetzt und dabei erhebliche Regelungsdefizite festgestellt. So fehlten vor allem hinreichende Bestimmungen über Datensicherungsmaßnahmen. Dazu habe ich eine Reihe von Vorschlägen unterbreitet.

Darüber hinaus sind folgende Problembereiche hervorzuheben. In den Gerichtsvollzieherbüros kommen offensichtlich marktgängige Datenverarbeitungsprogramme zum Einsatz, die weder von der Justizbehörde noch vom Präsidenten des Amtsgerichts auf ihre datenschutzrechtliche Unbedenklichkeit geprüft und anschließend für den Einsatz freigegeben wurden. Dies ist mit einer ordnungsgemäßen Datenverarbeitung nicht vereinbar. Die AV müßte deshalb ein Prüfungs- und Freigabeverfahren vorsehen.

Klärungs- und regelungsbedürftig ist auch die Abschottung der Daten, die zu dienstlichen Zwecken verarbeitet werden, von der Datenverarbeitung zu anderen Zwecken. Da die DV-Geräte vermutlich von den Gerichtsvollziehern aus eigenen Mitteln erworben werden, läßt sich möglicherweise eine Auflage, die Geräte nur zu dienstlichen Zwecken zu nutzen, nicht durchsetzen. Dann aber kommt der "Abschottungsproblematik" ein besonderes Gewicht zu.

Schließlich sollte die Frage der Kontrolle durch den Datenschutzbeauftragten geregelt werden. Soweit nämlich die Büros der Gerichtsvollzieher in ihren privaten Wohnungen untergebracht sind, könnte es im Hinblick auf § 20 Abs. 4 Satz 1 Ziff. 2 HmbDSG zu bisher nicht bedachten Problemen kommen. Diese könnten möglicherweise dadurch gelöst werden, daß die vorgesehene Genehmigung mit der Bedingung versehen wird, daß sich die betroffenen Gerichtsvollzieher ausdrücklich und schriftlich einer datenschutzrechtlichen Kontrolle unterwerfen.

Die Justizbehörde hat zugesichert, anhand meiner Vorschläge umfassend zu prüfen, welcher Regelungsbedarf besteht.

4.13.6 Einsicht in Justizakten zu Forschungszwecken

Justizdaten bieten Ansatzpunkte für die verschiedensten Forschungsbereiche. So ist an ihnen nicht nur die Kriminologie, sondern beispielsweise auch die Sozialforschung zur Untersuchung der Auswirkungen einzelner Familienrechtsbestimmungen (Unterhalt, Sorgerecht) interessiert. Diese Forschung ist zum Teil unentbehrlich; sie wird aus öffentlichen Haushalten gefördert und bietet dem Gesetzgeber wichtige Hinweise für seine Arbeit. Aus datenschutzrechtlicher Sicht ist sie gleichwohl als problematisch einzustufen, da weder das materielle Recht noch die verschiedenen Verfahrensordnun-

gen Befugnisnormen enthalten, die es erlauben, die für Justizzwecke erhobenen Daten ohne Zustimmung der Betroffenen für Forschungszwecke zu benutzen. Solche Befugnisnormen sind nach dem Volkszählungsurteil des Bundesverfassungsgerichts jedoch erforderlich und müssen daher dringend geschaffen werden. Bis dies bereichsspezifisch für die einzelnen Justizbereiche gelungen ist, kann voraussichtlich auf die allgemeine Forschungsklausel, um die das Hamburgische Datenschutzgesetz erweitert werden soll, zurückgegriffen werden. Um auch bis dahin nicht jede Forschungstätigkeit zu blockieren, hatte ich schon 1987 mit der Justizbehörde vereinbart, daß die Einsicht in Gerichtsakten zu Forschungszwecken für die Übergangszeit durch eine Allgemeine Verfügung der Justizbehörde geregelt wird, in der die schutzwürdigen Belange der Betroffenen mit den Forschungsinteressen zu einem Ausgleich gebracht werden sollen. Für eine solche Verfügung habe ich der Justizbehörde im März 1988 meine Vorschläge unterbreitet, die diese konstruktiv aufgegriffen und weitgehend in die "AV der Justizbehörde Nr. 12/1988 vom 27. September 1988" (HmbJVBl. 1988, S. 83 f.) umgesetzt hat.

Nunmehr ist verbindlich für alle Justizbereiche festgelegt, daß für die Akteneinsicht zu Forschungszwecken grundsätzlich die Einwilligung der Betroffenen erforderlich ist. Darauf darf nur dann verzichtet werden, wenn der Zweck auf andere Weise nicht erreicht werden kann, das öffentliche Interesse an der Durchführung des Forschungsvorhabens das Geheimhaltungsinteresse erheblich überwiegt und ein Mißbrauch der erlangten Daten nicht zu befürchten ist. Neben anderen Regelungen, die das informationelle Selbstbestimmungsrecht der Betroffenen sichern sollen, enthält die Verfügung darüber hinaus die Verpflichtung des akteneinsichtsuchenden Forschers, ein Konzept zur Gewährleistung des Datenschutzes (technische und organisatorische Datenschutzmaßnahmen) vorzulegen und sich der Datenschutzkontrolle durch den jeweils örtlich zuständigen Datenschutzbeauftragten zu unterwerfen.

Ich bin der Auffassung, daß mit dieser Verfügung den Belangen sämtlicher Beteiligter hinreichend Rechnung getragen wurde. Mit ihr ist schließlich ein datenschutzrechtlicher Standard erreicht, der auch für gesetzliche Forschungsklauseln angestrebt werden muß.

4.13.7 Veröffentlichung von Entmündigungsentscheidungen

Darüber, daß ich die öffentliche Bekanntmachung von Entmündigungen wegen Verschwendung, wegen Trunk- oder Rauschgiftsucht (§ 687 ZPO) für verfassungswidrig halte und mich entsprechend gegenüber dem Bundesverfassungsgericht geäußert habe, habe ich in meinem sechsten Tätigkeitsbericht (6. TB, 4.13.6) berichtet.

Diese Auffassung ist nunmehr vom Bundesverfassungsgericht bestätigt worden. Mit Beschluß vom 9. März 1988 (JZ 1988 S. 555 f.) hat das Gericht entschieden, daß § 687 ZPO mit dem in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG verankerten Recht auf informationelle Selbstbestimmung unvereinbar ist. Eine Abwägung zwischen der Schwere des Eingriffs und dem Gewicht der Gründe, die ihn rechtfertigen (Schutz des Rechtsverkehrs vor Schäden im Zusammenhang mit Rechtsgeschäften ohne die erforderliche Genehmigung oder Zustimmung des Vormundes), ergäbe, daß die Grenzen des Zumutbaren überschritten seien. Die Veröffentlichung solcher Entscheidungen könne die Gefahr der sozialen Abstempelung hervorrufen und die am Sozialstaatsprinzip orientierten Hilfsmaßnahmen zur Überwindung der Sucht und zur sozialen Wiedereingliederung erschweren.

Diese Entscheidung ist ausdrücklich zu begrüßen. Gleichzeitig muß ich in diesem Zusammenhang daran erinnern, daß die Zivilprozeßordnung einer weitergehenden Revision bedarf, um durch Überarbeitung veralteter Vorschriften und Beseitigung von Regelungsdefiziten dem informationellen Selbstbestimmungsrecht auch im Zivilrechtsverfahren hinreichend Geltung zu verschaffen. Inzwischen liegt ein Referentenentwurf eines Gesetzes über die Betreuung Volljähriger vor, in dem auch die Mitteilungspflichten der Vormundschaftsgerichte unter Beachtung der Rechtsprechung des Bundesverfassungsgerichts neu geregelt werden sollen.

4.13.8 Versendung amtsgerichtlicher Entscheidungen

In der Vergangenheit haben sich mehrfach Petenten bei mir beschwert, daß Entscheidungen des Amtsgerichts an andere Behörden und öffentliche Stellen offen verschickt werden. Die Beschlüsse enthalten durchaus vertrauliche Angaben über Bürger, so z.B.

— Gründe der Unterbringung Minderjähriger,

— Ehescheidungen (mit Aussagen über Alkoholkonsum, Gewalttätigkeiten usw.),

— Anhörungen vor Vormundschaftsrichtern,

— zwangsweise Unterbringung Erwachsener mit Begründung.

Die Beschwerden von Mitarbeitern der empfangenden Behörden und öffentlichen Stellen wurden vom Amtsgericht stets mit einem Hinweis auf die Arbeits- und Kostenersparnis des bisherigen Verfahrens abgetan. Außerdem solle nach einer Weisung des Senatsamtes für den Verwaltungsdienst vom 19. September 1975 behördeninterner Schriftverkehr grundsätzlich offen versandt werden. Auch hielt das Amtsgericht wegen der für alle Behördenbediensteten geltenden Verschwiegenheitspflicht eine Änderung der Versendungsform nicht für erforderlich.

Diese Hinweise können die datenschutzrechtlichen Bedenken nicht entkräften. Auch die von amtsgerichtlichen Entscheidungen betroffenen Personen haben einen Anspruch darauf, daß ihre Daten nicht unbefugten Dritten bekannt werden. Die Weitergabe von Daten an andere öffentliche Stellen hat sich ebenfalls an diesen Maßstäben zu orientieren. Dies kann aus meiner Sicht nur durch einen verschlossenen Versand erreicht werden. Die vom Amtsgericht erwähnte Weisung des Senatsamtes für den Verwaltungsdienst über den behördeninternen Schriftverkehr kann für die Behandlung von amtsgerichtlichen Entscheidungen, die hochsensible personenbezogene Daten enthalten, nicht herangezogen werden.

Das Amtsgericht hat wegen der grundsätzlichen Bedeutung die Angelegenheit dem Senatsamt für den Verwaltungsdienst zur Klärung vorgetragen. Bis zum Redaktionsschluß dieses Berichtes stand eine Stellungnahme noch aus.

4.14 Wissenschaft und Forschung

4.14.1 Erhebung von Studentendaten

Im Juni 1988 versandte die Behörde für Wissenschaft und Forschung einen Diskussionsentwurf für ein Hochschulrechtsänderungsgesetz. Eine Klausel zu den von den Studenten für Zwecke der Immatrikulation und der Prüfungen zu erhebenden Daten enthält dieser Entwurf nicht.

Am 23. August 1988 wurde in einem gemeinsamen Gespräch zwischen der Behörde für Wissenschaft und Forschung, dem Statistischen Landesamt, der Justizbehörde und dem Datenschutzbeauftragten die Notwendigkeit oder Nützlichkeit einer solchen Klausel erörtert. Zwar dürfen nach dem Hamburgischen Datenschutzgesetz diejenigen Studentendaten verarbeitet werden, die für Zwecke der Universitätsverwaltung und der Studien- und Prüfungsorganisation "erforderlich" sind. Dies ist jedoch auslegungsfähig, von dem Betroffenen nicht unmittelbar erkennbar und von Hochschule zu Hochschule möglicherweise verschieden. Eine bereichsspezifische gesetzliche Regelung wäre hier jedenfalls besser. Eine Festlegung in den Hochschulsatzungen — auch aufgrund einer entsprechend zu spezifizierenden Ermächtigung im Hochschulgesetz — könnte eine einheitliche Praxis nicht gewährleisten. Sowohl aus datenschutzrechtlichen wie aus praktischen Gesichtspunkten ist deswegen eine klare gesetzliche Ermächtigung zu einer umfassenden Datenverarbeitungsregelung für alle hamburgischen Hochschulen in einer eigenen Rechtsverordnung geboten.

Diesen Weg gehen auch das baden-württembergische Universitätsgesetz und das hessische Hochschulgesetz. In Hessen trat am 1. August 1988 bereits eine ausführliche "Verordnung über das Verfahren der Immatrikulation an den Hochschulen des Landes

Hessen" in Kraft. Ich habe angeregt, in der Hamburger Verordnung auch die für Prüfungszwecke notwendigen Datenverarbeitungen festzulegen und dies in die gesetzliche Ermächtigung mit einzubeziehen.

Als Diskussionsgrundlage für eine entsprechende Verordnung legte die Behörde für Wissenschaft und Forschung einen "Datenkatalog für die Erhebung von Verwaltungsdaten an den Hochschulen" der Ständigen Konferenz der Kultusminister vor. Ob alle dort aufgeführten Daten für alle Hamburger Hochschulen, Fachbereiche und Verwaltungszwecke erforderlich sind, werde ich prüfen, soweit sie in den von der Behörde für Wissenschaft und Forschung in Aussicht gestellten Verordnungs-Entwurf Eingang finden werden.

Zu der ebenfalls angesprochenen Frage der Hochschulstatistik (eigene Datenerhebungen für Statistikzwecke oder Sekundärstatistik mit den für Verwaltungszwecke erhobenen Daten) habe ich an anderer Stelle Ausführungen gemacht (s. Ziff. 4.3.3).

4.14.2 Einzelne Forschungsprojekte

— Sexuelle Belästigung von Frauen am Arbeitsplatz —

Die Leitstelle Gleichstellung der Frau bei der Senatskanzlei führte im Berichtszeitraum eine umfangreiche Befragung von weiblichen und männlichen Bediensteten der Hansestadt zum Thema "Sexuelle Belästigung von Frauen am Arbeitsplatz" durch. In die Vorbereitungen dieser Studie wurde ich frühzeitig einbezogen. So konnte ich mit der Leitstelle zusammen ein Verfahren entwickeln, das auch den Schutz der besonders sensiblen Daten und Fragebogen-Auskünfte gewährleistet. Sicherzustellen war vor allem, daß die Angaben im Fragebogen im Nachhinein nicht den Befragten zugeordnet werden können. Dazu dienten etwa folgende Maßnahmen.

— Die zu befragenden 2.000 Personen wurden aus der Personaldatei der Besoldungs- und Versorgungsstelle per Zufallsauswahl bestimmt und anschließend der Forschergruppe als Privatadressen-Aufkleber übermittelt.

— Ein dem Fragebogen beigefügtes Anschreiben stellte die Freiwilligkeit und Anonymität der Beantwortung heraus.

— Eine individuelle Rücklaufkontrolle, die Fragebogenempfänger und -absender hätte abgleichen müssen, fand nicht statt.

— Um die antwortende Person nicht aus den verschiedenen Angaben auf dem Fragebogen leicht identifizieren zu können, faßte die Leitstelle aufgrund meiner Anregung die Fragen zur allgemeinen Arbeitssituation (Aufgabenbereich, Funktion, Ausbildung, Arbeitsort, Geschlecht von Mitarbeitern/Vorgesetzten/Kollegen) wesentlich allgemeiner.

Abgesehen von der datenschutzrechtlichen Problematik der Zweckentfremdung der Personaldatei der Besoldungs- und Versorgungsstelle für diesen Forschungszweck sind Datenschutz-Defizite auch von Betroffenen weder bei der Leitstelle noch bei mir moniert worden.

Die Untersuchung soll Anfang des Jahres 1989 zur Verfügung stehen. Sie wird vor einer Veröffentlichung auf datenschutzrechtliche Schwachstellen durchgesehen.

— Hamburger Polizei 1945 bis 1962 —

Die "Hamburger Polizei 1945 bis 1962" ist Gegenstand eines Forschungsvorhabens von zwei Hamburger Wissenschaftlern. Datenschutzrechtlich problematisch war vor allem die Frage, ob dazu auch Personalakten von ehemaligen Polizei-Führungskräften eingesehen werden dürfen. In einer Stellungnahme gegenüber der Innenbehörde betonte ich den Vorrang der Einwilligung der Betroffenen. Nur wenn die Einholung der Einwilligung einen unzumutbaren Aufwand erfordert, kommt eine Abwägung zwischen dem öffentlichen Interesse an der zeitgeschichtlichen Forschung und dem Geheimhaltungsinteresse der Betroffenen in Betracht. Dabei ist der Schutz von Daten noch leben-

der Personen grundsätzlich stärker zu gewichten als der von verstorbenen Personen. Bei Personalakten Verstorbener, die im Staatsarchiv lagern, ist allerdings eine Schutzfrist von 60 Jahren nach Schließung der Akten einzuhalten (in Zukunft: 30 Jahre nach Tod, vgl. oben Ziff. 4.5). Ausnahmegenehmigungen setzen eine Einzelfallprüfung voraus. Die Innenbehörde schloß sich dieser Auffassung im wesentlichen an. Nach ihrer Auskunft sind inzwischen ca. 50 (ehemalige) Polizisten um Einwilligung zur Einsichtnahme in ihre Personalakten gebeten worden. Ohne Zustimmung läßt die Innenbehörde die Einsichtnahme in Personalakten noch lebender Personen nicht zu. Hinsichtlich der Personalakten verstorbener Polizisten sind einzelne Ausnahmegenehmigungen zur Verkürzung der Schutzfrist einzuholen.

4.14.3 Gentechnologie

1987 legte die Enquete-Kommission des Bundestages einen ausführlichen Bericht zu "Chancen und Risiken der Gentechnologie" vor (Bundestagsdrucksache 10/6775). In Abschnitt C 6. "Humangenetik" enthält der Bericht Aussagen zur "Genomanalyse und Gentherapie", die von hoher datenschutzrechtlicher Brisanz sind. Gentechnologische Verfahren können schon heute eindeutige Identifizierungsmerkmale ("genetischer Fingerabdruck"), vererbbare Krankheiten und Krankheitsanlagen bzw. -risiken, potentiell — d.h. bei weiterem wissenschaftlichen Fortschritt — aber darüberhinaus alle genetisch bedingten Eigenschaften einer Person diagnostizieren. Es liegt auf der Hand, daß es sich hierbei um höchst sensible und mißbrauchsgefährdete personenbezogene Daten handelt, die bisher im Verborgenen blieben, nun aber angesichts der modernen gentechnischen Entschlüsselungsmöglichkeiten des besonderen Schutzes bedürfen.

Die Datenschutzbeauftragten haben dies zum Anlaß genommen, einen eigenen Arbeitskreis "Gentechnologie" zu bilden, der die Datenschutzprobleme in folgenden Bereichen erörtert:

— Genomanalyse in Strafverfahren: Schon heute ermöglichen gentechnische Analysen von am Tatort gefundenem Gewebe, Blut oder Sperma über Vergleichsanalysen von Körperzellen Verdächtiger eine eindeutige Täteridentifizierung ("genetischer Fingerabdruck"). Dabei muß jedoch sichergestellt sein, daß die Analysen keine Aussagen über Krankheiten, Fähigkeiten, Eigenschaften des Betroffenen zulassen, sondern sich auf sog. "nicht-codierende", "persönlichkeitsneutrale" Ergebnisse beschränken. Dies sollte in der Strafprozeßordnung (§§ 81a, 81c) ebenso festgeschrieben werden wie ein Verbot, Genomanalysen außerhalb von dafür besonders zugelassenen Instituten vorzunehmen. Über den Identitätsnachweis hinaus könnten Genomanalysen in Strafverfahren zukünftig auch bei Fahndungsmaßnahmen — etwa, wenn ein Gentest von Blutresten am Tatort die Augen- oder Haarfarbe, die Größe oder besondere Kennzeichen des Täters offenbart —, beim Verwandtschaftsnachweis und möglicherweise zur Beurteilung der Schuldfähigkeit (Geisteskrankheit, Persönlichkeitsbewertung) eingesetzt werden. Vor dem Hintergrund umfassender Datenspeicherungsmöglichkeiten der Polizei und angesichts der potentiellen Sensibilität von Genomanalyse-Ergebnissen bedarf es einer besonders kritischen Beobachtung durch die Datenschutzbeauftragten.

— Genomanalyse an Arbeitnehmern: Betriebsärztliche Gentests an Arbeitnehmern werden heute bereits zur Diagnose von Unverträglichkeiten gegenüber bestimmten Arbeitsstoffen vorgenommen. Die große Gefahr von Genomanalysen an Arbeitnehmern liegt zum einen darin, daß Arbeitgeber lieber genetisch "günstig" veranlagte Mitarbeiter auswählen als objektiven Arbeitsschutz durch Vermeidung gefährlicher Arbeitsstoffe betreiben könnten. Zum anderen bedeutet die Nähe des Betriebsarztes zum Arbeitgeber immer auch das Risiko, daß Ergebnisse von Genomanalysen mißbräuchlich in personalwirtschaftliche Entscheidungen einfließen, zumal Gentests über den gegenwärtigen Gesundheitszustand hinaus Aussagen über zukünftige Entwicklungen Einzelner treffen können. Aus diesen Gründen trete ich für ein generelles Verbot von Genomanalysen an Arbeitnehmern ein: Der (Prognose-) Nutzen von Genomanalysen ist zur Zeit noch gering bzw. unsicher, das Mißbrauchs-

risiko — auch durch falsche Befund-Bewertung durch den Arbeitgeber — dagegen erheblich. Zur eigenen Vorsorge kann sich ein Arbeitnehmer auch außerhalb des Arbeitgeber-Bereichs einer Genomanalyse unterziehen und ggf. selbst Konsequenzen ziehen. Die Enquete-Kommission teilt diese grundsätzlich ablehnende Haltung nicht. Sie empfiehlt, durch Gesetze Einschränkungen und Bedingungen für die Zulässigkeit von Genomanalysen an Arbeitnehmern festzulegen. Ich bin dagegen der Auffassung auch des DGB, daß angesichts der berührten wirtschaftlichen Interessen, der Machtverhältnisse zwischen Arbeitgeber/Betriebsarzt einerseits und Arbeitnehmer andererseits sowie der Vertraulichkeit medizinischer Untersuchungen differenzierte Regelungen dem Mißbrauchsrisiko nicht gerecht werden, weil ihre Einhaltung praktisch nicht überprüft werden kann.

— Genomanalyse für Versicherungen: Insbesondere für Lebensversicherer und private Krankenversicherer ohne Zwangsmitgliedschaft könnten Genomanalysen ein Mittel zur wirtschaftlichen Risikoabschätzung werden. Einer Person würde möglicherweise eine Lebensversicherung verweigert; eine genetisch angelegte therapie- oder pflegekostenintensive Krankheit könnte zu besonderen Risikozuschlägen oder ebenfalls zur Antragsablehnung bei der privaten Krankenversicherung führen. Derzeit ist von Genomanalysen in der Versicherungspraxis noch nichts bekannt. Ich habe aber mit den Dachverbänden der Versicherungswirtschaft Kontakt aufgenommen, um die mögliche zukünftige Entwicklung zu erörtern, die ähnlich brisant ist wie die AIDS-Test-Problematik.

— Pränatale Diagnostik und "Neugeborenen-Screening": Bei der pränatalen Genomanalyse kommt zu den allgemeinen Mißbrauchsrisiken vor allem das ethische und soziale Problem des eugenisch begründeten und womöglich geforderten Schwangerschaftsabbruchs. Es ist auch Aufgabe des Datenschutzes, hier zu einer besonderen Sensibilität und Besonnenheit beizutragen und das informationelle Selbstbestimmungsrecht des Kindes und der Eltern gegen drohende gesellschaftliche und womöglich staatliche Angriffe zu verteidigen. Dazu gehört die Forderung einer eingehenden, neutralen Aufklärung durch den Arzt. Andererseits kann die Offenbarung einer unheilbaren Erbkrankheit des Neugeborenen dessen und seiner Eltern "Recht auf Nichtwissen" verletzen — ein Begriff der Enquete-Kommission, der dem traditionellen Datenschutzverständnis fremd ist, aber angesichts der neuen Erkenntnismöglichkeiten der Gentechnologie in der Tat als eine Ausprägung des informationellen Selbstbestimmungsrechts angesehen werden muß.

Vor dem Hintergrund hochkomplexer Datenschutzprobleme im Bereich der Human-Gentechnik war es für mich besonders ärgerlich, daß ich an der Vorbereitung der Senats-Stellungnahme zum EG-Forschungsprojekt "Prädiktive Medizin-Analyse des menschlichen Genoms" (Bundesratsdrucksache 407/88) nicht beteiligt wurde.

4.15 AIDS

4.15.1 HIV-Tests im Krankenhaus

Die Durchführung eines HIV-Antikörper-Tests berührt nicht nur das Grundrecht auf körperliche Unversehrtheit, sondern auch das informationelle Selbstbestimmungsrecht. Deshalb darf entnommenes Blut, das Träger einer Vielzahl persönlicher, höchst sensibler Daten ist, grundsätzlich nur mit Einverständnis des Betroffenen ausgeforscht werden. Die Umsetzung dieses Grundsatzes in die Praxis wird von den staatlichen Hamburger Krankenhäusern in der Praxis unterschiedlich gehandhabt.

Während die Gesundheitsbehörde für die Krankenhäuser des Landesbetriebs eine Dienstanweisung über die Aufklärung und Einwilligung der Patienten bei Vornahme des HIV-Tests erlassen hat, die seit dem 1. Juli 1988 in Kraft ist, wendet das UKE eine sehr allgemein gehaltene Dienstanweisung über das Verfahren bei ärztlichen Eingriffen aus dem Jahre 1977 an. Diese Dienstanweisung erscheint mir nicht geeignet, das erforderliche Aufklärungs- und Einwilligungsverfahren vor der Durchführung von HIV-Tests sicherzustellen.

Aus datenschutzrechtlicher Sicht halte ich grundsätzlich die Einholung der Einwilligung des Betroffenen vor Durchführung des Tests für erforderlich. Die Einwilligung ist nur wirksam, wenn ihr eine ausreichende Information über den Zweck und die Konsequenzen des Tests vorangeht. Ohne wirksame Einwilligung stellt der Test einen rechtswidrigen Eingriff in die körperliche Integrität und das Persönlichkeitsrecht des Betroffenen dar. Eine stillschweigende Einwilligung ist nur in eng begrenzten Ausnahmefällen anzunehmen. Nur wenn ein Patient mit Krankheitssymptomen unklaren Ursprungs einen Arzt zur diagnostischen Abklärung aufsucht und eine HIV-Infektion zum Kreis der möglichen Ursachen der Beschwerden gehört, kann davon ausgegangen werden, daß diese Untersuchung von der Einwilligung des Patienten umfaßt ist. Das schließt aber nicht aus, den Patienten trotzdem über die geplante Durchführung des Tests zu informieren und ihm Gelegenheit zum Widerspruch zu geben. Soll bei dem Patienten eine Blutdiagnostik zur Vorbereitung einer therapeutischen Maßnahme durchgeführt werden und erscheint ein HIV-Antikörper-Test entweder wegen der Art des Eingriffs oder wegen vorliegender konkreter Anhaltspunkte für eine HIV-Infektion erforderlich, kann m.E. eine stillschweigende Einwilligung nicht unterstellt werden. In aller Regel hat ein Patient keine konkreten Vorstellungen über den Umfang diagnostischer Maßnahmen, die über die herkömmliche Blutuntersuchung hinausgehen. Mit einer HIV-Antikörperuntersuchung ohne sein Wissen wird er schon deshalb nicht rechnen, weil in den Medien wiederholt auf die Rechtswidrigkeit sog. "heimlicher AIDS-Tests" hingewiesen wurde. Deshalb muß er über einen geplanten HIV-Test aufgeklärt werden, um Eingriffen in sein informationelles Selbstbestimmungsrecht wirksam zustimmen zu können. Auch in Fällen, in denen der HIV-Test nicht aus diagnostischen oder therapeutischen Gesichtspunkten, sondern allein zum Schutz des Krankenhauspersonals vor einer Ansteckung durchgeführt wird, ist in jedem Fall eine Aufklärung und Einwilligung vor dem Test erforderlich.

Nach meinen Informationen bleibt es im UKE weitgehend dem einzelnen Arzt überlassen, in welchem Umfang er seinen Patienten aufklärt. Bei einer allgemein gehaltenen Aufklärung über einen Eingriff, in der der geplante HIV-Test nicht erwähnt wird, besteht aber die Gefahr, daß die Einwilligung des Patienten unwirksam ist, da er nicht alle entscheidungsrelevanten Gesichtspunkte erfährt. Sofern mir konkrete Fälle einer unzureichenden Aufklärung vor Durchführung des Tests bekannt werden, beabsichtige ich, von meinem Beanstandungsrecht Gebrauch zu machen.

Ich habe dem UKE daher mitgeteilt, daß ich es für erforderlich halte, den Ärzten konkretere Hinweise und verbindliche Richtlinien für das Verfahren der Aufklärung und Einwilligungseinholung vorzugeben. Das Argument von ärztlicher Seite, daß nicht für jede Krankheit eine Spezialregelung getroffen werden kann, wird durch die Regelung des Landesbetriebs über Aufklärung und Einwilligung der Patienten bei Vornahme des HIV-Tests widerlegt. Auch im Sinne einer einheitlichen Regelung würde ich es begrüßen, wenn das UKE diese Dienstanweisung für seinen Bereich übernimmt.

4.15.2 HIV-Tests beim staatlichen Blutspendedienst

Während Krankenhauspatienten nur bei besonderer medizinischer Indikation einem HIV-Test unterzogen werden, untersuchen die Butspendedienste grundsätzlich jedes Spenderprodukt auf HIV-Antikörper, um die Empfänger vor einer Infektion zu schützen. Durch vertragliche Vereinbarung verpflichtet sich der Spender zur Information über Infektionsrisiken und unterzieht sich regelmäßigen Kontrolluntersuchungen. Diese Vorsichtsmaßnahmen gelten gleichermaßen für HIV- wie für sonstige, der Spendertätigkeit entgegenstehende Infektionen.

Auch bei Blutspendern bedarf es der Aufklärung und ausdrücklichen Einwilligung des Betroffenen vor Durchführung des HIV-Tests. Nach meiner Feststellung weisen alle staatlichen Hamburger Blutspendedienste auf die Ansteckungsgefahr HIV-infizierter Spender hin, Angehörige von Risikogruppen (z.B. homo- und bisexuelle Männer, intravenös Drogenabhängige) werden per Merkblatt aufgefordert, kein Blut zu spenden. Der Blutspendedienst des UKE klärt auch schriftlich darüber auf, daß bei jeder Spende

ein HIV-Antikörper-Test durchgeführt wird, im Merkblatt für die Blutspendedienste des Landesbetriebs fehlte ein solcher Hinweis bisher. Allerdings kann eine formularmäßige Aufklärung nicht die in aller Regel zu Beginn der Spendertätigkeit erforderliche individuelle Aufklärung ersetzen, sondern sie dient eher der Erleichterung bei der Dokumentation der Aufklärung. Dokumentiert werden muß auch das ausdrückliche Einverständnis des Betroffenen mit der Durchführung des Tests. Bei keinem der Blutspendedienste war bisher eine solche Erklärung in der Vereinbarung mit dem Spender enthalten. Ich habe deshalb mit den staatlichen Blutspendediensten vereinbart, eine Überarbeitung der Einverständniserklärung vorzunehmen, die den datenschutzrechtlichen Anforderungen an Aufklärung und Einwilligung entspricht.

4.15.3 AIDS-Beratungsstellen der Gesundheitsämter

Über datenschutzrechtliche Probleme, die aus der Mehrfunktionalität der Gesundheitsämter entstehen, habe ich schon mehrfach, zuletzt im 6. Tätigkeitsbericht (unter Ziff. 4.15.5) berichtet. Meine besondere Aufmerksamkeit galt daher den AIDS-Beratungsstellen der Gesundheitsämter. Neben allgemeinen Informationsveranstaltungen für Behörden, Schulen und interessierte Gruppen bieten die Beratungsstellen Einzelfallberatungen und die Durchführung kostenloser HIV-Antikörpertests an. Ich habe mich davon überzeugt, daß die Beratung streng anonym durchgeführt wird, und daß auch meine Forderung nach einer vollständigen organisatorischen Abschottung der verschiedenen Funktionsbereiche des Gesundheitsamts, insbesondere zwischen der Beratungsstelle und dem Seuchenreferat, im wesentlichen erfüllt ist.

In der Einzelfallberatung wird jeder Ratsuchende lediglich mit einer laufenden Nummer, dem Geschlecht, einer Kurzbezeichnung für die Beratungstätigkeit (Beratung, Blutentnahme, Mitteilung des Testergebnisses) sowie dem Namen des Beratenden in ein Tagebuch eingetragen. Wünscht er einen Test, erhält er eine Codenummer, die sich derzeit noch aus drei Buchstaben, die dem eigenen und dem Namen der Mutter entnommen werden, dem Geburtsjahr und der laufenden Tagebuchnummer zusammensetzt. Auch dieser Code wird in das Tagebuch aufgenommen. Für die vergebenen Codenummern werden Karteikarten geführt, in denen festgehalten ist, ob und wann getestet worden ist und welche weiteren Termine vereinbart wurden.

Die Weitergabe des Blutes zur Untersuchung an das Hygienische Institut erfolgt unter der Codenummer ohne weitere Angaben zur Person. Dort erhält das Begleitschreiben eine Labornummer für die Probe und geht urschriftlich unter Mitteilung des Testergebnisses an die Beratungsstelle zurück. Die Angaben, die das Hygienische Institut bei positiven Testergebnissen zur Erfüllung der Berichtspflicht aus der Laborberichtsverordnung benötigt, werden, da in den einzelnen Beratungsstellen nur sehr selten positive Testergebnisse anfallen, von allen Beratungsstellen gemeinsam an das Hygienische Institut gemeldet, um eine Zuordnung zu der einzelnen Beratungsstelle zu erschweren.

Das Codierungsverfahren für die Beratungsstellen wird in Abstimmung mit meiner Dienststelle gerade überarbeitet, um mit absoluter Sicherheit die Vergabe gleicher Codenummern auszuschließen.

Die Einhaltung einer strikten Funktionstrennung im Gesundheitsamt, die meiner Auffassung nach auch in der Vertretungsregelung durchgehalten werden muß, wird den Beratungsstellen durch die knappe personelle Besetzung erschwert. Die Stellenausstattung mit einer Arztstelle und einer ABM-Sozialarbeiterstelle läßt eine auf Dauer angelegte interne Vertretungsregelung nicht zu, zumal die ABM-Stelle in den meisten Beratungsstellen nach Ablauf der Befristung nicht verlängert wird. Die Beratungsstellen verweisen deshalb überwiegend im Krankheits- oder Urlaubsfall auf die Beratungsangebote der anderen Bezirksämter oder an die Beratungsstelle der Gesundheitsbehörde. Es kommt aber nach meiner Information auch vor, daß ein Ratsuchender auf der Beratung im zuerst aufgesuchten Gesundheitsamt besteht und dann ein ärztlicher Mitarbeiter aus einem Funktionsbereich vertretend tätig wird. Für hinnehmbar halte ich eine solche Vertretung nur dann, wenn sie nach Hinweis auf die Beratungsangebote anderer Stellen ausdrücklich vom Betroffenen gewünscht wird.

4.15.4 AIDS in polizeilichen Informationssystemen

In meinem 6. Tätigkeitsbericht (4.15.1) habe ich ausführlich die Diskussion über die Zulässigkeit und Erforderlichkeit von Notierungen über HIV-Infektionen in polizeilichen Informationssystemen, meine Haltung zu den vertretenen Positionen sowie die von mir gebilligte Hamburger Praxis dargestellt. Diese zeichnet sich dadurch aus, daß lediglich bei Fahndungsausschreibung ein Hinweis auf Ansteckungsgefahren und die Warnung vor Blutkontakt erfolgt, wenn

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

— die gesuchte Person gegenüber amtlichen Stellen glaubhaft erklärt hatte, Träger dieses Erregers oder an AIDS erkrankt zu sein und

— die gesuchte Person nach amtlichen Erkenntnissen zur Gewalttätigkeit neigt.

Wenn es zu Speicherungen kommt, werden diese automatisch gelöscht, wenn nach Erledigung der Fahndung die Fahndungsnotierung selbst gelöscht wird. Diese "Hamburger Linie", die seit März 1987 praktiziert wird, hat sich leider in den Beratungen der Innenministerkonferenz (IMK) nicht durchgesetzt. Nach einem von der IMK gebilligten Beschluß ihres Arbeitskreises II vom 7.9.1988 wird die Speicherung von HIV-Hinweisen in das Ermessen der jeweils einspeichernden Stelle, sei es Bund oder Land, gestellt. Sofern eine einspeichernde Stelle Speicherungen vornimmt, erfolgt dies mit Ausnahme der Laufzeit nach den gleichen Kriterien wie bei den übrigen Hinweisen auf Ansteckungsgefahr. Danach darf der Hinweis auf eine Ansteckungsgefahr "ANST-Vorsicht Blutkontakt" gespeichert werden, wenn ärztliche oder amtliche Hinweise oder Angaben des Betroffenen selbst hinsichtlich einer HIV-Infizierung vorliegen. Die Speicherung des Hinweises darf in den INPOL-Anwendungen, in der Datei Kriminalaktennachweis, Personenfahndung, Erkennungsdienstdatei und der Falldatei Rauschgift erfolgen. Speicherung und Übermittlung des Hinweises erfolgen ausschließlich zu dem Zweck der Eigensicherung der Polizeibeamten.

Zwar berücksichtigt dieser Beschluß einige Forderungen der Datenschutzbeauftragten, die ich ebenfalls im letzten Tätigkeitsbericht dargestellt habe, gleichwohl bleiben erhebliche Einwände bestehen.

Die Tatsache, daß die Speicherung von HIV-Hinweisen nunmehr in das Ermessen des Bundes oder eines jeden Landes gestellt wird, belegt geradezu, daß solche Hinweise im Regelfall nicht zum Schutze von Polizeibeamten erforderlich sind, denn erforderliche Schutzmaßnahmen können aus Gründen der Fürsorgepflicht des Dienstherrn nicht in dessen Ermessen gestellt werden.

Die Dateien, in denen der Hinweis gespeichert werden soll, sind diejenigen polizeilichen Dateien mit der größten Zahl von gespeicherten Personen, mit den längsten Speicherfristen sowie mit den meisten Zugriffsberechtigten. Da keine besondere Regelung über den befugten Benutzerkreis sowie über den Zweck des Abrufs getroffen wird, wird allen zum Zugriff auf die Anwendungen Kriminalaktennachweis, Personenfahndung, Erkennungsdienstdatei und Falldatei Rauschgift berechtigten Mitarbeitern der Hinweis auf HIV-Infizierung mitübermittelt, und zwar völlig unabhängig vom Anlaß des Abrufs. Damit wird der Gedanke der Eigensicherung von Polizeibeamten, denen der Hinweis zur Vorbereitung auf Situationen dienen kann, in denen es mit hoher Wahrscheinlichkeit zu gewaltsamen Auseinandersetzungen mit Infizierten kommen kann, praktisch aufgegeben.

In diesem Zusammenhang ist es nützlich, sich noch einmal den Grad der Gefährdung von Polizeibeamten vor Augen zu führen: Bei der Tagung des Exekutivkomitees der Vereinigung internationaler Polizeigewerkschaften (UISP) vom 23.-25.8.1988 in London, der 17 Organisationen angehören, wurde festgestellt, daß Fälle, bei denen sich Polizeibeamte im Dienst mit AIDS infiziert haben, in keiner der 17 Nationen bekannt waren (vgl. Deutsche Polizei 10/88, S. 8).

4.16 Gesundheitswesen

4.16.1 Gesetzliche Grundlagen

4.16.1.1 Gesundheitsreformgesetz

Das vom Bundestag nunmehr beschlossene Gesetz zur Strukturreform im Gesundheitswesen hat im Laufe des Gesetzgebungsverfahrens vielfältige Kritik von Leistungserbringern, Interessenverbänden, Krankenkassen, Sozialpolitikern und auch von Datenschutzbeauftragten auf sich gezogen. Aus datenschutzrechtlicher Sicht stand der Schutz des Versicherten vor unverhältnismäßigen Eingriffen in sein informationelles Selbstbestimmungsrecht durch die ursprünglich geplante umfassende Speicherung und Verarbeitung von sensiblen Versichertendaten im Vordergrund (s. 6. TB, 1.1.3). Unbestritten ist, daß die Krankenkassen zur Erfüllung ihrer Aufgaben bestimmte Versichertendaten verarbeiten dürfen und müssen. Auch gegen die Zielsetzung des Reformvorhabens, im Interesse der Funktionsfähigkeit des Versicherungssystems durch Schaffung von mehr Kostentransparenz und Kontrollmöglichkeiten den rapiden Kostenanstieg im Gesundheitswesen zu bremsen, bestehen unter Datenschutzgesichtspunkten keine grundsätzlichen Einwände. Die entscheidende Frage war jedoch, ob Art und Umfang der beabsichtigten Datenverarbeitung geeignet und erforderlich waren, um diese Ziele zu erreichen. Hier waren erhebliche Zweifel angebracht, die im Verlauf des Gesetzgebungsverfahrens zu einer grundlegenden Umgestaltung der datenschutzrechtlichen Vorschriften des Entwurfs geführt haben.

Trotz wesentlicher Verbesserungen bleibt zu kritisieren, daß der Entwurf im Eilverfahren durch das Gesetzgebungsverfahren gepeitscht wurde, weshalb weder eine ausreichende Anhörung von Experten noch eine gründliche Verarbeitung von Erkenntnissen aus Transparenzprojekten und Modellversuchen der Krankenkassen möglich war, zumal sie z.T. noch gar nicht abgeschlossen oder noch nicht ausgewertet sind.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat zum Entwurf des Gesundheitsreformgesetzes einen Beschluß mit Änderungsempfehlungen gefaßt. Die Empfehlungen mögen dazu beigetragen haben, daß der Entwurf in wesentlichen Punkten geändert und den datenschutzrechtlichen Anforderungen angepaßt worden ist.

Die Datenverarbeitung ist auf das erforderliche Maß beschränkt und einer konkreten Zweckbindung unterworfen worden. So dürfen — entgegen früheren Vorschlägen — nicht mehr alle Leistungsdaten der Versicherten in einem "Leistungskonto" erfaßt und gespeichert werden. Vielmehr ist die versichertenbeziehbare Speicherung ärztlicher Leistungen nur im Rahmen der Stichprobenprüfungen zulässig, der sich pro Quartal zwei Prozent der Ärzte unterziehen müssen. Für die Erprobung der Beitragserstattung, die gewährt wird, wenn keine oder nur geringfügige Leistungen der Krankenversicherung in Anspruch genommen werden, dürfen nicht mehr die einzelnen Leistungen, sondern nur noch Wert und Art der Leistung gespeichert werden. Ergänzt worden ist das Gesetz um Vorschriften für die Datenverarbeitung bei den Kassenärztlichen Vereinigungen und dem Medizinischen Dienst, der, wie bisher der Vertrauensärztliche Dienst, die Krankenkassen begutachtend und beratend bei der Erfüllung ihrer Aufgaben unterstützen wird. Um der Gefahr einer kassenübergreifenden Zentraldatei entgegenzuwirken, verbietet das Gesetz dem Medizinischen Dienst ausdrücklich, Gesundheitsdaten dateimäßig zu verarbeiten. Er darf nur eine Aktennachweisdatei mit Angaben zur Person führen. Durchgesetzt haben sich die Datenschutzbeauftragten auch mit ihrer Forderung, die Verwendung der Rentenversicherungsnummer als Krankenversichertennummer zu unterbinden. Nur für eine Übergangszeit bis Ende 1991 dürfen die Krankenkassen, die die Rentenversicherungsnummer schon jetzt als Versichertennummer nutzen, dieses Ordnungsmerkmal beibehalten. Mit dieser Regelung wird die Einführung eines einheitlichen Personenkennzeichens für den Sozialversicherungsbereich verhindert. Präzisiert worden sind auch Verwendungszweck und Inhalt der Krankenversichertenkarte, die ab 1992 den Krankenschein ersetzen wird. Sie darf nur als

Berechtigungsnachweis und zur Übertragung der auf ihr eingetragenen Angaben (Name, Anschrift, Geburtsdatum, Krankenversichertennummer und Art des Versicherungsverhältnisses) auf die Abrechnungsunterlagen verwendet werden.

Auch wenn durch diese Verbesserungen wesentliche Kritikpunkte ausgeräumt werden konnten, bleibt doch das Problem, daß das Gesetz viele Einzelregelungen, die durchaus Rechte der Versicherten berühren, der Vereinbarung der Verbände überläßt. So z.B. das Verfahren für Wirtschaftlichkeitsprüfungen, das Abrechnungsverfahren und die Datenübermittlung im Fall der Beitragsrückzahlung. Eine endgültige Bewertung der datenschutzrechtlichen Aspekte der Strukturreform des Gesundheitswesens kann deshalb erst erfolgen, wenn diese Vereinbarungen abgeschlossen sind und ihre datenschutzkonforme Ausgestaltung und Anwendung überprüft worden ist.

4.16.1.2 Hamburgisches Krankenhausgesetz

In meinem letzten Tätigkeitsbericht (6. TB, 4.16.1.1) hatte ich über den Referentenentwurf für ein Hamburgisches Krankenhausgesetz und meinen Gegenentwurf für die datenschutzrechtlichen Regelungen berichtet. Leider ist das Gesetzgebungsverfahren seither nicht wesentlich vorangekommen, so daß Hamburg gute Aussichten hat, als "Schlußlicht" bei der Verabschiedung der Landeskrankenhausgesetze zu glänzen.

Für den datenschutzrechtlichen Teil hat die Gesundheitsbehörde immerhin zu verstehen gegeben, daß sie im wesentlichen meine Vorschläge für den Patientendatenschutz übernehmen wird, wenngleich sie in Einzelfragen noch Änderungswünsche hat. Da die Behördenabstimmung noch nicht abgeschlossen ist und auch noch ein Anhörungsverfahren mit den betroffenen Kreisen durchgeführt werden soll, ist noch nicht abzusehen, wann der Gesetzentwurf vom Senat der Bürgerschaft zur Beschlußfassung zugeleitet wird.

4.16.1.3 Hamburgisches Maßregelvollzugsgesetz und Änderung des Gesetzes über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten

Der Entwurf eines Hamburgischen Maßregelvollzugsgesetzes und die damit verbundenen Änderungsvorschläge für das Gesetz über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten (HmbPsychKG) sind im Berichtsjahr den Ausschüssen der Bürgerschaft zur Beratung überwiesen worden. Ich habe weitere Verbesserungen der datenschutzrechtlichen Regelungen angeregt, z.B. die Einfügung einer Unterrichtungspflicht bei der Überwachung des Schriftverkehrs und eine Einschränkung der Befugnis zur Übermittlung von Erkenntnissen aus der Überwachung der Besuche und des Post- und Telefonverkehrs an die Polizei, die meiner Meinung nach nur noch zur Verhütung bestimmter, besonders schwerer Straftaten zulässig sein sollte.

Für die Forschung mit personenbezogenen Daten, die den forschenden Wissenschaftlern im Rahmen der Durchführung des Maßregelvollzugs bzw. der Unterbringung bekannt geworden sind, sollte eine Unterrichtungspflicht der Betroffenen über Art, Umfang und Zweck des Forschungsvorhabens vorgesehen werden, wodurch ihnen grundsätzlich die Möglichkeit zum Widerspruch eingeräumt wird. Etwaige Widersprüche wären dann bei der Prüfung der "schutzwürdigen Belange" des Betroffenen zu berücksichtigen.

Es ist noch nicht abzusehen, wann die Beratungen abgeschlossen sein werden. Noch nicht entschieden ist die Frage, ob an der Verbindung der Beschlußfassung zum Maßregelvollzugsgesetz und zur Änderung des PsychKG festgehalten werden soll. Gegen eine Zusammenfassung der beiden Gesetzgebungsverfahren sind Bedenken geltend gemacht worden, weil die Gefahr besteht, daß der Novellierung des PsychKG als "Anhängsel" nicht die gebührende Aufmerksamkeit zuteil wird und daß Aspekte der Gefahrenabwehr, die im Maßregelvollzug im Vordergrund stehen, in nicht erforderlichem Umfang auf das PsychKG übertragen werden. Ich würde mich einer Trennung beider Gesetzgebungsverfahren mit dem Ziel einer vertiefend zu diskutierenden Änderung des PsychKG unter Berücksichtigung der besonderen Hilfs- und Schutzbedürf-

nisse psychisch Kranker nicht widersetzen, wenn dadurch die Erfüllung meiner langjährigen Forderungen nach Einfügung datenschutzrechtlicher Bestimmungen in das PsychKG nicht auf unabsehbare Zeit verschoben wird.

4.16.1.4 Änderung des Krebsregistergesetzes

Die Gesundheitsbehörde bereitet einen Änderungsentwurf für § 2 Abs. 2 des Hamburgischen Krebsregistergesetzes vor, der die ärztliche Meldung zum Krebsregister ohne Einwilligung des Patienten regelt. Nach geltendem Recht kann die Meldung ausnahmsweise ohne Einwilligung erfolgen, wenn der Patient nicht um seine Einwilligung gebeten werden kann, weil er wegen der Gefahr einer sonst eintretenden ernsten 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.

Diese Regelung hält die Gesundheitsbehörde für unpraktikabel und zu eng, weil sie die Ausnahmefälle auf akut suizidgefährdete Personen beschränkt. Auf eine bedeutsame Gruppe von Patienten sei die Ausnahmeregelung nicht anwendbar, was zu einer Gefährdung der Aussagekraft des Krebsregisters führe. Es handele sich bei dieser problematischen Gruppe überwiegend um Patienten der medizinischen Abteilungen der Krankenhäuser in meist fortgeschrittenem Alter, bei denen entweder das Stadium der Erkrankung keine Primärtherapie, sondern nur noch eine Behandlung von Symptomen zulasse, oder die geistig dekompensiert bzw. wegen starker Sedierung durch Schmerzmittel in ihrer Entscheidungsfähigkeit eingeschränkt seien. Diese Patienten würden in der Regel über ihre Krebserkrankung nicht aufgeklärt und könnten deshalb nicht um ihre Einwilligung zur Meldung an das Krebsregister gebeten werden. Die Erfahrungen mit der Meldepraxis hätten gezeigt, daß die Einholung der Einwilligung bei therapierbaren Patienten unproblematisch sei, denn diese Patienten seien in der Regel über ihre Erkrankung aufgeklärt und verweigerten nur in Ausnahmefällen die Zustimmung zur Weitergabe ihrer Daten an das Krebsregister.

Um eine Meldung wenigstens eines Teils der nicht aufgeklärten Patienten zu ermöglichen, hat die Gesundheitsbehörde vorgeschlagen, die Ausnahmeregelung künftig wie folgt zu fassen: "Die Meldung kann ausnahmsweise ohne Einwilligung des Patienten erfolgen, wenn der Patient nicht nur vorübergehend einwilligungsunfähig ist oder weil er wegen der Gefahr einer sonst eintretenden ernsten 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." Die Dokumentationspflicht soll unverändert bestehen bleiben.

In den Beratungen mit der Gesundheitsbehörde habe ich deutlich gemacht, daß ich zwar Verständnis für die Bemühungen habe, die Aussagefähigkeit des Krebsregisters zu erhöhen, daß aber die Meldung ohne Einwilligung des Betroffenen nicht von der Ausnahme zur Regel werden darf. Nach einer Umfrage der Gesundheitsbehörde sind in einzelnen medizinischen Abteilungen mehr als die Hälfte der Patienten nicht über ihre Krebserkrankung aufgeklärt und werden deswegen auch nicht um ihre Einwilligung zur Meldung zum Krebsregister gebeten. Wegen des uneinheitlichen Umfrageergebnisses ist es mir bisher unmöglich, abzuschätzen, mit welcher Quote von Meldungen ohne Einwilligung bei einer Regelung wie der vorgeschlagenen zu rechnen wäre. Die Gesundheitsbehörde hat mir dazu weitere Informationen zugesagt.

Im Prinzip halte ich eine Erweiterung des Ausnahmetatbestandes auf nicht nur vorübergehend einwilligungsunfähige und gesundheitlich besonders gefährdete Patienten für akzeptabel, nicht aber die Ausdehnung der Ausnahmeregelung auf alle nicht aufgeklärten Krebserkrankten. Nach meinem Verständnis von Selbstbestimmung und einem vertrauensvollen Arzt-Patienten-Verhältnis halte ich es nicht für geboten, Patienten, die nicht mehr kausal behandelt werden können, grundsätzlich nicht aufzuklären. Offenbar ist die Aufklärungspraxis, wie die Umfrage der Gesundheitsbehörde belegt, auch in Abteilungen gleicher Fachrichtung sehr unterschiedlich. Deshalb könnte auch

ein Hinwirken auf eine verbesserte Aufklärung der Patienten zu einer Erhöhung der Meldungen an das Krebsregister beitragen.

4.16.2 Gesundheitsämter

Datenschutz im Gesundheitsamt ist ein Dauerthema in meinen Tätigkeitsberichten. Im vorangegangenen Berichtsjahr hatte ich über die abschließenden Arbeitsergebnisse des Arbeitskreises "Datenschutz im Gesundheits- und Umweltamt" zu den Themen "Gutachterwesen", "Überwachung des BTM-Verkehrs" und "Geburts- und Todesbescheinigungen" berichtet. Diesen Arbeitskreis hatten Vertreter der Gesundheitsbehörde und der Bezirksgesundheitsämter zur Aufarbeitung der datenschutzrechtlichen Probleme gebildet, die bei der Prüfung eines Bezirksgesundheitsamtes in den Jahren 1984/85 sichtbar geworden waren. Nachzutragen sind die Arbeitsergebnisse der Arbeitsgruppen "Zentralkartei", "Medizinalkartei" und "Sozial- und Jugendpsychiatrischer Dienst".

Die Ergebnisse der zum Teil mühsamen und langwierigen Verhandlungen in den Arbeitsgruppen bleiben nicht zuletzt deswegen unbefriedigend, weil die gesetzlichen Grundlagen für die Datenverarbeitung im Gesundheitsamt unzureichend und nicht mehr zeitgemäß sind. In den z.T. über 60 Jahre alten Vorschriften fehlen über die sehr allgemein gehaltenen Aufgabenzuweisungen hinausgehende, konkrete Befugnisnormen für die Erhebung, Speicherung und Nutzung personenbezogener Daten, so daß sich das Bewußtsein für eine zweckgebundene Datenverarbeitung nur unzureichend entwickeln konnte. Traditionell verstanden sich die Gesundheitsämter trotz vielfältiger, teils hoheitlich auszuübender, teils beratender und helfender Aufgaben als organisatorische Einheit, die alle dort vorhandenen Informationen uneingeschränkt nutzen darf.

Die Gesundheitsbehörde als zuständige Fachbehörde hat meine wiederholten Forderungen, den Entwurf bereichsspezifischer gesetzlicher Grundlagen zu erarbeiten, bisher nicht aufgegriffen. Auch sie hält die Schaffung zeitgemäßer Regelungen für den öffentlichen Gesundheitsdienst für erforderlich, jedoch behindern aus ihrer Sicht mangelnde Kapazität und schwierige politische Durchsetzbarkeit eine zügige Verwirklichung dieses Vorhabens. Ich rege an, dieses Problem gemeinsam mit den anderen betroffenen Bundesländern anzugehen und einen Musterentwurf zu erarbeiten. Bisher liegt nur mit dem Bayerischen Gesetz über den öffentlichen Gesundheitsdienst aus dem Jahre 1986 eine Regelung vor, die datenschutzrechtlichen Belangen Rechnung trägt. Zu den einzelnen Arbeitsgruppenergebnissen:

1) Zentralkartei

Für die Führung der Zentralkartei wurde eine Dienstanweisung mit dem Inhalt erlassen, daß die Zentralkartei nur noch als interne Datei für die Postverteilung verwendet werden darf. Die Erteilung von Auskünften an Dritte, auch an andere Dienststellen, ist nicht mehr zulässig. Als Daten dürfen nur noch Name, Vorname, Geburtsdatum, aktenführende Abteilung und Akten- oder Ordnungszeichen erfaßt werden. Es werden nur Vorgänge aufgenommen, die in den Abteilungen für Gutachterwesen, Körperbehinderten-Fürsorge und Sozialpsychiatrische Dienste anfallen. Die Datei darf nicht dazu genutzt werden, Erkenntnisse aus der Beratungstätigkeit dieser Dienststellen für den hoheitlichen Funktionsbereich zu erschließen. Geregelt sind ferner Zugangsberechtigung, Datensicherungsmaßnahmen und Aufbewahrungsfristen.

2) Medizinalkartei

In der Medizinalkartei, die der Überprüfung des Berechtigungsnachweises von Medizinalpersonen, der Überwachung ihrer Betätigung in den Grenzen ihres Befähigungszeugnisses sowie der Überwachung der Ausübung des Heilgewerbes durch staatlich nicht anerkannte Heilpraktiker dient, dürfen von allen registrierten Personen nur die Daten erfaßt und gespeichert werden, die zur Erfüllung der Aufgaben des Gesundheitsamtes erforderlich sind.

Eine sog. "tote Kartei" für aus dem Beruf ausgeschiedene oder verzogene Medizinalpersonen darf nicht geführt werden. Wechselt eine Medizinalperson innerhalb Ham-

burgs in den Zuständigkeitsbereich eines anderen Gesundheitsamtes, kann die Karteikarte mit ihrem Einverständnis an das nunmehr zuständige Gesundheitsamt übersandt werden. Bei Verlagerung der Tätigkeit aus Hamburg heraus oder bei Aufgabe der Tätigkeit ist die Karteikarte zu vernichten. Eine Besonderheit gilt für Ärzte, die ihre Praxis aufgeben, da sie noch privatärztlich oder als Praxisvertreter tätig sein können. Die Karteikarte ist dann, mit Einverständnis des Arztes, an das Gesundheitsamt des Wohnbezirks zu übermitteln.

3) Sozial- und Jugendpsychiatrischer Dienst

Die Sozial- und Jugendpsychiatrischen Dienste der Gesundheits- und Umweltämter bieten aufgrund des Hamburgischen Gesetzes über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten (PsychKG) Hilfe und Beratung für psychisch Kranke an, treffen aber auch Maßnahmen zur Abwendung einer Selbstgefährdung oder einer Gefährdung der öffentlichen Sicherheit und Ordnung, bis hin zur zwangsweisen Unterbringung in einer geschlossenen Anstalt.

Aus der engen Verbindung von beratender und hoheitlicher Funktion, die in Krisensituationen häufig ineinander übergehen, ergeben sich erhebliche datenschutzrechtliche Probleme, um deren Lösung in der Arbeitsgruppe in langen und kontroversen Diskussionen gerungen wurde. Es wurde Einigkeit darüber erzielt, daß grundsätzlich eine der Situation angemessene Information des Bürgers darüber erforderlich ist, in welcher Rechtsbeziehung er sich zu den Diensten befindet und ob Daten über ihn auf freiwilliger Basis oder auf gesetzlicher Grundlage erhoben werden. Bei gestörter Auffassungsfähigkeit des Patienten ist ggf. die Information zu einem geeigneten Zeitpunkt zu wiederholen. Wünsche des Patienten, seine Daten nicht aufzuzeichnen, sollen berücksichtigt werden. Allerdings sind Daten, die für die Dokumentation des Krankheitsverlaufs und zum Verständnis der getroffenen oder der zu treffenden Maßnahmen unbedingt erforderlich sind, auch gegen den Wunsch des Patienten in der Akte festzuhalten. Eine Löschung bereits früher aufgezeichneter Daten kann vom Patienten grundsätzlich nicht allein deshalb verlangt werden, weil er deren Aufzeichnung nunmehr nicht mehr wünscht.

Eine Information des Patienten über notwendige Datenübermittlungen an andere Dienste, z.B. bei Überschreitung der Altersgrenze vom Jugendpsychiatrischen zum Sozialpsychiatrischen Dienst oder beim Umzug des Patienten in den Zuständigkeitsbereich eines anderen Bezirksamtes, soll nur anlaßbezogen, nicht aber pauschal von vornherein gegeben werden. Bei Erreichen des 18. Lebensjahres des Klienten hat der Jugendpsychiatrische Dienst in jedem Einzelfall zu prüfen, ob eine Entlassung aus der Betreuung verantwortet werden kann oder ob der Vorgang an den Sozialpsychiatrischen Dienst weitergeleitet werden soll. Nach Möglichkeit soll die Aktenübermittlung im Einvernehmen mit dem Klienten erfolgen, wenn aber die weitere Betreuung aus in der Krankheit liegenden Gründen unbedingt geboten ist, sind die Akten auch ohne bzw. gegen den Willen des Betroffenen weiterzugeben.

Zuvor ist die Akte darauf zu überprüfen, daß unter dem Aspekt der Funktionalität unnötige Datenübermittlungen unterbleiben, notwendige Daten aber übermittelt werden. Innerhalb des gesetzlichen Rahmens muß nach therapeutischen Gesichtspunkten gehandelt werden. Das gleiche gilt für die Fälle, in denen ein betreuter Bürger entweder in den Zuständigkeitsbereich eines anderen Bezirksamtes oder in den außerhamburgischen Bereich umzieht.

Diese Grundsätze sind — vor dem Hintergrund der geplanten Ergänzung des PsychKG um Vorschriften zur Datenverarbeitung — als Übergangsregelung zu verstehen.

Zur Aktenführung wurde von den Diensten darauf hingewiesen, daß eine Rückgriffsmöglichkeit auf früher erhaltene Informationen und vorgeleistete Tätigkeiten unabdingbar ist, um für den Bürger notwendige Hilfen umfassend leisten zu können. Eine Einwilligung des Bürgers in die Nutzung dieser Akten sei, allein schon aus Krankheitsgründen, in Notsituationen häufig gar nicht zu erzielen.

Dieser Argumentation habe ich mich nicht entziehen können, habe aber gefordert, daß der Betroffene in geeigneter Form darüber aufzuklären ist, daß die von ihm erhaltenen Informationen zu einer späteren Verwendung aktenmäßig erfaßt werden und daß er der Speicherung widersprechen kann. Die Aktenaufbewahrungsfrist beträgt 15 Jahre, beginnend nach der letzten Aktivität des Dienstes.

Einigkeit wurde auch darüber erzielt, daß keine polizeilichen Meldungen über Freitodversuche an die Jugend- und Sozialpsychiatrischen Dienste mehr erfolgen. Die Krankenhäuser sind nochmals aufgefordert worden, im Rahmen einer Behandlung im Krankenhaus im Anschluß an einen Freitodversuch auf die Möglichkeit einer anschließenden Betreuung durch geeignete Institutionen hinzuweisen und den Patienten zu bitten, in die Weitergabe seiner Daten an die Dienste einzuwilligen.

4.16.3 Prüfung der Blutspenderverwaltung des Zentralinstituts für Transfusionsmedizin

Mit einem Spenderstamm von über 15.000 Personen und ca. 58.000 Blutspenden pro Jahr ist das Zentralinstitut für Transfusionsmedizin Hamburgs bedeutendster Blutspendedienst.

Im Rahmen der Spenderverwaltung werden sensible, der ärztlichen Schweigepflicht unterliegende personenbezogene Daten erhoben und verarbeitet, unter anderem, um die gesundheitliche Eignung des Spenders und die Einhaltung von Sperrfristen zu kontrollieren und um sicherzustellen, daß in Notfällen geeignete Spender zur Verfügung stehen.

Die Speicherung eines Teils der Daten erfolgt mittels PC in einer Blutspenderdatei, im übrigen werden die Daten aktenmäßig verarbeitet. Rechtsgrundlage für die Erhebung und Speicherung ist die Einverständniserklärung des Blutspenders, durch die ein Vertragsverhältnis mit dem Blutspendedienst begründet wird. Per Formblatt erklärt der Spender, daß er mit der Einholung von Auskünften über frühere Krankheiten einverstanden ist und daß er keiner AIDS-Risiko-Gruppe angehört.

Nach meiner Feststellung genügen die verwendeten Formulare nicht den Anforderungen an eine wirksame Schweigepflichtentbindungserklärung vor der Einholung von Informationen über den Spender und an eine umfassende Aufklärung als Grundlage für eine wirksame Einwilligung vor einem ärztlichen Eingriff, wie ihn die Blutentnahme mit obligatorischer Testung auf HIV-Antikörper darstellt. Ich habe daher mit dem Zentralinstitut vereinbart, die Einwilligungserklärung zu konkretisieren und insbesondere den HIV-Test mit einzubeziehen.

Gegen die automatisierte Datenverarbeitung habe ich in einem Punkt Bedenken angemeldet: Bei Verdacht auf eine Infektionskrankheit, die einer Verwendung der Blutkonserve entgegensteht (z.B. Hepatitis, Lues, HIV), enthält die Blutspenderdatei während der Zeitspanne für die erforderlichen Kontrolluntersuchungen einen nach Infektionsart differenzierten Hinweis auf die Sperrung der Spende. Statt einer Aufschlüsselung der Verdachtsdiagnose halte ich einen allgemeinen Sperrvermerk mit Hinweis auf nähere Informationen in der Blutspenderakte für ausreichend. Das Zentralinstitut hat zugesagt, das Programm entsprechend zu ändern.

Wenn der Spender aufgrund einer festgestellten Infektion endgültig vom Blutspenden ausgeschlossen werden muß, werden seine Daten in der Datei gelöscht. Informationen über die Sperrung und deren Grund sind dann nur noch in der Blutspenderakte, die wie eine Krankenakte geführt wird, enthalten.

Übermittlungen personenbezogener Daten an andere Blutspendedienste finden nicht statt, an behandelnde Ärzte nur nach Einholen einer Einwilligungserklärung im Einzelfall. Für die Produktverwaltung ist langfristig eine Vernetzung der Blutspendedienste zur Verbesserung der Vorratshaltung geplant, die aber aufgrund einer Verschlüsselung der Kennzeichnung nur dem einzelnen Blutspendedienst ermöglicht, seine eigenen Spender zu reidentifizieren. Hiergegen bestehen aus datenschutzrechtlicher Sicht keine Bedenken.

5. EINZELNE PROBLEME DES DATENSCHUTZES IM NICHT-ÖFFENTLICHEN BEREICH

5.1 Versandhandel/Interne Bonitätsprüfung

Ich hatte im 6. Tätigkeitsbericht (6. TB, 5.1.1, S. 121) über das interne Bonitätsprüfungsverfahren eines Versandhandels-Unternehmens berichtet. Zur Absicherung von Kreditrisiken, die mit der Vergabe eines Kundenkontos bei Erstbestellern verbunden sein können, welches es dem Besteller erlaubt, bis zu einer bestimmten Grenze Waren gegen offene Rechnung zu beziehen, hat das Unternehmen ein Verfahren entwickelt, bei dem anhand der vom Besteller angegebenen Daten eine abstrakte Bonitätsprüfung durchgeführt wird. Unter Verwendung der vom Kunden übermittelten Daten werden bestimmte Wahrscheinlichkeitsrechnungen angestellt, um zu klären, wie die Bonität des Betroffenen zu beurteilen ist und von welchen wirtschaftlichen Risiken das Unternehmen aufgrund der prognostischen Bewertung ausgehen muß.

Bei einer Untersuchung dieses Bonitätsprüfungsverfahrens bin ich zu dem Ergebnis gekommen, daß Kundenrechte aus dem Bundesdatenschutzgesetz unmittelbar nicht verletzt sind, da tatsächlich alle erfragten Daten für die vom Versandhaus vorgesehene Bonitätsprüfung erforderlich sind und der Kunde diese Angaben freiwillig hergibt.

Ich meine allerdings, daß der Kunde, wenn das Versandhaus es aufgrund der Bonitätsprüfung ablehnt, ein Kundenkonto einzurichten, hinreichend über die dafür maßgeblichen Gründe informiert werden muß, um ggf. seine Interessen geltend machen zu können. Diese Aufklärung ist unerläßlich, das zeigen immer wieder Eingaben von Bürgern, weil ansonsten Mißverständnisse und Vermutungen darüber entstehen können, das Versandhaus habe sich zu Unrecht über Dritte wirtschaftliche Negativdaten zur Person des Betroffenen beschafft.

Die jetzige Informationspraxis des Versandhandels-Unternehmens genügt diesen Erfordernissen nicht. Danach wird der Kunde lediglich formularmäßig aufgeklärt, daß nach den das Versandhaus bindenden Kreditbestimmungen keine Möglichkeit gesehen wird, ein Konto zu eröffnen. Ich meine, es wäre auch im Interesse des Versandhandels-Unternehmens, daß über die Gründe zur Versagung eines Kundenkontos detaillierter unterrichtet wird, um unnötige Auseinandersetzungen mit Rückfragen ihrer Kunden zu vermeiden. Das hieße, der Kunde müßte also davon in Kenntnis gesetzt werden, daß er bei einer Bonitätsprüfung durch das Selektionsraster gefallen ist. Ihm müßte zugleich angeboten werden, daß er zum Ergebnis dieser Prüfung Gegenvorstellungen erheben kann, denn da es sich um ein abstraktes Prüfungsverfahren handelt, bei dem die tatsächlichen Verhältnisse des Einzelfalles nicht hinreichend berücksichtigt werden können, kann es u.U. zu einer fehlerhaften hypothetischen Bewertung gekommen sein. Ich beabsichtige, eine solche im Interesse der Kundenaufklärung gebotene Informationspolitik mit den Versandhandels-Unternehmen abzustimmen.

5.2 Kreditwirtschaft/SCHUFA

5.2.1 Neues SCHUFA-Verfahren: kartellrechtliche Entwicklung

Nach dem sog. SCHUFA-Urteil des Bundesgerichtshofs vom 19. September 1985 hatte die SCHUFA einigen ihrer bisherigen Vertragspartner gekündigt, bei denen sich nicht der für den Anschluß an das SCHUFA-Auskunftsverfahren erforderliche Nachweis führen ließ, daß sie Risiken bei der Vergabe von Konsumenten (Endverbraucher)-Krediten eingehen, sondern lediglich Risiken aus sog. wirtschaftlichen Vorleistungen übernehmen. Dagegen hatten sich einzelne Vertragspartner beschwerdeführend an das Bundeskartellamt gewandt, weil sie durch die Kündigung das Diskriminierungsverbot des § 26 GWB als verletzt ansahen. Die daraufhin vom Bundeskartellamt durchgeführten Diskriminierungsverfahren waren bereits zum Zeitpunkt meines letzten Tätigkeitsberichtes (6. TB, 5.2.1, S. 123 bis 126) weitgehend abgeschlossen.

Offen war zuletzt noch, ob Inkasso-Büros und Kreditversicherer, die z.T. das Inkasso der bei ihnen versicherten Forderung betreiben, obwohl sie keine Konsumentenkredite

vergeben, SCHUFA-Vertragspartner sein dürfen, um jedenfalls die SCHUFA-Daten zur Suche nach verschwundenen Schuldnern benutzen zu können. Das Interesse der Inkasso-Unternehmen besteht nämlich im wesentlichen darin, bei Schuldnern mit titulierten Forderungen nach erfolglosen Vollstreckungsversuchen die aktuelle Anschrift des Schuldners zu erfahren. Als Gegenleistung erwartet die SCHUFA die Einmeldung offener titulierter Forderungen, fruchtloser Pfändungen sowie ggf. der Erledigung der Forderung. Eine Öffnung des SCHUFA-Systems für Inkasso-Büros hätte im übrigen eine Änderung der von den Kreditinstituten verwendeten SCHUFA-Klauseln vorausgesetzt.

Ich neige dazu, dem inzwischen von der Kreditwirtschaft unterbreiteten Vorschlag zuzustimmen, für die Inkasso-Unternehmen den Anschluß an das SCHUFA-System — begrenzt auf die Teilnahme am sog. Suchdienst — zu ermöglichen. Denn da aus dem Kreditinformationssystem der SCHUFA keine Negativdaten zur Verfügung gestellt werden sollen, sondern allein die aktuelle Anschrift des Schuldners, sehe ich keine schutzwürdigen Belange der Betroffenen berührt. Diese können jedenfalls nicht darin geschützt werden, ihren Aufenthaltsort verborgen zu halten.

Umgekehrt begegnet es keinen Bedenken, wenn als Gegenleistung für die Teilnehmer am Suchdienst titulierte Forderungen eingemeldet werden sollen, weil es sich hierbei um eindeutig kreditrelevante Daten im Sinne des SCHUFA-Urteils des BGH vom 19.9.1985 handelt.

Mit der von der Kreditwirtschaft vorgeschlagenen Ergänzung der SCHUFA-Klausel wird auch den Forderungen der Datenschutz-Aufsichtsbehörden nach einer hinreichenden Information des Kunden zu möglichen Übermittlungen seiner personenbezogenen Daten im wesentlichen Rechnung getragen. Allerdings ist für die erforderliche "informierte Einwilligung" klarzustellen, welche Daten aus dem Geschäftsbereich der Banken von der SCHUFA an die Inkasso-Unternehmen zu welchen Zwecken weitergegeben werden. Die Klausel sollte deshalb lauten:

"Die SCHUFA speichert die Daten, um den ihr angeschlossenen Kreditinstituten ... Informationen zur Beurteilung der Kreditwürdigkeit von Kunden geben zu können. Außerdem können Unternehmen, die gewerbsmäßig Forderungen einziehen, Vertragspartner sein. Diese Unternehmen erhalten nur Adreßdaten für ihren Schuldner-Suchdienst. Die SCHUFA stellt die Daten ..."

Dieser Problemkomplex muß noch mit der SCHUFA und den Verbänden der Kreditwirtschaft abgestimmt werden.

5.2.2 Erschleichen von SCHUFA-Auskünften

Immer wieder erreichen mich Beschwerden darüber, daß unberechtigt bei der SCHUFA angefragt wird. Dabei sind zwei Fälle zu unterscheiden. Es kommt vor, daß ein SCHUFA-Vertragspartner ein wirtschaftliches Interesse an einer SCHUFA-Auskunft hat, das die SCHUFA jedoch ablehnen müßte, weil nur mit den vertraglich genau festgelegten Begründungen angefragt werden darf. Andererseits fragen auch Mitarbeiter eines Unternehmens, das als SCHUFA-Vertragspartner durchaus zu Anfragen berechtigt ist, nicht aus geschäftlichen, sondern aus ganz privaten Gründen an.

Da sich die SCHUFA bei jeder Anfrage das jeweilige Interesse angeben läßt, muß ein unbefugter Interessent der SCHUFA eine unwahre Begründung liefern.

So kam es vor, daß ein Kreditinstitut eine SCHUFA-Auskunft über eine Person abforderte, mit der es in keiner geschäftlichen Beziehung stand, um die so erhaltenen Informationen aus Gefälligkeit an einen Kunden weiterzugeben, der sich als Vermieter für diese Person interessierte. In diesem Fall wurde die SCHUFA-Anfrage mit einem — nicht existierenden — Antrag auf Eröffnung eines Girokontos begründet. Der Betroffene erfuhr von dieser Anfrage, weil er sich eine Eigenauskunft über seine Daten von der SCHUFA geben ließ.

In einem anderen Fall hatte ein Mitarbeiter eines Kreditinstituts eigenmächtig eine SCHUFA-Auskunft eingeholt, weil er — aufgrund eines privaten Interesses als Vermie-

ter — Informationen über einen Mietbewerber erhalten wollte. Auch hier wurde der SCHUFA ein Grund für die Anfrage genannt, den es tatsächlich nicht gab.

In einem dritten Fall wurde eine Anfrage mit der Begründung eines Ratenkredits vorgenommen, obwohl tatsächlich eine Personaleinstellung beabsichtigt war, für die nach einer eindeutigen Regelung in den SCHUFA-Verträgen eine Auskunft nicht eingeholt werden darf.

In allen drei Fällen waren die Datenübermittlungen unzulässig. Ich habe die Betroffenen darauf hingewiesen, daß sie durch einen Strafantrag prüfen lassen können, ob eine strafbare Handlung vorlag. Meine strafrechtliche Bewertung eines solchen Vorgangs habe ich im 5. TB, Nr. 6.6.6.1 — allerdings in Bezug auf eine Wirtschaftsauskunftei — näher erläutert.

Diese Vorfälle zeigen im übrigen, daß alle, die unberechtigt bei der SCHUFA anfragen oder einen falschen Grund für eine Anfrage angeben, damit rechen müssen, entdeckt zu werden. Es wird deutlich, wie wichtig die Eigenauskunft für den Betroffenen sein kann und welche Konsequenzen sie für Personen haben kann, die sich nicht korrekt verhalten.

5.2.3 Identitätsprüfung und Verbreitungsverbot von SCHUFA-Daten bei nicht feststehender Identität

Den Datenschutz-Aufsichtsbehörden werden immer wieder Fälle bekannt, in denen es aufgrund einer unzureichenden Identitätsprüfung zur beauskunfteten Person zu Personenverwechslungen mit nachteiligen Folgen für den Betroffenen kommt. Als problematisch erweisen sich insofern vor allem die Informationen, die die SCHUFA aus dem Schuldnerverzeichnis erhält, bei denen i.d.R. das Geburtsdatum der betreffenden Person nicht vorliegt, da dieses Datum im Schuldnerverzeichnis bisher nicht geführt wird. Die Informationen aus dem Schuldnerverzeichnis betreffen hochsensible Negativmeldungen, da es sich um die Registrierung eidesstattlicher Versicherungen über die Vermögensverhältnisse der betreffenden Person oder die Haftanordnung zur Erzwingung der Abgabe einer eidesstattlichen Versicherung handelt. Die Folgen falscher SCHUFA-Meldungen aufgrund einer Personenverwechslung können darum für den Betroffenen von gravierender Art sein.

Die SCHUFA verfährt dabei so, daß Eintragungen im Schuldnerverzeichnis von der SCHUFA übernommen und beauskunftet werden mit dem Hinweis:

"Unter Vorbehalt, da ohne Geburtsdatum gemeldet.
Nutzungsverbot, wenn Identität durch Auskunftsempfänger nicht feststellbar."

Die SCHUFA meint, sie habe damit alles getan, um Identifizierungsfehler zu vermeiden. Im übrigen ergebe sich die gleiche Problematik für den Datenempfänger oft dann, wenn er Daten unmittelbar aus einem Schuldnerverzeichnis entnehme, welches bei dem örtlichen Amtsgericht geführt wird. In diesem Falle erhalte der Anfragende nicht einmal — wie bei der SCHUFA — den Hinweis, daß die Identität wegen des fehlenden Geburtsdatums gesondert nachzuprüfen sei. Die SCHUFA meint deshalb, bevor von ihr weitere Vorkehrungen verlangt würden, müßten auch den Amtsgerichten entsprechende Verpflichtungen zum Führen des exakten Identitätsnachweises auferlegt werden.

Ich bin mir hingegen mit den anderen Aufsichtsbehörden einig, daß die SCHUFA selbst weitere Sicherungsvorkehrungen zur Vermeidung von Personenverwechslungen treffen muß. Der Hinweis der SCHUFA, daß Daten ohne Geburtsdatum nicht genutzt werden dürfen, wenn die Identität durch den Auskunftsempfänger nicht feststellbar ist, kann sie von ihrer Verpflichtung, nur richtige Daten zu speichern, nicht entlasten.

Auch nach einem Beschluß des Hanseatischen Oberlandesgerichts Hamburg, über den ich im 6. Tätigkeitsbericht (vgl. 5.2.4, S. 127 f.) berichtet habe, sollen Daten, die nur möglicherweise auf eine bestimmte Person zutreffen, möglicherweise aber bezogen auf diese Person unrichtig sind, in analoger Anwendung von § 35 Abs. 2 Satz 1 BDSG

nicht verarbeitet und verwendet werden dürfen. Diese Rechtsfolge dürfe nicht dadurch umgangen werden, indem die Daten nach Auftreten von Richtigkeitszweifeln etwa mit dem einschränkenden Zusatz, ihre Richtigkeit stehe nicht fest, nun doch weiterverwendet würden; sie unterlägen vielmehr schlechthin der Sperrung.

Die SCHUFA hat mitgeteilt, daß sie in der Praxis auf der Basis des Beschlusses des Hanseatischen Oberlandesgerichts arbeite. Voraussetzung einer Sperrung solcher Daten mit einer unklaren Identitätszuordnung ist jedoch, daß ihre Richtigkeit vom Betroffenen bestritten wird, er also selbst das Vorliegen einer Personenverwechslung anzeigt. Um aber einem aufgrund einer Personenverwechslung zu Unrecht gemeldeten Betroffenen die Gelegenheit zu geben, sich mit einem entsprechenden Sperrungsverlangen an die SCHUFA zu wenden, muß er Kenntnis von entsprechenden Übermittlungsvorgängen erhalten. Das geschieht am einfachsten, wenn der Informationsempfänger in den Fällen, in denen die Identität ungeklärt geblieben ist, Nachfragen bei dem "angeblichen" Betroffenen hält. Hierbei ist zu klären, ob es sich um den "richtigen" Betroffenen handelt, außerdem müßte das Datenmaterial der SCHUFA durch das Ergebnis der Nachforschungen ergänzt werden.

Die Datenschutz-Aufsichtsbehörden haben der SCHUFA deshalb vorgeschlagen, in ihren Anschlußbedingungen die Anschlußnehmer in allen Fällen, in denen sie eine Meldung ohne Geburtsdatum erhalten haben, zu einer Rückmeldung zu verpflichten und nicht nur — wie es jetzt schon vorgesehen ist —, wenn der Auskunftsempfänger die Identität nicht eindeutig feststellen kann. Nur mit dieser regelmäßigen Mitteilungspflicht läßt sich durchsetzen, daß der Datenempfänger nicht einfach untätig bleibt, sondern auch tatsächlich Nachforschungen zur Identität des Betroffenen anstellt, weil er nämlich über das Ergebnis seiner Ermittlungen in jedem Fall Rechenschaft abzulegen hat. Auch wäre so zu gewährleisten, daß die SCHUFA den von ihr gespeicherten Datenbestand nicht nur im Falle negativer Identitätsprüfungen, sondern auch bei positiven Identitätsfeststellungen überarbeiten und auf den aktuellen und sachlich zutreffenden Stand bringen kann. Die Rückmeldungen sollen nach dem unterbreiteten Vorschlag innerhalb von vierzehn Tagen erfolgen. Die SCHUFA muß die Rückmeldungen fristgebunden (30 Tage) überwachen. Ergibt die Rückmeldung, daß die eidesstattliche Versicherung oder Haftanordnung nicht die beauskunftete Person betrifft, hat die SCHUFA dies intern zu vermerken, damit ausgeschlossen werden kann, daß bei einer weiteren Anfrage nochmals die eidesstattliche Versicherung oder die Haftanordnung bei dieser Person beauskunftet werden.

Die SCHUFA hat darauf hingewiesen, daß bei einer Meldung über eine fehlende Identität selbstverständlich schon jetzt ein entsprechender Eintrag im SCHUFA-Datenbestand vorgenommen werde. Sie betrachtet es allerdings als unnötigen Verwaltungsaufwand, auch bei einer positiven Identitätsprüfung eine obligatorische Meldung vorzusehen, da in diesem Fall nicht unbedingt zusätzliche Schritte erforderlich seien. Auch hält sie den Vorschlag, der Informationsempfänger solle zur Klärung der Identität bei dem angeblichen Betroffenen nachfragen, nur zum Teil für realistisch und insofern werde er bereits praktiziert, wenn nämlich der Vertragspartner der SCHUFA mit dem Betroffenen unmittelbar persönlichen Kontakt habe. Nicht zu übertragen sei der Vorschlag aber beispielsweise auf ein Versandhaus als Datenempfänger, da diesem nicht zugemutet werden könne, vor einer Entscheidung über eine Lieferung auf Rechnung den Betroffenen anzuschreiben und um Auskunft zu der SCHUFA-Eintragung zu bitten.

Eine Lösung des Problems von Personenverwechslungen könnte sicherlich auch in einer Novellierung des § 915 ZPO gesucht werden, indem das Geburtsdatum zu den Daten hinzugenommen würde, die in dem Schuldnerverzeichnis zu erfassen sind. Mit hoher Wahrscheinlichkeit muß jedoch davon ausgegangen werden, daß ein solcher Novellierungsvorschlag in der auslaufenden Legislaturperiode nicht mehr Gesetz wird, so daß uns die Folgen unklarer Identitätszuordnungen auch in der Zukunft beschäftigen werden.

5.2.4 Löschen von Anfragen bei der SCHUFA

Wie bereits im 6. Tätigkeitsbericht unter 5.2.3 geschildert, sind einige ehemalige SCHUFA-Vertragspartner dazu übergegangen, vom Betroffenen die sog. Eigenauskunft zu verlangen. Aber auch andere Unternehmen lassen sich gern diese Auskunft vom Betroffenen selbst vorlegen, weil sie auf diesem Wege ohne eigene Kostenbelastung gesicherte Informationen erhalten. Dazu ist anzumerken, daß der Betroffene einen Rechtsanspruch auf diese Auskunft der SCHUFA über die zu seiner Person gespeicherten Daten hat. Diese Auskunft ist umfangreicher als diejenige, die ein SCHUFA-Vertragspartner im Rahmen des üblichen Auskunftsverkehrs erhält. Beispielsweise durchbricht die SCHUFA ihren Grundsatz der Neutralität — nämlich nicht weiterzumelden, welche Information von welcher Stelle kommt — in der Auskunft an den Betroffenen zugunsten der Transparenz; ihm wird mitgeteilt, welches Kreditinstitut ein Girokonto eingemeldet hat und welches andere ggf. eine Anfrage an die SCHUFA richtete und wie diese Anfrage begründet worden war. Diese Anfragen werden seit mehr als zwei Jahren nicht mehr nur für zehn Tage, sondern für die Dauer eines ganzen Jahres gespeichert und in der Auskunft an den Betroffenen offengelegt.

Bei Vorlage dieser vollständigen Auskunft bei Dritten erscheint der Betroffene u.U. in einem nicht so günstigen Licht, wenn in jüngerer Zeit mehrere Anfragen mit einem Kreditantrag begründet waren, ein Kredit letztlich jedoch nicht gegeben wurde. Einige Betroffene verlangten deshalb von der SCHUFA die Löschung dieser gespeicherten Anfragen.

Eine Berechtigung, diese Daten auf direktem Wege von der SCHUFA zu erfahren, hätte ein Vertragspartner der SCHUFA nicht. Ihm würde, da diese Information nur für eine kurze Zeit tatsächlich für eine Bonitätsprüfung von Bedeutung sein könnte, nur innerhalb eines Zeitraumes von 10 Kalendertagen die Tatsache einer Anfrage, nicht aber das interessierte Unternehmen gemeldet werden. Die SCHUFA wäre deshalb durchaus bereit, diese Daten auf Antrag des Betroffenen zu löschen. Wegen des Konflikts mit der Pflicht zur Aufzeichnung des berechtigten Interesses an einer Datenübermittlung (§ 32 Abs.2 Satz 2 BDSG) trat die SCHUFA an die Länder-Aufsichtsbehörden heran, um gemeinsam nach einer Lösung zu suchen. Nachdem ich im 6. Tätigkeitsbericht keine ernsthaften Bedenken geäußert hatte, hat die SCHUFA GmbH Hamburg im Einzelfall diese Löschung auf Antrag vorgenommen.

In einem Gespräch zwischen der SCHUFA und einer Arbeitsgruppe des "Düsseldorfer Kreises" erläuterte die SCHUFA zusätzlich, daß sie die Löschung nur vornehmen wolle, wenn der Betroffene vorab seine Eigenauskunft abgefordert und die Löschung schriftlich verlangt habe. Diese Unterlage würde aufbewahrt werden, damit der Vorfall auch später nachvollzogen werden könne.

Die Aufsichtsbehörden meinten, sie könnten dem Verfahren zustimmen, weil in diesem Falle immer die Initiative vom Betroffenen ausginge und er bereits über alle Speicherungen und Datenübermittlungen informiert sei. Die Aufzeichnung des berechtigten Interesses würde zwar nicht mehr, wie in allen anderen Fällen, im Datenbestand der SCHUFA gespeichert sein, sondern in der Sammlung der schriftlichen Unterlagen.

Nachdem im Herbst auch der "Düsseldorfer Kreis" diesem Verfahren zustimmte, können nun bundesweit alle SCHUFA-Gesellschaften die hamburgische Praxis übernehmen, diese Anfragen zu löschen, damit sich die Betroffenen in ihrer ohnehin oft schon schwierigen Situation bei der Vorlage ihrer Selbstauskunft nicht mehr als nötig offenbaren müssen.

5.3 Automatisierung des Zahlungsverkehrs — Zur Wirksamkeit der Sonderbedingungen für die Benutzung von ec-Geldautomaten

Geldausgabeautomaten erfordern besondere Vorkehrungen für die Datensicherung, um Mißbräuche des Systems und daraus resultierende wirtschaftliche Folgen zu verhindern. Es ist Aufgabe des Datenschutzes, auch auf diesem Feld durch Prüfungen zu klären, ob die eingeführten Systeme den zu stellenden Anforderungen entsprechen. In

der Vergangenheit hat es eine ganze Reihe von Fällen gegeben, in denen sich das System als anfällig erwiesen hat, so daß nicht sämtliche Mißbrauchskonstellationen auszuschließen waren. Das sich dadurch stellende Problem, welche Seite — Benutzer oder Anbieter — für den aufgetretenen Schaden haften muß, hat mir Anlaß gegeben, mich auch mit den in den ec-AGB vorgesehenen Haftungsregelungen für denkbare Mißbrauchsfälle zu befassen und zu klären, ob sich die in den AGB getroffenen Haftungsverteilungen in Übereinstimmung mit den unter Datensicherheitsaspekten zu beurteilenden Schadens- oder Störungsursachen bei der Benutzung von Geldausgabeautomaten (GAA) bringen lassen.

Zwischen der Entwicklung der automatisierten Zahlungssysteme und den in ihnen verwirklichten Sicherheitsvorkehrungen einerseits sowie der rechtlichen Bewertung entstehender Haftungsfälle bei mißbräuchlichen Eingriffen in das System andererseits besteht eine wechselseitige Abhängigkeit. Ausbau und Wandel der Technik bedingen rechtliche Folgerungen ebenso wie umgekehrt die Gefährdung elementarer Rechtspositionen des Verbrauchers dazu zwingt, die technischen Anforderungen an ein System zu verschärfen.

Für die Aufsichtsbehörde liegt der rechtliche Ansatzpunkt für eine Beschäftigung mit den ec-Sonderbedingungen zur Benutzung von Geldausgabeautomaten darin, daß § 9 Abs. 2 Nr. 1 AGBG vorschreibt, daß eine Bestimmung in Allgemeinen Geschäftsbedingungen nicht unvereinbar sein darf mit wesentlichen Grundgedanken der gesetzlichen Regelung, von der abgewichen wird. Der Datenschutz hat mithin zu prüfen, ob die vom BDSG formulierten Anforderungen an die Datensicherung, die sog. 10 Gebote, in den Haftungsregelungen der AGB ihre Entsprechung gefunden haben oder ob es wesentliche Abweichungen gibt. In diesem Sinne war ich zwar darauf beschränkt, die AGB allein im Hinblick auf ihre datenschutzrechtliche Relevanz einer Prüfung zu unterziehen. Diese Prüfung mußte sich auf die technischen Seiten des Systems konzentrieren. Gleichwohl durften rechtliche Aspekte nicht ausgeklammert werden, weil andere zur Überprüfung der AGB berufene Stellen — wie Verbraucherzentralen — nicht über das Erfahrungswissen verfügen, um auftretende Fragen zum technischen Stand des GAA-Systems aus eigenem Sachverstand beurteilen zu können.

Die rechtlich schwierige Materie verlangte eine eingehende Auseinandersetzung mit der Frage, wie die Haftungsverteilung im Regelfall, d.h. nach dem geltenden Gesetzesrecht bestimmt ist, um im Vergleich damit zu prüfen, inwieweit die Regelungen des Bürgerlichen Gesetzbuches durch Vertragsrecht — Allgemeine Geschäftsbedingungen (AGB) der Banken und Sparkassen — abbedungen werden. Ich hatte mich zunächst mit den bisher in der Kreditwirtschaft verwendeten ec-AGB befaßt. Dabei hatte ich das Sicherungssystem nach dem Stand von Ende 1986 zugrunde gelegt. Am 1. Januar 1989 wird eine Neuregelung der ec-AGB in Kraft treten. Hierbei sind unterschiedliche Regelungen für die Banken einerseits (AGB Nr. 9.2 n.F. — Banken —) und für die Sparkassen andererseits (ec-AGB Nr. 9.2 n.F. — Sparkassen —) geschaffen worden. Inzwischen ist auch das Sicherungssystem für den Betrieb der ec-Geldautomaten weiterentwickelt worden. Eine noch weiter verbesserte Ausbaustufe wird 1989 erreicht werden. Bei der Prüfung der neuen AGB ist der jetzt realisierte Sicherheitsstandard des ec-Systems zu berücksichtigen.

Ich bin bei meiner Prüfung zu dem Ergebnis gelangt, daß zumindest die alten ec-AGB mit dem AGBG unvereinbar waren, weil sie zu Unrecht Haftungsregelungen zu Ungunsten des Kunden begründeten. Demgegenüber stellen die neuen ec-AGB eine deutliche Verbesserung für den Kunden dar. Jedoch sind auch bei diesen Klauseln nicht alle Zweifelsfragen ausgeräumt, weil es versäumt worden ist, die neuen Sonderbedingungen so zu fassen, daß alle denkbaren Mißbrauchskonstellationen und die daraus entstehenden Haftungsfolgen und Beweisfragen klar und eindeutig geregelt werden. Da meine verbleibenden Bedenken zu den neuen Sonderbedingungen auf der Kritik an den durch die neue Regelung überholten ec-AGB a.F. aufbauen, will ich damit beginnen.

a) Die Haftungsverteilung nach dem BGB

Die Rechtsprechung stuft das Rechtsverhältnis im Scheckverkehr zwischen dem Kunden und dem kontoführenden Kreditinstitut als Girovertrag ein, der sich als Geschäftsbesorgungsvertrag (§ 675 BGB) mit Dienstleistungscharakter darstellt. Entsprechend dieser allgemeinen Auffassung zum Scheckverkehr wird auch der bei einem Geldautomaten unter Eingabe der Codekarte nebst PIN (Persönliche Identifikations-Nummer) erteilte Auftrag als geschäftsbesorgungsrechtliche Weisung angesehen. Bei der mißbräuchlichen Benutzung einer unechten Codekarte bzw. bei der Benutzung der echten Codekarte durch einen Nichtberechtigten fehlt hingegen eine rechtlich wirksame Willenserklärung für die Benutzung des Geldautomaten. Es liegt dann kein geschäftsbesorgungsrechtlicher Auftrag vor, so daß ein Anspruch auf Rückerstattung des verauslagten Betrages für das Kreditinstitut nach geltendem Recht (§§ 670, 675 BGB) nicht besteht. Das Risiko für mangelnde Sicherheiten des GAA-Systems trägt also nach dem Gesetzesrecht das Kreditinstitut.

Wichtig ist auch die Feststellung, daß die Beweislast bei auftretenden Unregelmäßigkeiten nach dem geltendem Recht ebenfalls i.d.R. auf die Bank oder Sparkasse entfällt. So hat sie die Beweislast für die Echtheit der Unterschrift auf einem Scheck zu tragen. Entsprechend trägt die Bank auch die Beweislast dafür, daß der Kunde bzw. ein Bevollmächtigter mittels Eingabe von Codekarte und PIN die Weisung zur Zahlung des bestimmten Betrages an den Geldautomaten erteilt hat.

Das Gesetzesrecht schützt den Kunden mithin davor, für technische oder organisatorische Mängel im System des Geldautomaten in Anspruch genommen zu werden.

b) Die Abänderung der Haftungsverteilung in den AGB und ihre rechtliche Wirksamkeit.

Die sich aus dem Gesetzesrecht ergebende Haftungsverteilung zwischen Kunde und Kreditinstitut wird demgegenüber durch die ec-AGB z.T. zu Lasten des Kunden abgeändert.

aa) Zur Haftungsverteilung nach den ec-AGB Nr. 6, 7 a.F.

Die bislang in der Kreditwirtschaft verwendeten ec-AGB Nrn. 6, 7 hatten folgenden Wortlaut:

Nr. 6: "Der Kontoinhaber trägt, vorbehaltlich der in Nr. 7 getroffenen Bestimmung, gegenüber dem kontoführenden Kreditinstitut sowie gegenüber allen sonstigen Kreditinstituten und der Deutschen Bundespost, die einen ec-Geldautomaten betreiben, alle Schäden, die durch eine unsachgemäße oder mißbräuchliche Verwendung oder durch Verfälschung einer auf sein Konto ausgegebenen eurocheque-Karte mit Magnetstreifen entstehen. Das gleiche gilt für Schäden, die durch eine mißbräuchliche Verwendung der persönlichen Geheimzahl entstehen. Die Kreditinstitute bzw. die Deutsche Bundespost haften im Rahmen des von ihnen zu vertretenden Verschuldens nur in dem Maße, als sie im Verhältnis zu anderen Ursachen an der Entstehung des Schadens mitgewirkt haben."

Nr. 7: "Bei einem Verlust der eurocheque-Karte mit Magnetstreifen ist das ausgebende Kreditinstitut unverzüglich zu benachrichtigen. Das gleiche gilt, wenn ein Unbefugter Kenntnis von der persönlichen Geheimzahl erlangt hat oder zumindest der begründete Verdacht einer derartigen Kenntnisnahme besteht. Soweit Schäden durch die Benutzung von ec-Geldautomaten nach einer derartigen Benachrichtigung des ausgebenden Kreditinstituts eingetreten sind, haftet der Kontoinhaber für eine mißbräuchliche Verwendung der eurocheque-Karte im Sinne der Nr. 6 nur bis zu einem Betrag von DM 800,— bzw. bei Verfügungen an ec-Geldautomaten im Ausland bis zur zweifachen Höhe des in dem jeweiligen Land geltenden ec-Garantiehöchstbetrages."

Rechtlich ist in einer Klausel wie der Nr. 6 ec-AGB eine Risikoverteilung in Form eines vereinbarten Anspruchs auf Aufwendungsersatz zugunsten des Kreditinstituts zu sehen.

Es handelte sich bei der getroffenen Risikoverteilung um eine Haftung des Kunden, die garantieähnlich ausgestaltet war und die daran geknüpft wurde, daß es durch die Benutzung der an ihn ausgegebenen ec-Karte (Nr. 6, S. 1) oder die Verwendung der PIN (Nr. 6, S. 2) zu einer mißbräuchlichen Geldausgabe kam. Begrenzt wurde seine Haftung durch eine Mitverschuldensregelung in Nr. 6, S. 3 ec-AGB, die § 254 BGB vergleichbar ist. Nach den vertraglichen Regelungen in den Nrn. 6, 7 ec-AGB hatte der Kunde also in weiterem Umfang zu haften als nach dem Gesetzesrecht: Wo zuvor das Schadensrisiko der Bank zufiel, wurde es nun — zumindest teilweise — auf den Kunden übertragen.

Bei solchen Formen der Abbedingung des Gesetzesrechts ist allerdings zu prüfen, inwieweit sie nach dem AGBG wirksam sind. Nach § 9 Abs. 1 AGBG sind Bestimmungen in Allgemeinen Geschäftsbedingungen unwirksam, wenn sie den Vertragspartner entgegen den Geboten von Treu und Glauben unangemessen benachteiligen. Hierzu bedarf es einer umfassenden Würdigung der Interessen beider Vertragsparteien, in die die Anschauungen der beteiligten Verkehrskreise einzubeziehen ist. In Übereinstimmung mit der mehrheitlich in Literatur und Rechtsprechung vertretenen Auffassung sind dabei zur Beurteilung der Zulässigkeit einer Überbürdung verschuldensunabhängiger Schadensersatzpflichten auf den Kunden die Kriterien der sog. Sphärentheorie als Prüfungsmaßstab heranzuziehen. D.h. eine Haftungsverlagerung ist in der Regel unangemessen, wenn es um Gefahren geht, die in der Sphäre der Banken und Sparkassen selbst liegen. Die Überbürdung einer Haftung auf den Kunden ist hingegen zulässig, soweit es sich um Schäden handelt, die aus Schadensquellen herrühren, welche dieser mehr beherrscht als das Kreditinstitut.

Daneben und ergänzend kann als Unterfall des Gedankens der Risikoverteilung der Gesichtspunkt der Versicherbarkeit des Risikos Berücksichtigung finden: Für die Angemessenheit der Freizeichnung spricht, daß dem Kunden selbst die Risikobeherrschung möglich und zumutbar ist, für sie spricht auch, wenn die Freizeichnung Vermögensschäden betrifft, die beim Kunden üblicherweise unter Versicherungsschutz stehen. Umgekehrt ist eine Freizeichnung in der Regel unangemessen, wenn das Kreditinstitut das Risiko durch Abschluß einer Versicherung abdecken kann und beim Kunden üblicherweise kein Versicherungsschutz besteht.

Die durch Nrn. 6, 7 ec-AGB erfolgende Risikoverlagerung wäre danach nur wirksam gewesen, wenn sie sich auf Umstände beschränkt hätte, die sich der Sphäre des Kunden zuordnen ließen. Bei meiner Bewertung bin ich davon ausgegangen, daß etwa Fälle des Diebstahls der Codekarte aus der Wohnung des Kunden, des Verlusts oder des sonstigen Abhandenkommens der Karte in der Sphäre des Kunden als Karteninhaber liegen. Die meisten denkbaren Mißbrauchsfälle können somit der Risikosphäre des Kunden zugeordnet werden. Fallkonstellationen, in denen die Mißbrauchsgefahr jedenfalls zum Teil auch in der Sphäre des Kreditinstituts liegt, sind allerdings nicht von vornherein auszuschließen. Das muß in den AGB seinen Niederschlag finden, indem die Haftung beim Kreditinstitut liegt, wenn und soweit die Schadensursache dessen Risikosphäre zuzurechnen ist. Daran fehlte es in den ec-AGB a.F..

Zweifel an der Wirksamkeit der ec-AGB hatte ich weiter deshalb, weil die Haftung — ebenso wie bei der mißbräuchlichen Nutzung der Karte — so auch bei der mißbräuchlichen Verwendung der PIN nicht auf die Fälle beschränkt wurde, in denen das Risiko in der Sphäre des Kunden liegt. Der Kunde hatte auch beim zufälligen Auffinden der PIN zu haften, falls es einem Dritten gelingen sollte, zugleich ein Duplikat der Karte herzustellen, zu der die PIN gehört, um damit mißbräuchlich Geldabhebungen vorzunehmen. Ein (unbefugt hergestelltes) Kartenduplikat ist allerdings heute nicht mehr tauglich zur Bedienung eines ec-Geldautomaten, da die sog. MM-Sicherung inzwischen flächendeckend eingeführt ist. Vor 1987 waren noch nicht alle ec-Karten mit dem MM-Merkmal ausgestattet, nicht alle GAA verfügten über die MM-Box, und es war nicht sichergestellt, daß nach Ausfall einer MM-Box wegen technischer Störung der betreffende Automat stets außer Betrieb gesetzt wurde. Da die Herstellung einer einsatzfähigen Kartenfälschung daher theoretisch möglich war, war eine Grundlage für die

Zurechnung des PIN-Mißbrauchs in jedem Fall zur Sphäre des Kunden nicht zu erkennen. Durch die Verbesserungen im technischen Sicherheitsstandard des GAA-Systems könnte ich meine rechtlichen Bedenken in diesem Punkte heute aber nicht mehr aufrechterhalten.

Die Unangemessenheit der Klauseln ließ sich weiter daraus ableiten, daß die Banken Scheck- und Codekartenversicherungen abschließen, dem Kunden jedoch die von der Versicherung erbrachte Leistung lediglich im Kulanzwege gutbringen. Einem entsprechend allgemeiner Branchenübung bestehenden Versicherungsschutz kommt im Rahmen der Bewertung nach § 9 Abs. 1 AGBG maßgebliche Bedeutung zu. Wenn nämlich schon die bloße Möglichkeit einer Versicherung des Schadensrisikos zu dem Urteil führen kann, der Kunde werde durch eine Haftungsverlagerung auf ihn unangemessen benachteiligt, so liegt dieser Schluß erst recht nahe, wenn das Schadensrisiko üblicherweise versichert ist.

Im Ergebnis waren die Regelungen der Nrn. 6, 7 ec-AGB nur zum Teil mit dem Risikobeherrschungsgedanken zu rechtfertigen. Da aber die Klauseln nicht als teilweise wirksam angesehen werden konnten, mußte die Wirksamkeit der genannten AGB im ganzen in Frage gestellt werden.

Bei den neugefaßten Sonderbedingungen für den ec-Service, die am 1. Januar 1989 in Kraft getreten sind, ist zu differenzieren zwischen den Schadensregelungen, die im Bereich der Mitglieder des Bundesverbandes deutscher Banken e.V. und des Bundesverbandes der Deutschen Volksbanken und Raiffeisenbanken e.V. gelten und den AGB, die im Geschäftsbereich der Mitglieder des Deutschen Sparkassen- und Giroverbandes e.V. Anwendung finden.

bb) Zur Haftungsverteilung nach Nr. 9.2 ec-AGB — Banken —

Die neugefaßte Schadensregelung im Bereich des Bundesverbandes der Deutschen Volksbanken und Raiffeisenbanken e.V. sowie des Bundesverbandes deutscher Banken e.V. Nr. 9.2 ec-AGB-Banken lautet:

"Sobald der kontoführenden Stelle des Kreditinstituts oder dem Zentralen Sperrannahmedienst der Verlust der ec-Karte angezeigt worden ist, übernimmt das Kreditinstitut alle danach durch Verfügungen an ec-Geldautomaten bzw. durch Bezahlungen an POS-Kassen entstandenen Schäden. Bis dahin trägt das Kreditinstitut 90 % aller Schäden, die durch die mißbräuchliche Verwendung der dem Kontoinhaber ausgegebenen ec-Karte entstehen; der Kontoinhaber haftet nur für 10 % aller Schäden, die im Rahmen der Verfügungsmöglichkeit gemäß Nr. 7 entstehen können."

Für die Beurteilung der Wirksamkeit der geplanten Neuregelung ist wiederum entscheidend, welche Abweichungen gegenüber der Haftungsverteilung nach dem BGB festzustellen sind. Hierbei ist in Nr. 9.2 ec-AGB n.F. Banken ebenso wie in Nr. 6 ec-AGB a.F. die Regelung eines verschuldensunabhängigen Schadensersatzanspruchs zugunsten der Banken zu sehen, d.h. es wird eine Haftung des Kunden begründet, ohne daß ihn — wie nach dem Gesetzesrecht erforderlich — der Vorwurf eines schuldhaften Verhaltens treffen muß.

Der rechtlich bedeutsame Unterschied zu Nr. 6 ec-AGB a.F. liegt in der nunmehr begrenzten Höhe eines Schadensersatzanspruchs der Bank; der Kunde haftet nur noch für 10 % des entstehenden Schadens. Da der Verfügungsrahmen an ec-Geldautomaten fremder Geldinstitute täglich nur bis DM 400,— reicht, sind in diesen Fällen Schadenssummen von DM 40,— pro Tag denkbar. Bei der Benutzung eines Geldautomaten der kontoführenden Stelle, mit der ein größerer Verfügungsrahmen vereinbart werden kann, können höhere Schäden entstehen. Ebenso sind Fallkonstellationen denkbar, in denen der Kunde den Verlust der Karte nicht sogleich bemerkt oder Sonderabbuchungen auf seinem Konto nicht sofort registriert (Urlaub, Krankenhausaufenthalt etc.). In solchen Fällen ist es vorstellbar, daß der Kunde in Höhe von mehreren Hundert Mark zu haften hätte.

Da der verschuldensunabhängige Schadensersatzanspruch der Bank nach Nr. 9.2 ec-AGB n.F. Banken auf 10 % des Schadens begrenzt ist, der Schaden im übrigen aber

von den Banken durch eine Versicherung aufgefangen wird, lassen sich nunmehr im Gegensatz zu den Nrn. 6, 7 ec-AGB a.F. Bedenken gegen die Wirksamkeit der Klausel nicht mehr aus den Gesichtspunkten der Versicherbarkeit des Schadensrisikos und der vollen Überwälzung des Risikos auf den Kunden herleiten.

Bedenken habe ich allerdings deshalb, weil es in der AGB-Neufassung keine Bestimmung für den Fall gibt, daß die Schadensursache allein in der Risikosphäre des Kreditinstituts zu suchen ist. Ich vermisse weiter eine Nr. 6 S.3 ec-AGB a.F. entsprechende Klausel, also eine Mitverschuldensregelung (§ 254 BGB) der Kreditinstitute. Ohne diese Klarstellungen wird auch in den Fällen eine teilweise Haftung des Kunden begründet, in denen eine Bank selbst schuldhaft an der Entstehung eines Schadens mitgewirkt oder ihn sogar allein zu verantworten hat. Das kann insbesondere der Fall sein, wenn das Kreditinstitut Prüfungspflichten, die es im automatisierten Zahlungsverkehr einzuhalten hat, verletzt.

Anders als im Scheckverkehr findet bei den derzeitigen Geldautomatensystemen eine Unterschriftsprüfung nicht statt. Auch wird eine Prüfung verdachtserregender Umstände, die außerhalb der Eingabe von Karte und PIN liegen, aufgrund der Automatisierung und der damit einhergehenden Anonymisierung nicht vorgenommen. Die Prüfungspflicht erstreckt sich deshalb lediglich auf die Eingabe der echten Karte und die dem Kunden zugeordnete PIN.

Fraglich scheint mir, ob die Prüfungspflichten in bezug auf den die PIN betreffenden Teil soweit greifen, daß es nicht zu ungerechtfertigten Haftungsfällen zu Lasten des Kunden kommt.

Nach dem Stand des Sicherheitssystems von Ende 1986 waren auch Fälle denkbar, in denen der Kunde zu haften hatte, wenn die PIN — bis zur Eingabe der richtigen Kombination — mehr als dreimal hintereinander falsch eingegeben, also beliebig ausprobiert werden konnte. Solche Mißbrauchsfälle sind in der Vergangenheit auch vorgekommen. Der Täter konnte die auf einer echten Karte gespeicherten Daten (Fehlbedienungszähler = 3) auf eine Blankette kopieren. Er konnte dann mit drei Versuchen an einem Geldautomaten die PIN ausprobieren. (Fehlbedienungszähler = 0). Danach konnte er den alten Magnetstreifen von der Blankette auf die echte Karte zurückkopieren und erneut drei Versuche zum Erraten der PIN vornehmen usw. Der Fehlbedienungszähler auf der Karte war manipulierbar und eine Überprüfung der Integrität des Karteninhalts fand insoweit nicht statt.

Das ec-Sicherungssystem ist in den letzten Jahren weiter ausgebaut worden. Inzwischen ist die Manipulierbarkeit des Fehlbedienungszählers, die ihre Ursache in unverbundenen, off-line betriebenen GAA hatte, weitestgehend auszuschließen. Alle GAA sind inzwischen an eines von vier Netzen angeschlossen, es besteht eine bereichsinterne Absicherung in Form eines Transaktionsverbundes jeweils innerhalb der vier Institutsbereiche. Für jeden der vier Netzbereiche wird jetzt eine zentrale Transaktionsdatei geführt, und zentral werden nun auch die PIN-Fehlversuche registriert und protokolliert. Damit wird erkannt, wenn mit einer Karte mehr als drei Fehlversuche bei der PIN-Eingabe unternommen werden. Nach dem vierten Fehlversuch erfolgt die Kartensperre. In Zukunft soll eine bereichsübergreifende Absicherung erfolgen, d.h. daß in Zukunft für jede ec-Karte immer nur eine Stelle die Transaktionsdaten und die PIN-Versuchsdaten zu dieser Karte speichert und bei Verfügungen die erforderlichen Prüfungen durchführt. Z.Z. sind — wegen der vier Bereiche bzw. GAA-Netze — noch vier mal je drei Fehlversuche möglich. In der nächsten Ausbaustufe können nur noch drei Fehlversuche stattfinden, auch wenn am Fehlbedienungszähler auf der Karte manipuliert wird. Damit dürfte die Bank ihren Prüfungspflichten in hinreichendem Umfang nachkommen. Ob damit indes weitere Mißbrauchsfälle ausgeschlossen sind, läßt sich nicht sicher beantworten. Auf der einen Seite können zwar die Sicherheitsanforderungen an das System ständig verbessert werden, auf der anderen Seite sind allerdings auch der Phantasie derer keine Grenzen gesetzt, die mit kriminellen Methoden versuchen, das System zu manipulieren und es zu "knacken". Es wäre deshalb wünschenswert gewesen, wenn die Kreditwirtschaft für solche Fälle in den ec-AGB eine 100 %ige Haftungs-

regelung bzw. eine Mitverschuldensregelung vorgesehen hätte, die es ermöglichen würde, entprechend den Verantwortlichkeiten, die in ihrer eigenen Sphäre und der des Kunden liegen, eine Haftungsverteilung vorzunehmen.

Jedenfalls ließe sich die jetzt vorgesehene Haftungsbegrenzung auf 90 % nicht auf einen Schaden anwenden, der auf einer grobfahrlässigen Vertragsverletzung des Verwenders oder auf einer vorsätzlichen oder grob fahrlässigen Vertragsverletzung des gesetzlichen Vertreters oder eines Erfüllungsgehilfen des Verwenders beruht. Die 10 %ige Schadensüberwälzung auf den Kunden würde in diesen Fällen gegen § 11 Nr. 7 AGBG verstoßen, wonach ein Ausschluß oder eine Begrenzung der Haftung für einen Schaden, der auf einer grob fahrlässigen Vertragsverletzung des Verwenders oder auf einer vorsätzlichen oder grob fahrlässigen Vertragsverletzung eines gesetzlichen Vertreters oder Erfüllungsgehilfen des Verwenders beruht, unwirksam ist.

Das gleiche Problem stellt sich auch, soweit die Bank ihre Haftung für die Verletzung anderer vertraglicher Nebenpflichten (außer der Prüfungspflicht) ebenfalls auf 90 % begrenzt. Als Fallgruppen lassen sich hier u.a. denken:

— organisatorische Fehler, die den Eingang der Verlustanzeige des Kunden verzögern oder unmöglich machen;

— Verletzung der vertraglichen Nebenpflicht, die Fälschungssicherheit des Systems durch zumutbare Maßnahmen dem Stand von Technik und Wissenschaft anzupassen.

Die in diesen Fällen durch die ec-AGB vorgesehene Haftungsbeschränkung wäre ebenfalls gemäß § 11 Nr. 7 AGBG unwirksam, da eine Begrenzung der Haftung bei Vorliegen von groben Verschulden nicht zulässig ist.

Beide Fallgruppen haben allerdings an Bedeutung verloren, da der Kunde neuerdings zu jeder Zeit (also auch nachts und an Wochenenden) eine Verlustanzeige erstatten kann.

Es bleibt indes festzuhalten, daß durch das Fehlen einer 100 %igen Verschuldenshaftung der Bank und einer Mitverschuldensregelung Unklarheiten verbleiben, die zu rechtlichen Problemen führen können, wenn entsprechende Mißbrauchskonstellationen auftreten.

cc) Zur Haftungsverteilung nach Nr. 9.2 n.F. — Sparkassen —

Auch zu der Schadensregelung im Bereich des Deutschen Sparkassen- und Giroverbandes e.V., wie sie in Nr. 9.2 n.F. Sparkassen vorgesehen ist, habe ich Zweifel anzumelden, die aus einer fehlenden Eindeutigkeit der Klausel resultieren. In Nr. 9.2 n.F. Sparkassen heißt es u.a.:

"Ist der kontoführenden Stelle des Kreditinstituts oder dem Zentralen Sperrannahmedienst der Verlust der ec-Karte angezeigt worden, so übernimmt das Kreditinstitut alle durch Verfügungen an ec-Geldautomaten bzw. durch Bezahlungen an POS-Kassen entstandenen Schäden, die durch eine mißbräuchliche Verwendung der ec-Karte nach Eingang der Verlustanzeige entstehen. Bis dahin trägt das Kreditinstitut den Schaden, wenn der Karteninhaber den Verlust der ec-Karte unverzüglich angezeigt hat und keine wesentlichen vertraglichen Obliegenheiten — insbesondere die aus Nr. 5 — grobfahrlässig verletzt hat.

Insbesondere übernimmt das kontoführende Kreditinstitut den Schaden dann nicht, wenn der Schaden dadurch verursacht wurde, daß

— der Originalbrief, in welchem dem Kunden die persönliche Geheimzahl mitgeteilt wurde, zusammen mit der ec-Automatenkarte abhanden gekommen ist,

— die persönliche Geheimzahl auf der ec-Automatenkarte vermerkt oder mit der Karte in sonstiger Weise unmittelbar verbunden wurde.

In diesen Fällen trägt der Kontoinhaber den Schaden, jedoch begrenzt auf DM 400,— pro Kalendertag bzw. bei Verfügungen an ec-Geldautomaten im Ausland bis zur Höhe des in dem jeweiligen Land geltenden ec-Garantiehöchstbetrages.

Einen Anspruch auf Schadensübernahme kann der Karteninhaber nur geltend machen, wenn er die Voraussetzungen der Haftungsentlastung glaubhaft darlegt und Anzeige bei der Polizei erstattet."

Diese Regelung geht davon aus, daß die Sparkasse den Schaden trägt, wenn der Kunde den Verlust der ec-Karte unverzüglich angezeigt hat und glaubhaft darlegt, daß er keine wesentlichen vertraglichen Obliegenheiten grobfahrlässig verletzt hat. Die Sparkassen halten also inhaltlich an der Rechtslage ohne AGB fest, legen dem Kunden jedoch eine "glaubhafte Darlegung" des Nicht-Vorliegens einer Sorgfaltspflichtverletzung oder des Fehlens von Vorsatz/grober Fahrlässigkeit auf. Zwar scheint diese Regelung dem Kunden im Vergleich zur Rechtslage ohne AGB einen Vorteil zu verschaffen, weil er bei nur einfacher Fahrlässigkeit nicht haftet. Der Kunde muß jedoch "glaubhaft darlegen", daß eine grobfahrlässige Sorgfaltspflichtverletzung nicht vorlag. Fraglich ist deshalb, ob nicht Nr. 9.2 ec-AGB Sp. als eine nach § 11 Nr. 15 AGBG verbotene Beweislaständerung zum Nachteil des Kunden zu qualifizieren ist. Der Sparkassen- und Giroverband hat erklärt, mit den neuen Sonderbedingungen solle keine Beweislastumkehr erfolgen, dem Kunden falle allein die Aufgabe zu, die Tatsachen zu seiner Haftungsentlastung schlüssig darzulegen, um von vornherein das Vortäuschen eines Mißbrauchsfalles durch den Kunden zu verhindern. Ob diese Auffassung haltbar ist, müßten im Zweifelsfall die dazu berufenen Gerichte klären.

Ich habe meine Bedenken zu den inzwischen überholten Sonderbedingungen für den ec-Service und meine Vorschläge zu einer klareren Neufassung der AGB den Verbänden der Kreditwirtschaft mitgeteilt und darüber mit den Verbandsvertretern diskutiert. Dabei ist mir im einzelnen der neueste technische Sicherheitsstand des GAA-Systems erläutert worden. Die Kreditwirtschaft geht davon aus, nunmehr einen wirksamen Schutz gegen Mißbräuche und Manipulationen geschaffen zu haben. Auch ich meine, daß mit der Neufassung der AGB wesentliche Verbesserungen zugunsten des Kunden erreicht worden sind. Die jetzt noch anzubringende rechtliche Kritik an den Klauseln ist jedenfalls nicht mehr primär aus datenschutzrechtlichen Gründen herzuleiten. Die Datensicherungsanforderungen im System scheinen mir soweit realisiert, daß die entstehenden Haftungsprobleme durch die AGB zufriedenstellend gelöst werden. Ob darüber hinaus aus anderen Gründen über die Wirksamkeit der neuformulierten Sonderbedingungen weiter zu diskutieren ist, kann dahingestellt bleiben.

Die Entwicklung und Praxis des Betriebs der GAA wird jedoch auch weiter zu beobachten sein, um die durch die Technik aufgeworfenen Probleme mit dem rechtlichen Instrumentarium, das durch die Allgemeinen Geschäftsbedingungen bereitgestellt ist, abzustimmen.

5.4 Versicherungswirtschaft

5.4.1 Zentrale Dateien der Versicherungsverbände

Im Berichtszeitraum sind mit der Versicherungswirtschaft weitere Gespräche zu den in einzelnen Versicherungssparten bereits bestehenden oder geplanten zentralen Dateien geführt worden. Dabei ist der Sachstand im einzelnen wie folgt darzustellen:

5.4.1.1 Sonderwagnisdatei der Lebensversicherer

Zur Behandlung der AIDS-Problematik in der Versicherungswirtschaft

Im Berichtszeitraum war in der Öffentlichkeit die Befürchtung geäußert worden, in der Versicherungswirtschaft sei eine "AIDS-Datei" entstanden oder im Aufbau begriffen. Ich habe mich mit Vertretern der Lebensversicherer in Verbindung gesetzt, um zu klären, ob die von mir für unabdingbar erachteten datenschutzrechtlichen Essentialien im Umgang mit der AIDS-Problematik Beachtung finden.

Als obersten Grundsatz begreife ich es, daß im Umgang mit AIDS-infizierten Personen oder Personen, die für besonders gefährdet gehalten werden, jedwede Form der sozialen Ausgrenzung, Rasterung und Stigmatisierung vermieden wird. Bei der Behandlung

der Krankheit AIDS bedarf es angesichts der teils hysterische Züge tragenden gesellschaftlichen Diskussion einer besonderen Sensibilität und Zurückhaltung im Umgang mit den Betroffenen. Ansonsten ist zu befürchten, daß es als Folge von unbegründeten oder überzogenen Schutzmaßnahmen zu einer sozialen Ghettoisierung AIDS-infizierter Personen kommt.

Tatsächlich haben meine Überprüfungen die Presseberichte bestätigt, wonach von einem Versicherungsunternehmen ein "Risiko-Raster" verwendet wird, mit dem der Versicherungsmitarbeiter "Hinweise auf bestimmte AIDS-Risikogruppen" erhält. Die Mitarbeiter sollen mit Hilfe dieser Hinweise bei der Prüfung von Versicherungsanträgen auf Angehörige sog. AIDS-Risikogruppen aufmerksam werden, die dann einer besonderen Kontrolle vor Vergabe des Versicherungsschutzes unterzogen werden, um entstehende wirtschaftliche Risiken abschätzen und ggf. den Versicherungsschutz verweigern zu können. Zu diesen Personengruppen werden nach internen Arbeitspapieren etwa Friseure, Coiffeure und Stylisten, Künstler, Luftstewards und Entwicklungshelfer gerechnet.

In den von mir geführten Gesprächen bestand Einigkeit darüber, daß es indes keinerlei verläßliches wissenschaftliches oder statistisches Material gibt, wonach auf einen besonderen Gefährdungsgrad gerade dieser Gruppen geschlossen werden könnte. Somit fehlt es für die Verwendung von Risikorastern an einem berechtigten Interesse, weil diese nicht geeignet sind, wirtschaftliche Risiken bei der Versicherung von AIDS-gefährdeten Personen auszuschließen.

Von Seiten der Versicherungswirtschaft wurde demgegenüber das Interesse herausgestellt, sich vor den nicht übersehbaren Folgekosten zu schützen, die mit der Gewährung von Versicherungsschutz gegenüber HIV-Trägern verbunden sein können. Diesen Standpunkt kann ich selbstverständlich nur akzeptieren — und das ist eine weitere zentrale Forderung zur Behandlung des AIDS-Phänomens —, wenn für die Maßnahmen zur Schadensprophylaxe die gleichen Grundsätze Anwendung finden, wie sie bisher bereits unter datenschutzrechtlichen Gesichtspunkten in anderen vergleichbaren Risikofällen gebilligt werden konnten. Grundsätzlich erscheint es mir berechtigt und auch rechtlich zulässig, wenn sich die Versicherungen, wie in Fällen anderer Todesfallrisiken auch (z.B. Herzinfarktgefährdungen, Krebserkrankungen etc.), gegen die wirtschaftlich unkalkulierbare oder mißbräuchliche Inanspruchnahme von Versicherungsleistungen, die in dem Verschweigen gefahrerheblicher Umstände liegen kann, zu schützen suchen. Meines Erachtens muß jedoch sichergestellt werden, daß es angesichts der besonderen Diskriminierungsgefahren, die mit der Kennzeichnung als HIV-Infizierter verbunden sind, nur solche Prüfungen und Kontrollen durch die Versicherer durchgeführt werden, bei denen die beschriebenen Gefahren sozialer Selektion vermieden werden.

Zu den sachlich vertretbaren Maßnahmen rechne ich es, wenn in den Versicherungsantragsformularen Fragen nach den Gesundheitsverhältnissen des Versicherungskunden gestellt werden. Da es sich bei AIDS um eine medizinisch bisher nicht erfolgreich zu behandelnde Virus-Infektion handelt, ist es zu vertreten, wenn die Versicherungsunternehmen eine Aufklärung über ein insofern bestehendes herausgehobenes wirtschaftliches Risiko verlangen, um über die Vergabe des Versicherungsschutzes in Kenntnis aller gefahrerheblichen Umstände entscheiden zu können.

In der Versicherungswirtschaft gibt es bereits eine Praxis, bei der Anbahnung von Versicherungsabschlüssen im Antragsformular den Kunden speziell danach zu befragen, ob bei ihm eine HIV-Infektion festgestellt wurde. Mit der ausdrücklichen Frage nach einer HIV-Infektion wird klargestellt, daß Nachfragen des Versicherers bei den behandelnden Ärzten sich auch auf dieses besonders sensible Krankheitsbild erstrecken können. Auf diese Weise scheint mir sogar mehr Transparenz für den Versicherungskunden zu entstehen, denn es wird ihm bewußt gemacht, an welchen Erkrankungen ein besonderes Informationsinteresse des Versicherers besteht.

Weiter halte ich es tolerabel, wenn die Versicherer, außer der formularmäßigen Nachfrage nach eigenen Erkenntnissen des Antragstellers über eine HIV-Infektion, unter

bestimmten Voraussetzungen eine ärztlichen Untersuchung auf den Gesundheitszustand des Versicherungskunden verlangen. Zu den geeigneten Untersuchungsverfahren gehört der sog. HIV-Test. Es ist daher nicht angreifbar, wenn die Lebensversicherer ab einer bestimmten Versicherungssumme generell eine Gesundheitsuntersuchung verlangen und dabei einen HIV-Test einbeziehen. Unerläßlich ist es allerdings, daß für den Betroffenen die Freiwilligkeit der Untersuchung gesichert wird. Weiter ist zu garantieren, daß auch nach Vorliegen des Untersuchungsergebnisses allein der Betroffene selbst darüber entscheiden darf, ob er die sensiblen Daten an den Versicherer oder sonstige Personen weiterleiten will.

Nach den mir vorliegenden Informationen wird diesem Verlangen in der Praxis Rechnung getragen. Generell wird ein HIV-Test erst ab einer Versicherungssumme von DM 250.000,— gefordert. Dem Kunden steht es in einem solchen Fall frei, die Untersuchung bei einem Arzt seiner Wahl vornehmen zu lassen. Vor der Untersuchung hat der Kunde auf einem Formularblatt schriftlich sein Einverständnis zum HIV-Test zu erklären. Ebenso hat er zu bestätigen, daß er von dem untersuchenden Arzt über die Bedeutung des Testes aufgeklärt worden ist. Das abgenommene Blut wird dann im Labor untersucht. Nach Vorliegen des Testergebnisses wird der Kunde zunächst von seinem Arzt über das Resultat der Untersuchung informiert. Es steht ihm dann frei, das Ergebnis an den Versicherer weiterzuleiten oder es zu unterlassen; dem Arzt steht eine entsprechende Befugnis ohne Einwilligung des Betroffenen nicht zu. Wenn der Kunde die Weiterleitung eines (negativen) Untersuchungsergebnisses unterläßt, ergeben sich daraus — außer, daß eben kein Versicherungsschutz gewährt wird — keine negativen Konsequenzen. Vor allem ergehen keine Meldungen an Dritte oder an zentrale Warndateien.

Unterhalb so hoher Versicherungssummen, die ein besonderes wirtschaftliches Risiko für den Versicherer entstehen lassen, halte ich das Verlangen, der Antragsteller möge besondere gesundheitliche Atteste beibringen, nur dann für verhältnismäßig, wenn begründete Hinweise auf eine mögliche HIV-Infektion vorliegen. Das bislang von einem Versicherungsunternehmen verwendete "Risiko-Raster" ist allerdings — wie bereits dargestellt — ungeeignet, verläßliche prognostische Erwägungen zu ermöglichen. Solange brauchbare medizinische Daten nicht vorliegen, muß deshalb jegliche selektive Behandlung einzelner Personenkreise, die zu Stigmatisierungsprozessen führen muß, vermieden werden.

Das Entstehen einer AIDS-Datei wäre eine der größten Gefahren, die sich im Zusammenhang mit dem AIDS-Phänomen ergeben könnte. Das Interesse der Lebensversicherer, sich gegen die Risiken einer Versicherung von AIDS-erkrankten Kunden abzusichern, darf nicht dazu führen, daß entsprechende Risikomerkmale in Dateien gespeichert werden, die sich dann bestimmten Personen zuordnen lassen. Dadurch könnte nämlich ein Datenraster entstehen, mit dem HIV-infizierte Personen als soziale Gruppe auszuselektieren wären. In der Öffentlichkeit ist in diesem Zusammenhang die Befürchtung aufgetaucht, die von den Lebensversicherern bereits eingerichtete Sonderwagnisdatei könne dazu genutzt werden, durch Meldung von HIV-Trägern eine spezielle AIDS-Datei zu bilden.

Diese Gefahr besteht jedoch nicht, da in dem Meldeverfahren zur Sonderwagnisdatei der Lebensversicherer die Registrierung spezifischer Erkrankungen oder Krankheitsrisiken nicht vorgesehen ist. Bei der Sonderwagnis-Datei handelt es sich um eine zentrale Warndatei, an die die einzelnen Versicherungsunternehmen Meldung erstatten, wenn ein Vertragsabschluß mit dem Kunden wegen Vorliegens bestimmter wirtschaftlicher Risiken oder aus sonstigen Gründen (z.B. vertragswidriges Verhalten) unterblieben ist oder nur mit Erschwerungen angenommen oder durch Rücktritt aufgehoben wurde. Anfragenden Versicherungsgesellschaften soll es ermöglicht werden, mit den nur beim meldenden Unternehmen vorliegenden Informationen die Angaben eines Antragstellers auf ihre Richtigkeit zu überprüfen, die Risiken eines Versicherungsfalles aufzudecken und ggf. einen Versicherungsantrag abzulehnen.

Das Meldeverfahren sieht so aus, daß in die Wagnisdatei folgende Daten aufgenommen werden:

— Name und Nummer des meldenden Mitglieds-Unternehmens sowie Zeitpunkt der Meldung;

— Name, Vorname, Geburtsdatum, Geburtsort der Person, auf deren Leben die Versicherung beantragt worden ist.

Sodann wird das gemeldete Wagnis mit einem sog. Kennzeichen versehen, das aus dem Buchstaben "L" bei der Lebens- oder Rentenversicherung mit Todesfallrisiko und dem Buchstaben "B" bei der Berufsunfähigkeitszusatzversicherung (BUZ) besteht. Die Buchstaben haben — alternativ — die Bedeutung: Antrag/Versicherung wurde

— mit Erschwerung angenommen oder

— für länger als sechs Monate zurückgestellt oder

— aus versicherungsmedizinischen Gründen abgelehnt oder

— wegen verweigerter Nachuntersuchung o.ä. abgelehnt oder

— wegen Erschwerung vom Versicherungsnehmer abgelehnt oder

— aufgrund der Auskünfte anderer Versicherer abgelehnt oder — nachträglich durch Kündigung nach § 41 VVG, Rücktritt oder Anfechtung aufgehoben.

Die angeschlossenen Mitgliedsunternehmen melden nur diese Kurzinformationen (die jeweilige Bedeutung der Kennzeichen "L" und "B" wird nicht gemeldet) an die Zentrale Wagnisdatei und auch allein diese Daten werden an die angeschlossenen Unternehmen weitergegeben. Erkennbar sind aus der Wagnisdatei insofern nur bestimmte Erschwernisse, die einem Vertragsschluß entgegenstehen oder zu Risikozuschlägen Anlaß geben könnten. Über die konkrete Art des Erschwernisses wird das Versicherungsunternehmen erst im Falle einer weiteren Nachfrage bei dem Versicherer unterrichtet, der die Daten an die Wagnisdatei gemeldet hat. Auch bei derartigen Nachfragen wird aber in keinem Fall die Art der Erkrankung mitgeteilt.

Aufgrund dieser Sachlage gehe ich davon aus, daß weder durch das Meldeverfahren an die Zentrale Sonderwagnisdatei noch durch die Weitergabe an die Mitglieder eine spezielle AIDS-Datei entstehen kann. Es gibt also, soweit es für mich erkennbar ist, in der Versicherungswirtschaft keine eingerichtete oder auch nur geplante AIDS-Datei. Diese Aussage gilt für den Verband der Lebensversicherer wie für die einzelnen Mitgliedsunternehmen.

5.4.1.2 Zentrale Registrierstelle Rechtsschutz

In meinem letzten Tätigkeitsbericht hatte ich über den Diskussionsstand mit dem HUK-Verband über die Einführung eines geeigneten Match-Code-Verfahrens beim Meldeverfahren der Zentralen Registrierstelle Rechtsschutz unterrichtet. Nach den daraufhin weitergeführten Gesprächen kann ich folgenden aktuellen Sachstand mitteilen:

Ich habe es dem HUK-Verband gegenüber akzeptiert, wenn die Postleitzahl in den Match-Code aufgenommen wird, um so für eine Erhöhung der Trefferquote zu sorgen; ich habe zugleich darauf hingewiesen, daß dann aber umso mehr Anlaß besteht, den Möglichkeiten einer Deanonymisierung vorzubeugen, die sich durch die Aufnahme der Postleitzahl in den Match-Code nur erhöhen.

Ich habe vorgeschlagen, das Verfahren so zu gestalten, daß der Nachname des Versicherungsnehmers im Match-Code "verstümmelt" wird, indem man den ersten des insgesamt mit fünf Buchstaben im Match-Code geführten Nachnamens unterdrückt. Dadurch wäre die Gefahr beseitigt, daß durch den Blick in Adreß- oder Telefonbücher der Betroffene sogleich identifiziert werden könnte.

Der HUK-Verband hat gegen ein solches Verfahren technische Schwierigkeiten und einen hohen finanziellen Aufwand angeführt. Eine nachträgliche Änderung des vorhandenen Bestandes an Match-Codes sei nicht möglich, da der Verband die Volldaten der Meldungen nicht aufbewahre. Um die jetzt realisierte Trefferquote aufrechtzuerhal-

ten, genüge es nicht, wenn man einfach den ersten Buchstaben des Nachnamens im Match-Code unterdrücke. Anstelle des 1. Buchstabens müsse dann ein 6. Buchstabe des Nachnamens neu in den Match-Code aufgenommen werden. Eine Änderung der neuen Meldungen sei zwar technisch durchführbar, sie hätte jedoch zur Folge, daß die Unternehmen fünf Jahre lang die Neuanträge doppelt (mit und ohne den ersten bzw. den sechsten Buchstaben des Nachnamens) führen müßten, um Paarigkeiten mit dem alten Bestand feststellen zu können.

Bei einer Abwägung zwischen den entstehenden wirtschaftlichen Folgen für den HUK-Verband und den tatsächlich zu erwartenden Beeinträchtigungen für die Betroffenen, die durch einen mißbräuchlichen Umgang mit ihren Daten bei den Versicherern entstehen könnten, erscheint es mir hinnehmbar, wenn der HUK-Verband vorübergehend an dem jetzt erprobten Match-Code festhält, wenn schon jetzt Vorkehrungen getroffen werden, um die geforderten Verbesserungen zur Anonymisierung der personenbezogenen Daten im Match-Code einzuführen, soweit dies technisch machbar und wirtschaftlich vertretbar ist. Der HUK-Verband hat sich bereiterklärt, bei den eingehenden Neuanträgen der Mitgliedsunternehmen nunmehr auch den sechsten Buchstaben des Nachnamens zu erfassen, ohne ihn bereits jetzt in den Match-Code zu übernehmen. Auf diese Weise ist es möglich, nach Ablauf der Speicherungsdauer von fünf Jahren für die vorhandenen Datensätze den Match-Code vollständig umzustellen, den Nachnamen im Match-Code durch Unterdrückung des ersten Buchstabens zu verstümmeln und gleichzeitig um den sechsten Buchstaben zu ergänzen.

5.4.1.3 Meldeverfahren der Kfz-Versicherer

Für die Sparte der Kfz-Versicherer besteht beim HUK-Verband ein Auskunftsdienst, dessen Aufgabe es ist, dem Versicherungsbetrug zu begegnen. In der Zentralen Registrierstelle werden zu diesem Zweck mehrere Dateien geführt, zu denen die ca. 130 angeschlossenen Mitgliedsunternehmen ihre Angaben melden und aus denen sie im Bedarfsfalle Auskünfte erhalten können. Diese Informationen ermöglichen es einem Autoversicherer, sich mit einem anderen in Verbindung zu setzen, wenn in Schadensfällen Ähnlichkeiten oder Zusammenhänge erkennbar werden. Ich habe mich vom HUK-Verband über die einzelnen Dateien unterrichten lassen und kann damit meine bisherige Berichterstattung (6. TB, 5.4.1.3, S. 132-134) vervollständigen.

1. Der Sachverhalt

Insgesamt sind beim HUK-Verband im Kfz-Bereich ca. 6 — 700.000 Datensätze gespeichert, die über den Namen, die Fahrgestell-/Fahrzeug-Identitäts-Nr. oder das amtliche Kfz-Kennzeichen erschlossen werden können. Im Jahresdurchschnitt werden monatlich rund 17.000 neue Datensätze in die Kfz-Dateien der Zentralen Registrierstelle aufgenommen.

D a t e i A

Zur Datei A werden Personen gemeldet, die im Verdacht stehen, einen Versicherungsbetrug begangen zu haben. Diese Meldung resultiert aus einer Prüfung im Rahmen einer Schadensregulierung, bei der der Bearbeiter meist mehrere verdachterregende Momente festgestellt hat. Zur Entscheidungshilfe liegt ihm eine Checkliste für auffällige Vorkommnisse in K-(Kraftfahrzeug) Schäden nebst Erläuterung und eine besondere Checkliste für Kfz-Diebstähle vor. In den Check-Listen sind Fragen zum Schadenshergang oder zum Kfz-Diebstahl, zum Fahrzeug, zur Person des Versicherungsnehmers und zur Person des Halters, zum Versicherungsverhältnis, zu den Tatumständen u.a.m. aufgeführt.

In den Erläuterungen zur Check-Liste werden weitere Hinweise gegeben, anhand welcher Umstände ein betrugsrelevanter Verdacht konkretisiert werden soll.

Die Entscheidung, ob gemeldet wird, liegt zunächst bei dem Schadenssachbearbeiter. Der Fall wird jedoch durch den jeweiligen Abteilungs- oder Gruppenleiter geprüft, der allein die Berechtigung zur Meldung an den HUK-Verband hat. Die Zahl der meldebe-

rechtigten Stellen in der Bundesrepublik liegt insgesamt bei rund 1.000. In der Meldung wird dem Verband gegenüber der Verdacht nicht näher begründet, da ein Formblatt verwendet wird, in dem nur die Personalien des verdächtigen Versicherungsnehmers oder eines am Schadensfall beteiligten Dritten sowie die Daten zum Fahrzeug des Betroffenen aufzunehmen sind.

In der Datei A werden die folgenden Daten gespeichert:

— Kennung der meldenden Gesellschaft und meldenden Stelle

— Schaden-Nr.

— Art der Deckung (Kfz-Haftpflicht, Voll- oder Teilkasko)

— Art des Schadens (Totalschaden, Totaldiebstahl, fiktive Reparaturkosten, sonstiges)

— Schadentag

— Schadenort (PLZ und Name)

— Nachname

— Vorname

— Geburtstag

— PLZ des Wohnortes

— Art der Beteiligung (Versicherungsnehmer, Anspruchsteller, Zeuge, Werkstatt, Mietwagenverleih, Abschleppunternehmer, Sachverständiger, Fahrer, sonstige)

— amtliches Kfz-Kennzeichen.

Jede Meldung ist gleichzeitig eine Anfrage an den Verband, ob über diese Person bereits von anderer Seite Daten bekanntgeworden sind. Zur Suche kann der Nachname allein oder in Verbindung mit dem Vornamen und/oder der Postleitzahl des Wohnortes verwendet werden. Ist ein Datensatz vorhanden, wird der anfragenden Gesellschaft per Computerbrief der Datensatz mitgeteilt, damit sie sich an das andere Versicherungsunternehmen wenden kann. Nur dann ist es möglich, die Identität der Betroffenen aufzuklären.

Eine Durchschrift der Meldung verbleibt in der Schadensakte, damit — wenn sich die Verdachtsmomente nicht bestätigen — die Löschung in der Datei A veranlaßt werden kann. In diesem Fall sendet die meldende Stelle die in der Akte befindliche Durchschrift an den HUK-Verband, wo sodann die Löschung der gespeicherten Daten vorgenommen wird. An regelmäßige Prüfungsfristen ist ein solches Verfahren zur Aktualisierung des Datenbestandes nicht gebunden. Wird eine vorzeitige Löschung von der meldenden Gesellschaft nicht veranlaßt, bleibt ein Datensatz maximal 4 Jahre gespeichert, bevor er automatisch in einem monatlichen Sicherungs- und Reorganisationslauf gelöscht wird.

Die Datei A umfaßt z.Z. ca. 270.000 Datensätze.

D a t e i B

Zur Datei B werden Personen gemeldet, gegen die wegen des Verdachts, einen Versicherungsbetrug begangen zu haben, ein Strafantrag gestellt worden ist, bzw. die bereits wegen einer solchen Straftat verurteilt worden sind oder bei denen die Beweismittel für einen Strafantrag ausreichen würden und eine Verurteilung sehr wahrscheinlich wäre, das Versicherungsunternehmen jedoch auf einen Strafantrag verzichtet, weil es vornehmlich an der Schadensersatzleistung interessiert ist oder übergeordnete Gründe vorliegen (z.B. Rücksicht auf Großkunden).

Zur Meldung an die Datei B sind in dem jeweiligen Versicherungsunternehmen nur die Personen berechtigt, die üblicherweise mit der Bearbeitung von Großschäden befaßt werden und die in Zweifelsfällen eine juristische Beratung einholen. Die Zahl der meldeberechtigten Stellen beträgt 115.

Für die Meldung wird ebenso wie zur Datei A ein Formularblatt verwendet, auf dem die genauen Verdachtsgründe, die sich gegen den Betroffenen ergeben haben, nicht ausgewiesen sind.

Gespeichert werden in der Datei B:

— Kennung der meldenden Gesellschaft

— Nachname

— Vorname

— Geburtsdatum

— Postleitzahl, Wohnort, Straße und Haus-Nr.

— Schaden-Nr.

— Schadendatum

— Schadenort (PLZ und Name)

— Art der Beteiligung (verschlüsselt wie in Datei A)

— Fahrzeugart, Hersteller, Typ, Fahrgestell-/Fahrzeug-Identifizierungs-Nr.

— amtliches Kennzeichen

Beim HUK-Verband wird vor dem Einspeichern unter Angabe des Namens gesucht, ob diese Person schon bekannt ist. Ist dies der Fall, dann werden — wie bei der Datei A — die betroffenen Gesellschaften angeschrieben, um die Identität der beteiligten Personen überprüfen und sich gegenseitig über nähere Einzelheiten informieren zu können.

Eine Durchschrift der Meldung verbleibt in der Schadensakte, damit das Versicherungsunternehmen eine u.U. nötige Meldung zur Löschung der Daten vornehmen kann. Wird das Strafverfahren eingestellt, oder die gemeldete Person vom Vorwurf einer Straftat freigesprochen, wird die Löschung veranlaßt. Dann verbleibt in der Schadensakte keinerlei Hinweis auf die befristete Speicherung in der Datei B. Auch in der Datei des Verbandes werden alle Daten gelöscht — eine Historie wird nicht gespeichert. Auch eine denkbare Übertragung in die Datei A wird nicht vorgenommen; allerdings kann von dort nicht kontrolliert werden, ob ein Versicherungsunternehmen, das die Löschung zur Datei B veranlaßt, zugleich zur weitergefaßten Datei A meldet. Solche Fälle sind dem HUK-Verband bisher indes nicht bekannt geworden.

Wird der Datensatz nicht vorzeitig gelöscht, dann bleibt er bis zur automatischen Löschung nach 10 Jahren erhalten.

Die Datei B umfaßt z.Z. ca. 7.000 Datensätze.

D a t e i C

In die Datei C werden alle Fahrgestell-/Fahrzeug-Identifizierungsnummern von solchen Fahrzeugen aufgenommen, die bei Schäden mit Betrugsverdacht aufgefallen sind. Zusätzlich ist der HUK-Verband an allen Totalschäden und -diebstählen interessiert, auch ohne daß der Verdacht eines Versicherungsbetruges vorliegen muß; in diesen Fällen ist die Meldung zur Datei C sogar obligatorisch. Die Meldungen erfolgen mit demselben Formular wie die Meldung an die Datei A, jedoch ohne Angabe der Personalien des Betroffenen. Die Dateien A und C bestehen getrennt voneinander. Es liegt im Ermessen des meldenden Versicherungsunternehmens, ob es im Falle einer auffälligen Schadensabwicklung mit Personalien an die Datei A oder mit Fahrgestell-Nr. (und ohne Personalien) an die Datei C meldet. Der HUK-Verband erachtet die gesonderte Führung einer Verdachtsdatei im Fahrzeugbereich für sinnvoll, um Versicherungsbetrugsfälle aufzuklären, in denen beispielsweise Altschäden von inzwischen gewechselten Fahrzeugbesitzern doppelt abzurechnen versucht werden. Im einzelnen sind folgende Schäden an diese Datei zu melden:

a) Kraftfahrzeug-Haftpflichtversicherung

— Technischer Totalschaden;
Von einer Meldung soll abgesehen werden, wenn der Fahrzeugwert gering ist.

— Wirtschaftlicher Totalschaden;
Von einer Meldung soll abgesehen werden, wenn der Fahrzeugwert gering ist.

— Abrechnung auf der Basis der fiktiven Reparaturkosten. Es sind alle Fälle zu melden, in denen der Verdacht späterer Manipulationen naheliegt.

b) Fahrzeugversicherung

— Totaldiebstähle sind grundsätzlich zu melden;
Von einer Meldung kann Abstand genommen werden, wenn das Fahrzeug älter als 3 Jahre ist oder nur einen geringen Zeitwert hat.

— Reparaturfälle, in denen die Wiederherstellung des Fahrzeuges durch den Versicherungsnehmer nicht vorgenommen wird, ausgenommen sind Fahrzeuge mit geringem Zeitwert.

— Darüber hinaus sollen Fahrzeuge gemeldet werden, soweit die Meldung zur Ausschaltung evtl. nachfolgender Manipulationen zweckmäßig erscheint.

Nach Auskunft des HUK-Verbandes läßt sich die Person des Fahrzeughalters unmittelbar aus der Datei C nicht deanonymisieren; jedoch ist dies möglich, wenn beim meldenden Versicherungsunternehmen nachgefragt wird. Überdies bietet die Datei D als Hilfsdatei die Möglichkeit, Verbindungen zwischen Personengruppen und Fahrzeugen herzustellen (dazu unter Datei D).

In der Datei werden gespeichert:

— Kennung des Versicherungsunternehmens und der meldenden Stelle

— Schaden-Nr.

— Art der Deckung (wie bei Dateien A und B)

— Schaden-Tag und -ort

— Fahrgestell-/Fahrzeug-Identifizierungs-Nr.

— Fahrzeugart (PKW, LKW, Wohnwagen, Krad, sonstige)

— Datum der Erstzulassung

— Hersteller, Typ

— amtliches Kennzeichen.

Wenn bei einer Meldung/Anfrage zur Datei A das amtliche Kennzeichen aufgegeben wird, so sucht man auch in der Datei C, ob das gemeldete Fahrzeug bereits bekannt ist.

Die Datei C umfaßt z.Z. ca. 470.000 Datensätze.

D a t e i D

In der Datei D werden in einem Datensatz lediglich amtliche Kennzeichen und der Name oder die Fahrgestell-Nr. als Verknüpfungsmerkmal zu den Dateien A und/oder C gespeichert. Sie dient als Hilfsdatei, um mittels amtlicher Kennzeichen Querverbindungen in den Dateien A und C zwischen Personengruppen und Fahrzeugen aufzudecken. Eine alleinige Meldung zu dieser Datei gibt es nicht. Die Speicherfrist beträgt zwei Jahre. Mittels der Datei D kann in den Fällen eine Verknüpfung zwischen den Dateien A und C hergestellt werden, wo das amtliche Kennzeichen jeweils übereinstimmt.

D a t e i E

In der Datei E sind tabellarisch Schaden-Nr. und die Namen von Beteiligten gespeichert. Sie ist eine interne Hilfsdatei und dient über die Schadennummer der Verknüp-

fung sämtlicher zur Datei B gemeldeten Personen — also Versicherungsnehmern und Außenstehenden —, die jeweils an einem konkreten Schadensfall beteiligt waren.

Alle Dateien sind miteinander nicht verbundene sequenzielle Dateien, deren Inhalte nicht durch eine Datenbank-Abfragesprache auf unterschiedlichste Weise miteinander in Beziehung gesetzt werden könnten.

Um in der Praxis mit diesen Dateien arbeiten zu können, muß sich ein Mitarbeiter der Zentralen Registrierstelle mit seinem Password beim System anmelden. Nach der Berechtigungskontrolle wird in einer Abfragemaske die Suche nach Namen (auch in Verbindung mit dem Vornamen und/oder der PLZ des Wohnortes), nach amtlichen Kennzeichen oder nach Fahrgestell-/Fahrzeug-Identifizierungs-Nrn. angeboten.

Bei Eingabe des Namens wird in den Dateien A und B gesucht; gefundene Datensätze werden bereitgestellt und können mit Hilfe der Funktion "Blättern" nacheinander am Bildschirm angezeigt werden, dabei wird auch angegeben, aus welcher Datei der angezeigte Datensatz stammt.

Bei Eingabe des amtlichen Kennzeichens wird zunächst in der vorgeschalteten Datei D, dann aber nur in der Datei A und bei Eingabe der Fahrgestell-/Fahrzeug-Identifizierungs-Nr. nur in der Datei C gesucht; die Datei B wird in beiden Fällen nicht abgefragt.

2. Rechtliche Wertung

Zu dem Meldeverfahren der Kfz-Versicherer sind rechtlich insbesondere folgende Fragen und Überlegungen anzubringen.

Unter den Aufsichtsbehörden besteht Einigkeit darüber, daß die Tätigkeit der Zentralen Registrierstelle auskunfteibezogen ist, da sie hauptsächlich im Speichern und Übermitteln personenbezogener Daten im Melde- und Auskunftsverfahren mit den angeschlossenen Mitgliedsunternehmen besteht (§ 31 Abs. 1 Nr. 1 BDSG). Sie ist deshalb dem 4. Abschnitt des BDSG zuzuordnen, so daß die §§ 32 ff. BDSG die Beurteilungsmaßstäbe für das Meldeverfahren im Kraftfahrzeug-Versicherungsbereich abgeben.

Bei der rechtlichen Beurteilung sind die einzelnen Dateien jeweils für sich zu behandeln, da sie unterschiedlichen Zwecken dienen und unterschiedlich aufgebaut sind. Näher befaßt habe ich mich bisher mit den Dateien A und B.

2.1 Datei A — Zulässigkeit von Speicherung und Übermittlung

Nach § 32 Abs. 1 BDSG ist das Speichern personenbezogener Daten nur zulässig, soweit schutzwürdige Belange des Betroffenen nicht beeinträchtigt sind. Für die Beurteilung der Zulässigkeit der Speicherung kommt es darauf an, in welchem konkreten Verwendungskontext die Daten genutzt werden sollen, denn die Schutzwürdigkeit individueller Belange läßt sich nicht ohne die beabsichtigte Verwendung der Daten konkretisieren. Die Berücksichtigung des Verwendungszusammenhangs bedeutet, daß es im Einzelfall einer Interessenabwägung bedarf, bei der die Zielsetzung des Verwenders der Daten einerseits und die damit entstehenden Auswirkungen für den Betroffenen andererseits miteinander abzuwägen sind.

Hierzu ist festzustellen, daß die Kfz-Versicherer die Datei A im Auskunftsdienst des HUK-Verbandes nutzen, um im Schadensfall Informationen zu Personen, bei denen der Verdacht von Unregelmäßigkeiten entstanden ist, die auf einen Versicherungsbetrug hindeuten, austauschen zu können. Damit dient also die Datei der Aufklärung und Abwicklung eines konkreten Schadenfalles, indem bei Vorliegen von Informationen zur Person des Betroffenen weitere Nachforschungen zur Überprüfung eines Verdachts möglich werden. Gegen diese Aufklärungsversuche der Versicherer können schutzwürdigen Interessen der Betroffenen i.d.R. nicht ins Feld geführt werden. Umgekehrt ist es ein verständliches und überwiegendes Interesse der Versicherer, mögliche Betrügereien aufzuklären, um die Versichertengemeinschaft nicht mit Kosten für die unbegründete Inanspruchnahme von Versicherungsleistungen zu belasten.

Problematisch ist es hingegen, wenn die Daten des Betroffenen auch nach Abschluß des Schadensfalles zu präventiven Zwecken weiter gespeichert werden, also auf Vorrat

gehalten werden, um sie zur Aufklärung und Abwehr von Versicherungsbetrugsfällen zu verwenden, die in einer noch ungewissen Zukunft liegen. Durch die weitere Speicherung können schutzwürdige Belange der Betroffenen berührt werden, indem etwa ihre Daten in der Datei verbleiben, obwohl sich der gegen sie entstandene Verdacht nicht hat bestätigen lassen, so daß in einem erneuten Schadensfall Informationen gegen sie verwendet werden könnten, die unzutreffend, veraltet oder überholt sind.

Die Datenverarbeitung durch die Kfz-Versicherer zu präventiven Zwecken ist vergleichbar dem Sammeln und Speichern personenbezogener Daten, die im Rahmen der Strafverfolgung durch die Polizei anfallen und von ihr nach Abschluß der Ermittlungen zur vorbeugenden Verbrechensbekämpfung weiter verwendet werden sollen. Es handelt sich bei diesen Daten mit strafrechtsrelevantem Hintergrund um besonders sensible Datenkategorien, die, das zeigt § 35 Abs. 3 Satz 3 BDSG, nur unter restriktiven Voraussetzungen verarbeitet werden dürfen. Auch der Polizei ist diese Form der Datensammlung nur in engen Grenzen erlaubt, um die schutzwürdigen Belange der Betroffenen nicht zu verletzen. Die Verbrechensbekämpfung ist eine hoheitliche Aufgabe. Wenn in der Privatwirtschaft tendenziell ähnliche Maßnahmen angestellt werden, um den sich ausbreitenden Formen einer Wirtschaftskriminalität zu begegnen, so kann die Speicherung tatverdächtiger Personen in Warn- oder Risikodateien nur in einem Rahmen erlaubt sein, der die der Polizei zustehenden Befugnisse nicht überschreitet. Deshalb ist es sinnvoll, bei der Prüfung, nach welchen Kriterien eine Speicherung zu präventiven Zwecken in dieser Datei zulässig sein kann, auf die Maßstäbe zurückzugreifen, denen sich auch die Polizei zu unterwerfen hat.

Maßgeblich sind die Grundsätze, die das Bundesverwaltungsgericht zur Speicherung von Unterlagen zu Zwecken des Erkennungsdienstes nach § 81 b StPO entwickelt hat. Danach dürfen personenbezogene Daten von Verdächtigen, die im Rahmen von Strafermittlungsverfahren gewonnen worden sind, zur vorbeugenden Bekämpfung von Straftaten nur gespeichert werden, wenn der festgestellte Sachverhalt aufgrund einer prognostischen Bewertung zu

— Art und Ausführung der Tat und zur

— Persönlichkeit des Täters

sowie unter Berücksichtigung des Zeitraumes, während dessen der Betroffene strafrechtlich nicht (mehr) in Erscheinung getreten ist, Anhaltspunkte für die Gefahr der Begehung weiterer erheblicher Straftaten bietet und die zu speichernden personenbezogenen Daten geeignet sind, die dann zu führenden Ermittlungen zu fördern. Für Personen, deren Daten in einer — privaten — Warn- oder Risikodatei zur Verhütung weiterer Versicherungsbetrugsfälle gespeichert werden sollen, müssen mindestens diese Kriterien verlangt werden. D.h., der Betreffende muß

— Verdächtiger im Rahmen eines eingeleiteten Ermittlungsverfahrens gewesen sein,

— obwohl es nicht zu einer Verurteilung gekommen ist, muß weiterhin (nach Einstellung o.ä.) ein Verdacht bestehen geblieben sein,

— der nach Art und Form der Tatausführung und der Persönlichkeit des Täters Anlaß zur Besorgnis der Begehung weiterer Versicherungsbetrugsfälle gibt.

Nicht hingenommen werden kann es, Daten über jeden "Tatverdächtigen" unabhängig von der Art und Ausführung der Straftat, der Persönlichkeit des Täters und seiner Beziehungen zum geschädigten Versicherungsunternehmen sowie der Eignung der Daten, künftig zu führende Ermittlungen zu fördern, zum Zwecke der vorbeugenden Schadensbekämpfung dateimäßig zu speichern. Ein solcher Umfang der Datenerfassung wäre mit dem Erforderlichkeits- und Verhältnismäßigkeitsgrundsatz nicht zu vereinbaren und würde der Privatwirtschaft mehr Befugnisse zugestehen, als sie staatlichen Strafverfolgungsorganen gegeben sind.

Bei Anwendung der dargelegten Maßstäbe habe ich gegen die Datei A, soweit sie zu Zwecken der vorbeugenden Schadensbekämpfung gebraucht wird, aus mehreren

Gründen rechtliche Bedenken. Festzustellen ist, daß in der Datei A auch Personen geführt werden, gegen die ein Strafantrag nicht gestellt und ein strafrechtliches Ermittlungsverfahren nicht eingeleitet wurde. Damit fehlt es an der aus meiner Sicht an sich erforderlichen Voraussetzung, daß gegen den Betroffenen ein hinreichender Verdacht vorliegt, der in einem Ermittlungsverfahren geprüft wurde. Vielmehr können zur Meldung an die Datei A auch Verdachtsgründe führen, die deutlich unterhalb dieser Schwelle liegen. Mehr noch; durch die für die Meldung zu benutzende Check-Liste bleibt völlig unkonkretisiert, in welchen Fällen und bei welcher Art des Verdachts der Betreffende gemeldet und seine Daten gespeichert werden dürfen.

Weder geben die Check-Points zuverlässig Aufschluß über eine abgesicherte Prognose, wann mit möglichen Versicherungsbetrügereien zu rechnen ist, noch sind den meldenden Stellen irgendwelche verläßlichen Anhaltspunkte gegeben, welche Mindestvoraussetzungen erfüllt sein müssen, bevor von einem Verdacht gesprochen werden kann, der auf einen Betrugsfall hindeutet. In der heutigen Praxis können deshalb auch mehr oder weniger haltlose Vermutungen, subjektive Bewertungen des Schadenssachbearbeiters oder Verdachtsmomente, die sich aufgrund der Verkettung unglücklicher Umstände ergeben haben, den Anlaß für eine Meldung an den Zentralverband darstellen. Aufgrund der unbestimmten Verdachtsmomente können auch keine verläßlichen Erwägungen zu den Tatumständen und der Täterpersönlichkeit angestellt werden, um eine Prognose zur Wahrscheinlichkeit eines erneuten Schadensfalles abzugeben.

Schließlich ist selbst in den Fällen, in denen ein strafrechtliches Ermittlungsverfahren gegen den Betroffenen eingeleitet wurde, also der zu verlangende Tatverdacht vorgelegen hat, nicht gesichert, daß der meldende Versicherer oder der HUK-Verband von Polizei oder Staatsanwaltschaft über den Stand der Ermittlungen unterrichtet wird. Das ist jedoch eine unabdingbare Voraussetzung, da eine Prüfung, ob ein entstandener Verdacht nach Abschluß des Ermittlungs- oder nach Durchführung eines Strafverfahrens bestehen geblieben ist, für die weitere Speicherung zu präventiven Zwecken unerläßlich ist. Die Daten müssen gelöscht werden, wenn es zu einem Freispruch wegen erwiesener Unschuld gekommen ist oder das Ermittlungsverfahren mangels Tatverdachts eingestellt wurde (§ 170 Abs. 2 StPO). Der HUK-Verband hat indes keine Verfahren geschaffen, um genau diese Überprüfung der gespeicherten Daten auf ihre Richtigkeit und Aktualität, entsprechend dem Stand der gegen den Verdächtigen geführten Ermittlungen, zu gewährleisten. Deshalb kann nicht ausgeschlossen werden, daß auch Daten vom Betroffenen vorrätig gehalten werden, bei denen sich der gegen sie gerichtete Verdacht nicht hat verifizieren lassen.

Ein Versicherungskunde, dessen Daten unter dem unzutreffenden Verdacht, einen Versicherungsbetrug begangen zu haben, gespeichert bleiben, muß im Falle einer Meldung an ein anfragendes Mitgliedsunternehmen mit Diskriminierungen und möglichen wirtschaftlichen Nachteilen bei der Abwicklung seines Schadensfalles rechnen. Aufgrund der angeblichen Auffälligkeit wird sein Fall abweichend von den normalen Maßstäben behandelt. Es ist zu erwarten, daß die Versicherer die beantragte Versicherungsleistung — anders als im Regelfall — nicht ohne besondere Prüfverfahren oder sogar erst nach Durchführung eines Rechtsstreits erbringen werden. Dritte, die nicht selbst Versicherungsnehmer sind, aber als Beteiligte am Schadensfall angesehen werden, haben mit ebenso vielen Unannehmlichkeiten zu rechnen. Diese können etwa darin liegen, daß auffällig gewordene Sachverständige keine Aufträge mehr erhalten oder Reparaturwerkstätten besonderen Prüfungen unterzogen werden. Schon solche Formen der Behandlung stellen eine Beeinträchtigung schutzwürdiger Belange dar.

Zusammenfassend gehe ich davon aus, daß zwar die Speicherung in der Datei A zulässig ist, soweit es um die Abwicklung und Aufklärung des jeweiligen Schadensfalles geht, daß indes bisher nicht die Voraussetzungen geschaffen sind, um die gesammelten Daten auch nach Abschluß der Schadensbearbeitung zu präventiven Zwecken weiterzuspeichern. Ich muß annehmen, daß in der Datei A in großem Umfange Daten über Betroffene geführt werden, die nicht (mehr) als Versicherungsbetrüger verdächtigt werden dürfen. Diese Daten müssen deshalb aus der Warndatei gelöscht werden.

Ausgehend von diesem Befund ist die Zulässigkeit von Datenübermittlungen aus der Datei A zu beurteilen.

Sie richtet sich nach § 32 Abs. 2 BDSG und ist danach zulässig, wenn der Empfänger ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat. Ich gehe davon aus, daß die Datenübermittlung durch den HUK-Verband an das meldende Versicherungsunternehmen vom angestrebten Zweck, der in der Abwendung mißbräuchlicher Inanspruchnahme von Versicherungsleistungen zu sehen ist, umfaßt wird und zur Erfüllung des Geschäftszwecks auch erforderlich ist. Denn die Auskunft, die in der Übermittlung von Daten zu einer Schadensauffälligkeit liegt, wird in dem Fall erteilt, in dem sich das anfragende Versicherungsunternehmen mit einem ähnlich gelagerten Sachverhalt an den HUK-Verband wendet, um die Frage eines möglichen Versicherungsbetruges zu klären. Als berechtigt können die Interessen der beteiligten Unternehmen indessen nur anerkannt werden, soweit Daten übermittelt werden, die im Zeitpunkt der Übermittlung noch in der Datei gespeichert werden durften.

Nach § 32 Abs. 2 BDSG ist weiter vorausgesetzt, daß das berechtigte Interesse des Datenempfängers glaubhaft dargelegt und zum Nachweis über die Berechtigung der Datenübermittlung auch aufgezeichnet wird (§ 32 Abs. 2 Satz 2 BDSG). Soweit ich es übersehen kann, fehlt es aber bei dem Meldeverfahren der Kfz-Versicherer bisher an einer entsprechenden Protokollierung zu den aus der Datei A übermittelten Daten. Auch hierfür wären Vorkehrungen zu treffen, wenn die Datei fortgeführt werden soll.

2.2 Datei B — Zulässigkeit von Speicherung und Übermittlung

Die beim HUK-Verband eingerichtete Datei B begegnet keinen datenschutzrechtlichen Bedenken, soweit solche Personen gemeldet werden, gegen die ein Strafantrag gestellt wurde oder die bereits in einem Strafverfahren verurteilt wurden. Wenn indes ein Versicherungsunternehmen aus "übergeordneten geschäftlichen Gründen" darauf verzichtet, einen Strafantrag zu stellen, dann gelten die gleichen Bedenken wie gegen die Datei A: Der Verdacht gegen den Betroffenen bleibt unkonkretisiert und er wird auch keiner gerichtlichen Überprüfung zugeführt. Es muß schon aus diesem Grunde auf eine weitere Speicherung verzichtet werden.

Das noch nicht gelöste Problem der Datei B liegt in der Aktualisierung und Fortschreibung des Datenbestandes. Denn zu präventiven Zwecken dürfen die Daten des Betroffenen aus den dargelegten Gründen nur gespeichert werden, solange ein Verdacht gegen ihn erhalten geblieben ist, weil er nicht wegen erwiesener Unschuld freigesprochen wurde oder mangels Tatverdacht von einer Verfolgung abgesehen wurde.

Zu verlangen ist die Einführung regelmäßiger Prüfungsfristen beim Verband, die dazu dienen, den aktuellen Sachstand aufzuklären. Dieses Verfahren müßte mit entsprechenden Nachmeldepflichten der Versicherungsunternehmen an die Zentrale Registrierstelle gekoppelt werden. Wenn diese Voraussetzungen geschaffen werden, so ist aus meiner Sicht die Speicherung in der Datei B zu präventiven Zwecken zu akzeptieren.

Bedenken habe ich ferner noch insoweit, als entgegen der nach § 35 Abs. 2 Satz 2 BDSG vorgesehenen Höchstspeicherungsdauer von fünf Jahren die Daten in der Datei B über zehn Jahre geführt werden.

2.3 Zur Benachrichtigung des Betroffenen

Von erheblicher Bedeutung für die Sicherung der schutzwürdigen Belange des Betroffenen ist die Frage, ob er im Falle einer erstmaligen Datenübermittlung gem. § 34 Abs. 1 BDSG über die Datenspeicherung zu benachrichtigen ist. Nur wer weiß, welche Stelle welche Daten speichert, kann sich gegen unzulässige Eingriffe in seine Persönlichkeitsrechte zur Wehr setzen. Der HUK-Verband vertritt die Ansicht, daß mit der Benachrichtigung der Geschäftszweck der geübten Datenverarbeitung konterkariert werde.

M.E. bedarf es auch insoweit einer differenzierten Beurteilung, bei der zu berücksichtigen ist, welche Daten zu welchen Zwecken über den Betroffenen gespeichert werden.

Wenn ein Betroffener, der im Rahmen einer Schadensabwicklung zur Datei A oder B gemeldet wird, weil er in den Verdacht des Versicherungsbetruges geraten ist, nach § 34 Abs. 1 Satz 1 1. Halbsatz BDSG über die Tatsache der Speicherung benachrichtigt wird, solange der Schadensfall noch nicht abgewickelt ist, könnte er gewarnt werden und hätte Gelegenheit zu Manipulations- und Verdunkelungsmaßnahmen. Da mit der Benachrichtigung dem Betroffenen Rückschlüsse über das meldende Versicherungsunternehmen und damit auf den im Streit stehenden Schadensfall möglich wären, liegt es auch nach meiner rechtlichen Beurteilung im überwiegenden Interesse eines Dritten — des meldenden Versicherungsunternehmens —, die gespeicherten Daten bis zur Aufklärung und Regulierung des Schadens geheim zu halten (§ 34 Abs. 4 BDSG).

Ein Geheimhaltungsinteresse ist jedoch nicht mehr zu begründen, wenn die Daten des Betroffenen nach Abwicklung des Schadensfalles weiter zu präventiven Zwecken gespeichert werden sollen. Da die Speicherung zu Zwecken der Schadensverhütung jedoch — jedenfalls dann, wenn meinen Forderungen entsprochen wird — die Einleitung eines strafrechtlichen Ermittlungsverfahrens voraussetzt, dürfte die Ausnahmeregelung von § 32 Abs. 1 BDSG Anwendung finden, wonach der Betroffene nicht benachrichtigt werden muß, wenn er auf andere Weise Kenntnis von der Speicherung seiner Daten erlangt. Dabei berücksichtige ich, daß — jedenfalls in Zukunft (s. 5.4.2) — die Versicherungswirtschaft den Versicherungskunden mit dem ihm bei Vertragsabschluß auszuhändigenden Merkblatt über die Einrichtung zentraler Warn- und Risikodateien bei den einzelnen Fachverbänden unterrichtet. Der Betroffene muß deshalb damit rechnen, bei entsprechenden strafrechtlichen Ermittlungen in eine solche Datei aufgenommen zu werden.

3. Abweichende rechtliche Beurteilung des HUK-Verbandes

Ich habe den HUK-Verband über meine Beurteilung des Meldeverfahrens zu den Dateien A und B unterrichtet. Er teilt meine Rechtsauffassungen nicht und hat seine abweichenden Standpunkte wie folgt dargestellt:

Für die Dateien des HUK-Verbandes gelte der 3. Abschnitt des BDSG, denn entsprechend der Verbandssatzung würden die Dateien für eigene Zwecke, d.h. als wichtiges Hilfsmittel zur Erfüllung der satzungsgemäßen Aufgaben geführt. Richtigerweise müsse für die Prüfung der Zulässigkeit der Datenspeicherung auf § 23 Satz 1 BDSG (nicht § 32 Abs. 1) abgestellt werden. Nach beiden Vorschriften komme es im übrigen u.a. nur darauf an, daß kein Grund zu der Annahme besteht, daß schutzwürdige Belange des Betroffenen beeinträchtigt sind; ob dies tatsächlich der Fall sei, brauche nicht jeweils im Einzelfall geprüft zu werden. Es reiche vielmehr eine summarische Prüfung. Die Behauptung, daß "unzutreffende, veraltete oder überholte" Informationen in der Datei A enthalten seien, sei nicht richtig, denn dies entspräche schon nicht den Intentionen der Mitglieder, welche ausschließlich Interesse an aktuellen und vor allem zutreffenden Informationen hätten. Daher werde die Datei A laufend aktualisiert mit der Folge, daß schutzwürdige Belange der Betroffenen auch nach Abschluß des Schadenfalles nicht beeinträchtigt würden.

Die Rechtsauffassung, daß für das Führen der Datei A beim HUK-Verband dieselben Zulässigkeitsvoraussetzungen wie bei der Polizei für die Speicherung personenbezogener Daten im Rahmen der vorbeugenden Verbrechensbekämpfung gelten müßten, entbehre jeder rechtlichen Grundlage. Sie würde ferner dazu führen, daß völlig verschiedene Lebensbereiche einer einheitlichen Regelung unterworfen würden. Unberücksichtigt bliebe insbesondere, daß die Polizei die Daten mit staatlichen Machtmitteln zur Gewährleistung der öffentlichen Sicherheit und Ordnung erhebt und speichert, die Versicherer dagegen nur ihrer Pflicht zur Abwehr unbegründeter Ansprüche im privatrechtlichen Bereich nachkommen wollen. Dies werde letztlich auch — und darauf komme es hier ausschließlich an — in den unterschiedlichen Rechtsgrundlagen deutlich: Einerseits das BDSG für die Versicherer, andererseits insbesondere die StPO sowie die Polizeigesetze für den Staat. Die Hypothese, daß nach Abschluß der Schadenregulierungen die Daten der Betroffenen in der Datei A nur dann weiter gespeichert werden dürften, wenn ein hinreichender Verdacht vorliege, der in einem staatlichen

Ermittlungsverfahren überprüft worden sei, wäre unhaltbar, denn sie finde im BDSG (§ 23) keinerlei Grundlage. Die Zulässigkeit der Speicherung richte sich vielmehr nach den dort aufgestellten Voraussetzungen, die sämtlich gegeben seien.

Weil die Datei A dem 3. Abschnitt des BDSG unterfalle, richte sich die Datenübermittlung nach § 24 (nicht § 32) BDSG. Dessen Voraussetzungen seien ebenfalls erfüllt. Eine Verpflichtung zur Protokollierung statuiere diese Norm nicht.

Für die Datei B gelte das zur Datei A Gesagte sinngemäß, insbesondere hinsichtlich der Zulässigkeit der Speicherung und der Aktualisierung des Datenbestandes. Es könne überlegt werden, im Hinblick auf die zehnjährige Speicherungsdauer nach fünf Jahren bei den Unternehmen eine Regelprüfung vorzunehmen.

Eine Benachrichtigung über die Speicherung in den Dateien könne unterbleiben, weil die Ausnahmebestimmungen des § 26 Abs. 4 Nr. 1 bzw. 3 BDSG gelten würden.

Eine Diskussion über die unterschiedlichen Standpunkte wird demnächst stattfinden.

5.4.1.4 Meldeverfahren der Unfallversicherer

Ich hatte mich in meinem 6. Tätigkeitsbericht (vgl. 5.4.1.1, S. 135) mit dem Meldeverfahren der Unfallversicherer beschäftigt und darin meine Bedenken gegen dieses Verfahren angeführt.

Es konnte inzwischen mit dem HUK-Verband Einigkeit darüber erzielt werden, daß es grundsätzlich zwar ein berechtigtes Interesse an der Verteilung von Ermittlungs-Rundschreiben gibt, in die auffällige Versicherungsfälle aufgenommen werden, bei denen der Verdacht von Betrugshandlungen durch den Versicherungsnehmer gegeben ist. Allerdings dürfen die Daten nur zu den mit dem Meldeverfahren der Unfallversicherer beabsichtigten Zwecken von den Einzelversicherern verwendet werden, also nur, um bei der Antrags- oder Leistungsbearbeitung den Verdacht auf verschwiegene anderweitige Versicherungen oder sonstige anzeigepflichtige Umstände bei anderen, dem Verband angeschlossenen Mitgliedsunternehmen überprüfen zu können.

Indessen könnten die übermittelten Daten von den einzelnen Mitgliedsunternehmen zum Zwecke des Aufbaus einer Risiko- oder Warndatei in manuell oder automatisiert geführten Dateien auf Vorrat gespeichert werden. Mir ist bekannt, daß Überlegungen dazu von einzelnen Unternehmen bereits angestellt worden sind. Der HUK-Verband stimmt meinen Bedenken gegen solche Warndateien zu: Das einzelne Mitgliedsunternehmen wird nicht in jedem Einzelfall ein berechtigtes Interesse an einer Vorratsspeicherung zum Zwecke der präventiven Schadensbekämpfung nachweisen und die Verletzung schutzwürdiger Belange von Betroffenen ausschließen können.

Den Möglichkeiten zum Aufbau von Warn- und Risikodateien wäre wirksam zu begegnen, indem die Rundschreiben nach der Verteilung an die Unternehmen von diesen vernichtet würden, sobald ein Abgleich mit ihrem Datenbestand vorgenommen worden ist, um die Frage der jeweils aktuellen Mehrfachversicherungen abzuprüfen. Das geschieht bisher offenbar jedoch nicht. Statt dessen werden die Rundschreiben bei den Mitgliedsunternehmen abgelegt; ob sie auch ausgewertet werden, indem die Informationen auf Karteikarten gebracht oder in EDV-Anlagen gespeichert werden, ist dem HUK-Verband nicht bekannt. Für eine Aufbewahrung der Rundschreiben vermag ich keine Rechtfertigungsgründe zu erkennen. Auch der HUK-Verband konnte kein berechtigtes Interesse für eine Informationssammlung über längere Zeit bei den Mitgliedsunternehmen anführen, zumal die Rundschreiben — da nicht nach bestimmten Merkmalen sortiert — nach den Erklärungen des HUK-Verbandes ungeeignet erscheinen, um sie zur Überprüfung verdächtiger Schadensfälle zu einem noch nicht bestimmten Zeitpunkt heranzuziehen. Ich meine darum nach wie vor, daß eine längerfristige Aufbewahrung der Ermittlungsrundschreiben zu unterbleiben hat und der HUK-Verband zumindest auf eine entsprechende Übung der Mitgliedsunternehmen hinwirken sollte, auch wenn er — wie er zutreffend erklärt hat — in diesem Punkt selbst keine Durchsetzungsbefugnisse gegenüber den unabhängigen Unternehmen hat. Der HUK-Verband hat mir

zwischenzeitlich ein Rundschreiben übersandt, mit dem er seine Mitgliedsunternehmen über meine Rechtsauffassung unterrichtet hat.

Darüberhinaus hat mir der HUK-Verband zugesichert, daß er sich mit den Aufsichtsbehörden rechtzeitig in Verbindung setzen wird, sobald daran gegangen werden sollte, eine zentrale Datei bei dem Verband selbst einzurichten. Das Verlangen nach einer solchen zentralen Hinweisdatei wird von einzelnen Mitgliedsunternehmen im Bereich der Unfallversicherer immer wieder an den HUK-Verband herangetragen; bisher sei aus Kostengründen auf die Einrichtung einer zentralen Datei verzichtet worden. Von Bedeutung dafür ist auch, daß eine Zentraldatei — anders als in anderen Versicherungssparten — aufgrund der relativ seltenen mißbräuchlichen Inanspruchnahme von Versicherungsleistungen vom Verband nicht als besonders dringlich erachtet wird. Es stehen aber noch im Jahre 1989 in den zuständigen Gremien des Verbandes neue Beratungen über die Einrichtung einer Zentraldatei an. Die weitere Diskussion beim HUK-Verband und die Datennutzung bei den einzelnen Mitgliedsunternehmen wird also von den Aufsichtsbehörden noch mit Interesse zu verfolgen sein.

5.4.1.5 Sachschadendatei

Der Verband der Sachversicherer (VdS) plant — wie ich bereits berichtet habe, vgl. 6. TB, 5.4.1.5, S. 136-138 — die Errichtung einer zentralen Sachschadendatei, die der Aufdeckung und Abwehr von Betrugshandlungen und Brandstiftungen dienen soll. Die darüber aufgenommenen Verhandlungen zwischen den Datenschutz-Aufsichtsbehörden und der Versicherungswirtschaft sind im Berichtszeitraum fortgeführt worden und stehen nunmehr kurz vor dem Abschluß. Zu einer Reihe bisher noch offener Einzelfragen sind Lösungen erarbeitet worden; in anderen Punkten konnte noch keine Einigung erzielt werden. Der Sachstand stellt sich wie folgt dar:

Die Versicherungswirtschaft beabsichtigt, ein Hinweissystem zu schaffen, das es Einzelversicherern ermöglichen soll, einerseits bei der Prüfung aktueller Schäden weitere relevante Informationen zu festgestellten Schadensauffälligkeiten zu erhalten. Die Meldung an den Verband hat durch die Weiterleitung an andere Versicherungsunternehmen zunächst einmal den Zweck abzufragen, ob der Betroffene schon einen meldepflichtigen Schaden bei anderen Unternehmen hatte. Andererseits soll die Hinweisdatei präventiven Zwecken dienen. Die Einzelversicherer halten einen Datenbestand von Schadensmeldungen vorrätig, den sie zur Prüfung von Schäden oder zur Risikobeurteilung bei Vertragsabschlüssen abgleichen können. Ziel ist es dabei, Mehrfachtäter zu ermitteln, unberechtigte Forderungen abzuwehren oder riskante Vertragsabschlüsse zu vermeiden.

Zur Erfüllung dieser Aufgaben soll eine Datenbank errichtet werden, an die die einzelnen Versicherungsunternehmen Schäden aus allen Sparten der Sachversicherung melden. Meldepflichtig sollen Fälle ab einem Schadensaufwand von DM 10.000,— sein, in denen es zur Aufhebung des Vertrages durch das Versicherungsunternehmen gekommen ist, weil Tatbestände strafrechtlicher Art (z.B. Einleitung eines strafrechtlichen Ermittlungsverfahrens, Anklageerhebung), vertragsbezogener Art (z.B. Verschweigen von Vorverträgen, einer vorläufigen Deckungszusage oder Vorschäden, Verschweigen von Antragsablehnungen oder Kündigungen durch Vorversicherer) oder schadensbezogener Art (z.B. Gefahrerhöhung, Verletzung von Sicherheitsvorschriften oder -obliegenheiten, Verletzung von Schadensminderungspflichten oder Schadensaufklärungspflichten, Herbeiführung oder Vortäuschung des Schadens) vorliegen, die der Versicherungsnehmer oder ein beteiligter Dritter zu vertreten haben. Darüber hinaus sind Brandstiftungsfälle ab DM 10.000,— meldepflichtig.

Gemeldet werden die Daten von natürlichen wie von juristischen Personen, wobei die Daten von natürlichen Personen beim meldenden Versicherungsunternehmen zum Zwecke der Anonymisierung in einen Match-Code umgewandelt und an den VdS gesandt werden. Die gesammelten Daten werden monatlich auf Datenträgern an alle Mitglieds-Versicherungsunternehmen weitergeleitet und dort mit dem eigenen Datenbestand abgeglichen.

Bei der Bildung des Match-Codes wäre es an sich sinnvoll, das Geburtsdatum aufzunehmen, um eine genaue Identifizierung des Betroffenen zu ermöglichen und so eine hohe Trefferquote im Abgleichverfahren zu erzielen. Nach Aussagen der Versicherungswirtschaft steht das Geburtsdatum für die Aufnahme in einen Match-Code jedoch nicht zur Verfügung, weil die Angabe dieses Datums bei dem Versicherungskunden nicht durchsetzbar sei.

Um gleichwohl eine hohe Trefferquote zu gewährleisten, denkt der VdS daran, einen relativ breiten Match-Code zu bilden, zu dem auch der Nachname des Betroffenen mit den ersten 6 Buchstaben gehören soll. Viele Betroffene können also aus dem Match-Code ohne weiteres Zusatzwissen reidentifiziert werden. Die Aufsichtsbehörden haben deshalb vorgeschlagen, den Nachnamen innerhalb des Match-Codes zu verstümmeln, indem der erste Buchstabe des Nachnamens unterdrückt wird. Dem hat die Versicherungswirtschaft vorerst nicht zustimmen wollen. Sie hat sich lediglich bereit erklärt, den von ihr vorgesehenen Match-Code zunächst (maximal zwei Jahre) nur testweise zu verwenden; sie wird mich dann über die Ergebnisse unterrichten.

Kontrovers ist in den Verhandlungen auch die Frage nach der Speicherungsdauer diskutiert worden. Nach den Vorstellungen des VdS sollen die beim Verband gespeicherten Daten erst nach zehn Jahren gelöscht werden. Dieser Zeitraum sei erforderlich, da sich die Abwicklung der Schadensbearbeitung häufig über längere Zeit erstrecke. Die Aufsichtsbehörden, die gegen eine Speicherungsdauer von mehr als fünf Jahren Bedenken haben, halten folgenden Kompromiß für rechtlich vertretbar:

Dem VdS wird die Speicherung von Daten in der Sachschadendatei für einen Zeitraum von zehn Jahren beginnend mit dem Datum der Einspeicherung gestattet. Jedoch hat nach Ablauf von fünf Jahren eine Überprüfung des gespeicherten Datenbestandes stattzufinden; nicht mehr aktuelle Daten sind spätestens zu diesem Zeitpunkt zu löschen, wenn nicht zuvor bereits ihre Löschung zu veranlassen war. Damit wird dem Gedanken des § 35 Abs. 2 Satz 2 BDSG entsprochen, der eine Speicherung von Daten zu Auskunftszwecken — und damit auf Vorrat — nicht unbegrenzt erlaubt, weil die Daten unaktuell werden können und dann ein unzutreffendes Bild über den Betroffenen abgeben.

Im Mittelpunkt der datenschutzrechtlichen Problematik stand auch bei den Diskussionen über die geplante Sachschadendatei die Bestimmung des Personenkreises, der in der Datei gespeichert werden darf, ohne daß die schutzwürdigen Belange der Betroffenen verletzt erscheinen. Hierbei ist zu beachten, daß mit der Speicherung der Daten von Versicherungsnehmern, die beim Abschluß eines Versicherungsvertrages oder bei der Abwicklung eines Schadensfalles auffällig geworden sind, und sonstigen am Schadensfall beteiligten dritten Personen hochsensible Daten — teilweise mit strafrechtlichem Bezug — gespeichert werden. Sicherlich ist es ein berechtigtes Anliegen der Versicherer, Versicherungsbetrugsfälle aufzudecken und zu einer Schadensbegrenzung im Interesse auch der Versichertengemeinschaft beizutragen. Zu diesem Zweck muß prinzipiell auch die Speicherung von Daten über tatverdächtige Personen als erlaubt angesehen werden. Es müssen jedoch Kriterien bestimmt werden, nach denen einzelne Personengruppen erfaßt werden können. Hierbei ist wie folgt zu differenzieren:

Für die Gruppe der Versicherungsnehmer selbst kann ein hinreichend objektives Kriterium darin gesehen werden, daß es zur Aufnahme in die Sachschadendatei nur im Falle einer Vertragskündigung oder einer Brandstiftung kommt. Dies soll — so die bereits bezeichneten Voraussetzungen einer Meldung — auch nur dann der Fall sein, wenn die Vertragsaufhebung auf Umständen strafrechtlicher, vertrags- oder schadensbezogener Art beruht. Bagatellschäden führen dabei nicht zu einer Meldung, sondern nur solche ab einer Schadenssumme von DM 10.000,—. Damit geht es primär um eine wirtschaftliche Interessenabwägung. Der verursachte Schaden ist so schwerwiegend, daß die Versicherer ihr an sich bestehendes Interesse an der Anbahnung oder Aufrechterhaltung von vertraglichen Beziehungen mit dem Betroffenen zurückstellen, weil das wirtschaftliche Risiko für den Versicherer unkalkulierbar und unverhältnismäßig geworden ist.

Da bei der Entscheidung zur Meldung von Versicherungsnehmern an die Sachschadendatei auch Umstände strafrechtlicher Art eine Rolle spielen können, stellt sich die Frage, inwieweit eine Verdächtigendatei aufgebaut wird. Die Versicherungswirtschaft weist darauf hin, daß keine Verdächtigendatei, sondern ein Hinweissystem aufgebaut werden solle und daß die Gründe für eine Meldung vielfältig und nicht unbedingt von strafrechtlicher Bedeutung seien. Denn gemeldet werden sollen auch Vertragsaufhebungen, die deshalb erfolgt sind, weil der Versicherungsnehmer Obliegenheiten oder Schadensminderungspflichten verletzt oder Vorschäden oder Vorverträge verschwiegen hat, die für die Risikobewertung Bedeutung haben. Im Vordergrund steht also eine wirtschaftliche Interessenabwägung des Versicherers. Demgegenüber tritt zurück, ob und in welcher Weise ein strafrechtlicher Verdacht gegen einen Betroffenen begründet wurde. Es bestand deshalb Einigkeit darüber, daß insofern das Kriterium der Vertragskündigung wie auch das der Brandstiftung ein hinlänglich ausgewiesenes objektives Kriterium für die Berechtigung der Versicherer darstellt, um den Betroffenen an die Sachschadendatei zu melden. Im Verhältnis zu diesem überwiegenden Interesse an der Aufklärung, Einschränkung und Veränderung von auffälligen Versicherungsschäden sind keine entgegenstehenden Belange der Betroffenen ersichtlich, die für schutzwürdig zu erachten wären.

Da davon auszugehen ist, daß die Betroffenen durch die Kündigung des Vertragsverhältnisses bereits auf andere Weise Kenntnis von der Speicherung ihrer personenbezogenen Daten erhalten haben, müssen sie über ihre Aufnahme in die Sachschadendatei auch nicht besonders benachrichtigt werden, um ihre Rechte wahrnehmen zu können.

Den Versicherungsnehmern vergleichbar sind Dritte, die zwar nicht selbst Versicherungsnehmer sind, die aber in einer engen rechtlichen Beziehung zu einer gemeldeten juristischen Person stehen, mit der das Versicherungsunternehmen den Schadensfall abzuwickeln hat (Geschäftsführer, Kommanditisten, sonstige Repräsentanten, die als Vertreter der juristischen Personen handeln, für sie haften oder durch sie begünstigt werden).

Die Aufhebung des Vertragsverhältnisses mit dem Betroffenen läßt sich als objektives Kriterium für den Nachweis eines berechtigten Interesses des Versicherers an der Speicherung weiter auch auf die in Verdacht geratenen Dritten übertragen, die mit dem gekündigten Versicherungsnehmer als eine wirtschaftliche Einheit zu sehen sind und deshalb als unmittelbare wirtschaftliche Nutznießer in Betracht kommen, also Personen mit engen familiären Beziehungen (Ehefrauen/männer, Kinder) oder auch Personen, die mit dem Betroffenen in einer eheähnlichen Lebensgemeinschaft zusammenleben.

Ein berechtigtes Interesse der Versicherer an der Speicherung von Daten über Angehörige dieser beiden Personengruppen, die mit dem Versicherungsnehmer in enger rechtlicher oder persönlicher Verbundenheit stehen, kann anerkannt werden, da sie entweder selbst Adressat der ihnen gegenüber durch die Vertragsaufhebung zum Ausdruck gebrachten Wertung des Versicherungsunternehmens sind, ihr Vertragsrisiko nicht länger tragen zu wollen; oder aber diese Beurteilung ist deshalb auf sie anzuwenden, weil sie mit dem gekündigten Versicherungsnehmer eng verbunden sind und sich zugleich in einer Weise verdächtig gemacht haben, die Anlaß zur Vertragsaufhebung gegeben hat.

Auch bei diesen beiden Personengruppen ist davon auszugehen, daß ihnen bereits durch die Bearbeitung des Schadensfalles bekannt geworden ist, daß sie Gründe für eine Aufhebung des Vertragsverhältnisses geliefert haben. Sie haben deshalb mit der Aufnahme in eine Warndatei zu rechnen und brauchen über diesen Tatbestand nicht gesondert unterrichtet zu werden.

Besondere Schwierigkeiten wirft die Frage auf, ob und ggf. unter welchen Voraussetzungen sonstige Dritte, die an einem Schadensfall beteiligt waren, bei dem es zur Kündigung des Vertrages mit dem Versicherungsnehmer gekommen ist, in der Sachscha-

dendatei gespeichert werden dürfen. Das können Zeugen, Sachverständige, angeblich geschädigte Antragsteller u.a.m. sein. Diesen "Dritten" gegenüber versagt das Aufnahmekriterium "Vertragskündigung", da sie selbst in keinen vertraglichen Beziehungen mit dem Versicherer gestanden haben. Bei ihnen steht der Verdacht im Vordergrund, Täter oder Teilnehmer eines Versicherungsbetruges oder einer anderen Straftat gewesen zu sein. Vor solchermaßen verdächtig gewordenen Personen soll zu Zwecken der präventiven Schadensbekämpfung gewarnt werden. Damit wird das Speichern von Daten über diese Personen m.E. dem Führen von Datensammlungen durch die Polizei für Zwecke der Straftatenverhütung ähnlich, womit nicht gesagt werden soll, daß die Versicherungswirtschaft ebenso wie die Polizei Aufgaben der Strafverfolgung und vorbeugenden Verbrechensbekämpfung ausübt. Jedoch können private Wirtschaftsunternehmen für Datensammlungen, die sich mit den Daten straftatverdächtiger Personen befassen, keineswegs weiterreichende Befugnisse haben als sie der Polizei im Rahmen ihrer hoheitlichen Tätigkeit zur Verfügung stehen. Das bedeutet:

Die Daten dieser Personen dürfen in der Sachschadendatei gespeichert werden, sofern gegen sie ein strafrechtliches Ermittlungsverfahren eingeleitet wurde wegen des Verdachts, Täter oder Teilnehmer einer Straftat (Versicherungsbetrug) gewesen zu sein. Wenn es nicht zu einer Verurteilung kommt, muß für eine weitere Speicherung der Person, die präventiven Zwecken dienen soll, ein Verdacht bestehen geblieben sein, der nach kriminalistisch-prognostischer Erwägung zur Art und Form der Tatausführung und der Persönlichkeit des Täters Anlaß zur Besorgnis der Begehung weiterer Versicherungsbetrugsfälle gibt. Wird also das Verfahren mangels Tatverdachts (§ 170 Abs. 2 StPO) eingestellt oder der Betroffene wegen erwiesener Unschuld freigesprochen, so berechtigt dies nicht zur weiteren Speicherung. Zulässig ist die Speicherung selbstverständlich, wenn das gerichtliche Verfahren mit einer Verurteilung des Betroffenen geendet hat. Auch für diese Gruppe tatverdächtiger Dritter bedarf es m.E. keiner besonderen Benachrichtigung, da sie bereits im Rahmen des staatsanwaltschaftlichen Ermittlungsverfahrens von den gegen sie gerichteten Verdachtsmomenten erfahren haben und daher mit der Aufnahme in eine Warndatei rechnen müssen.

Die Versicherungswirtschaft hat in den Gesprächen weiter ein Interesse an der Erfassung solcher Personen angemeldet, die im Zusammenhang mit der Abwicklung eines Schadensfalles in Betrugsverdacht geraten sind, bei denen es aber aus unterschiedlichen Gründen nicht zur Einleitung eines strafrechtlichen Ermittlungsverfahrens gekommen ist, obwohl der Versicherer hinreichende tatsächliche Anhaltspunkte für eine Beteiligung an einer Betrugshandlung vorliegen hat. Hier besteht die Gefahr, daß intuitiv-subjektive Bewertungen zu Fehlschlüssen bei der Zuordnung von strafrechtlichen Verdachtsgründen führen. Es wurde diskutiert, die Daten solcher Personen nur dann in die Sachschadendatei aufzunehmen, wenn sie zugleich über diese Tatsache in einer qualifizierten Form unterrichtet werden, d.h. sie müssen der Benachrichtigung entnehmen können, daß sie in die Warndatei aufgenommen wurden. Die Benachrichtigungspflicht ist als ein Korrektiv anzusehen, um dem Betroffenen Gelegenheit zu geben, einen unberechtigterweise gegen ihn gerichteten Verdacht zu entkräften und um im Zweifel gerichtlich gegen den Versicherer vorzugehen, soweit der Betroffene durch die Speicherung seiner Daten in seinen Persönlichkeitsrechten verletzt wird.

Die Versicherungswirtschaft hat mitgeteilt, sie stimme mit meiner Beurteilung zur Speicherung von Daten tatverdächtiger "Dritter" nicht überein. Auch diese "Dritten" würden nur dann aufgenommen, wenn die allgemeinen Voraussetzungen, d.h. Kündigung oder Brandstiftung sowie Schäden über DM 10.000,— vorliegen. Dies bedeute aber, daß wirtschaftliche Interessen letztlich ausschlaggebend für die Aufnahme in das Hinweissystem seien. Wenn der Versicherer sich nicht zu einer Kündigung entschließe, würde der Dritte auch bei erheblichem Verdacht, Täter oder Teilnehmer eines Versicherungsbetruges oder einer anderen Straftat zu sein, nicht in das Hinweissystem aufgenommen. Damit werde zugleich ein Unterschied zum Führen von Datensammlungen durch die Polizei für Zwecke der Straftatenverhütung deutlich: Für die Polizei sei das Vorliegen eines Tatverdachts entscheidend und ausreichend. Darüber hinaus erhebe die

Polizei ihre Daten mit den hoheitlichen Zwangsmitteln des Staates zur Wahrung der öffentlichen Sicherheit und Ordnung auf der Grundlage der Strafprozeßordnung bzw. der Polizeigesetze. Zweck des Hinweissystems der Sachversicherer sei es aber, nur eine bessere Risikobeurteilung zu ermöglichen bzw. im Schadensfall unberechtigte Forderungen abzuwehren. Rechtsgrundlage für die Datenverarbeitung in diesem Rahmen sei allein das BDSG. Insofern bestehe keine Übereinstimmung, daß auch in das Hinweissystem der Sachversicherer diese Dritten nur nach Maßgabe der Befugnisse aufgenommen werden sollen, wie sie der Polizei zur Verfügung stehen.

Auch über die Pflicht zur Benachrichtigung derjenigen Personen, die von einem Versicherungsunternehmen zur Sachschadendatei gemeldet werden sollen, obwohl gegen sie kein förmliches Ermittlungsverfahren geführt wurde, konnte mit der Versicherungswirtschaft bisher keine Einigung erzielt werden, da die Befürchtung gehegt wird, durch die Benachrichtigung könnten zu Recht Verdächtigte gewarnt werden. Solange die angesprochenen Streitfragen nicht geklärt worden sind, kann die von der Versicherungswirtschaft geplante Sachschadendatei datenschutzrechtlich nicht akzeptiert werden. Es bleibt abzuwarten, ob der bestehende Dissens auszuräumen ist.

5.4.2 Einwilligungsklausel nach dem BDSG

Über die in der Versicherungswirtschaft verwendeten Einwilligungsklausel zur Datenverarbeitung, die der Versicherungsnehmer bei Abschluß eines Vertrages unterzeichnet, ist zu berichten, daß nunmehr eine Einigung nicht nur über eine neue Klausel, sondern auch über ein neues Merkblatt erzielt wurde, das der Aufklärung und Erläuterung zu einzelnen Formen der Datenverarbeitung in der Versicherungswirtschaft dienen soll. Entsprechend dem Verlangen der Datenschutz-Aufsichtsbehörden sind von der Klausel nun auch die Datenübermittlungen zwischen einzelnen Versicherungsunternehmen und den bei einzelnen Fachverbänden geführten zentralen Dateien umfaßt; in dem Merkblatt werden dazu nähere Erläuterungen gegeben.

Kontrovers war lange Zeit die Forderung der Aufsichtsbehörden, die Aushändigung des Merkblatts an den Versicherungsnehmer obligatorisch zu machen und in die Klausel einen Hinweis aufzunehmen, mit dem der Versicherungsnehmer die Aushändigung des Merkblatts bestätigt. Die Aufsichtsbehörden haben diese Position deshalb mit Nachdruck vertreten, da die Einwilligungsklausel und das Merkblatt als Einheit gesehen werden müssen, denn erst das Merkblatt bietet eine Aufklärung, die den Versicherungsnehmer die Tragweite seiner Einwilligungserklärung erkennen läßt.

Nunmehr ist folgender Satz in die Klausel aufgenommen worden:

"Diese Einwilligung gilt nur, wenn ich (d.h. der Kunde) die Möglichkeit hatte, in zumutbarer Weise vom Inhalt des vom Versicherer bereitgehaltenen Merkblatts zur Datenverarbeitung Kenntnis zu nehmen."

So wird der Kunde einerseits besonders auf das Merkblatt hingewiesen und er kann von sich aus die Aushändigung verlangen, andererseits hat der Versicherer, wenn es zum Streit über die Einhaltung seiner Aufklärungspflichten kommt, den Nachweis zu führen, daß er dem Versicherungskunden Einblick in das Merkblatt gegeben bzw. es ihm ausgehändigt hat.

Das Merkblatt dient der von den Aufsichtsbehörden für notwendig erachteten Aufklärung des Versicherungsnehmers über die möglichen Datenübermittlungsvorgänge in den einzelnen Versicherungssparten. Er wird nunmehr darüber informiert, welche Warn- und Risikodateien es gibt, welchen Zwecken die Dateien und Hinweissysteme dienen und unter welchen Voraussetzungen er selbst mit einer Aufnahme in die Datei zu rechnen hat. Diese Konkretisierungen waren wichtig, da es sich bei den in den Warndateien gespeicherten Daten um besonders sensible Datenkategorien handelt. Der Versicherungsnehmer kann auf diese Weise leicht ermessen, zu welchen Datenübermittlungen er mit Unterzeichnung der Klausel seine Einwilligung erteilt.

5.4.3 Schweigepflichtentbindungsklauseln

Nachdem bereits eine Klausel für Lebensversicherungsverträge vereinbart worden war, ist es jetzt auch gelungen, eine Neuformulierung der Klausel für die Krankenversicherer und Unfallversicherer abzustimmen.

Die neue Fassung der Schweigepflichtentbindungsklausel für die Krankenversicherungsverträge lautet wie folgt:

"Mir ist bekannt, daß der Versicherer — soweit hierzu ein Anlaß besteht — Angaben über meinen Gesundheitszustand und bei anderen Krankenversicherern auch Angaben über frühere oder bestehende Versicherungsverträge zur Beurteilung der Risiken eines von mir beantragten Vertragsabschlusses überprüft. Zu diesem Zweck befreie ich Ärzte, Zahnärzte, Angehörige anderer Heilberufe sowie Angehörige von Krankenanstalten und Gesundheitsämtern, die mich in den letzten zehn Jahren vor Antragstellung untersucht, beraten oder behandelt haben, von ihrer Schweigepflicht — und zwar auch über meinen Tod hinaus — und ermächtige sie, dem Versicherer die erforderlichen Auskünfte zu erteilen. Dies gilt auch für Angehörige anderer Kranken-, Lebens- und Unfallversicherer, mit denen ich bisher in Vertragsbeziehungen stand oder stehe. Diese Ermächtigung endet fünf Jahre nach Antragstellung.

Mir ist ferner bekannt, daß der Versicherer zur Beurteilung seiner Leistungspflicht auch Angaben überprüft, die ich zur Begründung etwaiger Ansprüche mache oder die sich aus von mir eingereichten Unterlagen (z.B. Rechnungen, Verordnungen) sowie von mir veranlaßten Mitteilungen eines Krankenhauses oder von Angehörigen eines Heilberufes ergeben. Auch zu diesem Zweck befreie ich die Angehörigen von Heilberufen oder Krankenanstalten, die in den vorgelegten Unterlagen genannt sind oder die an der Heilbehandlung beteiligt waren, von ihrer Schweigepflicht; dabei hat die Geltendmachung eines Leistungsanspruches die Bedeutung einer Schweigepflichtentbindung für den Einzelfall. Von der Schweigepflicht entbinde ich auch zur Prüfung von Leistungsansprüchen im Falle meines Todes. Die Schweigepflichtentbindung für die Leistungsprüfung bezieht sich auch auf die Angehörigen von anderen Kranken und Unfallversicherern, die nach dort bestehenden Versicherungen befragt werden dürfen.

Diese Erklärung gebe ich auch für meine mitzuversichernden Kinder sowie die von mir gesetzlich vertretenen mitzuversichernden Personen ab, die die Bedeutung dieser Erklärung nicht selbst beurteilen können."

Mit dieser Klausel sind alle wesentlichen Bedenken ausgeräumt, die ich gegen die bisher verwendete Klausel anzubringen hatte. Im einzelnen ist zur Schweigepflichtentbindungsklausel noch folgendes anzumerken:

In der lange Zeit umstrittenen Frage der Zukunftswirkung der Schweigepflichtentbindung wird unterschieden zwischen der Beurteilung der Risiken bei Abschluß eines Versicherungsvertrages und der Geltendmachung eines Leistungsanspruches.

Für die Überprüfung des Gesundheitszustandes bei Vertragsschluß ist eine zeitliche Befristung der Schweigepflichtentbindung vorgesehen. Die Frist endet fünf Jahre nach der Antragstellung. Einigkeit wurde weiter darüber erzielt, daß die Schweigepflichtentbindung im Falle der Risikoprüfung auch über den Tod hinausgehen muß, um entstandene Streitfragen zwischen Versicherer und Versicherungsnehmer mit den Rechtsnachfolgern des Verstorbenen abklären zu können.

Anders als im Falle der Risikoprüfung bei Vertragsschluß kommt der Schweigepflichtentbindung zur Überprüfung des Leistungsfalls grundsätzlich keine Zukunftswirkung zu. Erst mit dem Einreichen von Unterlagen wie Rechnungen u.a.m. entbindet der Versicherungsnehmer die Beteiligten von ihrer Schweigepflicht, und dies, um dem Versicherungsunternehmen die Überprüfung des im jeweiligen Einzelfall konkret geltend gemachten Anspruches zu ermöglichen. Allerdings braucht der Versicherungsnehmer den behandelnden Arzt nicht in jedem Einzelfall schriftlich von der Schweigepflicht zu entbinden. Vielmehr nimmt er mit der Unterzeichnung der Schweigepflichtentbindungsklausel davon Kenntnis, daß das Einreichen von Unterlagen zur Leistungs-

abrechnung die Bedeutung einer — konkludenten — Schweigepflichtentbindung hat. Der von der Versicherungswirtschaft befürchtete bürokratische Aufwand, der mit schriftlichen Schweigepflichtentbindungserklärungen in jedem Einzelfall entstehen könnte, wird also vermieden.

Von dem Grundsatz, daß es keine Zukunftswirkung bei der Schweigepflichtentbindung im Leistungsfall gibt, wird eine Ausnahme für mögliche Ansprüche im Todesfall gemacht. Für diesen Fall muß sichergestellt werden, daß das Versicherungsunternehmen Versicherungsleistungen überprüfen kann. Die Erben könnten hierzu nicht rechtsgültig ermächtigen.

Präzisiert worden ist in beiden Teilen der Klausel, welcher Personenkreis durch den Versicherungsnehmer von der Schweigepflicht entbunden wird. Es können dies stets nur Angehörige von Heilberufen sein, die in den eingereichten Unterlagen genannt sind oder an der Behandlung des Versicherungskunden mitgewirkt haben, sowie die Angehörigen von Versicherungsunternehmen, mit denen der Versicherungsnehmer bisher bereits in Vertragsbeziehungen stand.

In der Klausel wird der Kunde darüber aufgeklärt, daß er auch zur Überprüfung einer Leistungspflicht des Versicherers gegenüber einem Krankenhaus von der Schweigepflicht entbindet. Damit ist nunmehr auch das von mehreren Unternehmen der privaten Krankenversicherung eingeführte Krankenhaus-Ausweisverfahren in die Klausel integriert worden.

Von der Schweigepflichtentbindung ausgenommen worden sind die Sozialleistungsträger. Wenn an diese Stellen Anfragen gerichtet werden sollen, bedarf es nach dem Sozialgesetzbuch (SGB) einer ausdrücklichen Einwilligung des Betroffenen im Einzelfall.

5.5 Handels- und Wirtschaftsauskunfteien

5.5.1 Automation bei Auskunfteien und neue Serviceleistungen

Der zunehmende Einsatz der automatisierten Datenverarbeitung und die damit entstandenen Möglichkeiten, den Auskunftsverkehr bei den Wirtschafts- und Handelsauskunfteien zu effektivieren und flexibler auf Nachfragewünsche der Kunden reagieren zu können, führt zur Entwicklung immer neuer Serviceleistungen, die von den Datenschutz-Aufsichtsbehörden auf ihre Zulässigkeit hin überprüft werden müssen.

5.5.1.1 On-line-Verfahren bei Handelsauskunfteien

Zu den neuen Angeboten innerhalb der Dienstleistungspalette zählt das On-line-Verfahren. Eine überregionale Handelsauskunftei, die in einzelne Mitgliedsvereine aufgegliedert ist und durch einen Zentralverband zusammengefaßt wird, bietet ihren Kunden die Möglichkeit, durch einen On-line-Anschluß direkt auf alle von den einzelnen Mitgliedsunternehmen gespeicherten Daten zuzugreifen. Die On-line-Nutzervereinbarung wird durch Vertrag zwischen der örtlichen Auskunftei und ihrem Kunden abgeschlossen. Gegenstand ist der Direktzugriff des Kunden auf die Datenbank des Verbandes, in der die Archivdaten der angeschlossenen örtlichen Auskunfteien gespeichert werden.

Dem Anfrager wird es durch das On-line-System ermöglicht, die abgefragte Information über die Postleitung auf den PC zu ziehen und ausdrucken zu lassen. Überlegt wird, Großunternehmen in der Zukunft einen sog. File-Transfer Report anzubieten, mittels dessen sie Datenmaterial, das nach den von der Auskunftei bestimmten Schlüsselwerten strukturiert ist, zur Speicherung und Übersetzung auf der eigenen Großrechneranlage übermittelt erhalten. Von dort können dann die übermittelten Schlüsselwerte in die ihnen zugrundeliegenden Informationen übersetzt und ausgedruckt werden.

Zur Nutzung der Datenbank ist die Eingabe eines Passwortes nötig. Das Passwort ist dreiteilig und besteht aus einer zwölfstelligen Mitglieds-Nummer, einem achtstelligen

allgemeinen Passwort und einem bis zu achtstelligen persönlichen Passwort. Die Passwörter werden nicht an ein Unternehmen vergeben, sondern die jeweiligen zuständigen Mitarbeiter des Unternehmens erhalten ein eigenes Passwort. Dadurch sollen Sicherheit und Kontrolle bei der Datennutzung gewährleistet werden. Auf Wunsch werden die vergebenen Passwörter durch die Auskunftei geändert; feste Rhythmen, in denen — aus Sicherheitsgründen — die Passwörter ausgetauscht oder geändert werden, gibt es allerdings nicht.

Bei der datenschutzrechtlichen Beurteilung des On-line-Verfahrens gibt es verschiedene — z.T. noch offene — Fragen, die zwischen den Handelsauskunfteien und den Aufsichtsbehörden diskutiert werden.

Ungeklärt war, wie das Verhältnis zwischen den örtlichen Auskunfteien und dem Zentralverband dieser Auskunfteien zu bewerten ist. Es gab die Frage, ob der Verband im Rahmen eines Auftragsverhältnisses nach § 37 BDSG arbeitet oder ob eine Datenübermittlung von der örtlichen Auskunftei an den Verband vorausgeht, die nur unter den in § 32 BDSG genannten Voraussetzungen zulässig wäre.

Inzwischen ist durch einen Rechenzentrumsvertrag einheitlich für die angeschlossenen regionalen Mitgliedsvereine geregelt worden, daß der Verband die Datenbank und die Datenverarbeitung als Auftragnehmer im Sinne von § 37 BDSG betreibt. Er speichert — und übermittelt — also die Daten nicht für sich selber, sondern im Auftrag der örtlichen Auskunfteien und ist abhängig von deren Weisungen. Durch diese Vertragskonstruktion sind bisher bestehende Rechtsunsicherheiten behoben worden.

Bei dem On-line-Verfahren liegt ein weiteres Problem darin, die Zulässigkeit des einzelnen Abrufs zu prüfen. Hierbei muß der Nachweis eines berechtigten Interesses für die abgerufenen Auskünfte erbracht werden (§ 32 Abs. 2 S. 1 BDSG). Nach der On-line-Nutzungsvereinbarung wird die Prüfung der rechtlichen Zulässigkeit des einzelnen Abrufs dem Mitglied als Anschlußteilnehmer auferlegt. Die Auskunftei prüft die Zulässigkeit der Abrufe nur, wenn hierfür im Einzelfall Anlaß besteht. Das Mitglied gewährleistet, daß die Zulässigkeit der Übermittlung personenbezogener Daten durch geeignete Stichprobenverfahren von der Auskunftei überprüft werden kann.

Die Aufsichtsbehörden sind der Auffassung, daß der Verband bzw. die örtlichen Auskunfteien sämtliche Abrufe, bei denen personenbezogene Daten übermittelt werden, zumindest so protokollieren muß, daß der örtlichen Auskunftei eine stichprobenweise Überprüfung des berechtigten Interesses möglich ist. Dieser Forderung wird dadurch entsprochen, daß der Verband nach einem on-line-Abruf noch am selben Tag eine automatische Telex-Mitteilung an die Auskunftei als speichernde Stelle weiterleitet. In der Mitteilung werden aufgeführt die Tatsache des Abrufes, der Abrufende und der abgerufene Datensatz, das berechtigte Interesse und das Datum der letzten Änderung der abgerufenen Auskunft. So können die notwendigen Stichproben durch die örtliche Auskunftei durchgeführt werden, ebenso wie es möglich ist, daß bei Änderungen des Datenbestandes Nachtragsmeldungen an den Datenempfänger ergehen. Die stichprobenweisen Überprüfungen durch die örtliche Auskunftei müssen jedoch durchgeführt werden, ohne daß hierfür im Einzelfall ein konkreter Anlaß vorausgesetzt wird. Die von mir geprüfte Auskunftei hat erklärt, daß sie so verfährt.

Bisher haben die Aufsichtsbehörden verlangt, daß die Auskunftei mindestens bei einer von 1000 Abfragen stichprobenweise das berechtigte Interesse bei der anfragenden Stelle überprüft. Wegen der zunehmenden Zahl von Teilnehmern am automatisierten Abrufverfahren wird die Zahl der erforderlichen Stichproben jedoch erhöht werden müssen.

Kritisch ist auch das im On-line-Dienst praktizierte Suchverfahren mit sog. "Wortstämmen" zu bewerten. Die Handelsauskunfteien setzen das Verfahren dort ein, wo die genaue Schreibweise der Firma, über die eine Auskunft eingeholt werden soll, nicht bekannt ist oder wo gewisse Verwechslungen vorliegen. Bei dem Verfahren wird jede in der Datenbank gespeicherte Firma oder Einzelperson als Treffer gemeldet, bei dem der Anfang des Firmennamens mit dem Suchbegriff übereinstimmt. Angezeigt werden

jeweils Name und vollständige Anschrift der gefundenen Firma oder Einzelperson. Einzelpersonen werden — so die Auskunft der von mir geprüften Handelsauskunftei — in der Datenbank nur erfaßt, wenn sie mit einer Firma in Verbindung stehen, d.h.:

— Inhaber bei Gewerbetrieb, Einzelfirma, freiem Beruf,

— Gesellschafter bei GbR, oHG,

— Komplementäre bei KG

— Kommanditisten bei KG, GmbH&Co. KG,

— Geschäftsführer bei GmbH

— Aufsichtsrat und Vorstand bei AG, eG, e.V.

Die Befürchtung der Aufsichtsbehörden, daß es auf diese Weise zur Übermittlung von personenbezogenen Daten kommen kann, für die ein berechtigtes Interesse des Mitglieds nicht besteht, werden von der Auskunftei nicht geteilt.

Nach ihrer Auffassung geht es nicht um eine Datenübermittlung, sondern um eine Recherche mit Wortstämmen, mit Hilfe derer das gesuchte Unternehmen, das übermittelt werden soll, überhaupt erst ausfindig zu machen versucht werde. Dem könne man den Gebrauch von Telefon- oder öffentlich zugänglichen Branchen- oder Adressbüchern gleichstellen. Dem anfragenden Mitglied sei es auch nicht möglich, sich bei dem Wortstamm-Verfahren sämtliche auf dem Bildschirm erscheinenden Firmen übermitteln zu lassen. Über die Postleitung werde immer nur der Datensatz zu einem jeweils angefragten Einzelunternehmen übermittelt. Die Verwendung personenbezogener Daten einer Firma oder Einzelperson, die zunächst nicht gesucht sei, setze also voraus, daß das anfragende Mitglied neben den Kosten für die Auskunft über die an sich gewünschte Firma Zusatzkosten für eine Auskunft über weitere im Wortstamm-Verfahren bekanntgewordene Firmen aufwende. Bei einer Abwägung des berechtigten Interesses mit den schutzwürdigen Belangen des Betroffenen ist nach Ansicht der Handelsauskunftei weiter zu berücksichtigen, daß in der beim Zentralverband geführten Datenbank z.Z. keine Privatpersonen — außer im Falle von Einzelunternehmen — enthalten seien, über die Informationen im On-line-Verfahren weitergeleitet werden könnten. Auch würden alle gespeicherten Firmen und damit zusammenhängende Personen bereits bei der Erfassung in der EDV-Anlage davon in Kenntnis gesetzt, daß eine Archivierung bei der Auskunftei vorgenommen wird. Deshalb werde auch auf eine weitere Benachrichtigung nach Abruf der On-line-Auskünfte verzichtet.

Nach diesen Informationen scheint mir gesichert, daß die Suche mit Wortstämmen nur bei der gezielten Suche nach einer Firma im Einzelfall angewendet wird. Wenn in die Suche mit Wortstämmen nur Firmen und mit ihnen rechtlich verbundene natürliche Personen, nicht jedoch sonstige "Privatpersonen" aufgenommen werden, kann von einem überwiegenden berechtigten Interesse ausgegangen werden, Auskünfte über Firmen mit nicht restlos geklärter Identität zu erhalten, ohne daß schutzwürdige Belange der Betroffenen bedroht werden. Denn aufgrund der Publizität des Wirtschaftsverkehrs kann nicht erkannt werden, daß die handeltreibenden Firmen ein Interesse an der Geheimhaltung ihrer Daten haben könnten. Außerdem wird durch die Benachrichtigung der im On-line-Verfahren gespeicherten Firmen dafür Vorsorge getragen, daß die Betroffenen entgegenstehende Interessen an der Übermittlung ihrer Daten geltend machen können.

Abschließend ist die Frage diskutiert worden, ob die Handels- und Wirtschaftsauskunfteien verpflichtet sind, alle On-line-Nutzer zum Register der Aufsichtsbehörden zu melden. Dagegen hatten sie Bedenken vorgebracht, da sie auf diese Weise ihre Kunden an das jederman — also auch der Konkurrenz — zur Einsicht offenstehende Register melden müßten. Gleichwohl hat sich die von mir geprüfte Auskunftei dem Meldeverlangen ordnungsgemäß unterworfen.

Die Aufsichtsbehörden haben auch keine Zweifel, daß § 39 Abs. 2 Nr. 8 BDSG die namentliche Meldung sämtlicher Teilnehmer am automatisierten Abrufverfahren (On-

line-Direktauskunft) verlangt. Auch der Entwurf eines Artikelgesetzes zur Neufassung des BDSG nach dem Stand vom 5. November 1987 sieht in § 29 Abs. 3 eine solche Meldung vor, lediglich der Registereintrag entfällt.

5.5.1.2 Marketing-Dienste der Handelsauskunfteien

Zu den Serviceleistungen mit wachsender Bedeutung im Gesamtdienstleistungsangebot der Wirtschafts- und Handelsauskunfteien sind im weiteren die Marketing-Dienste zu rechnen.

Dem Kunden werden auf diesem Sektor von der von mir geprüften Handelsauskunftei einerseits aktuelle Strukturdaten (basis) und andererseits qualifizierte Marketing-Adressen (select) zur Verfügung gestellt. Bei basis handelt es sich um den Gesamtbestand der Datensammlung, in dem bei Bedarf eine Vielzahl von Informationen sein können, z.B.

— Postleitzahl,

— Branche,

— Umsatz,

— Rechtsform,

— Mitarbeiter,

— Gründungsdatum,

— Auftragslage,

— Unternehmensentwicklung,

— Zahlungsverhalten usw.

Die select-Datenbank, die sich inhaltlich nicht von basis unterscheidet, erlaubt die Selektion einer gewünschten Zielgruppe nach einer Vielzahl verschiedener Merkmale. Die möglichen, frei kombinierbaren Kriterien können liegen in:

— Auftragslage,

— Bankverbindung,

— Branchenschlüssel,

— Gründungsdatum,

— Handelsregistereintragung,

— Immobilienbesitz,

— Mitarbeiter,

— Postleitzahl,

— Rechtsform,

— Umsatz,

— Unternehmensentwicklung,

— Zahlungsverhalten o.v.a.m.

Das Ergebnis dieser Selektion sind qualifizierte Firmenadressen. Zusätzlich können weitere Informationen geliefert werden, wie z.B.

— Aufsichtsratsmitglieder,

— Geschäftsführer,

— Gesellschafter,

— Inhaber,

— Vorstände.

Einzelpersonen des mittleren Managements, das heißt Prokuristen und Handlungsbevollmächtige, werden hingegen in der EDV zur Auskunftsspeicherung nicht erfaßt, da in diesem Bereich erfahrungsgemäß eine sehr große Fluktuation besteht.

Es handelt sich bei diesen Marketing-Diensten dem Grunde nach um den Vertrieb bonitätsgeprüfter Adressen. Über die dagegen bestehenden datenschutzrechtlichen Bedenken habe ich bereits berichtet (vgl. 5. TB, 6.6.1, S. 128 ff.). Die Hamburger Auskunftei, die dieses Datenmaterial vertreibt, setzt leider auch weiterhin die von mir für unzulässig gehaltene Praxis fort. Sie ist der Meinung, damit nicht gegen geltendes Recht zu verstoßen.

5.5.2 Verbindung zwischen Inkasso- und Auskunfteiverkehr

Wirtschafts- und Handelsauskunfteien weisen häufig die Besonderheit auf, daß sie in ihrem Geschäftsbereich neben der eigentlichen Auskunftei zugleich Inkassoabteilungen unterhalten, die gewerblich die Beitreibung übernommener, offener Forderungen betreiben. Aufgrund einer Eingabe hatte ich mich mit dem Problem zu beschäftigen, inwieweit Inkassodaten — die in der Regel wirtschaftliche Negativdaten zur Kreditwürdigkeit des Betroffenen darstellen — für Auskunfteizwecke genutzt werden dürfen. Durch die Verwendung der Daten im Auskunfteibereich könnten schutzwürdige Belange der Betroffenen beeinträchtigt sein, weil Auswirkungen auf den wirtschaftlichen Ruf und die Kreditwürdigkeit möglich sind. Es mußte deshalb geprüft werden, ob die Nutzung von Inkassodaten in den Handelsauskunfteien nach den Bestimmungen des Bundesdatenschutzgesetzes zu billigen ist.

Bei einer Hamburger Auskunftei habe ich mich darüber informieren lassen, welche Formen des Datenaustausches zwischen den wirtschaftlich selbständigen Arbeitsbereichen Inkasso und Auskunftei bei einer Wirtschafts- und Handelsauskunftei geübt werden. Der Sachstand ist danach folgender:

Rechtlich handelt es sich bei den Inkasso- und Wirtschaftsauskunfteiabteilungen nicht um selbständige juristische Personen, sondern um zwei Aufgabenbereiche, die von einer juristischen Person wahrgenommen werden. Dennoch werden die personenbezogenen Daten aus den Bereichen Inkasso und Wirtschaftsauskunftei in einer gemeinsamen EDV-Anlage gespeichert.

Mitarbeiter beider Arbeitsbereiche können theoretisch wechselseitig Zugriff auf die Daten nehmen, die in dem jeweils anderen Bereich erhoben und verarbeitet werden. Dabei findet nach Ansicht der Auskunftei allerdings keine Datenübermittlung i.S.d. BDSG statt, sondern eine "hausinterne" Nutzung der im jeweiligen Aufgabenbereich erhobenen Datenbestände. Für die Verwendung der Daten im Inkasso- und Auskunfteibereich gelten bei der Handelsauskunftei besondere Regeln, die von den Mitarbeitern der entsprechenden Abteilungen zu beachten sind.

a) Den Mitarbeitern der Inkasso-Abteilung ist ein jederzeitiger Zugriff auf die Daten im Auskunfteibereich möglich. Das ist nach Auffassung der Auskunftei auch nötig, da nur mit Hilfe entsprechender Informationen — etwa über die Abgabe einer eidesstattlichen Versicherung — der Inkassoauftrag effektiv abgewickelt werden könne.

b) Für die Verwendung der Inkasso-Daten im Auskunftei-Verfahren gelten besondere interne Regelungen:

Mit Eingang des Inkasso-Auftrages werden zunächst die Daten des Inkassofalles in die Datei eingespeichert; das sind die Daten über Gläubiger, Schuldner und die einzuziehende Forderung. Es wird dann anhand dieser Daten ein Archivbericht gefertigt, der laufend im Hinblick auf den aktuellen Stand der Inkasso-Abwicklung fortgeschrieben, jedoch nicht automatisch in den Auskunfteibestand der Wirtschaftsauskunftei eingestellt wird. Vielmehr differenziert die Auskunftei hier zwischen Inkassoaufträgen im Mahn- und im sog. Überwachungsverfahren. Das Mahnverfahren betrifft alle Forderungen, die im vorgerichtlichen Verfahren bis zur Titulierung und der ersten Vollstreckungsmaßnahme einzuziehen gesucht werden. Im Überwachungsverfahren werden die bereits titulierten, vollstreckbaren Forderungen verfolgt.

Von den personenbezogenen Daten, die im Mahnverfahren der Auskunftei bekannt werden, gehen zunächst keine Daten in die Nutzung des Auskunfteibereichs. Erst bei Vorliegen eines Abschlußberichts wird eine entsprechende Information in den Auskunfteidatenbestand eingestellt. Die Informationen im Abschlußbericht können lauten:

— Zahlung

— Übergang vom Mahn- ins Überwachungsverfahren

— strittige Forderung.

Die Auswirkungen dieser Datenerhebungen im Inkasso-Verfahren auf den Auskunfteibereich liegen in folgendem: Daten aus dem Mahnverfahren fließen nur dann in die erteilte Wirtschaftsauskunft ein, wenn

a) mindestens eine Häufigkeit von drei Mahnverfahren pro Jahr gegeben ist und es sich

b) um unstrittige Forderungen handelt; strittige Forderungen werden von der Auskunftei nicht beauskunftet.

Soweit noch keine drei Mahnverfahren aufgelaufen sind, werden abweichend von der vorgenannten Regel personenbezogene Daten aus dem Mahnverfahren nur dann beauskunftet, wenn es sich um Mahnverfahren mit einer außergewöhnlich hohen Streitsumme handelt und Recherchen ergeben haben, daß es sich um eine unstrittige Forderung handelt.

Hingegen werden die personenbezogenen Daten bei Inkassofällen im Überwachungsverfahren sogleich in den Auskunfteidatenbestand eingestellt. Dazu zählen: Daten von Gläubiger und Schuldner, erwirkter Titel, Höhe der Forderung.

Diese Daten — ohne Gläubigerdaten — werden auch sogleich im Auskunfteiverfahren beauskunftet, da in einer titulierten Forderung ein sog. hartes wirtschaftliches Negativmerkmal gesehen wird.

Die im Auskunfteiverfahren beauskunfteten Informationen werden entsprechend dem jeweiligen Stand der Inkasso-Abwicklung aktualisiert. Soweit in einer Auskunft Negativdaten übermittelt worden sind, jedoch nachträglich etwa Informationen über einen Ausgleich der Forderung bekannt werden, so erfolgt eine Nachmeldung an den Datenempfänger. Sobald sich aus dem Abschlußbericht zu einem Inkassoauftrag ergibt, daß die Forderung getilgt und der Auftrag ordnungsgemäß abgewickelt wurde, werden die Daten gelöscht; weitere Negativauskünfte im Auskunfteibereich sind dann nicht mehr möglich.

Hinsichtlich der Benachrichtigung des Betroffenen praktiziert die Auskunftei ein zweigleisiges Verfahren. Der Betroffene wird einerseits nach § 26 BDSG über die erstmalige Speicherung seiner Daten im Inkassobereich unterrichtet und er wird andererseits nach § 34 BDSG über die Speicherung seiner Daten im Auskunfteibereich informiert, sobald Inkassodaten in den Auskunfteidatenbestand eingestellt werden.

Bei einer rechtlichen Bewertung des dargestellten Verfahrens muß das eigentliche Problem in der Nutzung von Inkassodaten für Auskunfteizwecke gesehen werden. Soweit sich das Inkassobüro der Daten aus dem Auskunfteibereich bedient, liegt ein berechtigtes Interesse vor, da es darum geht, offene Forderungen vom Schuldner einzutreiben. Der Schuldner kann keine schutzwürdigen Belange dagegen anführen, wenn über ihn vorliegende Informationen genutzt werden, um die Schuldenregulierung zu organisieren und zu effektivieren. Anders ist die Verwendung von Inkassodaten im Auskunfteibereich zu beurteilen, da in diesem Fall Dritte Kenntnis von möglichen wirtschaftlichen Negativdaten des Betroffenen erhalten.

Für die Prüfung der Frage, ob die Verwendung von Inkassodaten rechtlich zulässig ist, ist die Besonderheit zu beachten, daß es sich formal betrachtet nicht um eine Datenübermittlung i.S.v. § 24 BDSG handelt, sondern um eine Nutzung von Daten, die zum Zwecke der Abwicklung eines Inkassoauftrages gespeichert worden sind, nun auch für

den Auskunfteibereich. Hierfür bildet § 32 BDSG die maßgebliche Rechtsgrundlage. Möglich ist es somit, daß eine Datenspeicherung zur Besorgung des Inkassoauftrages zulässig ist (§ 23 3. Alt. BDSG), nicht aber, soweit es um die Beurteilung des Nutzungszweckes "Auskunftserteilung" geht. Dementsprechend ist in jedem Fall bei Aufnahme von Inkassodaten in den Auskunftsdatenbestand eine erneute Prüfung unter Berücksichtigung der schutzwürdigen Belange des Betroffenen einerseits und des neuen Nutzungszweckes andererseits erforderlich. Darüber hinaus ergeben sich grundsätzliche Bedenken aus dem Gedanken der Zweckbindung, wenn Daten, die ursprünglich vom Auftraggeber des Inkassoauftrages zur Abwicklung eben dieses einzelnen Geschäftes der Auskunftei übermittelt worden sind, von dieser nun aber in völlig anders gearteter Absicht in ihren sonstigen Geschäftsbereichen weiter verwendet werden. Das ist nur hinnehmbar, weil anderenfalls zu befürchten wäre, daß vom Schuldner wirtschaftliche Negativdaten zu Inkassofällen, die für die Abschätzung von Risiken im Wirtschaftsverkehr bedeutsam sind, verborgen gehalten würden.

Um die schutzwürdigen Interessen der Betroffenen nicht zu verletzen, muß es jedoch eine Einzelfallprüfung geben, bei der darauf geachtet wird, daß nur Daten aus dem Inkasso- in den Auskunfteibereich übernommen und beauskunftet werden, die sog. "harte Negativmerkmale" darstellen. Diese Voraussetzungen sind erfüllt, wenn es sich um die Beitreibung unstrittiger Forderungen handelt oder um die Beitreibung solcher Forderungen, die bereits durch gerichtlich erwirkte Titel verifiziert sind.

Ich gehe davon aus, daß diesen Anforderungen durch das von der Auskunftei praktizierte Verfahren Rechnung getragen wird, da nur erhärtete Negativdaten beauskunftet werden.

Da mit der doppelten Benachrichtigung — sowohl nach § 26 BDSG wie nach § 34 BDSG — eine Aufklärung des Betroffenen über die Speicherung zum Zwecke der Abwicklung des Inkassoauftrages einerseits und der Beauskunftung in der Wirtschaftsauskunftei andererseits erfolgt, wird der Betroffene auch hinreichend über die Nutzung seiner Daten durch die Auskunftei informiert und so in die Lage versetzt, entgegenstehende Belange geltend zu machen.

Im Ergebnis halte ich den Umgang mit den im Rahmen von Inkassoaufträgen erhobenen und gespeicherten Daten in der Wirtschaftsauskunftei für akzeptabel.

5.6 Arbeitnehmerdatenschutz

Wie in den Vorjahren habe ich 1988 einzelne Arbeitnehmer, Betriebsräte und Arbeitgeber in Fragen des Datenschutzes bei der Verarbeitung von Beschäftigten-Daten beraten. Hierzu einige Beispiele:

— Telefondatenerfassung —

So ging es mehrfach um die zulässigen Speicherungen und Auswertungen einer Telefondaten-Erfassungsanlage. In diesem Zusammenhang teilte mir ein Unternehmen mit, daß es bei privaten Telefongesprächen der Mitarbeiter den Ausdruck von Zielnummer und -ort technisch sperre. Zur Klärung von Zweifelsfragen können nur Personalabteilung und Betriebsrat zusammen in Anwesenheit des Mitarbeiters den vollständigen Ausdruck auslösen, den allein der Mitarbeiter zur Überprüfung in Empfang nehme. "In der Regel erinnert sich der Mitarbeiter anhand der Aufzeichnung, daß er tatsächlich dieses Privatgespräch geführt hat." Ich halte dieses Verfahren für eine gelungene Regelung.

— Computerlisten mit Daten von Kollegen —

Ein eindeutiger Verstoß gegen das Bundesdatenschutzgesetz lag in folgendem: Aufgrund eines Fehlers der Personalverwaltung wurde in einem Unternehmen einigen Mitarbeitern zunächst zuviel Lohn/Gehalt ausgezahlt. Der Rückzahlungs-Aufforderung fügte der Arbeitgeber eine Computerliste bei, die alle betroffenen Mitarbeiter mit Personalnummer, Name, Bankverbindung, Kontonummer sowie dem Überzahlungsbetrag aufführte. Eine derartige Offenlegung personenbezogener Daten von Kollegen lag

nicht "im Rahmen der Zweckbestimmung eines Vertragsverhältnisses" (des Beschäftigungsverhältnisses) und war auch nicht "zur Wahrung berechtigter Interessen der übermittelnden Stelle (des Arbeitgebers) oder eines Dritten oder der Allgemeinheit erforderlich", § 24 Abs. 1 BDSG. Auf meine Kritik an diesem Verfahren sicherte der Arbeitgeber zu, in Zukunft auf die Versendung derartiger Computerlisten zu verzichten.

— Zusendung einer Arbeitgeber-Zeitung an die Privatadresse der Arbeitnehmer —

Im November 1988 wandten sich sowohl der Betriebsrat als auch der Arbeitgeber eines mittelständischen Unternehmens mit folgendem Fall an mich: Der Arbeitgeber hatte einem Verlag die Privatadressen seiner Arbeitnehmer mitgeteilt, an die der Verlag auftragsgemäß eine vom Arbeitgeberverband finanzierte Zeitung verschickte. Einige Arbeitnehmer fühlten sich durch Inhalt und Verbreitungsform des Informationsblattes belästigt. Nach Meinung des Betriebsrats lag ein Verstoß gegen die Betriebsvereinbarung über die Personaldatenverarbeitung, die einerseits die Datenverarbeitung nur im Rahmen der Zweckbestimmung des Arbeitsverhältnisses oder im Rahmen der Erfordernisse des Betriebes erlaubt und Datenübertragungen an Dritte nur nach den Vorschriften des Bundesdatenschutzgesetzes gestattet.

Ich machte dem Betriebsrat deutlich, daß es sich in diesem Fall rechtlich um eine Auftragsdatenverarbeitung nach § 37 BDSG, also nicht um eine Datenübermittlung im Sinne des § 24 BDSG handelte. Es blieb aber die Frage, ob nach § 23 BDSG die Datenspeicherung und -nutzung zum Zweck der Zeitschriftenversendung "zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich" war und keine Anhaltspunkte für eine Beeinträchtigung schutzwürdiger Belange der betroffenen Arbeitnehmer vorlagen. Auf meine Zweifel an der Erforderlichkeit und aufgrund der Proteste des Betriebsrates beschloß der Arbeitgeber, sich in Zukunft auf die Verteilung bzw. Auslage der Zeitung im Betrieb zu beschränken.

— Übermittlung von Arbeitnehmerdaten an das Arbeitsamt zur Bekämpfung der Schwarzarbeit —

Aufgrund einer Anfrage hatte ich einem Unternehmen mitgeteilt, daß § 132a des Arbeitsförderungsgesetzes (AFG) es rechtfertige, dem Arbeitsamt im Rahmen einer Prüfung die Namen, Anschriften und Geburtsdaten aller Arbeitnehmer zu offenbaren, daß aber vor Übermittlung weiterer Angaben über einzelne Arbeitnehmer das Arbeitsamt konkrete Anhaltspunkte für einen Leistungsmißbrauch bzw. einen Ordnungswidrigkeiten-Tatbestand vortragen müsse. Dies veranlaßte den Direktor des Arbeitsamtes Hamburg, einerseits meine Zuständigkeit für derartige Auskünfte in Frage zu stellen und andererseits darauf hinzuweisen, daß § 132a AFG eine Überprüfung von Arbeitnehmerdaten nicht von konkreten Anhaltspunkten für einen Leistungsmißbrauch abhängig mache.

In meinem Antwortschreiben habe ich folgende Auffassung vertreten: Richtig ist, daß für die Kontrolle der Arbeitsverwaltung allein der Bundesbeauftragte für den Datenschutz zuständig ist; richtig ist aber auch, daß die §§ 30, 40 BDSG die Aufsichtsbehörde ermächtigen, Wirtschaftsunternehmen zu beraten. In dieser Zuständigkeit hatte ich die Auskunft erteilt. Hinsichtlich des Prüfungsumfanges aus § 132a AFG hielt ich daran fest, daß für eine Überprüfung zunächst nur die Grundpersonalien der Arbeitnehmer "erforderlich" (AFG) sind, um sie mit Listen der Leistungsempfänger des Arbeitsamtes zu vergleichen. Erst wenn sich hieraus eine Doppelnennung und damit ein konkreter Verdacht bzw. Anhaltspunkt für eine Unregelmäßigkeit ergibt, sind weitere Datenoffenbarungen — beschränkt auf diese Person — "erforderlich". Dieses zweistufige Verfahren wenden die Mitarbeiter des Hamburger Arbeitsamtes vor Ort auch tatsächlich an.

Während ich dem betreffenden Unternehmen zugestehen konnte, die Listen mit den Grundpersonalien nicht nur vorzuzeigen, sondern auch an das Arbeitsamt auszuhändigen, habe ich das Arbeitsamt darauf hingewiesen, daß es dies vom Arbeitgeber nicht verlangen kann, sondern durch § 132a AFG auf ein bloßes Einsichts- und Auskunftsrecht verwiesen ist. Da der gesamte Vorgang in die Kontrollkompetenz des Bundesbeauftragten für den Datenschutz hineinreicht, habe ich ihn mit ihm abgestimmt.

— Weitergabe einer an die Verwaltung gerichteten Eingabe an den Arbeitgeber des Petenten —

In einem Schreiben an den Senat machte ein Bürger seinem Unmut über die Volkszählung Luft, beschwerte sich über die herausgeworfenen Steuergelder und die Beamten, die nicht wüßten, was richtige Arbeit ist. Dies habe er selbst in einer "Behörde", einer großen Forschungseinrichtung privaten Rechts, erlebt, wo er eine zeitlang beschäftigt war und wo "nur Kaffee getrunken und Schiffe versenken gespielt" worden sei. Die für die Volkszählung zuständige Innenbehörde sandte dieses Schreiben dem ehemaligen Arbeitgeber des Petenten "mit der Bitte um Kenntnisnahme und Bearbeitung in dortiger Zuständigkeit". Meine Frage nach einer Rechtsgrundlage für diese Weiterleitung wurde beantwortet mit der Anmerkung "Urschriftlich zurück unter Hinweis darauf, daß nach Auffassung der Behörde für Inneres ein Eingriff, der eine Rechtsgrundlage bedürfe, nicht vorliegt". Ich teile diese Rechtsauffassung nicht. Die Weitergabe des Briefes offenbart dem ehemaligen Arbeitgeber die persönliche Einstellung des früheren Arbeitnehmers zum öffentlichen Dienst, zur Volkszählung und zu seiner früheren Beschäftigungsstelle. Ich fürchte darüber hinaus, daß der Brief beim Empfänger — offen — durch viele Hände gegangen ist, weil eine "Zuständigkeit zur Bearbeitung" nicht ersichtlich ist. Neben dem Grundrecht auf informationelle Selbstbestimmung könnte im übrigen auch das Briefgeheimnis des Art. 10 Abs. 1 GG durch das Verhalten der Innenbehörde berührt sein. Eine Stellungnahme steht noch aus.

5.7 Sonstige Probleme

5.7.1 Telefonmarketing

5.7.1.1 Darstellung und Abgrenzung

1. Werbung und Kundenkontakte bei Privatpersonen
Das Telefonmarketing ist die spezielle Art der Werbung oder der Kundenpflege, den Betroffenen am Telefon persönlich anzusprechen. Es ist die logische Folge der angewachsenen Telefondichte und ersetzt eine ganze Palette von Einzelmaßnahmen, die sonst bei hohem Aufwand durch einen eigenen Außendienst oder Handelsvertreter bewältigt werden müssen. Dazu zählen u.a. die folgenden Aufgaben, die unter Mitwirkung eines meiner Mitarbeiter in einem Aufsatz im "Datenschutzberater" Nr. 4/1988 beschrieben sind:

1.1 Nachfragen bei Interessierten
Telefonische Nachfragen werden vorgenommen, nachdem zuvor ein anderes Werbemittel eingesetzt worden war und es erfolgreich erscheint, den Umworbenen aufgrund seiner Reaktion (zum Beispiel Rücksendung eines Coupons, Teilnahme an einem Preisausschreiben) noch einmal anzusprechen.

1.2 Nachbearbeitung nach Probe-Lieferungen
Diese Nachbearbeitung spielt z.B. eine besondere Rolle im Bereich der Verlagswerbung, wenn eine angeforderte Probe-Belieferung mit einer Tageszeitung oder Fachzeitschrift nicht sofort zu einem dauerhaften Abonnement geführt hat. Es wird aber nur zurückgefragt, wenn der Interessent seine Telefonnummer selbst abgegeben und damit eine gewisse Bereitschaft zu einem Telefongespräch deutlich gemacht hat. In diesem Gespräch wird versucht zu ergründen, warum das Interesse fehlt oder ob ein Vertragsschluß doch möglich ist; u.U. wird die Probe-Belieferung noch einmal verlängert.

1.3 Nachfragen zum Kunden-Verhalten
Eine telefonische Nachbearbeitung wird zum Beispiel im Versandhandel eingesetzt, um Kunden, die das bekanntermaßen sehr weit reichende Waren-Rückgaberecht häufig in Anspruch nehmen, nach den Gründen zu befragen. Das Ziel besteht darin festzustellen, wo Mängel in der Leistung des Versandhauses liegen könnten (z.B. Produktbeschreibung oder Abbildung im Katalog, Lieferservice oder Mängel bei Herstellern).

1.4 Kündigungs-Nachbearbeitung
Nach Vertragskündigungen (z.B. bei Verlagen, Vereinen, gemeinnützigen Institutionen, Kreditkarten-Organisationen) ist es interessant, nach dem Grund zu fragen, damit ein Anbieter Anhaltspunkte dafür bekommt, wie er gegebenenfalls seine Leistung dem Bedarf anpassen kann oder seinen oder fremden Service verbessern sollte.

1.5 Telefonisches Mahnverfahren
Auch in Fällen von Zahlungsschwierigkeiten hat es sich bewährt, den Schuldner am Telefon direkt anzusprechen. Oft sind dadurch Zusagen zu erreichen, die auch eingehalten werden. Eine schriftliche Mahnung hätte diesen Erfolg nicht gehabt.

2. Telefonmarketing im geschäftlichen Bereich
Über die bisher beschriebenen Möglichkeiten hinaus gibt es eine Reihe von weiteren Einsatzarten des Telefonmarketing, die jedoch nur oder fast nur eingesetzt werden, wenn Geschäftsleute angesprochen werden sollen. Als Beispiele seien genannt die Bedarfsermittlung, der Bestelldienst, das Aussprechen von Einladungen, das Vereinbaren von Terminen und das Vorstellung von Produkten.

Alle diese Möglichkeiten werden — jeweils ausgerichtet auf das gewünschte Ergebnis — miteinander kombiniert oder auch verfeinert.

3. Marktforschung

Die Marktforschung per Telefon nimmt eine Sonderstellung ein. Genauso wie Sozialforschungsinstitute mit eigenem Personal telefonische Umfragen vornehmen können, kann dies auch auftragsgebunden von einem Telefonmarketing-Unternehmen durchgeführt werden.

Die im Arbeitskreis Deutscher Marktforschungsinstitute e.V. (ADM) oder im Berufsverband Deutscher Markt- und Sozialforscher e.V. (BVM) zusammengeschlossenen Institute setzen sich jedoch deutlich von jeder Tätigkeit ab, die auch nur den Anschein einer Verbindung zu einer Werbung oder zum Verkauf erwecken könnte. Standesrechtlich wird besonders hervorgehoben, daß ihnen jede, auch eine räumliche Verbindung zwischen einem Institut und einem Telefonmarketing-Unternehmen nicht gestattet ist.

Die telefonische Marktforschung ist deshalb nicht dem Telefonmarketing-Bereich zuzurechnen. Für Marktforschungsinstitute gilt — auch beim Einsatz von Telefon-Interviews — § 36 BDSG mit den Vorschriften zur Anonymisierung.

5.7.1.2 Datenschutzrechtliche Bewertung

1. Telefonmarketing in eigener Regie

Bei einigen Einsatzarten steht deutlich ein werbender Aspekt im Vordergrund. Hier ist das Unternehmen interessiert, vom Angerufenen Informationen zu erhalten, die es ermöglichen, auf ihn einzuwirken und ihm das angebotene Produkt noch schmackhafter zu machen.

Bei dieser gezielten Ansprache spielen psychologische Gründe eine große Rolle. Der Angerufene fühlt sich aufgewertet, wenn er den Eindruck hat, das große Unternehmen "X", das seinen Sitz in der Ferne hat, ruft gerade ihn an, um ihm ein (neues) Produkt vorzustellen.

Geschieht dies, ohne daß vorher ein Kontakt bestanden hatte, und wird der Angerufene gar in seiner Privatwohnung von einem solchen Anruf überrascht, dann kann man sich Situationen vorstellen, in denen es ihm schwerfallen könnte, auf die Frage nach einer Bestellung noch "Nein" zu sagen. In einem Streitfall hat der BGH mit seinem Urteil vom 19.6.70 — I ZR 115/68 — festgestellt:

"Es verstößt gegen die guten Sitten des lauteren Wettbewerbs, unaufgefordert Inhaber von Telefonanschlüssen, zu denen bislang keine Beziehungen bestehen, in ihrem privaten Bereich anzurufen, um Geschäftsabschlüsse anzubahnen oder vorzubereiten, insbesondere um Waren oder sonstige Leistungen anzubieten."

Diese Rechtsprechung ist auch bei einer datenschutzrechtlichen Betrachtung von Bedeutung. Die Erhebung von Informationen ist nur dann zulässig, wenn der Betroffene nicht durch Täuschung, Druck oder geschickte psychologische Manipulation dazu veranlaßt wurde, seine Daten herzugeben. Das bedeutet, daß dann auch die Speicherung unzulässig ist, wenn die Daten durch eine gegen das Wettbewerbsrecht verstoßende Maßnahme gewonnen wurden.

2. Telefonmarketing durch Service-Unternehmen

Da das Telefonmarketing als Mittel, einen Menschen wegen eines konkreten Anlasses direkt anzusprechen, eine besondere Tätigkeit darstellt, hat sich die hierauf spezialisierte Branche der Telefonmarketing-Unternehmen entwickelt, die diese Leistungen als Service anbietet. Um besonders gute Ergebnisse zu erreichen, wird Personal eingesetzt, das gründlich geschult und laufend fortgebildet wird.

Eine Reihe der Telefonmarketing-Unternehmen hat sich dem Deutschen Direktmarketing-Verband (DDV) angeschlossen, der für sie eine eigene Mitgliedergruppe gebildet hat. Diese Mitgliedergruppe sich einen Ehrenkodex geschaffen, nach welchem die Unternehmen verpflichtet sind, datenschutzrechtliche Vorschriften einzuhalten, gewonnene Erkenntnisse nur den jeweiligen Auftraggebern zuzuleiten und keine Täuschung unter Vorgabe eines Zwecks der Markt-, Meinungs-, oder Sozialforschung vorzunehmen und die Privatsphäre des Angerufenen zu akzeptieren.

In einem Gespräch meldet sich der Anrufer mit seinem Namen, aber mit der Firmenbezeichnung des Auftraggebers. Dem Angerufenen wird dabei nicht klar, daß sein Gesprächspartner überhaupt nicht zu dem Unternehmen zählt, mit dem er sich verbunden glaubt. Dies erscheint widersprüchlich, ist aber nach Ansicht des DDV die Konsequenz aus der BGH-Rechtsprechung. Der Angerufene soll nämlich gerade nicht von einem ihm völlig fremden Unternehmen durch den Anruf überrascht, sondern deutlich auf den Anlaß und die bereits bestehende Beziehung zum Auftraggeber hingewiesen werden. Eine entsprechende Regelung hat der DDV in den Ehrenkodex aufgenommen. Ich halte es jedoch für selbstverständlich, dem Angerufenen im Laufe des Telefongesprächs mitzuteilen, daß ein Telefonmarketing-Unternehmen zwischengeschaltet ist.

Grundsätzlich ist gegen den Einsatz eines fremden und selbständigen Telefonmarketing-Unternehmens nichts einzuwenden, denn wie jedes Unternehmen seine Organisationsfreiheit hat und einzelne Leistungen an andere spezialisierte Service-Unternehmen abgibt, kann dies auch in diesem Bereich geschehen. Dabei sind allerdings einige Besonderheiten zu beachten.

2.1 Funktionsübertragung

Wird dem Telefonmarketing-Unternehmen eine ganze Funktion (z.B. die Kundenbetreuung) übertragen, also ein globaler Auftrag, der ihm Freiheiten läßt für die Entscheidung, ob, wann oder welche Daten erfragt, gespeichert oder weitergegeben werden, dann ist diese Tätigkeit als Datenverarbeitung für eigene Zwecke anzusehen, denn sie dient lediglich als Hilfsmittel für einen eigenen, über die Datenverarbeitung weit hinausgehenden Zweck. Das Unternehmen hat also alle Rechte und Pflichten als selbständige speichernde Stelle und muß die Vorschriften des 3. Abschnitts des BDSG anwenden. Dazu zählt vor allem die Pflicht zur Benachrichtigung nach § 26 Abs.1 BDSG. Mir ist nicht bekannt, daß jemals ein Telefonmarketing-Unternehmen über die Tatsache der Speicherung benachrichtigt hätte. Da in der derzeitigen Praxis die Identität verborgen bleibt, ist dies ein Indiz dafür, daß eine Funktionsübertragung nicht erfolgt.

2.2 Auftrags-Datenverarbeitung

In der Praxis werden die Beziehungen jedoch so gestaltet, daß das Telefonmarketing-Unternehmen alle Daten als "Eigentum" des Auftraggebers betrachtet und selbst nach außen hin nicht in Erscheinung treten will. Dies spricht für eine Datenverarbeitung im Auftrag, die dem 4.Abschnitt des BDSG zuzuordnen ist (§ 30 Abs.1 Nr.3 BDSG); dann gilt § 37 BDSG.

Für eine einwandfreie rechtliche Zuordnung ist es wichtig, daß die Vertragsgestaltung eindeutig ist. Und hieran mangelt es nach meinen Kenntnissen. Durchweg gibt es nur mündliche und deshalb später nicht nachvollziehbare Absprachen, die zudem datenschutzrechtliche Belange gar nicht oder nur sehr grob berücksichtigen.

Da das BDSG dem Auftragnehmer aufgibt, streng die Weisungen des Auftraggebers zu befolgen, müssen hierfür die Voraussetzungen geschaffen sein. Erst durch detaillierte Regelungen wird auch deutlich, daß der Auftraggeber Herr der Daten bleiben und die Bearbeitung und Nutzung der hergegebenen Daten auf ganz bestimmte Verarbeitungen beschränkt wissen will.

Deshalb sollten alle Auftraggeber darauf dringen, neue Verträge schriftlich zu schließen. Aus der Sicht des Datenschutzes kommt es vor allem darauf an, daß geregelt ist,

— wer Herr der Daten ist (und damit Träger von Rechten und Pflichten (vor allem Benachrichtigungs- und Auskunftspflicht),

— wie im Detail mit den überlassenen Daten umzugehen ist,

— daß die überlassenen Daten nicht anders als vereinbart genutzt und keinesfalls an Dritte übermittelt werden dürfen (zu diesem Punkt sollte eine Vertragsstrafe vereinbart werden),

— ob und welche Subunternehmer-Verhältnisse erlaubt sind,

— Maßnahmen der Datensicherung (u.a. Transportwege),

— Kontrollrechte des Auftraggebers.

Meine Beratungsgespräche mit den Telefonmarketing-Unternehmen werde ich in diese Richtung fortsetzen.

5.7.2 Zusammenarbeit zwischen Vermietern und Auskunfteien

Schon in früheren Jahren hatte ich immer wieder Anlaß, zu neu auftretenden Fragen im Zusammenhang mit der Einholung von Auskünften über Mieter bei der SCHUFA sowie bei Handels- und Wirtschaftsauskunfteien Stellung zu nehmen. Wohnungsvermieter holen Auskünfte über Mietbewerber ein in der Absicht, deren Zahlungsfähigkeit überprüfen zu können. Diese Auskunftsverfahren waren für die Betroffenen immer schon ein Ärgernis, da sie zu befürchten hatten, gänzlich von der Vergabe von Wohnungen auf dem freien Wohnungsmarkt ausgeschlossen zu werden. Auch aus datenschutzrechtlichen Gründen war die Auskunftspraxis von SCHUFA und Handels- und Wirtschaftsauskunfteien zu kritisieren, weil die Weitergabe von Negativmerkmalen aus dem Bestand von SCHUFA oder Wirtschaftsauskunfteien zum Zwecke der Überprüfung von Mietbewerbern sich nicht mit deren Geschäftszwecken in Übereinstimmung bringen ließ, dem Kredit- bzw. dem Wirtschaftsverkehr Informationen zur Abschätzung von Kreditrisiken zu liefern (vgl. 2. TB, 4.5.2, S. 128 ff.). Dieser bedenklichen Auskunftspraxis schien vorübergehend Einhalt geboten, nachdem die SCHUFA im Gefolge des BGH-Urteils zur SCHUFA-Klausel den Wohnungsvermietern die bisher bestehenden Vertragsbeziehungen aufkündigte.

Dies hat jedoch nur dazu geführt, daß sich die Auskunftsersuchen der Wohnungsvermieter zunehmend auf die Handels- und Wirtschaftsauskunfteien verlagert haben. Von deren selbst definierten Geschäftszwecken — der Verhinderung des Kreditmißbrauchs — ist eine Auskunft über Mietbewerber indes auch nicht umfaßt, da durch die Vergabe von Mietraum Kreditrisiken gerade nicht geschaffen werden. Allerdings ist zuzugeben, daß es im Einzelfall ein berechtigtes Interesse des Vermieters/Verpächters geben kann, Informationen zu erhalten, die geeignet sind, ihn vor finanziellen Verlusten im Vermietungs- und Verpachtungsgeschäft zu schützen. Keineswegs jedoch kann ich ein berechtigtes Interesse in folgendem Fall erkennen:

Ein großes Wohnungsbauunternehmen, von dem mir bisher nur bekannt war, daß es bei der Vermietung von Gewerberäumen in Ausnahmefällen Auskünfte von Wirtschafts-

auskunfteien eingeholt hat, ist dazu übergegangen, von Mietinteressenten die Beibringung von Selbstauskünften bei Handels- und Wirtschaftsauskunfteien zu verlangen. Dies geschieht zwar nur in Einzelfällen, jedoch richtet sich das Auskunftsverlangen insbesondere gegen solche Mietbewerber, die einen Dringlichkeitsschein oder eine Mietübernahmeerklärung eines Sozialamtes besitzen. Das Wohnungsbauunternehmen hat dazu geltend gemacht, daß mit der Aufgabe, gerade auch Bevölkerungsschichten mit geringerem Einkommen mit Wohnraum zu versorgen, ein berechtigtes Interesse verbunden sei, Auskünfte über die Mietzahlungsfähigkeit von Mietinteressenten zu erhalten. Insofern schließe selbst das Vorliegen von Mietübernahmeerklärungen eines Sozialamtes das berechtigte Interesse an den verlangten Selbstauskünften nicht aus, da die Mietübernahmeerklärung nicht den Charakter einer Bürgschaft hätte und sich im übrigen die Berechtigungsvoraussetzungen zum Bezug von Sozialhilfe ändern könnten.

Diesen Rechtsstandpunkt teile ich nicht. Solange die Mietübernahmeerklärung Gültigkeit hat, treten wirtschaftliche Risiken für den Vermieter nicht auf; entfallen indes die Sozialhilfeberechtigungsvoraussetzungen, so wird in der Regel davon auszugehen sein, daß der Mietbewerber sich nunmehr in einer wirtschaftlichen Situation befindet, die es ihm gestattet, selbst für die zu leistende Miete aufzukommen. Mir scheint, daß für Sozialhilfeempfänger durch die Auskunftsverlangen allein ein ohnedies schon empfundenes Gefühl der Ausgrenzung und Stigmatisierung nur noch verstärkt wird, ohne daß Gründe einer wirtschaftlichen Risikoabsicherung dies rechtfertigen könnten. Die Gefahr solcher Diskriminierungsprozesse erachte ich deshalb als besonders groß — das hat auch der konkret geprüfte Fall bestätigt —, weil durch eine Auskunftei häufig Negativdaten zur Person eines Mietbewerbers erteilt werden, die entweder inaktuell geworden sind oder ein nur unvollständiges und fehlerhaftes Bild über seine wirtschaftliche Situation abgeben. In der kurzen Zeit zwischen Ausschreibung und Vergabe des Mietobjektes wird er meist nicht die Möglichkeit haben, unzutreffende Angaben zu seiner Person noch richtigzustellen. Das führt zur Ausgrenzung eines Personenkreises, der im besonderen Maße darauf angewiesen ist, mit Unterstützung des Staates oder gemeinnütziger Einrichtungen überhaupt eine Mietunterkunft zu finden. Ich meine, daß die Bonitätsprüfung von Wohnungssuchenden, die im Besitz von Dringlichkeitsscheinen oder Mietübernahmeerklärungen sind, umgehend eingestellt werden sollte.

5.7.3 Zur datenschutzrechtlichen Kontrolle von Detekteien

Detekteien und die von ihnen angewandten Methoden bei der Informationsbeschaffung haben schon häufiger öffentliche Diskussionen ausgelöst. Die Kritik bezieht sich dabei u.a. auf das unzureichend geschulte Personal und die bisher nicht geregelte Zulassung zum Beruf des Detektivs, sie betrifft aber auch die anhand konkreter Fälle dokumentierte Gefahr, daß die Detekteien außerhalb des staatlichen Gewaltmonopols eine den Aktivitäten der staatlichen Strafverfolgungsorgane vergleichbare Beobachtungs-, Ermittlungs-, Fahndungs- und Verfolgungstätigkeit betreiben, ohne sich dabei jedoch an rechtsstaatliche Prinzipien zu halten. Dies aber läßt die Frage entstehen, ob und wie die Ermittlungstätigkeit der Detekteien zu beschränken und zu kontrollieren ist. Mit diesem Problem zu befassen haben sich auch die Datenschutz-Aufsichtsbehörden, da es bei der Informationsbeschaffung durch die Detekteien im Regelfall zu einer Verarbeitung personenbezogener Daten kommt, so daß zu prüfen ist, ob das BDSG Anwendung finden muß.

Die Datenschutz-Aufsichtsbehörden der Länder gingen in der Vergangenheit von der Annahme aus, daß bei den Detekteien eine auf den Einzelfall bezogene Verarbeitung personenbezogener Daten erfolge, die sich in Aktenvorgängen niederschlage. Soweit sich die Detekteien auch heute noch auf das Führen von Daten in Akten beschränken, entzieht sich ihre Arbeit einer Aufsicht durch die Datenschutzbehörden. Da es in den letzten Jahren jedoch zu einer zunehmenden Automatisierung von Bürodienstleistungen gekommen ist, die sich auch die Detekteien bei ihrer auskunfteibezogenen Tätigkeit zunutze machen können, müssen die Aufsichtsbehörden erneut prüfen, ob sie an

der bisherigen rechtlichen Beurteilung festhalten können. Ich habe mich mit einer Umfrage an die in meinem Aufsichtsbereich ansässigen Auskunfteien und Detekteien gewandt und sie aufgefordert mir mitzuteilen, ob sie mit ihrer Tätigkeit in den Anwendungsbereich der Vorschriften des BDSG fallen. Die Erhebung ist noch nicht abgeschlossen, jedoch ist mir bei den bisherigen Rückmeldungen in der überwiegenden Zahl der Fälle angezeigt worden, daß eine Speicherung oder Bearbeitung personenbezogener Daten in Dateien nicht erfolge. Ich werde im nächsten Jahr bei den Detekteien in meinem Aufsichtsbereich weitere Prüfungen anstellen, um zu untersuchen, ob sie aufgrund ihrer tatsächlichen Arbeit und Arbeitsorganisation nicht bereits heute den Vorschriften des BDSG unterliegen.

Unabhängig davon zeigt mir die konkrete Arbeit der Detekteien, insbesondere die Praxis ihrer Informationsbeschaffung und -verarbeitung aber, daß es sachlich ungerechtfertigt und mit einer Gefährdung für die Belange der Betroffenen verbunden ist, die Detekteien von einer datenschutzrechtlichen Kontrolle auszunehmen. So ist mir erst jüngst folgender Sachverhalt bekannt geworden: Eine Detektei beschaffte sich unter Einschaltung von Mitarbeitern eines Unternehmens, das als Mitglied einer großen Wirtschafts- und Handelsauskunftei angeschlossen ist, Auskünfte bei dieser Auskunftei, ohne sich selbst dabei als Datenempfänger zu erkennen zu geben und ohne das wahre Interesse ihrer Auftraggeber an den abgefragten Informationen anzugeben. Es konnte nicht mehr aufgeklärt werden, an wen und zu welchen Zwecken die Daten von der Detektei weitervermittelt wurden. Denkbar ist es, daß die Daten — anders als es die selbstdefinierten Geschäftszwecke der Handelsauskunfteien vorschreiben — nicht zur Beurteilung irgendwelcher wirtschaftlichen Risiken im Geschäftsverkehr, sondern zu anderen Zwecken genutzt werden. Insofern wäre die Handelsauskunftei nicht nur über die Person des Datenempfängers, sondern auch über sein berechtigtes Interesse an der übermittelten Auskunft getäuscht worden. Nicht nur dagegen richten sich meine Bedenken. Da nämlich häufig nicht erkennbar ist, für welchen ihrer Auftraggeber eine Detektei Auskünfte bei den Wirtschafts- und Handelsauskunfteien abfragt und welche berechtigten — wirtschaftlichen — Interessen dabei geltend gemacht werden, hatten die Datenschutz-Aufsichtsbehörden schon in der Vergangenheit generelle Vorbehalte dazu angebracht, daß Handelsauskunfteien Auskünfte an Detekteien erteilen. Die Auskunfteien hatten auch zugesichert, solche geschäftlichen Verbindungen nicht einzugehen und keine Daten zu übermitteln. Bei den von mir angestellten Nachforschungen in dem dargestellten Fall bin ich darauf aufmerksam geworden, daß entgegen dieser Absprache eine andere Wirtschafts- und Handelsauskunftei doch mit der geprüften Detektei in Vertragsbeziehungen stand. Auf meine Intervention ist zwischenzeitlich der Vertrag durch die Auskunftei gekündigt worden. Die Detektei erhielt zuvor von der Auskunftei auf Anfrage regelmäßig Daten übermittelt und entrichtete dafür quartalsmäßig einen Mitgliedsbeitrag von ca. DM 1.000,—. Diese Größenordnung zeigt bereits, daß die Detektei sich des Datenbestandes der Auskunftei in erheblichem Umfang bediente. Es gibt ganz offensichtlich einen zunehmenden Bedarf der Detekteien, für ihre Auftraggeber das Datenmaterial der Handels- und Wirtschaftsauskunfteien zu gebrauchen, um sich eine eigene Recherchierarbeit zu ersparen oder sie zu minimieren.

Zugleich wird damit deutlich, daß sich viele Detekteien längst nicht mehr auf traditionelle Gebiete ihrer Arbeit, wie die der Personenkontrolle und Überwachung, des Werk- und Betriebsschutzes oder der individuellen Recherche in Ehe- und Partnerschaftsangelegenheiten beschränken. Teilweise betreiben sie das Geschäft der Wirtschafts- und Handelsauskunfteien, nur daß sie, anders als diese, sich nicht auf Auskünfte zur Beurteilung von Kredit-Risiken im Wirtschaftsverkehr beschränken, sondern in einem umfassenderen Sinne Daten zur wirtschaftlichen, finanziellen und persönlichen Situation einer Person sammeln, um sie an ihren Auftraggeber weiterzuleiten. Wie die Wirtschafts- und Handelsauskunfteien, so sind auch die Detekteien Informationsbeschaffer und Auskunftsinstitute. Sie unterscheiden sich von ihnen nur dadurch, daß an die Stelle der formularmäßigen Auskünfte umfangreiche Dossiers über die Person des Betroffenen treten. Dabei baut die Informationssammlung jedoch auf dem Grunddatenbestand auf, wie er von den Wirtschafts- und Handelsauskunfteien gesammelt und zur Verfügung gestellt wird. Obwohl also die Detekteien einer den Handelsaus-

kunfteien vergleichbaren Tätigkeit nachgehen, richten sich die meisten von ihnen nicht nach den Vorschriften des BDSG. Einer Datenschutzkontrolle bedarf es aber um so mehr, weil die Detekteien in einer umfassenderen und intensiveren Form Daten aus der Privatsphäre des Bürgers sammeln und beauskunften. Vor den damit einhergehenden Gefahren müssen die Bürger geschützt werden.

Dies läßt sich nur dann in dem gebotenen Umfang sicherstellen, wenn auch den Detekteien die Erhebung, Speicherung und Übermittlung personenbezogener Daten nur unter streng definierten Voraussetzungen erlaubt ist. Es muß gewährleistet sein, daß über die Betroffenen nur zutreffende Daten verarbeitet werden; und es muß Berichtigungs-, Löschungs- und Sperrungsvorschriften geben, die die Detekteien zu beachten haben. Unabdingbar ist schließlich, daß der Bürger, dessen Daten von einer Detektei registriert und weitervermittelt werden, hiervon benachrichtigt wird und sein Auskunftsrecht ausüben kann.

Die Novellierung des BDSG sollte Veranlassung sein, auch für die Tätigkeit der Detekteien gesetzliche Voraussetzungen festzulegen und zu bestimmen, zu welchen Zwecken ihnen die Verarbeitung personenbezogener Daten erlaubt sein soll.

Der Bundesverband Deutscher Detekteien (BDD), dem ich Gelegenheit gegeben habe, zu meinem Bericht Stellung zu nehmen, hat mir zwar bestätigt, daß der Berufszugang für Detektive vom Gesetzgeber bisher nicht geregelt ist. Er hat mich jedoch darauf hingewiesen, daß der BDD mit anderen Verbänden deshalb in einem Akt der Selbsthilfe die Zentralstelle für die Ausbildung im Detektivgewerbe (ZAD) gegründet habe. Die ZAD führe einen zweijährigen Ausbildungsgang durch, der mit einer Abschlußprüfung an der Industrie- und Handelskammer abschließen soll.

Auch der BDD hat nochmals bekräftigt, daß die Rechtsauffassung, die Detektive unterlägen dem BDSG, von ihm nicht geteilt würde. Durch den Einsatz moderner Bürosysteme hätten sich keine Änderungen ergeben, die zur Aufgabe bisher vertretener Rechtspositionen führen müßten. Schließlich hat mir der BDD erklärt, er halte in diesem Zusammenhang auch die Gleichsetzung von Detekteien mit Auskunfteien für verfehlt, da Detektive personenbezogene Daten jeweils nur an einen einzelnen Auftraggeber weiterleiten würden, ohne daß eine erneuter Zugriff für andere Auftraggeber stattfinde, während Auskunfteien die Daten speichern, bearbeiten und ergänzen würden, um sie auf Anfrage an viele Dritte weiterzuleiten.

5.7.4 Auskunftspflicht einer datenverarbeitenden Stelle im nicht-öffentlichen Bereich bei Anfragen von Strafverfolgungsbehörden

Der Hamburgische Datenschutzbeauftagte hat sich wiederholt zur Auskunftspflicht datenverarbeitender Stellen im nicht-öffentlichen Bereich bei Anfragen von Strafverfolgungsbehörden äußern müssen. Gemeint sind damit die Auskunftsersuchen im Rahmen von Strafermittlungen, die von der Staatsanwaltschaft oder der Polizei gestellt werden. Bei den privaten Stellen bestehen Unklarheiten, ob und wann nach welchen gesetzlichen Grundlagen sie gegenüber welchen Strafverfolgungsorganen Auskunft erteilen müssen. Die Rechtslage beurteile ich wie folgt:

Es ist zunächst zu fragen, ob es vorrangige Vorschriften im Sinne von § 45 Satz 1 BDSG gibt, in denen spezielle Regelungen für die Datenübermittlung im Ermittlungsverfahren getroffen sind. In Betracht kommen die §§ 160 ff. StPO, die die Befugnisse von Staatsanwaltschaft und Polizei im Ermittlungsverfahren regeln. In § 45 Satz 2 Nr. 3 BDSG wird unmittelbar zwar nur auf § 161 StPO Bezug genommen. Da die Aufzählung jedoch nur beispielhaft ist, können auch weitere Bestimmungen, die Polizei und Staatsanwaltschaft zu bestimmten Ermittlungshandlungen berechtigen, den Übermittlungsvorschriften des BDSG vorgehen.

Betrachtet man die Vorschriften über die Ermittlungsbefugnisse von Staatsanwaltschaft und Polizei im einzelnen, so kommt man zu folgenden Feststellungen:

Für Auskunftsverlangen der Staatsanwaltschaft ergibt sich eine Auskunftsverpflichtung öffentlicher Behörden nach § 161 StPO. § 161a Abs. 1 StPO sieht daneben eine Befug-

nis der Staatsanwaltschaft vor, Zeugen zu vernehmen. Für private Stellen läßt sich damit indirekt über § 161a StPO eine Verpflichtung zur Auskunftserteilung gegenüber der Staatsanwaltschaft ableiten. Diese Vorschriften über die Auskunftsrechte der Staatsanwaltschaft haben Vorrang vor den Vorschriften des BDSG.

Weiter ist der Staatsanwaltschaft ein Zugriff auf personenbezogene Daten bei privaten Stellen auch im Wege der Beschlagnahme möglich. Datenträger, auf denen personenbezogene Daten i.S.v. § 2 Abs. 2 Nr. 1 BDSG gespeichert sind, sind Gegenstände i.S.d. §§ 94 ff. StPO. Die Staatsanwaltschaft (oder ausnahmsweise die Polizei) können also, wenn entsprechende Datenträger von privaten Stellen nicht herausgegeben werden, die Beschlagnahme erwirken bzw. bei Gefahr im Verzuge selbst anordnen (§ 98 Abs. 1 Satz 1 StPO). Eine wesentliche Einschränkung liegt aber darin, daß es im Regelfall — soweit nicht Gefahr im Verzuge ist — nicht den Strafverfolgungsbehörden überlassen ist, sich auf diese Weise Kenntnis von beweiserheblichen Daten zu verschaffen, sondern daß es einer richterlichen Anordnung bedarf. Bei der Anordnung der Beschlagnahme ist der Verhältnismäßigkeitsgrundsatz zu beachten, so daß die potentielle Beweisbedeutung und die Eingriffe für die Betroffenen miteinander abzuwägen sind.

Der Polizei hingegen stehen die in den genannten Vorschriften der Staatsanwaltschaft gegebenen Befugnisse — mit Ausnahme der Anordnung der Beschlagnahme bei Gefahr im Verzuge — nicht zu. Zwar hat auch die Polizei im Rahmen ihres allgemeinen Ermittlungsauftrages (§ 163 StPO) das Recht und die Pflicht, Auskünfte einzuholen; hingegen ermächtigt § 163 StPO die Polizei nicht, private Stellen zur Beantwortung von Auskunftsverlangen anzuhalten. Weiter ist zwar auch der Polizei das Recht gegeben, Zeugen zu vernehmen (§ 163a Abs. 5 StPO), jedoch gibt es nur bei der Vernehmung durch die Staatsanwaltschaft eine Verpflichtung des Zeugen zum Erscheinen und zur Aussage (§ 161a Abs. 1 Satz 1 StPO). Bei Ermittlungen der Polizei wird für den Zeugen ein Aussagezwang nicht begründet. Die privaten Stellen haben darum zu prüfen, ob sie eine Auskunft geben dürfen oder nicht. Um diese Frage zu entscheiden, sind die in §§ 24, 32 BDSG niedergelegten Voraussetzungen zur Datenübermittlung als Abwägungskriterien heranzuziehen.

Auch nach § 24 Abs. 1 oder § 32 Abs. 2 und 3 BDSG gibt es keine Verpflichtung der datenverarbeitenden Stellen, den Auskunftsverlangen der Polizei zu entsprechen. Bei der geltenden Rechtslage können also private Stellen Anfragen der Polizei beantworten, soweit sich nach der grundsätzlich notwendigen Einzelfallprüfung, unter Abwägung des berechtigten Interesses der Allgemeinheit einerseits und der Beeinträchtigung schutzwürdiger Belange der Betroffenen andererseits, ergibt, daß die Datenübermittlung zulässig ist.