Archiv-Exemplar
Deutscher Bundestag
LEIHWEISE
Rückgabe erforderlich!

Deutscher Bundestag
10. Wahlperiode

Drucksache 10/6816

28. 01. 87

Sachgebiet 204

Unterrichtung

durch den Bundesbeauftragten für den Datenschutz

Neunter Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz gemäß § 19 Abs. 2 Satz 2 des Bundesdatenschutzgesetzes (BDSG)

Gliederung

		Seite
1.	**Gesamtüberblick**	4
1.1	Die 10. Legislaturperiode	4
1.2	Das Berichtsjahr	5
1.3	Übergangsbonus	6
1.4	Kontrollen und Beratungen — Übersicht —	7
1.5	Kooperation	10
1.6	Öffentlichkeitsarbeit	11
1.7	Die Dienststelle	11
2.	**Neue Informations- und Kommunikationstechniken für den Deutschen Bundestag (PARLAKOM)**	13
3.	**Innere Verwaltung**	14
3.1	Neue Personalausweise und Pässe	14
3.2	Ausländerzentralregister	15
3.3	Personenstandswesen	16
3.4	Wahlrecht	17
3.5	Zivildienst	18
3.5.1	Aufbewahrung von Anerkennungsunterlagen	18
3.5.2	Arbeitsberichte von Zivildienstleistenden	18
4.	**Rechtswesen**	19
4.1	Mitteilungen in Zivilsachen (MiZi) Mitteilungen in Strafsachen (MiStra)	19
4.2	Strafprozeßordnung	19
4.3	Veröffentlichung von Gerichtsentscheidungen	20
5.	**Finanzwesen**	20
6.	**Bauwesen**	21
6.1	Baugesetzbuch	21
6.2	Datenschutzkontrolle der Bundesbaudirektion	22
7.	**Personalwesen**	22
7.1	Konventionelle Personaldatenverarbeitung	22
7.1.1	Personalaktenrecht	22
7.1.2	Beihilfe	22
7.1.3	Besoldung/Versorgung	24
7.1.4	Einzelfälle	25
7.2	Automatisierte Personaldatenverarbeitung	26
7.2.1	Personalinformationssysteme	26
7.2.2	Telefondatenverarbeitung	28
7.2.3	Verhaltens- und Leistungskontrolle	29
8.	**Deutsche Bundespost**	29
8.1	Probleme der Zusammenarbeit mit dem Bundesministerium für das Post- und Fernmeldewesen	29
8.2	Telekommunikationsordnung	30
8.3	Bekanntgabe der Daten von Kabel- bzw. Satellitenfunkteilnehmern	31
8.4	Kabelpilotprojekt Dortmund	33
8.5	Anschriftenermittlung zu posteigener Werbung	34

Zugeleitet mit Schreiben des Bundesbeauftragten für den Datenschutz — I — 192 111/11 — vom 28. Januar 1987 gemäß § 19 Abs. 2 des Bundesdatenschutzgesetzes.

		Seite
9.	**Verkehrswesen**	35
9.1	Fahrzeugregistergesetz (ZEVIS)	35
9.2	Verkehrszentralregister	36
9.2.1	Stand der Gesetzesvorbereitung	36
9.2.2	Auskunftserteilung nach § 30 StVG (Vollauskunft)	37
9.3	Kfz-Zulassungsdaten	37
9.3.1	Zusatzerhebung bei Ausländern	37
9.3.2	Übermittlung an die Automobilindustrie	38
9.4	Führerschein auf Probe	38
9.5	Luftfahrt-Bundesamt (LBA)	39
9.5.1	Fehlende Rechtsgrundlagen	39
9.5.2	Technische und organisatorische Mängel	40
9.6	Deutsche Bundesbahn (DB)	40
9.6.1	Deutsche Bundesbahn als Teilnehmer an Verkehrsverbünden	40
9.6.2	Videoaufzeichnungen	41
10.	**Statistik**	42
10.1	Bundesstatistikgesetz	42
10.2	Zweites Statistikbereinigungsgesetz	44
10.3	Volkszählung 1987	45
10.4	Wissenschaftlicher Beirat für Mikrozensus und Volkszählung	45
10.5	Handels- und Gaststättenzählung und Steuergeheimnis	45
10.6	Agrarberichterstattung — Zusatzprogrammverordnung —	46
10.7	Veröffentlichung von Statistikdateien	46
11.	**Sozialwesen**	47
11.1	Arbeitsverwaltung	48
11.1.1	Arbeitsvermittlung/-beratung	48
11.1.2	Leistungsverwaltung	49
11.1.3	Ärztlicher/Psychologischer Dienst	50
11.1.4	Berufsförderung	50
11.2	Krankenversicherung	50
11.2.1	Kontrollen	50
11.2.2	Einzelfragen	52
12.	**Öffentliche Sicherheit**	55
12.1	Probleme und Hindernisse	55
12.2	Gesetzgebungsvorhaben	56
12.3	Neufassung der Sicherheitsüberprüfungsrichtlinien	56
12.4	Neufassung der Richtlinien für die Sicherheitsüberprüfung von Personal in kerntechnischen Anlagen	57
13.	**Bundeskriminalamt**	58
13.1	Datenschutzrechtliche Kontrolle im Bereich der Bekämpfung der Rauschgiftkriminalität	58
13.2	Weitere Zunahme der SPUDOK-Anwendungen	59
13.3	Inbetriebnahme der Datei APIS	60
14.	**Bundesamt für Verfassungsschutz (BfV)**	62
15.	**Bundesnachrichtendienst (BND)**	63
16.	**Bundesgrenzschutz**	63
16.1	Grenzaktennachweis (GAN)	63
16.2	Restriktive Datenschutzpraxis beim Grenzschutzkommando Nord	64
17.	**Zollkriminalinstitut und Zollfahndungsdienst**	64
18.	**Verteidigung**	65
18.1	Fehlende Rechtsgrundlage für die Datenverarbeitung beim MAD	65
18.2	Neukonzeption für die Merkmalsspeicherung beim MAD	65
18.3	Eignungs- und Verwendungsprüfung (EVP)	65
18.4	Verband der Reservisten	66
18.5	Umgang mit KDV-Unterlagen	67
19.	**Nicht-öffentlicher Bereich**	68
19.1	Kreditsicherung	68
19.2	Versicherungen	70
20.	**Datensicherung**	70
20.1	Personal-Computer	70
20.2	Bürokommunikation	72
20.3	Vernetzung	72
20.4	Abstrahlung	74
21.	**Novellierung des Bundesdatenschutzgesetzes**	75
21.1	Anwendungsbereich	75
21.2	Zweckbestimmung	76
21.3	Transparenz	77
21.4	Kontrolle	78
22.	**Ausland und Internationales**	79
22.1	Europarat	79
22.2	Entwicklung des Datenschutzes im Ausland	79
22.3	Zusammenarbeit der Datenschutz-Kontrollinstitutionen	80
23.	**Bilanz**	80

Seite

Anlage 1 (zu 1.5):

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. Januar 1986 zu den Sicherheits- und Datenschutzgesetzen 84

Anlage 2 (zu 1.5):

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14. März 1986 zur Änderung des Bundesdatenschutzgesetzes 86

Anlage 3 (zu 1.5):

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14. März 1986 zum Datenschutz im Krankenhaus .. 89

Seite

Anlage 4 (zu 1.5):

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. April 1986 zur Änderung des Bundesverfassungsschutzgesetzes 90

Anlage 5 (zu 1.5):

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. April 1986 zum Entwurf einer Telekommunikationsordnung 92

Anlage 6 (zu 19.1):

SCHUFA-Klausel für Kontoeröffnungs- und für Kreditanträge 94

Sachregister 96

Abkürzungsverzeichnis 98

1. Gesamtüberblick

1.1 Die 10. Legislaturperiode

Das Ende der 10. Legislaturperiode gibt aus besonderem Grunde Anlaß zur Rückbesinnung und zu einer Bilanz:

Am 15. Dezember 1983 hat das Bundesverfassungsgericht sein Urteil zum Volkszählungsgesetz 1983 verkündet und darin vor allem mit der Herausstellung des Rechts auf informationelle Selbstbestimmung — über den Statistikbereich hinaus — wichtige allgemeine Grundsätze zum Datenschutz aufgestellt. In Wissenschaft und Praxis bestand kein Zweifel, daß das Urteil gleichzeitig auch als Auftrag an den Gesetzgeber zu gelten hat, wobei allerdings manchmal kontrovers blieb, wie umfangreich dieser Auftrag zu verstehen ist. Der Gesetzgeber hatte drei Jahre Zeit, um die entsprechenden gesetzgeberischen Konsequenzen zu ziehen und gleichzeitig auch prägende Wirkung auszuüben auf den Umgang mit personenbezogenen Daten durch die gesamte öffentliche Verwaltung und die Privatwirtschaft. Am Ende dieser Legislaturperiode muß daher die Frage erlaubt sein, wie sich die Gesetzgebungsorgane diesem Auftrag gestellt haben und in welchem Umfange sie ihm nachgekommen sind.

Die Antwort hierauf fällt nicht schwer, wenn es um die Auswirkungen des Urteils auf die Volkszählung selbst geht. Hier hat der Gesetzgeber mit dem neuen Volkszählungsgesetz schnell gehandelt und die Vorgaben des Bundesverfassungsgerichts ohne Frage umfassend berücksichtigt. Das gleiche gilt für das Mikrozensusgesetz 1985. Dies ist verständlich, denn bei der Volkszählung und dem Mikrozensus handelt es sich um unverzichtbare politische Vorhaben. Die gesetzlichen Grundlagen müssen daher unangreifbar sein.

Beim Bundesstatistikgesetz fällt die Antwort schon schwerer, da in ihm beispielsweise auch Regelungen enthalten sind, die über die Übermittlungsmöglichkeiten nach dem alten Bundesstatistikgesetz hinausgehen und daher zumindest als problematisch anzusehen sind. Sie entsprechen einem Wunsch der Länder und wurden letztlich deshalb aufgenommen, um das Gesetzgebungsvorhaben nicht im Bundesrat scheitern zu lassen.

Beim Gesetz über den maschinenlesbaren Personalausweis handelt es sich um ein Vorhaben, das im Laufe seiner langjährigen gesetzgeberischen Entwicklung zu einem unverzichtbaren politischen Postulat geworden ist. Die datenschutzrechtlichen Verbesserungen seit dem ersten Entwurf aus dem Jahre 1979 sind unbestreitbar und verdienen Anerkennung, wenn auch nicht übersehen werden kann, daß der erst in der Schlußphase der Beratungen eingeführte § 163d StPO (s. unten 3.1) viele datenschutzrechtliche Fragen offen läßt.

Wenn man von diesen Gesetzen, die jeweils von politischen Programmen getragen wurden und zu denen auch das noch in letzter Minute verabschiedete Fahrzeugregistergesetz zu rechnen ist, einmal absieht, dann weist die gegenwärtige Gesetzeslage in datenschutzrechtlicher Hinsicht ohne Zweifel Defizite auf.

Hat der Gesetzgeber durch die Einbringung der sog. Sicherheitsgesetze auch klar zu erkennen gegeben, daß er einen umfangreichen gesetzgeberischen Nachholbedarf anerkennt, so wurde durch die Art der Vorbereitung und ihre Dauer doch offenkundig, welche Probleme sich bei der Bewältigung dieser komplexen und schwierigen Materie stellen: Die umfangreichen Entwürfe wurden — entgegen sonstiger Gepflogenheit — von den Koalitionsfraktionen ausgearbeitet, da der sonst übliche Gesetzgebungsweg über die Bundesressorts wegen deren unterschiedlichen Zuständigkeiten offenbar zu beschwerlich und zeitraubend erschien. Das führte dazu, daß die Entwürfe erst nach langer Bearbeitungszeit eingebracht wurden und sich zu diesem Zeitpunkt bereits abzeichnete, daß sie in der laufenden Legislaturperiode nicht mehr verabschiedet werden konnten.

Abgesehen von dieser gesetzestechnischen Besonderheit leiden die Gesetzentwürfe auch an einem inhaltlich-konzeptionellen Mangel. Sie erwecken den Eindruck, daß mit ihnen der Versuch unternommen wird, die bisher geübte Praxis soweit wie möglich zu erhalten und sogar auszubauen. Ich habe Zweifel, ob sich so das vom Bundesverfassungsgericht entwickelte Recht auf informationelle Selbstbestimmung in der täglichen Praxis von öffentlicher Verwaltung und Privatwirtschaft auch wirklich durchsetzen läßt. Gewiß werden Ansätze dafür erkennbar, so wenn z. B. die Zweckbindung und die Voraussetzungen für eine zweckfremde Nutzung der Daten detailliert geregelt werden. Wenn die normative Regelung dann allerdings so gestaltet wird, daß in der Praxis trotzdem eine weitgehende Zweckfreiheit eintreten dürfte, dann ist eines deutlich: Die Konzeption der Entwürfe ist von den Vorstellungen für ein neues datenschutzrechtliches Verständnis, das das Recht des Bürgers auf informationelle Selbstbestimmung in den Mittelpunkt jedes Umgangs mit personenbezogenen Daten stellt, noch ziemlich weit entfernt und scheint sich eher damit begnügen zu wollen, einer veränderten datenschutzrechtlichen Situation jeweils durch Anpassung einzelner Vorschriften Rechnung zu tragen. Die Entwürfe lassen insgesamt die Bereitschaft zu einem Neubeginn als Ergebnis eines Umdenkprozesses vermissen und verstehen die Forderung nach mehr Rechtsstaatlichkeit vor allem in dem Sinne der Herstellung von Legalität, wo doch die Frage nach der Legitimität der einzelnen Datenverarbeitungsmaßnahmen eigentlich viel näher liegt. Zu beklagen ist danach nicht so sehr der Umstand, daß bestimmte Gesetzesvorhaben in dieser Legislaturperiode nicht mehr verabschiedet werden konnten, sondern die auseinandergehenden Vorstellungen darüber, wie die datenschutzrechtliche Landschaft künftig aussehen soll.

Ein Beispiel dafür ist auch die Behandlung der Frage, ob die im BDSG enthaltene Verklammerung der Datenverarbeitung von öffentlichem und nicht-öffentlichem Bereich künftig zugunsten von zwei verschiedenen Gesetzen aufgelöst werden soll. Diese zunächst kaum ernst genommene Frage wurde in den vergangenen Monaten vor allem deshalb als Problem aufgegriffen und ernsthaft diskutiert, weil Befürchtungen aus dem nicht-öffentlichen Lager laut wurden, durch das Volkszählungsurteil bedingte Restriktionen könnten sich negativ auf das Wirtschaftsgeschehen auswirken.

Dem Bundesgesetzgeber kommt für die Gestaltung des Datenschutzes in der Bundesrepublik eine Schlüsselrolle zu. Dies sollte von niemand in Frage gestellt werden. Seine Aufgabe wird indes um so schwieriger zu erfüllen sein, je mehr die Bundesländer vor ihm im Rahmen ihrer Zuständigkeit als Gesetzgeber im Vollzug des Volkszählungsurteils in Erscheinung treten. Denn es ist kaum vorstellbar, daß für den Bundesbereich andere datenschutzrechtliche Standards Gültigkeit haben können als für die Landesverwaltung. Daher erscheint es um so dringlicher, daß der Bund seiner Rolle als rechtsvereinheitlichende Kraft gerecht wird und unmißverständliche Signale setzt.

Die Perspektive für die kommende Legislaturperiode muß daher lauten, die allgemeinen datenschutzrechtlichen Grundvorstellungen sowohl durch Gesetzesbeschlüsse wie auch durch Empfehlungen an die Exekutive transparent zu machen und damit sowohl im Verhältnis zu den Bundesländern maßstabbildend wie auch gegenüber Regierung und Verwaltung richtungsweisend zu wirken.

1.2 Das Berichtsjahr

Das Berichtsjahr 1986 begann für den Datenschutz recht hoffnungsvoll. Im Januar wurde von den Fraktionen der CDU/CSU und der FDP der Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes und des Verwaltungsverfahrensgesetzes, des Bundesverfassungsschutzgesetzes und des Straßenverkehrsgesetzes (Drucksache 10/4737) in den Bundestag eingebracht. Dieser umfassende Gesetzentwurf war ein wesentlicher Teil des sogenannten Pakets der Sicherheitsgesetze (in dem freilich das BDSG wie eine Fremdkörper wirkte), zu dem außerdem der dem Bundestag schon vorliegende Gesetzentwurf zur Änderung des Personalausweisgesetzes und des Paßgesetzes einschließlich einer Änderung der Strafprozeßordnung sowie die etwas später von der Bundesregierung eingebrachten Entwürfe eines Zusammenarbeitsgesetzes und eines Gesetzes über den Militärischen Abschirmdienst gehörten. Alle diese Gesetzentwürfe waren ausweislich ihrer Begründung darauf angelegt, den Grundsätzen des Volkszählungsurteils des Bundesverfassungsgerichts Rechnung zu tragen; sie sollten im jeweiligen Anwendungsbereich die Rechtsgrundlagen für die Erhebung und Verwendung personenbezogener Informationen schaffen bzw. präzisieren. Inwieweit das gelungen ist, wird an anderer Stelle dieses Berichts zu behandeln sein. In jedem Falle konnte erwartet werden, daß der bislang nicht verfassungsgemäße Zustand nunmehr bereinigt werden würde. Doch schon bald stellte sich heraus, daß die bis zum Ende der Legislaturperiode verbleibende Zeit für eine angemessene Beratung der in jedem dieser Gesetze liegenden komplexen Rechtsprobleme nicht ausreichen werde. Spätestens in den vom Innenausschuß des Bundestages zu den Gesetzentwürfen veranstalteten Anhörungen, an denen ich neben zahlreichen anderen Sachverständigen teilgenommen habe, wurde endgültig klar, daß mit einer Verabschiedung aller Gesetze in dieser Legislaturperiode nicht mehr zu rechnen war. Nur das schon früher eingebrachte Gesetz zur Änderung des Personalausweisgesetzes und des Paßgesetzes konnte noch im Frühjahr verabschiedet werden.

Die schon als erledigt geltenden übrigen Gesetzentwürfe gerieten noch einmal in die politische Diskussion, als nach dem brutalen Mordanschlag auf den Diplomaten von Braunmühl am 10. Oktober 1986 nach einem neuen Fahndungs- und Sicherheitskonzept gesucht wurde. Aus dem ursprünglichen Gesetzespaket wurde das Gesetz zur Änderung des Straßenverkehrsgesetzes, das der Polizei den Online-Zugriff auf die Daten des Zentralen Fahrzeugregisters beim Kraftfahrt-Bundesamt eröffnet, als ein geeignetes Instrument zu der aktuell notwendigen Verbesserung der polizeilichen Fahndung ausgewählt in der Annahme, daß eine kurzfristige Verabschiedung noch möglich sein werde. In nur wenigen Ausschußsitzungen wurde das Gesetz durchberaten und — abgesehen von einigen marginalen Änderungen — in der Fassung des Entwurfs beschlossen. Ich habe an den Beratungen teilgenommen. Meine Verbesserungsvorschläge, die nicht zu einer Behinderung der Terroristenfahndung geführt hätten — wie gelegentlich zu lesen war —, sondern eine stärkere Anpassung an die im Volkszählungsurteil entwickelten Verfassungsgrundsätze und ein besseres Verständnis des Gesetzes zum Ziel hatten, fanden keine Zustimmung. Ich halte es für möglich, daß ohne den Zeitdruck, unter dem die Beratungen zwangsläufig standen, meine Anliegen eher Berücksichtigung gefunden hätten. Unter diesem Aspekt sehe ich es nicht als einen Nachteil an, daß die übrigen Gesetzentwürfe nicht mehr beraten werden konnten.

Zu den vorliegenden Entwürfen der Sicherheitsgesetze habe ich — wie bereits erwähnt — in mehreren öffentlichen Anhörungen, die der Innenausschuß des Deutschen Bundestages veranstaltet hat, mündlich und schriftlich Stellung genommen. Ich konnte dabei an die von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder gemeinsam formulierten Anforderungen an Datenschutzregelungen im Polizeirecht und für den Verfassungsschutz anknüpfen (vgl. 8. TB S. 65 bis 70). Ich halte es entsprechend meinem gesetzlichen Auftrag für meine Pflicht, dabei einen kritischen Maßstab anzulegen und auf Probleme hinzuweisen, die sich unter verfassungsrechtlichen Gesichtspunkten zum Recht auf informationelle Selbstbestimmung ergeben. Leider wird diese Position und werden meine daraus resultierenden Vorstellungen

und Forderungen bei den beteiligten Stellen, in manchen politischen Kreisen und auch in den Medien zum Teil immer wieder mißverstanden.

So machte beispielsweise eine überregionale Tageszeitung in mehreren aufeinander folgenden Ausgaben im Zusammenhang mit der Ermordung des Diplomaten von Braunmühl den angeblich überzogenen Datenschutz für Mißerfolge bei der Terrorismusbekämpfung verantwortlich, sprach von einem „Abbau erfolgversprechender Fahndungsmittel zugunsten eines ins Groteske aufgeblähten Datenschutzes" und forderte schließlich dazu auf, die „Heilige Kuh Datenschutz" endlich zu schlachten. Auch aus manchen politischen Kreisen waren Äußerungen ähnlicher Tendenz zu hören. Vereinzelt wurde ich auch persönlich diffamiert.

Ich weise diese über eine sachliche Kritik an meiner Arbeit hinausgehenden Vorwürfe mit allem Nachdruck zurück. Bisher ist mir kein Fall bekannt geworden — und man hätte ihn mir sicherlich vorgehalten —, in dem Fahndungserfolge am Datenschutz oder an den Aktivitäten der Datenschutzbeauftragten gescheitert wären. Das gilt insbesondere für den dem Datenschutz angelasteten Verzicht auf den Einsatz der Rasterfahndung. Diese Fahndungsmethode wird vielmehr deshalb kaum mehr angewandt, weil sie mittlerweile wenig Erfolg verspricht. Den Terroristen sind die polizeitaktischen Maßnahmen nämlich inzwischen bekannt und sie verhalten sich entsprechend unauffällig. Die Rasterfahndung wurde im übrigen von den Datenschutzbeauftragten nie für unzulässig gehalten (vgl. 3. TB S. 50 ff.). Es gibt auch auch keinen Beleg dafür, daß bessere Fahndungsergebnisse erzielt worden wären, wenn die Polizeien aller Länder schon einen Online-Zugriff auf das Zentrale Fahrzeugregister gehabt hätten; auf herkömmliche Art und Weise erhielt die Polizei schon bisher Auskünfte aus diesem Datenbestand. Und schließlich scheitert der absurde Vorschlag, alle verfügbaren Computer zusammenzuschalten, um dem Terrorismus beizukommen, bereits an den technischen Bedingungen und Möglichkeiten.

Niemand kann sich heutzutage gegenüber den schrecklichen Gewalttaten der Terroristen gleichgültig zeigen, kein vernünftiger Mensch wird sich der Bekämpfung des Terrorismus widersetzen. Ich trete aber dafür ein, sachgerechte Lösungsansätze und polizeiliche Arbeitsmethoden mit den verfassungsmäßig verbürgten Freiheitsrechten der Bürger in Einklang zu bringen. Nach den Klarstellungen, die das Bundesverfassungsgericht im Volkszählungsurteil getroffen hat, gehört dazu die Schaffung einwandfreier Rechtsgrundlagen für die Arbeit der zuständigen Behörden. Diese von mir beharrlich vertretene Forderung entspricht nicht einer einseitigen oder überspitzten Fehleinschätzung der Realität oder meiner Amtspflichten, sondern kann sich unmittelbar auf die Verfassung und ihre authentische Interpretation berufen. Wer dies nicht erkennen will und statt dessen gegen den Datenschutz polemisiert, muß sich den Vorwurf gefallen lassen, die schlimmen Auswüchse des Terrorismus und seine tragischen Folgen für die Opfer dazu zu benutzen, die eigene ablehnende Auffassung und persönliche Aversion gegen den „lästigen" Datenschutz einer bei der Suche nach Schuldigen dafür besonders empfänglichen Öffentlichkeit aufreden zu wollen. Eine solche Haltung ignoriert zudem völlig die Verfassungsqualität, die dem Datenschutz durch das Volkszählungsurteil bestätigt worden ist.

1.3 Übergangsbonus

Die im sog. Sicherheitspaket zusammengefaßten, noch nicht verabschiedeten Entwürfe eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes und des Verwaltungsverfahrensgesetzes, des Verfassungsschutzgesetzes, eines Zusammenarbeitsgesetzes und eines Gesetzes über den Militärischen Abschirmdienst sollen — wie verlautet — schon kurz nach Beginn der nächsten Legislaturperiode wieder in den Bundestag eingebracht werden. Es wäre wünschenswert, wenn die Beratungen dann auch bald aufgenommen würden, da der Zeitbedarf für die Erörterung einer so komplizierten und auch in der Öffentlichkeit viel beachteten und umstrittenen Materie erfahrungsgemäß hoch eingeschätzt werden muß.

Auf der anderen Seite darf nicht übersehen werden, daß der Zeitpunkt, zu dem die Neuregelungen erlassen werden, durchaus verfassungsrechtliche Bedeutung hat. Nach den Grundsätzen zur Einschränkung des Rechts auf informationelle Selbstbestimmung bedarf die Erhebung personenbezogener Daten im Bereich der Sicherheitsbehörden präziser gesetzlicher Grundlagen. Solche fehlen derzeit für den MAD und den BND; für die Verfassungsschutz- und die Polizeibehörden sind sie — gemessen an den Anforderungen des Volkszählungsurteils — unzureichend. Geht man deshalb von einer zur Zeit nicht verfassungsgemäßen Rechtslage in diesen Bereichen aus, so stellt sich die Frage, wie lange der gegenwärtige Zustand noch hingenommen werden kann oder — im vorliegenden Zusammenhang — wieviel Zeit der Gesetzgeber noch hat, um durch Erlaß entsprechender Gesetze verfassungsgemäße Rechtsgrundlagen für die Arbeit dieser Behörden zu schaffen.

Diese für meine Kontrolltätigkeit wichtige Problematik habe ich eingehend geprüft. Sie wird in der Verfassungsrechtsprechung unter dem Stichwort *„Übergangsbonus"* behandelt. Das Bundesverfassungsgericht hat sich damit in mehreren Entscheidungen, insbesondere in BVerfGE Bd. 41 S. 266 ff. und Bd. 51 S. 287 ff., eingehend beschäftigt und dabei zusammengefaßt folgende Auffassung vertreten:

Grundsätzlich hat die Feststellung, daß eine Verwaltungsmaßnahme, die in einen grundrechtlich geschützten Bereich eingreift und der verfassungsrechtlich gebotenen gesetzlichen Grundlage entbehrt, zwar die Aufhebung dieser Maßnahme zur Folge. Das Bundesverfassungsgericht hat jedoch in einer Reihe von Fällen, in welchen eine verfassungsrechtlich ursprünglich unbedenkliche Maß-

nahme aufgrund einer gewandelten Rechtsauffassung oder völlig veränderter tatsächlicher Umstände, die der bisherigen gesetzlichen Regelung zugrunde lagen, verfassungsrechtlich bedenklich geworden ist, die Notwendigkeit von Übergangsfristen anerkannt, in welchen der Gesetzgeber die Gelegenheit einer verfassungsgemäßen (Neu-)Regelung haben sollte. Eine solche Übergangsfrist kann insbesondere dann notwendig sein, wenn eine sonst eintretende Funktionsunfähigkeit staatlicher Einrichtungen vermieden werden soll, die der verfassungsmäßigen Ordnung noch ferner stünde als der bisherige Zustand. Bei der Zubilligung von Übergangsfristen ist nach der Schwere des Eingriffs zu differenzieren: Je tiefergreifender eine Verwaltungsmaßnahme Grundrechte des Betroffenen berührt, desto strengere Anforderungen sind an die Einräumung von Übergangsfristen und die innerhalb dieser Fristen unerläßlichen Maßnahmen zu stellen; ist der Eingriff weniger schwerwiegend, kann eine großzügigere Anerkennung von Übergangsfristen in Betracht kommen.

Für die Dauer derartiger Übergangsfristen können keine allgemein gültigen Maßstäbe gesetzt werden. Das Bundesverfassungsgericht hat verschiedentlich darauf abgestellt, daß eine gesetzliche Regelung bis zum Ende der laufenden Legislaturperiode des Parlaments erfolgen müsse, gelegentlich aber auch längere Fristen zugestanden. Eine Übergangsfrist könnte jedenfalls dann nicht mehr länger anerkannt werden, wenn der Gesetzgeber eine Neuregelung ungebührlich verzögert.

Während dieser Übergangsfrist kann die alte, verfassungsrechtlich zu beanstandende Regelung allerdings nur noch bedingt weiter angewandt werden. Bis zur Herstellung eines verfassungsmäßigen Zustandes durch den Gesetzgeber reduziert sich die Befugnis zu Eingriffen in verfassungsrechtlich geschützte Positionen auf das, was im konkreten Fall für die geordnete Weiterführung eines funktionsfähigen Betriebs unerläßlich ist. Die Prüfung, was in der jeweiligen Situation unerläßlich ist, darf sich nicht einfach darin erschöpfen, ob die ohnehin nur als Provisorium fortbestehende bisherige Regelung als solche korrekt angewandt worden ist. In Fällen der vorliegenden Art gehört dazu auch die weitere Prüfung, ob nicht unter Berücksichtigung der gegebenen Verhältnisse eine bislang nicht vorgesehene schonendere Maßnahme ausreicht, um die Funktionsfähigkeit sicherzustellen.

Diese Grundsätze sind nach meiner Auffassung auch anwendbar, wenn im konkreten Fall (z. B. Recht der Sicherheitsbehörden) die dabei vorausgesetzten verfassungsrechtlichen Bedenken noch nicht gerichtlich bestätigt sind, sondern sich wegen der in § 31 Abs. 1 Bundesverfassungsgerichtsgesetz vorgesehenen Bindungswirkung der Entscheidungen des Bundesverfassungsgerichts aus einer in anderem Zusammenhang ergangenen verfassungsgerichtlichen Entscheidung ergeben. Denn diese Bindungswirkung betrifft nicht nur die auf den entschiedenen Rechtsstreit bezogene Entscheidungsformel, sondern sie erstreckt sich auch auf die tragenden Gründe der Entscheidung, soweit sie allgemeine verfassungsrechtliche Auslegungsgrundsätze enthalten. Die wesentlichen Feststellungen des Bundesverfassungsgerichts im Volkszählungsurteil, insbesondere die dort dargelegten Voraussetzungen zulässiger Einschränkungen des Rechts auf informationelle Selbstbestimmung, gehören ohne Zweifel zu den tragenden Gründen dieser Entscheidung. Sie sind deshalb auch für die verfassungsrechtliche Beurteilung der Rechtsgrundlage für Datenerhebungen durch Sicherheitsbehörden relevant und begründen zumindest Bedenken gegen deren Verfassungsmäßigkeit.

Für die Frage, wie lange der Übergangsbonus andauert, d. h. welche Zeit dem Gesetzgeber zur Verfügung steht, um eine an sich verfassungsrechtlich bedenkliche Rechtslage zu beseitigen, hat das Bundesverfassungsgericht eine Reihe von Kriterien festgelegt. Zu berücksichtigen sind danach die Komplexität der zu erlassenden Regelungen, ihr Zusammenhang mit anderen Rechtsmaterien, die Divergenz der dazu in der Öffentlichkeit bestehenden Auffassungen, die Belastungen des Gesetzgebers, andererseits aber auch die Tiefe der Grundrechtseingriffe, die ohne ausreichende Rechtsgrundlage vorgenommen werden, und die Dauer der darüber schon geführten Diskussion.

Wenn man in Betracht zieht, daß das Bundesverfassungsgericht — für Einzelvorschriften — im allgemeinen das Ende der Legislaturperiode, in der die Entscheidung getroffen wurde, für die Frist als Ansatzpunkt genommen hat, so wird man hier bei der Fülle des zu regelnden Stoffes und dessen Komplexität, aber auch bei der schon lange andauernden Auseinandersetzung um die Bewertung des Volkszählungsurteils, dem Stand der Vorbereitungen der Gesetzgebung und der seit der Entscheidung verstrichenen Zeit verlangen müssen, daß spätestens bis zum Ende der nächsten Legislaturperiode die notwendigen Gesetze erlassen sind.

1.4 Kontrollen und Beratungen — Übersicht —

Bei folgenden Behörden haben Mitarbeiter meiner Dienststelle im Berichtsjahr Kontrollen, Beratungen oder Informationsbesuche durchgeführt:

Bundesminister des Innern

Bundesminister für das Post- und Fernmeldewesen

Bundeszentralregister

Bundesdruckerei

Bundesgesundheitsamt

Bundesanstalt für Arbeit

Bundesamt für den Zivildienst

Deutsche Bundesbahn

Bundesbaudirektion

Bundesnachrichtendienst

Bundesamt für den Verfassungsschutz

Militärischer Abschirmdienst

Bundeskriminalamt	Krankenversorgung der Bundesbahnbeamten
Deutsches Patentamt	eine Oberpostdirektion
Statistisches Bundesamt	eine Wehrbereichsverwaltung
Luftfahrt-Bundesamt	eine Betriebskrankenkasse
Stiftung Preußischer Kulturbesitz	mehrere Kreiswehrersatzämter
zwei Banken des Bundes	ein Postamt
Deutsche Beamtenversicherung	

Nachfolgend sind die wichtigsten bearbeiteten Themen und die Art ihrer Erledigung aufgeführt:

Thema	Art der Erledigung
Novellierung des BDSG (Drucksachen 10/4737 und 10/5343)	Anhörung im Innenausschuß des Deutschen Bundestages mit schriftlicher Stellungnahme
Novellierung des Verfassungsschutzgesetzes (Drucksachen 10/4737 und 10/5343)	Anhörung im Innenausschuß des Deutschen Bundestages mit schriftlicher Stellungnahme
Entwurf eines MAD Gesetzes (Drucksache 10/5342)	schriftliche Stellungnahme gegenüber dem Innenausschuß des Deutschen Bundestages
Novellierung des Straßenverkehrsgesetzes — ZEVIS, Fahrzeugregistergesetz — (Drucksachen 10/4737, 10/5343 und 10/6613)	Anhörung im Innenausschuß des Deutschen Bundestages mit schriftlicher Stellungnahme und Beteiligung bei der Beratung des Gesetzentwurfs in Ausschüssen des Deutschen Bundestages mit weiterer schriftlicher Stellungnahme gegenüber dem Innenausschuß des Deutschen Bundestages
Novellierung des Bundesstatistikgesetzes	Anhörung im Innenausschuß des Deutschen Bundestages mit schriftlicher Stellungnahme und weiteren Beratungen im Innenausschuß
Novellierung des 2. Statistikbereinigungsgesetzes	Beratung im Innenausschuß des Deutschen Bundestages mit schriftlicher Stellungnahme
Personalausweisgesetz, Paßgesetz, Verfahren zur Herstellung der Personalausweise	Beratungen im Innenausschuß und im Rechtsausschuß des Deutschen Bundestages, schriftliche Stellungnahme gegenüber dem BMI
Neufassung des Verkartungsplanes der Abteilung III (Linksextremismus) des BfV	Beratung im Innenausschuß des Deutschen Bundestages, Beratungen und schriftliche Stellungnahme gegenüber dem BMI
Maßnahmenkatalog nach dem Mordfall Denali	Beratung im Innenausschuß des Deutschen Bundestages mit schriftlichen Stellungnahmen
Entwurf eines Gesetzes zur Änderung des Berufsrechts der Rechtsanwälte, der Patentanwälte und der Notare	schriftliche Stellungnahme gegenüber dem Rechtsausschuß des Deutschen Bundestages
Einsichtsrecht in Umweltakten	Beratung der Fraktion DIE GRÜNEN des Deutschen Bundestages
Beteiligung in drei Verfassungsbeschwerden betr. Mithören von Telefongesprächen im Betrieb, betr. Mitteilungen in Strafsachen (MiStra), betr. Datenübermittlungen an die Schufa	schriftliche Stellungnahmen gegenüber dem BVerfG
Durchführung des Mikrozensus und der Volkszählung	Beratung des Wissenschaftlichen Beirats beim Statistischen Bundesamt
Entwurf einer 6. Verordnung zur Änderung straßenverkehrsrechtlicher Vorschriften (Einzelregelungen zur Durchführung der Fahrerlaubnis auf Probe)	schriftliche Stellungnahme gegenüber dem Bundesrat und dem Bundesminister für Verkehr und dessen Beratung
Datenverarbeitung im Bundeskanzleramt	Beratung und schriftliche Stellungnahme gegenüber dem Bundeskanzleramt
Strafverfolgungsstatistik	Beratung und schriftliche Stellungnahme gegenüber dem BMJ und Beratung des Bundeszentralregisters

Thema	Art der Erledigung
Änderung des Strafvollzugsgesetzes	schriftliche Stellungnahme gegenüber dem BMJ
Grundbuchordnung	schriftliche Stellungnahme gegenüber dem BMJ
Einsicht in Akten der Familiengerichte für Forschungszwecke	schriftliche Stellungnahme gegenüber dem BMJ
Neukonzeption des Ausländerzentralregisters	Beratungen und schriftliche Stellungnahme gegenüber dem BMI
Neuordnung der Datenverarbeitung bei der Abteilung Staatsschutz des BKA und Auswirkungen auf die informationelle Zusammenarbeit mit dem BfV	schriftliche Stellungnahme gegenüber dem BMI
Grenzaktennachweis (GAN)	Beratung und schriftliche Stellungnahme gegenüber dem BMI und dem BGS
Neufassung der Dienstvorschrift „Ausland" (Übermittlung von Daten an ausländische Sicherheitsbehörden)	Beratung und schriftliche Stellungnahme gegenüber dem BMI
Sicherheitsüberprüfungsrichtlinien	Beratung und schriftliche Stellungnahme gegenüber dem BMI
Sonderdatei im Rahmen der Spionagebekämpfung	Beratung und schriftliche Stellungnahme gegenüber dem BMI
Regelung des Personalaktenrechts	Beratung der Interministeriellen Arbeitsgruppe beim BMI
Gesetzliche Regelungen für das Zollkriminalinstitut im Finanzverwaltungsgesetz	schriftliche Stellungnahme gegenüber dem BMF
Finanzwesen	
— Entwurf einer Rechtsverordnung zu § 93a AO (Kontrollmitteilungsverordnung)	schriftliche Stellungnahme gegenüber dem BMF
— Entwurf einer Steuerdatenabrufverordnung	Beratung und schriftliche Stellungnahme gegenüber dem BMF
Neufassung der Dienstanschlußvorschriften	Beratung und schriftliche Stellungnahme gegenüber dem BMF
Planung und Einrichtung von Personalinformationssystemen, Einsatz von PC, Verhaltens- und Leistungskontrolle	Beratung und schriftliche Stellungnahme gegenüber dem BMF, dem BMP, dem BMV, der Bundesanstalt für Arbeit, der Deutschen Bundesbahn, der Gewerkschaft ÖTV, der Gewerkschaft der Eisenbahner Deutschlands
Erstellung der Diagnosenstatistik nach der Bundespflegesatzverordnung	Beratung und schriftliche Stellungnahme gegenüber dem BMA und dem Deutschen Krankenhausinstitut
Entwurf eines Gesetzes zur Verwendung der Versicherungsnummer	Fortsetzung der Beratungen und schriftliche Stellungnahmen gegenüber dem BMA
Regelung des BMVg zur personellen Vorbeugung des MAD	Beratung und schriftliche Stellungnahme gegenüber dem BMVg
Neukonzeption der Datenverarbeitung beim MAD	Beratung und schriftliche Stellungnahme gegenüber dem BMVg
Einführung eines computergestützten Verfahrens der Eignungs- und Verwendungsprüfung nach dem Wehrpflichtgesetz	Beratung und schriftliche Stellungnahme gegenüber dem BMVg
Deutsche Bundespost	
— Telekommunikationsordnung	Beratung und schriftliche Stellungnahme gegenüber dem BMP und dem Verwaltungsrat der Deutschen Bundespost
— Temex-Dienst	Beratung und Mitwirkung im Begleitgremium
Bauwesen	
— Baugesetzbuch	Beratung und schriftliche Stellungnahmen gegenüber dem BMBau
— Durchführung des Wohnungsbindungsgesetzes	schriftliche Stellungnahme und Empfehlung gegenüber dem BMBau

Thema	Art der Erledigung
Bürokommunikationssystem des BMFT	Beratung des BMFT
Richtlinien für die Sicherheitsüberprüfung von Personal in kerntechnischen Anlagen	Beratung und schriftliche Stellungnahme des BMU
EDV-gestützte Rechnungsprüfung	Beratung des BRH
Datenschutz bei der Deutschen Bundesbahn	Beratung der Hauptverwaltung der Deutschen Bundesbahn
Bibliothekswesen	schriftliche Stellungnahme gegenüber der Stiftung Preußischer Kulturbereich
Grundfragen der Datenschutzgesetzgebung	Beratung ausländischer Regierungsstellen
Adressenhandel	Beratung des Data Registrar des Staates Israel
Automatisierung der Dateienübersicht gem. § 15 Nr. 1 BDSG; autom. Zugangskontrollsystem	Beratung der Bau-Berufsgenossenschaft Hamburg
Datenschutz in der Psychiatrie	Beratung von Klinikärzten
SCHUFA-Klauseln, SCHUFA-Verfahren	Zusammenarbeit mit den Aufsichtsbehörden der Länder, Beratung der Kreditwirtschaft, Beratung des Bundeskartellamtes
Datenschutz in der Versicherungswirtschaft	Zusammenarbeit mit den Aufsichtsbehörden der Länder, Beratung des Bundesaufsichtsamtes für das Versicherungswesen

Nicht aufgenommen in die vorstehende Zusammenstellung ist eine Vielzahl von Aktivitäten geringeren Umfangs, die jedoch in der Summe erhebliche Arbeitskapazität der Dienststelle beansprucht haben.

1.5 Kooperation

Als sehr wichtig erwies sich auch im Berichtsjahr die Zusammenarbeit und die Diskussion mit den Datenschutzbeauftragten der Länder und der Datenschutzkommission Rheinland-Pfalz. Die wichtigsten Diskussionsthemen waren hier

— die Novellierung der Datenschutzgesetze,

— die Datenschutzregelungen in den geplanten Sicherheitsgesetzen,

— Statistik und Volkszählung.

Dazu und zu anderen gemeinsam interessierenden Fragen hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder folgende in den Anlagen 1 bis 5 abgedruckte Entschließungen verabschiedet:

— Entschließung vom 27. Januar 1986 zu den Sicherheits- und Datenschutzgesetzen

— Entschließung vom 14. März 1986 zur Änderung des Bundesdatenschutzgesetzes

— Entschließung vom 14. März 1986 zum Datenschutz im Krankenhaus

— Entschließung vom 18. April 1986 zur Änderung des Bundesverfassungsschutzgesetzes

— Entschließung vom 18. April 1986 zum Entwurf einer Telekommunikationsordnung

Außerdem wurden auch viele Einzelfragen beraten und praktische Erfahrungen aus Prüfungen und Beratungen ausgetauscht.

Meine Mitarbeiter haben auch an den Beratungen des Düsseldorfer Kreises teilgenommen, in dem die Aufsichtsbehörden der Länder für den Datenschutz im nicht-öffentlichen Bereich ihre Erfahrungen austauschen, länderübergreifende Probleme diskutieren und gemeinsame Empfehlungen erarbeiten. Dominierende Themen waren

— die Datenverarbeitung der Kreditwirtschaft, insbesondere die Datenübermittlung an die SCHUFA und deren Übermittlungen an weitere Empfänger, und

— die zentralen Dateien der Verbände der Versicherungswirtschaft über die Versicherten, z. B. zur Erfassung von risikoreichen Sonderwagnissen oder zur Verhinderung von Doppelversicherungen.

Von den Kontakten zu Institutionen außerhalb der öffentlichen Verwaltung, die sich besonders um Datenschutz und Datensicherung bemühen, ist meine Mitarbeit in verschiedenen Normungsgremien des Deutschen Instituts für Normung e. V. (DIN) und in der Arbeitsgemeinschaft für wirtschaftliche Verwaltung e. V. (AWV) hervorzuheben. Gerade in diesen sehr unterschiedlich besetzten Arbeitsgremien, denen weniger an der Grundsatzdiskussion als an realisierbaren Lösungen und Hilfen für die praktische Arbeit gelegen ist, kommt es oft zu gegenseitigen Anregungen und zu Ergebnissen, die zur Anwendung in der Praxis empfohlen werden können. Dies gilt z. B. für die AWV-Schrift Nr. 400, einem Leitfaden für Datenschutz und Datensicherung bei dezentraler individueller Datenverarbeitung.

Schließlich konnte ich mich im Berichtsjahr anläßlich eines Besuches bei einem bedeutenden Hersteller von Datenverarbeitungsanlagen über die zu erwartende Entwicklung auf verschiedenen Gebieten der Datenverarbeitung informieren und meine Vorstellungen über die dabei auftretenden Datenschutz- und Datensicherheitsrisiken diskutieren. Ich beabsichtige, im nächsten Jahr auch diese Möglichkeit gegenseitiger Information weiter zu nutzen.

1.6 Öffentlichkeitsarbeit

Wie schon in den Vorjahren lag der Schwerpunkt meiner Öffentlichkeitsarbeit beim Versand der von mir herausgegebenen Broschüren

— Bürgerfibel Datenschutz,

— Der Bürger und seine Daten und

— Der Bürger und seine Daten im Netz der sozialen Sicherung.

Die Bürgerfibel Datenschutz wurde im Berichtsjahr überarbeitet. Insgesamt habe ich bisher mehr als 600 000 Exemplare dieser Broschüren versandt, häufig auf Einzelanfragen, aber auch für Unterrichtszwecke an Schulen, für Seminare und Kurse sowie für Firmen und Behörden, für deren Mitarbeiter und gelegentlich auch an öffentliche Büchereien.

Neben diesen allgemeinen Informationen versandte ich zur Information über meine Arbeit etwa 6 000 Exemplare meines Achten Tätigkeitsberichts und, soweit noch verfügbar, oft auch Tätigkeitsberichte aus zurückliegenden Berichtsjahren, wenn dies zur Beantwortung von Fragen zweckmäßig war.

Im Rahmen des Möglichen haben meine Mitarbeiter und auch ich selbst durch Veröffentlichungen, durch Vorträge und in Seminaren der Bundesakademie für öffentliche Verwaltung und anderer Bildungseinrichtungen über allgemeine oder aktuelle Probleme des Datenschutzes berichtet.

Weiter zugenommen hat die Betreuung von Besuchergruppen, die durch Vermittlung des Bundespresseamtes oder nach direkter Vereinbarung mit mir meine Dienststelle besuchen, um sich über den Datenschutz und die Mittel zu seiner Gewährleistung zu informieren. Die dabei geführten Gespräche mit politisch interessierten Bürgern sind für mich auch deswegen wichtig, weil im Rahmen der Korrespondenz häufig eine Beschwerde oder ein spezielles Anliegen im Vordergrund steht, dagegen Meinungen, Vermutungen und Erwartungen für die Zukunft kaum zur Sprache kommen. In den sehr offenen Diskussionen zeigt sich immer wieder ein wenig konkretes, aber von vielen Bürgern deutlich empfundenes Unbehagen an der Undurchsichtigkeit des Geflechts von Datenverarbeitungen, die das moderne Leben begleiten. Zugleich zeigt sich in diesen Gesprächen deutlich, daß die öffentliche Verwaltung, aber auch die großen Datenverarbeiter der privaten Wirtschaft ihre Datenverarbeitung zu wenig erläutern und damit ihren Beitrag zur Transparenz oft schuldig bleiben.

Im Berichtsjahr habe ich neben zahlreichen Presse- und Rundfunkinterviews, zu denen ich jeweils gebeten wurde, auf eigene Initiative zwei umfangreichere Presseerklärungen herausgegeben, und zwar zu meinem Achten Tätigkeitsbericht sowie zur Einbringung der Sicherheitsgesetze in den Deutschen Bundestag. Beide Erklärungen fanden in den Medien weitgehende Beachtung.

1.7 Die Dienststelle

Ich habe in den letzten Jahren wiederholt auf die angespannte Personalsituation in meiner Dienststelle aufmerksam gemacht (7. TB S. 6, 8. TB S. 4 f.). Dies hat dazu geführt, daß mir im Jahr 1986 — übrigens erstmalig seit der Aufbauphase der Dienststelle (1978 bis 1980) — eine Personalaufstockung bewilligt wurde. Im Jahr 1986 habe ich eine zusätzliche Stelle des höheren Dienstes und nunmehr für das Jahr 1987 eine weitere Stelle des gehobenen Dienstes erhalten. Für die Verbesserung der Arbeitsfähigkeit meiner Dienststelle bin ich dankbar. Sie reicht indessen nicht aus, um den — nicht zuletzt durch das Volkszählungsurteil des Bundesverfassungsgerichts verursachten — erhöhten Arbeitsanfall zu bewältigen.

Ich freue mich, daß der Deutsche Bundestag in seinem Beschluß vom 10. Dezember 1986 zu meinem Sechsten und Siebenten Tätigkeitsbericht auch meinen Mitarbeitern für die geleistete Arbeit gedankt hat, die sie zum Teil bis zur Grenze ihrer Belastbarkeit in Anspruch nahm, und daß auch zugleich die erhebliche Zunahme des Arbeitsanfalls Anerkennung gefunden hat. Ich erinnere an die verschiedenen Stellungnahmen, die ich gegenüber den Ausschüssen des Deutschen Bundestages auf deren Ersuchen abgegeben habe, an die Anhörungen, zu denen ich als Sachverständiger geladen wurde, sowie an die zahlreichen Beratungsersuchen von Bundesbehörden zu datenschutzrelevanten Regelungen und Vorhaben (siehe oben 1.4). Der Sechste und der Siebente Tätigkeitsbereich sind allein im Innenausschuß in dreizehn Sitzungen beraten worden, an denen ich teilgenommen habe. Alle diese Aktivitäten werden durch meine Mitarbeiter vorbereitet und unterstützt, die insoweit der eigentlichen Kontrolltätigkeit, die meinem Amt im Interesse der betroffenen Bürger aufgegeben ist, entzogen werden. Das Volkszählungsurteil des Bundesverfassungsgerichts hat zu einer umfangreichen Gesetzgebungstätigkeit geführt, an der ich — was ich begrüße — regelmäßig beteiligt werde; sie wird weiter anhalten. Durch die informationstechnische Entwicklung sind der Datenschutzkontrolle in unerwartetem Ausmaß zusätzliche Aufgaben zugewachsen. Die von mir in diesem wie schon in früheren Tätigkeitsberichten geschilderten Probleme bei dem sich rasch ausbreitenden Einsatz von Personal-Computern betreffen in besonderem Maße den Datenschutz und können nur durch verstärkte Kontrollen gelöst werden. Das gilt ebenso für die neuen Kommunikationsdienste, die von der Deutschen Bundespost angeboten werden, und für die Anwendungsplanungen im Zusammenhang mit dem neuen ISDN (Integrated Services Digital Network).

Für solche spezifischen Kontrollaufgaben steht mir qualifiziertes Personal nicht in ausreichendem Maße zur Verfügung. Nicht zu übersehen ist aber auch die aktuelle Ausdehnung der Datenverarbeitung auf anderen Gebieten. Als Beispiele nenne ich das Zentrale Verkehrsinformationssystem ZEVIS, dessen neu geschaffene gesetzliche Grundlagen ausdrücklich eine intensive Datenschutzkontrolle vorsehen, die Neuorganisation des Ausländerzentralregisters, den Ausbau der Datenverarbeitung bei den Sicherheitsbehörden, die Einführung des maschinell lesbaren Personalausweises und Passes, wodurch neue DV-Strukturen entstehen werden, und nicht zuletzt die bevorstehende Volkszählung, bei der die Bürger auf eine wirksame Datenschutzkontrolle, wie sie das Bundesverfassungsgericht verlangt hat, vertrauen. Ich kann diesen Erwartungen auf Dauer nur gerecht werden, wenn mir auch die dafür notwendige Personalkapazität zur Verfügung steht. Ich sehe mich deshalb gezwungen, noch weitere Personalforderungen zu stellen, und bitte den Deutschen Bundestag, mich dabei im Rahmen der Haushaltsentscheidungen zu unterstützen. Dies ist auch angesichts des Verhältnisses der Kosten meiner Dienststelle zu den Kosten der Datenverarbeitung der Bundesbehörden vertretbar. Denn eine zurückhaltende Schätzung aufgrund der Zahlen des Haushaltsplans für das Berichtsjahr zeigt, daß die Datenverarbeitungskosten der Bundesbehörden mehr als das Hundertfache des Gesamtetats meiner Dienststelle von ca. 2,7 Mio. DM betragen, wobei die ebenfalls meiner Kontrolle unterliegenden großen Bereiche Verteidigung, Polizei, Nachrichtendienste, Sozialversicherungsträger, Bahn, Post und Banken des Bundes sowie die Ausgaben für die überwiegend nicht personenbezogene Datenverarbeitung des Wetterdienstes und des Bundesministers für Forschung und Technologie noch nicht einmal einbezogen sind.

Seit Beginn der Tätigkeit des Bundesbeauftragten für den Datenschutz im Jahre 1978 wird zwischen dessen Dienststelle und dem Bundesministerium des Innern ein Personalverbund in der Weise praktiziert, daß die Planstellen beider Häuser gegenseitig genutzt werden. Das bedeutet, daß die Mitarbeiter des BfD in die Personalwirtschaft des BMI insoweit integriert sind, als sie hinsichtlich ihrer besoldungsmäßigen Einstufung und ihrer Beförderung den Bediensteten des BMI gleichgestellt und in den dortigen Dienstalters- und Beförderungslisten mitgeführt werden. Die Konsequenz daraus ist, daß das Personal des BfD zwar zahlenmäßig und laufbahnmäßig dem in Kapitel 06 07 ausgebrachten Stellenplan entspricht, nicht aber im Einzelfall auch dem Stellenplan entsprechend eingestuft sein muß. So wird beispielsweise ein Berufsanfänger nicht höher als ein vergleichbarer Beamter im BMI eingestuft, auch wenn im Stellenplan des BfD eine besser dotierte Stelle vorhanden ist, während ein dienstälterer Beamter auch ohne entsprechende Planstelle befördert werden kann. In diesen Beispielsfällen werden Stellen des BMI in Anspruch genommen, während dieser seine entsprechend eingestuften Beamten auf Stellen des BfD führt. Diese allgemein als „Topfwirtschaft" bezeichnete Praxis hat sich bewährt, weil es damit möglich ist, in der verhältnismäßig kleinen Dienststelle des BfD eine Flexibilität in der Personalwirtschaft zu erreichen, die sonst nur in einem großen Haus besteht. Es wird dadurch auch möglich, gerade für die Aufgaben des BfD besonders qualifiziertes Personal zu gewinnen bzw. zu behalten, auch wenn nach dem eigenen Stellenplan des BfD die entsprechende Einstufung nicht möglich wäre. Auch wird Bediensteten, die sich verändern wollen, der Wechsel vom BfD zum BMI und umgekehrt leichter möglich sein, wenn ihre bisherige berufliche Entwicklung infolge einer einheitlichen Personalwirtschaft gleichartig verlaufen ist.

Diese Praxis wurde von meinem Amtsvorgänger schon im Jahre 1978 mit dem Bundesminister des Innern vereinbart. Rechtliche Bedenken wurden nicht gesehen, weil nach § 17 Abs. 5 Bundesdatenschutzgesetz der BfD beim BMI eingerichtet ist, der Dienstaufsicht des BMI untersteht und dieser dem BfD die für die Erfüllung seiner Aufgaben notwendige Personalausstattung zur Verfügung zu stellen hat. Es ist unbestritten, daß die Mitarbeiter des BfD Angehörige des BMI sind, so daß es naheliegt, wenn nicht sogar geboten ist, sie personalwirtschaftlich mit den anderen Beamten des BMI gleichzustellen.

Im Berichtsjahr hat der Bundesminister der Finanzen haushaltsrechtliche Bedenken gegen diese bisher unangefochtene Praxis erhoben. Sie wurden letztlich dadurch ausgeräumt, daß in den Bundeshaushalt 1987 ein Haushaltsvermerk des Inhalts aufgenommen wurde, daß die in Kap. 06 01 (BMI) und Kap. 06 07 (BfD) ausgebrachten Planstellen und Stellen „in gegenseitigem Einvernehmen im jeweils anderen Kapitel genutzt" werden können. Diese Formulierung entspricht der im Gesetzentwurf zur Änderung des Bundesdatenschutzgesetzes (Drucksachen 10/4737 und 10/5343) vorgesehenen Neufassung des § 17 Abs. 5 BDSG, wonach die Stellen des Bundesbeauftragten im Einvernehmen mit ihm zu besetzen sind. Über die Ausübung der sich nach meiner Auffassung daraus ergebenden Mitwirkungsrechte des Bundesbeauftragten an Entscheidungen, die sein Personal und seine Stellen betreffen, stehe ich noch in Verhandlungen mit dem Bundesminister des Innern. Die Handhabung des Haushaltsvermerks muß jedenfalls sicherstellen,

- daß die Mitarbeiter des BfD hinsichtlich ihrer beruflichen Entwicklung und ihrer Beförderungschancen gegenüber den im BMI tätigen Bediensteten nicht benachteiligt werden,
- daß die vom Deutschen Bundestag mit Bedacht und unter Berücksichtigung meiner gesetzlichen Aufgaben zugewiesenen Planstellen im ganzen gesehen nicht auf Dauer unterhalb der im Stellenplan vorgesehenen Einstufung besetzt sind
- und daß durch Personalentscheidungen weder meine Unabhängigkeit beeinträchtigt noch die Arbeitsfähigkeit meiner Dienststelle geschwächt werden.

Im Zusammenhang mit diesen Fragen stand auch eine am 29. Juli 1986 eingebrachte Kleine Anfrage der Fraktion der SPD (Drucksache 10/5895) zur „Unabhängigkeit des Bundesbeauftragten für den Datenschutz". Die in der Kleinen Anfrage zum Aus-

druck kommende Kritik an Personalentscheidungen, die meine Dienststelle betreffen, sowie an dem geschilderten Personalverbund mit dem BMI erweckte den Eindruck, als sei meine Unabhängigkeit dadurch beeinträchtigt worden und müsse erst wieder hergestellt werden. Dem ist die Bundesregierung in ihrer Antwort (Drucksache 10/5922) entgegengetreten und hat festgestellt, daß meine Unabhängigkeit zu keiner Zeit in Frage gestellt war. Ich möchte diese Feststellung hier ausdrücklich und mit Nachdruck bestätigen: Die mir gesetzlich zugesicherte Unabhängigkeit der Amtsführung ist weder durch Personalmaßnahmen noch auf andere Weise durch die Bundesregierung beschränkt worden.

2. Neue Informations- und Kommunikationstechniken für den Deutschen Bundestag (PARLAKOM)

In den vergangenen Jahren sind auch in der Öffentlichkeit Äußerungen von Mitgliedern des Deutschen Bundestages über deren schwierige technisch-organisatorische Arbeitsbedingungen bekanntgeworden. Insbesondere wurden unzureichende Möglichkeiten beklagt, auf Informations- und Dokumentationsdienste zugreifen und sich schneller technischer Kommunikation bedienen zu können. Im Mai 1984 beschloß daher der Ältestenrat die Einsetzung einer Kommission, die klären sollte, wie Abgeordnete durch neue Informations- und Kommunikationstechniken unterstützt werden können. Auf der Grundlage einer von zwei Beratungsfirmen im Auftrag der Kommission erstellten Studie beschloß der Ältestenrat des Deutschen Bundestages am 27. Februar 1986, zur Verbesserung der Arbeitsmöglichkeiten und Arbeitsbedingungen seiner Mitglieder und der Mitarbeiter ein gemeinsames Informations- und Kommunikationssystem für das Parlament, die Fraktionen und die Wahlkreisbüros der Abgeordneten einzuführen (PARLAKOM). In einem Modellversuch sollen mindestens fünfzig Abgeordnetenbüros und eine geeignete Anzahl Büros in Ausschüssen, Fraktionen usw. mit entsprechenden technischen Einrichtungen ausgestattet werden.

Das technische Konzept von PARLAKOM sieht vor, die Abgeordnetenbüros mit kommunikationsfähigen Bildschirm-Terminals auszustatten, die eigene Verarbeitungs- und Speicherkapazität und jeweils einen eigenen Drucker haben sollen. Diese Konfiguration soll nicht nur eine komfortable Text- und Informationsverarbeitung im Büro ermöglichen, sondern auch Auswertungen für eigene Informationssammlungen (Termine, Adressen usw.) sowie die Unterstützung der individuellen Archivierung von Materialien. Die vorgesehene Kommunikationsfähigkeit der Geräte soll zum einen den Zugang zu bestehenden Datenbanken eröffnen wie z. B. zu JURIS, STATIS-BUND usw. Zum anderen sollen die Geräte dem Teletex-Standard der Deutschen Bundespost entsprechen, so daß nicht nur komfortabel und schnell „elektronische Briefe" verschickt, sondern auch Mitteilungsdienste — wie etwa der Telebox-Dienst der Deutschen Bundespost — benutzt werden können. Die Verbindung der Bildschirmarbeitsplätze untereinander sowie die Verbindung mit dem Leitungsnetz der Deutschen Bundespost erfolgt mittels einer ISDN-Nebenstellenanlage. Hierbei handelt es sich um eine elektroniche Datenverarbeitungsanlage, die — als technische Weiterentwicklung der bekannten relais- oder wählergesteuerten Telefonzentralen — den Vorschriften der Deutschen Bundespost für das geplante digitale diensteintegrierte Datennetz (Integrated Services Digital Network — ISDN) entspricht.

Aus der Sicht des Datenschutzes weist ein parlamentarisches Informations- und Kommunikationssystem wie PARLAKOM eine Reihe von Besonderheiten auf, die sich in anderen Nutzungsbereichen der verwendeten Technik nicht oder nur in wesentlich geringerem Umfang als Problem darstellen. Keiner Diskussion bedarf, daß an die technisch-organisatorischen Sicherungsmaßnahmen gegen unbefugte Kenntnisnahme, Veränderung oder Übermittlung der im Abgeordneten-Terminal verarbeiteten Daten besonders hohe Anforderungen zu stellen sind. Diese können durch extensive Anwendung bekannter Verfahren erfüllt werden. Bei allen Sicherungsmaßnahmen ist jedoch zu beachten, daß die Mehrzahl der Teilnehmer an PARLAKOM nicht Beschäftigte der das System betreibenden Stelle sind, sondern Abgeordnete, deren verfassungsrechtlicher Status Maßnahmen ausschließt, die zu einer Beeinträchtigung ihrer Unabhängigkeit führen könnten.

Im Oktober 1986 bat mich die Vorsitzende der Ältestenratkommission, Frau Abgeordnete Dr. Skarpelis-Sperk, kurzfristig um meine Beratung zu PARLAKOM. In der zur Verfügung stehenden Zeit war mir allerdings eine umfassende Stellungnahme nicht möglich, so daß ich mich auf einige grundsätzliche Bemerkungen sowie Hinweise zu Einzelpunkten beschränken mußte. Ich habe u. a. betont, daß bereits für die Durchführung des Modellversuchs ein Konzept zur Datensicherung vorliegen muß, das Maßnahmen zur Sicherung der zu verarbeitenden Daten vorsieht. Dies gilt sowohl für die Einrichtung der Infrastruktur als auch für die Beratung der Anwender, weil auch die Formen einer sinnvollen Beratung erprobt und geübt werden müssen. Darüber hinaus habe ich angeregt, Prinzipien für die Zulässigkeit der Verarbeitung personenbezogener Daten zu entwickeln, die sowohl den Anforderungen der Abgeordneten des Deutschen Bundestages und ihrer Mitarbeiter als auch dem informationellen Selbstbestimmungsrecht der betroffenen Bürger gerecht werden.

Bei der Auswahl und Erprobung von Sicherungsmaßnahmen sollte besonders darauf geachtet werden, daß die notwendigen Maßnahmen zur Systemüberwachung (Protokollierung von Aktivitäten) die Unabhängigkeit des einzelnen Parlamentariers nicht beeinträchtigen dürfen. Auch ist zu berücksichtigen, daß Online-Zugriffe der Parlamentarier und ihrer Mitarbeiter auf externe Datenbanken, z. B. die von Ministerien oder des Bundespresseam-

tes, dort zwecks Sicherung der angesprochenen Systeme möglicherweise protokolliert werden. Insgesamt halte ich schon aus diesen Gründen die Konzeption von PARLAKOM für so komplex, daß ihre Realisierung sehr behutsam und in kleinen Schritten erfolgen sollte, auch um eine schnelle Reaktion auf eventuelle Fehlentwicklungen zu ermöglichen.

Ich habe zugesagt, mich auf Wunsch der Kommission an der weiteren Diskussion zu einem integrierten Datenschutz- und Datensicherungskonzept beratend zu beteiligen.

3. Innere Verwaltung

3.1 Neue Personalausweise und Pässe

Mit dem Zweiten Gesetz zur Änderung personalausweisrechtlicher Vorschriften vom 19. April 1986 und mit dem Paßgesetz und Gesetz zur Änderung der Strafprozeßordnung vom 19. April 1986 ist meine Beratungstätigkeit in bezug auf die datenschutzgerechte Gestaltung der nunmehr verabschiedeten Bundesgesetze vorläufig abgeschlossen. Sie erstreckte sich über mehrere Jahre (vgl. 8. TB S. 8 ff.; 7. TB S. 7 ff.; 6. TB S. 6 ff.) und führte gegenüber früheren Regelungen und Entwürfen zu einer Reihe von Verbesserungen. In einigen Punkten, in denen meine Empfehlungen nicht berücksichtigt wurden, betrachte ich dagegen die Gesetze unter datenschutzrechtlichen Gesichtspunkten noch nicht als befriedigend.

Positiv bewerte ich vor allem

- die abschließende Bestimmung der in den Ausweisen enthaltenen Daten,
- die eindeutige Regelung der Zusammensetzung der Seriennummer,
- das Verbot der Speicherung der Seriennummer im Melderegister (ab 1. September 1991),
- die Beschränkung einer Datenspeicherung bei der Bundesdruckerei nach Herstellung der Ausweise auf den Nachweis ihres Verbleibs,
- die engen Beschränkungen der Verwendung der Seriennummer zum Abruf personenbezogener Daten,
- die Beschränkungen der behördlichen Verwendung der Ausweise zum automatischen Abruf personenbezogener Daten sowie zur Datenspeicherung beim automatischen Lesen auf gesetzlich zugelassene Ausnahmefälle,
- das Verbot des automatischen Lesens der Ausweise im nicht-öffentlichen Bereich.

Schwächen in den genannten Bundesgesetzen sehe ich dagegen in folgenden Punkten:

- Für die Zulassung des automatischen Lesens der Ausweise fehlt es — zumal angesichts des weiteren Abbaus der Grenzkontrollen — an einer überzeugenden Begründung.
- Die in den genannten Gesetzen enthaltenen Regelungsansätze zur Verwendungsbeschränkung der in den Ausweisregistern gespeicherten Daten sind unzureichend, weil ausdrücklich zugelassen wird, daß die Erhebung, Übermittlung, sonstige Verarbeitung oder Nutzung dieser Daten auch durch andere Gesetze oder Rechtsverordnungen bestimmt werden können.
- Das (ab 1. September 1991 geltende) Verbot der Speicherung der Seriennummer im Melderegister ist zu eng; es fehlt ein Gesetzesvorbehalt für die Aufnahme der Seriennummer in andere Datensammlungen.
- Mit der Einfügung eines neuen § 163d in die Strafprozeßordnung ist die Speicherung automatisch gelesener Daten aus Anlaß von Personenkontrollen — Protokollierung zur sog. Schleppnetzfahndung — zugelassen, wenn der Verdacht besteht, daß bestimmte schwerwiegende Straftaten begangen worden sind. Während die Errichtung derartiger Dateien zunächst nur dann vorgesehen war, wenn ohne sie die Aufklärung oder Verhütung der Straftat aussichtslos oder wesentlich erschwert wäre, verlangt das Gesetz nunmehr lediglich, daß die Maßnahme erfolgversprechend und nicht unverhältnismäßig ist.
- Die Regelung des § 163d StPO erlaubt zudem neben der Speicherung von Identitätsdaten, die dem maschinenlesbaren Ausweis entnommen werden können, die Speicherung von „Umständen, die für die Aufklärung der Straftat oder für die Ergreifung des Täters von Bedeutung sein können". Sie ermöglicht dem kontrollierenden Beamten damit praktisch die Speicherung jeder Art von Informationen, und dies unabhängig von einem Tatverdacht gegen den Betroffenen.
- Die Frage, ob eine durch den Staatsanwalt angeordnete Speicherung personenbezogener Daten für das Strafverfahren genutzt werden darf, wenn die gesetzlich vorgesehene richterliche Bestätigung deshalb unterbleibt, weil die Maßnahme inzwischen beendet ist — etwa weil sie zum Erfolg geführt hat oder aber sich als nicht mehr erfolgversprechend erwiesen hat —, sollte eindeutig gesetzlich geregelt werden.
- Eine Verwendung von Zufallsfunden sollte auf die Verfolgung derjenigen Straftaten beschränkt sein, die bei begründetem Verdacht nach § 163d StPO die Anordnung einer Protokollierungsmaßnahme erlauben würden (vgl. auch unter Nr. 4.2 Überlegungen zu Datenschutzregelungen im Strafverfahren).

Nach Erlaß der genannten Bundesgesetze richtet sich meine Beratungstätigkeit auf den Vollzug der Vorschriften.

Die Bundesdruckerei hat im Oktober 1986 einen Betriebsversuch zur Vorbereitung der Herstellung der neuen Ausweise durchgeführt. Ich habe sie dabei datenschutzrechtlich beraten. Ich begrüße es, daß entsprechend meinen Anregungen im Februar 1987 noch ein Probebetrieb unter Einbeziehung der Personalausweisbehörden stattfinden soll.

Mit dem Bundesminister des Innern und mit der Bundesdruckerei habe ich über Vorkehrungen gesprochen, die die laufende Vergabe der Ausweisnummer (§ 1 Abs. 3 Nr. 5 des Gesetzes über Personalausweise und § 4 Abs. 2 Nr. 6 des Paßgesetzes) sicherstellen bzw. die Aufdeckung einer etwaigen Mehrfachvergabe ermöglichen. Erfreulicherweise wurde hierbei — soweit es um die Mitverantwortung des Bundes geht — ein Einvernehmen über das notwendige Vorgehen erzielt.

Außerdem habe ich dem Bundesminister des Innern empfohlen, in Abstimmung mit den Innenressorts der Länder darauf hinzuwirken, daß — in Anlehnung an § 6 Abs. 3 des Paßgesetzes — in allen Landesausführungsgesetzen zum Personalausweisgesetz eine entsprechende gesetzliche Klarstellung zu dem bislang nur in internen Verwaltungsvorschriften geregelten Personenfeststellungsverfahren erfolgt. Wenn die Polizei zur Unterstützung bei der Identitätsfeststellung herangezogen wird, gelangt sie in den Besitz von wichtigen Daten des Betroffenen wie Lichtbildaufnahmen, Fingerabdrücke etc. Auf meine Empfehlung schreibt § 6 Abs. 3 des Paßgesetzes in diesen Fällen vor, daß nach Feststellung der Identität die im Zusammenhang hiermit angefallenen Unterlagen zu vernichten sind und über die Vernichtung eine Niederschrift anzufertigen ist. Dieser Regelung lag die Sorge zugrunde, daß die angefallenen Unterlagen u. U. zweckfremd verwendet und/oder ohne Erforderlichkeit weiter aufbewahrt werden könnten. Die Vorschrift ist bewußt so allgemein gehalten, daß sie gleichermaßen für die Polizeibehörden wie auch für die Paßbehörden gilt. Ein Auseinanderfallen der gesetzlichen Bestimmungen für gleichartige Sachverhalte nach dem Paßgesetz und dem Personalausweisgesetz wäre mißlich und könnte zu Auslegungsschwierigkeiten führen. Deshalb begrüße ich es, daß der Bundesminister des Innern meine Auffassung teilt und die Innenminister bzw. -senatoren der Länder gebeten hat, in die Personalausweisgesetze der Länder eine dem § 6 Abs. 3 Sätze 2 bis 5 PaßG entsprechende Regelung aufzunehmen.

Weiterhin haben mich Regelungsentwürfe der Länder veranlaßt, dem Bundesminister des Innern zu empfehlen, in Abstimmung mit den Innenressorts der Länder darauf hinzuwirken, daß ein eigenes Datenübermittlungsverfahren zwischen den beteiligten Personalausweisbehörden unterbleibt. Ein solches ist nicht erforderlich und m. E. auch nicht zulässig. Die den Ausweis ausstellende Personalausweisbehörde kann nach einem Umzug des Ausweisinhabers die von ihr nach § 2a Abs. 1 Nr. 1 in Verbindung mit § 1 Abs. 2 Nr. 8 Personalausweisgesetz zu speichernde gegenwärtige (neue) Anschrift gemäß § 2b Abs. 4 von der für sie zuständigen Meldebehörde erfahren. Diese kennt die gegenwärtige Anschrift aufgrund der Rückmeldung nach § 17 Abs. 1 Melderechtsrahmengesetz (MRRG). Nach § 1 Abs. 2 i. V. m. § 18 Abs. 1 MRRG gehört die Unterrichtung anderer Behörden, also auch der Personalausweisbehörde, zu den ausdrücklichen Aufgaben der Meldebehörden. Durch das Melderechtsrahmengesetz ist ferner festgelegt, daß Datenübermittlungen einer formellen Rechtsgrundlage bedürfen; das gilt insbesondere für regelmäßige Datenübermittlungen (§ 18 Abs. 4 MRRG). Eine solche Rechtsgrundlage für ein eigenes Datenübermittlungsverfahren zwischen den beteiligten Personalausweisbehörden ist nicht vorhanden; es besteht auch kein Bedürfnis dafür. Auch in diesem Punkte habe ich ein Einvernehmen mit dem Bundesminister des Innern erreicht. Auf meine Empfehlung hin hat er die Innenressorts der Länder davon unterrichtet, daß ein Änderungsdienst zum Personalausweisregister zwischen den Personalausweisbehörden nicht erforderlich ist.

Mit Bedauern habe ich dagegen festgestellt, daß die Verordnung zur Bestimmung der Muster der Personalausweise vom 2. Juli 1986 den nach der früheren Verordnung bislang auf der Rückseite der Ausweise vorgesehenen Hinweis auf Beschränkungen der automatischen Verwendung nicht mehr enthält. Der Bundesminister des Innern hat mich bei der Vorbereitung dieser Entscheidung nicht beteiligt, obwohl ich mich in früheren Erörterungen für den bislang vorgesehenen Hinweis besonders eingesetzt hatte (vgl. 3. TB S. 14). Die hierfür gegebene Begründung, daß nämlich eine Zitierung des neugefaßten § 3a des Gesetzes über Personalausweise aus Raumgründen weder möglich noch sinnvoll sei, überzeugt mich nicht. Einen in verkürzter Form durchaus möglichen Hinweis auf bestehende Verwendungsbeschränkungen bei automatischer Nutzung des Ausweises halte ich nach wie vor für angemessen.

3.2 Ausländerzentralregister

Anknüpfend an meine früheren Äußerungen zur Neukonzeption des Ausländerzentralregisters — AZR — (5. TB S. 15f., 6. TB S. 9, 7. TB S. 10, 8. TB S. 10f.) lassen sich auch für das zurückliegende Jahr Arbeitsfortschritte berichten; eine wichtige Phase der Bemühungen steht mit der vom Bundesminister des Innern in Angriff genommenen Vorbereitung einer gesetzlichen Regelung aber erst noch bevor. Der vom Bundesminister des Innern auf der Basis der Beratungsergebnisse der von ihm eingesetzten Arbeitsgruppe erstellte „Bericht über die Neukonzeption des AZR" enthält hierfür erfreuliche Ansätze: Nicht nur die Speicherung der Daten im Register selbst, sondern auch ihre Anlieferung und Weitergabe an andere Dienststellen sollen gesetzlich geregelt werden. Nur wenn die Datenverarbeitung klar und eindeutig festgelegt wird, kann der Betroffene den Eingriff in sein Recht auf informationelle Selbstbestimmung einschätzen. Aus Gründen der Bestimmtheit der Zwecke bedarf es auch einer Regelung des Ausmaßes der Datennutzung durch die Datenempfänger. So ist namentlich der Datenaustausch zu Fahndungszwecken und zur Erfüllung anderer polizeilicher Aufgaben gesetzlich zu regeln, wobei noch zu prüfen sein wird, ob dies in dem vorgesehenen Registergesetz selbst oder aber in der Strafprozeßordnung bzw. in den Polizeigesetzen zu erfolgen hat. Schon jetzt ist m. E. auch die Notwendigkeit abzusehen, parallel zu der Schaffung registerrechtlicher Regelungen das Ausländer-

recht hinsichtlich der zu verarbeitenden Daten einer Überarbeitung zu unterziehen.

In meiner Stellungnahme zu dem Bericht des Bundesministers des Innern habe ich herausgestellt, daß Hinweise auf die Funktion des AZR als eines zentralen Melderegisters nicht ausreichen, um die zentrale Datenspeicherung im vorgesehenen Umfange zu rechtfertigen. Damit läßt sich lediglich das Grundprinzip des AZR als eines Hinweissystems begründen, in dem Identifizierungsdaten gespeichert und die in bezug auf den Ausländer tätig gewordenen Behörden angegeben werden. Eine hierüber hinausgehende Datenspeicherung und -nutzung kann unter dem Gesichtspunkt eines überwiegenden Allgemeininteresses nur dann und insoweit in Betracht kommen, als bestimmte Behörden in bezug auf Ausländer rasche Entscheidungen zu treffen haben, die es aus zeitlichen Gründen durchweg nicht erlauben, erst Auskünfte bzw. Unterlagen von bereits tätig gewordenen Behörden einzuholen. Nur unter solchen Voraussetzungen kommt zusätzlich eine zentrale Speicherung von Daten in Betracht, die im Regelfall den Rückgriff auf Ausgangsunterlagen entbehrlich macht. Demgegenüber sollte der Benutzer auch aus dem Register entnehmen können, in welchen Einzelfällen die Beiziehung der Akten geboten erscheint.

Der Bundesminister des Innern hat sich in einer ergänzenden Überarbeitung seines Berichts diese Überlegungen zu eigen gemacht. Einer kritischen Betrachtung bedarf besonders das Datum „Einreisebedenken". Damit wird auf Vorgänge im Umfeld des Ausländers hingewiesen, die noch keine ausländerrechtlichen Maßnahmen ausgelöst haben, wohl aber für ausländerrechtliche Entscheidungen relevant sein und insbesondere Gründe gegen eine (erneute) Einreise ergeben könnten. Der Mangel an Genauigkeit dieses Datums bedingt es nach meiner Auffassung, daß z. B. ein bei einer Grenzpolizeibehörde beantragter Ausnahmesichtvermerk nicht ohne Hinzuziehung der zugrundeliegenden Akte versagt werden kann. Die Voraussetzungen der Entstehung dieses Datums sowie seiner Verwendung bedürfen der Präzisierung. Dabei verkenne ich nicht, daß sich diese Regelung in denjenigen Fällen positiv auswirken wird, in denen in diesem Datenfeld keine Eintragung vorliegt, und dies dürfte die große Mehrheit sein. Wenn nämlich das Datum „Einreisebedenken" nicht belegt ist, besteht die Möglichkeit, etwa über einen Ausnahmesichtvermerk in einem beschleunigten Verfahren zu entscheiden, ohne daß auf die Ausgangsunterlagen zurückgegriffen werden muß.

In den Erörterungen mit den Landesbeauftragten für den Datenschutz hat sich die Frage ergeben, ob EG-Angehörigen nach geltenden EG-Regelungen bzw. nach dem Aufenthaltsgesetz/EWG (vgl. § 1 und § 2 Abs. 1) im Rahmen einer Grenzkontrolle die Einreise wegen Einreisebedenken verwehrt werden kann. In diesem Zusammenhang stellt sich auch die Frage, ob der Rechtsanspruch von EG-Angehörigen auf Erteilung der Aufenthaltserlaubnis (vgl. §§ 3 ff. a. a. O.) durch Einreisebedenken tangiert werden kann. Davon hängt es ab, ob eine Datenspeicherung in diesem Datenfeld bzw. der Zugriff auf diese Daten bei EG-Angehörigen zulässig ist. Auch zu dieser Frage habe ich gegenüber dem Bundesminister des Innern eine Prüfung und weitere Erörterung angeregt.

3.3 Personenstandswesen

In früheren Tätigkeitsberichten (vgl. 6. TB S. 12, 7. TB S. 11) habe ich über meine Empfehlungen für eine bereichsspezifische Regelung der Mitteilungen im Personenstandswesen berichtet, die ich dem Bundesminister des Innern nach Abstimmung mit den Datenschutzbeauftragten der Länder gegeben habe. Inzwischen hat der BMI, gestützt auf die Beratungen einer Bund-Länder-Arbeitsgruppe, einen Vorentwurf für ein Fünftes Gesetz zur Änderung und Ergänzung des Personenstandsgesetzes (5. PStÄndG) erarbeitet. Im Zusammenwirken mit den Datenschutzbeauftragten der Länder bereite ich hierzu eine Stellungnahme vor, die dem Bundesminister noch vor der Erstellung eines Referentenentwurfs zugehen soll.

In dem folgenden Punkt habe ich mich aber schon jetzt zu einer Äußerung veranlaßt gesehen: Der Bundesminister der Finanzen fordert, in das Personenstandsgesetz eine Bestimmung aufzunehmen, die dem Standesbeamten auferlegt, dem zuständigen Finanzamt „Sterbefälle nach dem hierfür maßgebenden Muster des Erbschaftssteuer- und Schenkungssteuergesetzes oder der Durchführungsverordnung zu diesem Gesetz in der jeweils geltenden Fassung mitzuteilen". Das bedeutet, daß in den sogenannten Totenlisten Informationen nicht nur über Todesfälle, sondern auch über den Nachlaß und den Nachlaßwert gegeben werden. Hiergegen bestehen die folgenden Bedenken:

Die Problematik verlangt im Rahmen der Neuregelung der Mitteilungspflichten eine grundlegende Entscheidung und berührt wesentliche Fragen des Datenschutzes. Während es sich nämlich bei den herkömmlichen Mitteilungen der Standesbeamten um Personenstandsdaten handelt, die der Standesbeamte im Rahmen der rechtmäßigen Erfüllung der in seiner Zuständigkeit liegenden Aufgaben erhebt oder über die er im Rahmen seiner Tätigkeit verfügt, geht es bei den Fragen nach Nachlaß und Nachlaßwert um Informationen, die er selbst für die Erfüllung seiner Aufgaben nicht benötigt. Die Erhebung und Weitergabe solcher Daten steht — angesichts der Art dieser Daten — auch zum tradierten Amtsverständnis des Standesbeamten im Widerspruch, denn hier wird ihm nicht lediglich eine Weitergabe vorhandener Personenstandsdaten, sondern eine Datenerhebung für fremde Zwecke zur Pflicht gemacht. Ich rate davon ab, den Standesbeamten gewissermaßen als Hilfsbeamten der Finanzbehörde zur Erhebung steuerrelevanter Vermögensdaten einzusetzen.

Muß eine Verpflichtung des Standesbeamten zur Erhebung von Steuerdaten schon aus grundsätzlichen Erwägungen auf Bedenken stoßen, so sprechen auch die mir vorliegenden Erkenntnisse aus

der Praxis dagegen, die Standesbeamten mit einer solchen Aufgabe zu betrauen. In einem Schreiben des Niedersächsischen Ministers der Finanzen an den Bundesminister der Finanzen vom 17. Februar 1986 heißt es u. a.:

„Wie mir die Oberfinanzdirektion Hannover hierzu berichtet hat, wird die Frage nach dem Nachlaß und dem Nachlaßwert von den Standesämtern nur noch in wenigen Fällen beantwortet ... Die niedersächsischen Finanzämter ermitteln die Besteuerungsgrundlagen daher hauptsächlich nach den Angaben der Nachlaßgerichte und der Vermögensverwahrer. Die gegenwärtige Regelung führt somit nur noch zu ‚Zufallsfunden'."

Nach den Feststellungen des Niedersächsischen Datenschutzbeauftragten wird die sog. Totenliste in der Praxis fast ausnahmslos vom beauftragten Bestattungsunternehmen ausgefüllt; der Standesbeamte kann allenfalls durch dieses Daten über Nachlaß und Nachlaßwert erfahren. Die Erhebung dieser Daten bei den Hinterbliebenen ist aber unter den besonderen Umständen eines Sterbefalles entweder nicht möglich oder nicht zumutbar; sie wird von den Bestattungsunternehmen selbst als peinlich empfunden, die hier gleichsam im staatlichen Auftrag tätig werden müßten. Mich überrascht nicht, daß die so ermittelten Angaben zum Nachlaß und zum Nachlaßwert — wie der Niedersächsische Datenschutzbeauftragte bei einer Vielzahl von Standesämtern festgestellt hat — fast durchweg falsch, zumindest aber unzuverlässig sind. So erscheint es mir auch verständlich, daß die Standesbeamten die Frage nach dem Nachlaß und dem Nachlaßwert zunehmend nicht beantworten bzw. „unbekannt" eintragen.

Eine Verpflichtung des Standesbeamten zur Erhebung und Übermittlung von Angaben zum Nachlaß und zum Nachlaßwert begegnet im übrigen auch rechtlichen Bedenken. Der Vorschlag des Bundesministers der Finanzen soll der Vermeidung von „Mißverständnissen zwischen den Standesämtern und den Erbschaftssteuer-Finanzämtern über den Umfang der Anzeigepflichten" dienen. Doch die Formulierung „beurkundete Sterbefälle nach dem hierfür maßgebenden Muster des Erbschaftssteuer- und Schenkungssteuergesetzes oder der Durchführungsverordnung" entbehrt erst recht der Normenklarheit und erweckt den Anschein, als handele es sich um Personenstandsdaten, die Gegenstand standesamtlicher Beurkundung sind, während der Bundesminister der Finanzen tatsächlich Vermögensdaten, nämlich Angaben über den Nachlaßwert, meint. Er hat in seiner Erwiderung auf meine Bedenken auf den Untersuchungsgrundsatz des § 88 Abs. 1 Satz 1 Abgabenordnung (AO) hingewiesen, der die Finanzbehörde zu derjenigen Sachverhaltsaufklärung verpflichtet, die erforderlich sei, um die Gleichmäßigkeit der Besteuerung zu gewährleisten; die Finanzbehörde handele daher in Erfüllung ihres gesetzlichen Auftrages, wenn sie von den Standesämtern Auskünfte über erbschaftssteuerrelevante Ermittlungsgrundlagen verlange. Dieser Auffassung muß m. E. das in § 93 Abs. 1 Satz 3 AO verankerte Subsidiaritätsprinzip entgegengehalten werden, das allgemein als eine Konkretisierung des Verhältnismäßigkeitsgsrundsatzes verstanden wird. Hiernach dürfen andere Personen und Stellen als die Beteiligten erst dann zur Auskunft angehalten werden, wenn die Sachverhaltsaufklärung durch die Beteiligten nicht zum Ziele führt oder keinen Erfolg verspricht. Dieser Rechtsgedanke muß hier entsprechend gelten, zumal, wie im vorliegenden Falle, Dritte nicht nur zu einer Auskunft, sondern sogar zur Erhebung der gewünschten Informationen herangezogen werden sollen.

Der Bundesminister des Innern hält eine weitere Erörterung dieser Problematik für notwendig und weist zu Recht darauf hin, daß die Menschen meistens in Krankenhäusern oder ähnlichen Einrichtungen sterben, der Standesbeamte also nur in wenigen Fällen unmittelbar von Angehörigen Auskünfte für die Totenliste einholen könne. Die Angehörigen des Toten seien nicht verpflichtet, dem Standesbeamten Auskünfte für Steuerzwecke zu erteilen; gleiches gelte für die genannten Anstalten und für die Bestattungsunternehmen. Der Landesbeauftragte für den Datenschutz in Schleswig-Holstein hat vorgeschlagen, die Finanzbehörden sollten ein Formblatt mit entsprechenden Erläuterungen entwerfen, in das die Hinterbliebenen die zu erhebenden Vermögensdaten eintragen müssen. Die Pflicht des Standesbeamten könnte sich darauf beschränken, dieses Formblatt den Betroffenen auszuhändigen, die dieses ausgefüllt direkt an die zuständigen Finanzbehörden zurückzugeben hätten. Ich unterstütze diesen Vorschlag.

Was die gegenwärtige Rechtslage anbelangt, so teile ich die Auffassung des Niedersächsischen Datenschutzbeauftragten, daß die Erbschaftssteuerdurchführungsverordnung, die in dem Formularmuster 3 zu § 9 detaillierte Fragen nach dem Nachlaß und Nachlaßwert enthält, der Verordnungsermächtigung des § 34 Erbschaftssteuergesetz nicht entspricht. Diese Gesetzesvorschrift begründet lediglich eine Verpflichtung der Standesämter, Sterbefälle anzuzeigen. Eine Mitteilung von Angaben zum Nachlaß und zum Nachlaßwert läßt sich auch bei großzügiger Auslegung nicht als eine Sterbefall-Anzeige deuten. Ebensowenig vermag ich die Überlegung des Bundesministers der Finanzen zu teilen, die Verordnungsermächtigung des § 36 Abs. 1 Nr. 1 ErbStG „zur Vereinfachung des Besteuerungsverfahrens" sei eine geeignete Grundlage, den Mitteilungsumfang nach § 34 Abs. 2 Nr. 1 ErbStG (Anzeige von Sterbefällen) auf Nachlaßbestandteile und Vermögenswerte zu erweitern. Ich habe daher empfohlen, in § 354 der Dienstanweisung für die Standesbeamten — DA — eine Klarstellung der Rechtslage vorzunehmen.

3.4 Wahlrecht

Bereits Anfang 1985 habe ich den Bundesminister des Innern im Hinblick auf die nächste Bundestagswahl auf das Problem der Benennung von Wahlhelfern durch Behörden hingewiesen (vgl. 8. TB S. 11). Ich habe angeregt, in das Bundeswahlgesetz oder in die Bundeswahlordnung klarstellende Regelungen aufzunehmen. Der Bundesminister des Innern hat

hierzu ausgeführt, daß nach § 11 Bundeswahlgesetz grundsätzlich jeder Wahlberechtigte zur Übernahme des Amtes eines Beisitzers eines Wahlausschusses bzw. eines Mitgliedes eines Wahlvorstandes verpflichtet sei. Daraus lasse sich aber kaum die Pflicht einer Behörde ableiten, einer Wahlbehörde Listen ihrer Bediensteten mit deren Personalangaben zur Verfügung zu stellen. Aus wahlorganisatorischer Sicht hielten die Bundesregierung und die überwiegende Mehrheit der Länder sowie der Bundeswahlleiter eine Benennungspflicht der Behörden bis auf weiteres nicht für notwendig. Vielmehr reiche es zur Gewinnung von Personen zur Übernahme eines Wahlehrenamtes aus, wenn Dienststellen ihre Beschäftigten auf den Aufruf von Wahlbehörden zur Übernahme eines Wahlehrenamtes hinweisen mit der Empfehlung, sich — soweit möglich — hierfür freiwillig zur Verfügung zu stellen.

Ich begrüße diese Feststellung, daß eine Verpflichtung zur Benennung von Bediensteten zum Zwecke der Bestellung als Wahlhelfer nicht besteht. Mir vorliegende Eingaben zeigen jedoch, daß sich immer wieder Gemeinden bzw. örtliche Wahlleiter an Behörden wenden und um die Benennung geeigneter Wahlhelfer bitten.

Ich rege an, den Behörden und ihren Bediensteten für künftige Wahlen eine geeignete Orientierungshilfe auf der Basis der geltenden Rechtslage an die Hand zu geben. Sollte sich die Notwendigkeit einer gesetzlichen Regelung herausstellen, empfiehlt sich eine Bestimmung im Sinne von § 10 Abs. 3 des Volkszählungsgesetzes 1987 (Benennung von Angehörigen des öffentlichen Dienstes für die Zähltätigkeit).

3.5 Zivildienst

3.5.1 Aufbewahrung von Anerkennungsunterlagen

Wie in meinem Achten Tätigkeitsbericht (S. 11) bereits dargestellt, werden beim Bundesamt für den Zivildienst (BAZ) die Anerkennungsunterlagen der Kriegsdienstverweigerer wegen ihres sensiblen Inhalts von den übrigen Personalunterlagen getrennt aufbewahrt. Ich habe mich hiervon im Berichtsjahr überzeugt (siehe Bilanz). Nach wie vor bedarf es aber auch einer Festlegung, für welchen Zeitraum diese Anerkennungsunterlagen — einschließlich der darin enthaltenen besonders schutzwürdigen Daten über die Gewissensentscheidung des Betroffenen — überhaupt aufzubewahren sind und welche Daten aus diesen Unterlagen für welchen Zweck genutzt werden dürfen. Die Frage, wie nach einer noch zu bestimmenden Frist mit den Unterlagen zu verfahren ist — etwa Rückgabe an den Zivildienstleistenden oder Vernichtung der Akten — schließt sich zwangsläufig an. Ich halte eine gesetzliche Regelung für geboten. Dabei ist zu klären, ob und welchen Beitrag Anerkennungsunterlagen für die Erfüllung der Zivildienstpflicht leisten können und sollen. Dies betrifft zunächst die Ableistung des Zivildienstes von in der Regel zwanzig Monaten, wobei u. a. in den Fällen, in denen der Zivildienstpflichtige nicht selbst akzeptable Vorschläge für seine Verwendung macht, sondern die Zuweisung eines Platzes durch das BAZ abwartet, aus den Anerkennungsunterlagen gelegentlich Hinweise für einen sinnvollen und erfolgreichen Einsatz gewonnen werden können. M. E. wäre aber zu prüfen, ob nicht speziell für diesen Zweck nach der Anerkennungsentscheidung in einem gesonderten Verfahren geeignete Daten beim Betroffenen erhoben werden können. Damit würde auch eine Gleichbehandlung insoweit erreicht, als Gründe für eine bestimmte Zuweisung auch dann berücksichtigt werden könnten, wenn sie sich nicht zufällig aus den Anerkennungsunterlagen ergeben.

Hinsichtlich der Aufbewahrung der Anerkennungsunterlagen bis zur Vollendung des 60. Lebensjahres des Betroffenen, also weit über die Zeit der Ableistung des planmäßigen Zivildienstes hinaus, stützt sich das BAZ in seiner Argumentation auf die Vorschriften des § 79 Zivildienstgesetz in Verbindung mit § 3 Abs. 5 Wehrpflichtgesetz. Danach ist im Verteidigungsfall eine Zivildienstpflicht bis zur Vollendung des 60. Lebensjahres vorgesehen. Hier läge es sicherlich im Allgemeininteresse wie im Interesse des Betroffenen selbst, daß sich dessen Einplanung und Heranziehung zu einer bestimmten Tätigkeit nach seinen dann vorliegenden Kenntnissen und Fähigkeiten richten, also z. B. nach den im Rahmen der Zivildienstleistung durchgeführten Tätigkeiten oder nach dem erlernten und dem ausgeübten Beruf. Zweifelhaft erscheint jedoch, ob daneben die u. U. sehr lange zurückliegenden Erklärungen, Zeugenaussagen und Verhandlungsprotokolle über die Gewissensgründe noch eine tragfähige Grundlage für eine dann zu treffende Einsatzentscheidung sein können.

Das BAZ hat meine Überlegungen aufgegriffen und dem zuständigen Bundesministerium für Jugend, Familie, Frauen und Gesundheit einen Vorschlag unterbreitet, der dort allerdings noch der weiteren Abstimmung bedarf. Der Bundesminister der Verteidigung ist übrigens — soweit es sich um Betroffene handelt, denen die Anerkennung als Kriegsdienstverweigerer versagt wurde — mit vergleichbaren Problemen konfrontiert.

3.5.2 Arbeitsberichte von Zivildienstleistenden

Im Rahmen der Ableistung des Zivildienstes können anerkannte Kriegsdienstverweigerer in der Betreuung von alten Menschen, Behinderten und Kranken eingesetzt werden, um damit die Lebensbedingungen dieser Bevölkerungsgruppen zu verbessern.

Durch Eingaben von Zivildienstleistenden, die in den Bereichen Mobile Soziale Hilfsdienste sowie offene Altenhilfe eingesetzt sind, bin ich auf die für diese Tätigkeiten geltende Dienstanweisung hingewiesen worden. Danach haben die Zivildienstleistenden Wochenarbeitsberichte zu erstellen. Die Petenten bezweifeln, ob die Dienstanweisung den Datenschutzvorschriften genügt. Insbesondere vermuten sie, daß dadurch nicht nur der für ihren Einsatz zuständigen Zivildienststelle, sondern auch überge-

ordneten Zivildienstbehörden personenbezogene Daten aus der Intimsphäre der Betreuten offenbart werden.

Mit dem Bundesminister für Jugend, Familie, Frauen und Gesundheit und dem Bundesamt für den Zivildienst habe ich Einvernehmen über die Notwendigkeit erreicht, diese Dienstanweisung grundlegend zu überarbeiten und datenschutzfreundlicher zu gestalten. Dabei ist geplant, die Verpflichtung der Verwaltung zur Aufsicht über den Zivildienstleistenden und zur Fürsorge für ihn mit dem Anspruch der betreuten Personen auf Wahrung ihrer Privatsphäre in der Weise in Einklang zu bringen, daß Angaben über sie in den Wochenarbeitsberichten nur in verschlüsselter Form zu machen sind. Außerdem sollen jeweils mehrere Tätigkeitsmerkmale unter einer Schlüsselnummer zusammengefaßt werden. Der Name des Betreuten soll lediglich in Form einer Kennzahl angegeben werden, die nur einem ganz kleinen Personenkreis zugänglich ist. Ferner habe ich angeregt, die Aufbewahrungsfrist für die Arbeitsberichte erheblich zu verkürzen.

Das Vorhaben, ein derart verbessertes Verfahren der Erstellung und Prüfung der Arbeitsberichte einzuführen, ist gegenwärtig noch Gegenstand von Erörterungen zwischen dem Bundesminister für Jugend, Familie, Frauen und Gesundheit und der Bundesarbeitsgemeinschaft der Freien Wohlfahrtspflege. Ich hoffe, daß es bald zu einer für alle Beteiligten akzeptablen Lösung kommt.

4. Rechtswesen

4.1 Mitteilungen in Zivilsachen (MiZi) Mitteilungen in Strafsachen (MiStra)

In früheren Tätigkeitsberichten (letztmals im 8. TB S. 12) habe ich darauf hingewiesen, daß die Mitteilungen in Zivilsachen (MiZi) sowie die Mitteilungen in Strafsachen (MiStra) einer gesetzlichen Grundlage und besseren inhaltlichen Ausgestaltung bedürfen, um den Anforderungen der Entscheidung des Bundesverfassungsgerichts zum Volkszählungsgesetz gerecht zu werden. Hierzu liegt nunmehr ein Referentenentwurf des Bundesministers der Justiz für ein „Justizmitteilungsgesetz" vor, den er den Bundesressorts und den Landesjustizverwaltungen „als Diskussionsgrundlage" und mit der Bitte um Mitprüfung und Stellungnahme übersandt hat. Danach ist beabsichtigt, die Mitteilungen in Zivilsachen und in Strafsachen in den §§ 168 a bis 168 i Gerichtsverfassungsgesetz sowie in § 38 a Jugendgerichtsgesetz gesetzlich zu regeln und dadurch die übergangsweise geltenden bundeseinheitlichen Verwaltungsanordnungen der Mitteilungen in Strafsachen (s. Bundesanzeiger Nr. 60/1985) und der Mitteilungen in Zivilsachen (s. Bundesanzeiger Nr. 219/1985) sowie Verwaltungsanordnungen der Länder über Mitteilungen von Klagen, Vollstrekkungsmaßnahmen pp. gegen bestimmte Angehörige rechtsberatender Berufe zu ersetzen. Der Entwurf wählt — wie der Bundesminister der Justiz in der Begründung näher erläutert hat — „einen Lösungsweg, der eine geringere Regelungsdichte aufweist". Der Entwurf „beschränkt die bereichsspezifische Zweckbestimmung der Übermittlungsregelungen auf eine gegenständliche Umschreibung, die nicht bis in alle Einzelheiten präzisiert ist". Er bedarf unter datenschutzrechtlichen Gesichtspunkten einer näheren Prüfung vor allem im Hinblick auf Normenklarheit, Praktikabilität und Transparenz.

Der Bundesminister der Justiz beabsichtigt, durch Verwaltungsanordnungen die „erforderlichen Einzelheiten so aufzubereiten, daß es wie bisher für eine Mitteilung nur in Ausnahmefällen einer Anordnung des Richters oder Staatsanwalts bedarf". Mangelnde Bestimmtheit der Vorschriften des Entwurfs wie auch der Vorschriften, auf die er Bezug nimmt, läßt sich m. E. aber nicht durch Verwaltungsvorschriften ausgleichen. Neben eine Neuregelung der Mitteilungen müssen ergänzend bereichsspezifische Vorschriften über Aufgaben und Befugnisse der Empfängerbehörden treten. So muß z. B. eine Antwort zu § 168 a Abs. 1 Satz 2 Nr. 8 des Entwurfs auf die Frage, welcher mitzuteilende Vorgang zu ausländerrechtlichen Maßnahmen Anlaß geben kann, durch konkrete Rechtsvorschriften des Ausländerrechts gegeben werden. Deutlicher als bisher läßt der Entwurf jedenfalls die Notwendigkeit hervortreten, den Informationsbedarf „zur Erfüllung gesetzlicher Aufgaben des Empfängers" hinreichend klar zu bestimmen. Daneben stellt sich die Frage, ob Vorschriften zur Durchführung des vorliegenden Gesetzentwurfs nicht zumindest zu einem Teil die Form einer Rechtsverordnung erhalten müssen.

Besondere Bedeutung kommt zudem der notwendigen Beschränkung des Inhalts der Mitteilungen auf das jeweils erforderliche Maß zu. Für den Regelfall sollte die Mitteilung der Tatsache einer Verurteilung unter Angabe der Straftat bzw. des Tenors der Entscheidung im Bereich der streitigen Zivilgerichtsbarkeit bzw. der freiwilligen Gerichtsbarkeit genügen. Derartige Festlegungen enthält der Entwurf jedoch leider noch nicht.

Gegenwärtig bereite ich unter diesen Gesichtspunkten eine Stellungnahme zu dem Entwurf vor. Da es sich bei den Mitteilungen überwiegend um solche von Justizbehörden der Länder an andere Behörden und sonstige öffentliche Stellen in den Ländern handelt, kommt es mir hierbei besonders auf ein enges Zusammenwirken mit den Datenschutzbeauftragten der Länder an.

4.2 Strafprozeßordnung

Das Strafverfahrensrecht enthält in wesentlichen Bereichen noch keine den Anforderungen der Rechtsprechung des Bundesverfassungsgerichts genügende Vorschriften über den Umgang mit personenbezogenen Daten. Dies ist — mit Blick auf einzelne Problembereiche, so z. B. die Akteneinsicht und die Erteilung von Auskünften — von den Datenschutzbeauftragten schon früher deutlich gemacht und eine Prüfung und gesetzliche Regelung

gefordert worden (vgl. meinen 5. TB S. 19 f., 6. TB S. 14, 7. TB S. 14). Inzwischen wird — nicht nur bei den Datenschutzbeauftragten — zunehmend die Auffassung vertreten, daß das Strafverfahrensrecht unter datenschutzrechtlichen Gesichtspunkten einer Überarbeitung auf breiterer Basis bedarf. Dabei geht es vor allem darum, für die strafprozessuale Ermittlungstätigkeit mit Hilfe bestimmter hergebrachter und neuartiger Ermittlungsmethoden sowie für die Akteneinsicht im Strafverfahren die für Grundrechtseingriffe verfassungsrechtlich gebotenen, im Interesse der Rechtssicherheit und Rechtsklarheit notwendigen gesetzlichen Grundlagen zu schaffen. Angesichts der besonders wichtigen Aufgabe der wirksamen Bekämpfung des Terrorismus ist mir daran gelegen, daß differenzierte Lösungsansätze gefunden werden, um die strafprozessualen Befugnisse zu präzisieren, ohne wesentliche Elemente des freiheitlichen Rechtsstaats in Frage zu stellen. Unter diesen Gesichtspunkten betrachte ich es als einen deutlichen Fortschritt, daß der Bundesminister der Justiz „um die Diskussion voranzutreiben" einen Arbeitsentwurf eines Gesetzes zur Regelung der rechtlichen Grundlagen für Fahndungsmaßnahmen, Fahndungshilfsmittel und für die Akteneinsicht im Strafverfahren vorgelegt hat — auch wenn er sich damit zunächst nur auf einen Teil der regelungsbedürftigen Gegenstände beschränkt. Zur weiteren Beteiligung an dieser Diskussion bereite ich im Zusammenwirken mit den Landesbeauftragten für den Datenschutz einen Katalog von „Überlegungen zu Datenschutzregelungen im Strafverfahren" vor. Ziel dieser Überlegungen ist es, besondere Fahndungsmethoden und den Einsatz besonderer technischer Hilfsmittel — wie lesender oder mithörender technischer Geräte bzw. Bildaufzeichnungen —, also von Methoden und Mitteln mit besonderem Eingriffscharakter, die oft auch die Rechte Unverdächtiger berühren, zu präzisieren und unter Gesichtspunkten der Verhältnismäßigkeit auf genau zu bezeichnende Tatbestände der Schwerkriminalität zu beschränken. Der Arbeitsentwurf des Bundesministers der Justiz sieht z. B. zur Rasterfahndung eine Verwertung von Zufallsfunden nur im Rahmen des Kataloges von Straftaten vor, bei denen die Rasterfahndung selbst zulässig wäre (§ 98 b Abs. 3 a. E. des Entwurfs). Die von mir vorbereiteten Empfehlungen gehen in die gleiche Richtung. Vergleichbare Regelungen halte ich u. a. auch bei der polizeilichen Beobachtung, der planmäßigen Observation, beim Einsatz von Ton- und Bildgeräten sowie bei der Überwachung des Post- und Fernmeldeverkehrs für geboten. Das bedeutet, daß die Verwendung von Zufallsfunden nur zulässig sein sollte, soweit es sich um Straftaten handelt, die ihrerseits die jeweilige Maßnahme rechtfertigen würden. Ich hoffe, diese Empfehlungen dem Bundesminister der Justiz in Kürze zuleiten zu können.

4.3 Veröffentlichung von Gerichtsentscheidungen

Wiederholt bin ich um eine Stellungnahme zu der Frage gebeten worden, in welcher Form Verfahrensbeteiligte und auch Richter eine Veröffentlichung von Gerichtsentscheidungen hinnehmen müssen. Gelegentlich sind dabei auch Besorgnisse von Richtern lautgeworden, mit Mitteln der automatischen Datenverarbeitung wie des vom Bundesminister der Justiz ins Leben gerufenen Juristischen Informationssystems JURIS könnte eine Kontrolle der richterlichen Tätigkeit ermöglicht werden und die Gefahr der Aufzeichnung eines „Richterprofils" entstehen.

Ich halte in der Frage der Veröffentlichung von Gerichtsentscheidungen eine Abwägung zwischen den schutzwürdigen Belangen der Beteiligten und den Anforderungen für notwendig, die im Rahmen eines überwiegenden Allgemeininteresses an die Rechtsfortbildung in Wissenschaft, Lehre und Rechtsprechung zu stellen sind. Unter diesen Gesichtspunkten ist durch Schwärzung von Namen und — weitestgehend — von Ortsbezeichnungen in der Sachverhaltsdarstellung in aller Regel ein hoher Grad von Anonymisierung zu erreichen, ohne daß das im Interesse der Rechtsfortbildung in Praxis und Lehre gebotene Verständnis der Entscheidungsgründe beeinträchtigt wird. Es muß aber erkennbar sein, welches Gericht, auch welche Kammer oder welcher Senat etc., wann die Entscheidung getroffen hat. Eine namentliche Angabe der beteiligten Richter ist dagegen entbehrlich.

Vor diesem Hintergrund hat meine Beobachtung der Praxis der Gerichte des Bundes, für deren datenschutzrechtliche Kontrolle — soweit es sich nicht um die richterliche Entscheidungsfindung handelt — ich zuständig bin, erfreulicherweise bislang keinen Anlaß zur Kritik gegeben. Der Bundesminister der Justiz hat mir zudem bestätigt, daß er die von mir genannten Prinzipien teile. Die JURIS-Rechtsprechungsdatenbank dokumentiere das Gericht und — soweit ersichtlich — den Spruchkörper nebst Aktenzeichen und Datum der Entscheidung, nicht aber (außer bei Minderheitsvoten des Bundesverfassungsgerichts) die Namen der entscheidenen Richter. Auch das Justizstatistik-Informationssystem JUSTIS speichert — wie mir der Bundesminister der Justiz mitgeteilt hat — verfahrensbezogene und keine personenbezogenen Daten.

5. Finanzwesen

Bei meinen datenschutzrechtlichen Stellungnahmen zu den sog. Kontrollmitteilungen nach § 93 Abgabenordnung (AO), d. h. den Mitteilungen anderer Behörden an Finanzbehörden über Maßnahmen, die für die Besteuerung von Bedeutung sind, ging es bisher darum, einen vertretbaren Ausgleich zwischen dem überwiegenden Allgemeininteresse an der Sicherung der Besteuerung und dem informationellen Selbstbestimmungsrecht des Bürgers zu erreichen (vgl. 5. TB S. 24 f., 6. TB S. 15 f., 7. TB S. 16). Ich habe empfohlen, dafür eine Rechtsgrundlage zu schaffen, die den Anforderungen der Normenklarheit und Verhältnismäßigkeit entspricht. Mit dem neuen § 93 a, der im Zuge des Steuerbereinigungsgesetzes 1986 vom 19. Dezember 1985 in die AO aufgenommen wurde, besteht nunmehr eine Ermächtigung für den Erlaß von Rechtsverordnungen über

allgemeine Mitteilungspflichten der Behörden gegenüber der Finanzverwaltung. Der Bundesminister der Finanzen hat mir einen ersten Entwurf dieser als Kontrollmitteilungsverordnung (KMV) bezeichneten Rechtsverordnung zugeleitet, der von einer Unterkommission der Finanzverwaltungen erarbeitet worden ist. Er ist bislang weder mit den obersten Finanzbehörden der Länder noch mit den Ressorts der Bundesregierung abgestimmt worden. Wegen der Bedeutung dieser Vorschriften für den Datenschutz habe ich hierzu gleichwohl bereits eine erste Stellungnahme abgegeben. Angesichts der Tatsache, daß zwar § 93, nicht aber § 93a AO in § 71 Abs. 1 Nr. 3 SGB X genannt ist, stellt sich die Frage, wie weit die Offenbarungsbefugnis für Sozialdaten zur Erfüllung von Mitteilungspflichten gegenüber Finanzbehörden reicht. Dabei wird es darauf ankommen, ob § 93a AO als eine eigenständige Regelung oder lediglich als eine Verordnungsermächtigung zur teilweisen Konkretisierung der in § 93 Abs. 1 AO enthaltenen Vorschrift über die Heranziehung „anderer Personen zur Auskunft" verstanden wird. Wegen dieses Themenkreises habe ich gegenüber dem Bundesminister der Finanzen angeregt, den Bundesminister für Arbeit und Sozialordnung in die weitere Erörterung einzubeziehen und mich hierbei weiterhin zu beteiligen.

6. Bauwesen

6.1 Baugesetzbuch

In seiner Sitzung am 23. Oktober 1986 hat der Deutsche Bundestag den von der Bundesregierung eingebrachten Entwurf eines Gesetzes über das Baugesetzbuch verabschiedet, das am 1. Juli 1987 in Kraft treten wird. Das Baugesetzbuch umfaßt die bisherigen Regelungsbereiche des Bundesbaugesetzes (BBauG) und des Städtebauförderungsgesetzes (StBauFG).

Der Bundesminister für Raumordnung, Bauwesen und Städtebau hatte mir schon im August 1985 einen Referentenentwurf dieses Gesetzgebungsvorhabens übersandt und um Beratung zu mehreren datenschutzrelevanten Vorschriften gebeten (vgl. 8. TB S. 13). Ich habe feststellen können, daß als Ergebnis der Beratungen in dem verabschiedeten Gesetz die wichtigsten — wenn auch nicht alle — meiner Anregungen Berücksichtigung gefunden haben.

In der Vergangenheit haben mich Bürgereingaben insbesondere bezüglich der Befragungen im Zusammenhang mit städtebaulichen Sanierungsmaßnahmen erreicht. Zur Beurteilung der Sanierungsbedürftigkeit eines Stadtgebietes sowie zur Vorbereitung und Durchführung der Sanierung selbst benötigt die Gemeinde insbesondere auch Angaben, die ihr nur die betroffenen Bürger geben können. Bislang sieht das Städtebauförderungsgesetz daher für die Bewohner des betroffenen Stadtgebietes eine Auskunftspflicht vor (§ 3 Abs. 4 StBauFG), deren Verletzung mit einem Zwangsgeld bedroht ist (§ 87 StBauFG). In ihren Eingaben hatten sich die Bürger nicht nur darüber beschwert, daß sich die von der Gemeinde geforderten Angaben oftmals auf Sachverhalte der engsten Privatsphäre beziehen, sondern daß auch die Fragenkataloge in den Ländern und Gemeinden stark voneinander abweichen. Nach den Grundsätzen des Volkszählungsurteils des Bundesverfassungsgerichts sind an die einschlägigen neu zu gestaltenden Vorschriften des Baugesetzbuches hohe Anforderungen bezüglich Normenklarheit und Verhältnismäßigkeit zu stellen. In diesem Sinne beschränkt sein § 138 die Auskunftspflicht nicht nur auf solche Angaben, die für Sanierungszwecke erforderlich, d. h. unerläßlich sind, sondern nennt auch einen Katalog von Daten, der regelmäßig für diese Zwecke ausreichend sein dürfte.

Die Verwendung der personenbezogenen Daten wird grundsätzlich auf Sanierungszwecke beschränkt. Soweit die hierfür erhobenen Daten auch „für die Besteuerung erforderlich sind", dürfen sie gemäß § 138 Abs. 2 Satz 4 Baugesetzbuch allerdings an die Finanzbehörden weitergegeben werden. Zweifellos stellt dies eine Änderung der Zweckbestimmung der erhobenen Daten dar: Während Sanierungsmaßnahmen den Bürgern zumindest tendenziell Vorteile bringen und somit ihre Auskunftsbereitschaft fördern, entsprechen Zwecke der Besteuerung einer solchen Zielsetzung selbst dann nicht, wenn sie im Einzelfall zu steuerlichen Erleichterungen führen. Eine solche Kombination tendenziell unvereinbarer Verwendungszwecke für zwangsweise erhobene Daten hat das Bundesverfassungsgericht im oben genannten Urteil gerügt. Personenbezogene Daten, die für einen bestimmten, besonders hervorgehobenen „Haupt"-Zweck erhoben wurden, dürfen ohne Aufklärung des Bürgers daneben nicht noch für einen demgegenüber zurücktretenden, völlig anders gearteten Zweck verwendet werden. Die in § 138 Abs. 2 Satz 4 Baugesetzbuch geregelte Datenübermittlung an die Finanzbehörden muß daher unter datenschutzrechtlichen Gesichtspunkten auf erhebliche Bedenken stoßen.

Beim Kauf von Baugrundstücken steht schon nach bislang geltendem Recht den Gemeinden in vielen Fällen ein Vorkaufsrecht zu. Damit die Gemeinde prüfen kann, ob sie dies wahrnehmen will, hat ihr der Verkäufer im Falle einer Grundstücksveräußerung den Inhalt des Kaufvertrages unverzüglich mitzuteilen (§ 24 Abs. 5 BBauG). Nach mir vorliegenden Informationen machen die Gemeinden jedoch nur in weniger als 1% aller Fälle von ihrem Vorkaufsrecht Gebrauch. Ich habe dem Bundesminister für Raumordnung, Bauwesen und Städtebau daher empfohlen, zur Wahrung des Grundsatzes der Verhältnismäßigkeit auf eine engere Begrenzung der Mitteilungspflichten hinzuwirken und begrüße es, daß die entsprechenden Vorschriften des Baugesetzbuches (§§ 24 ff.) in dieser Hinsicht nunmehr eine erhebliche Einschränkung vorsehen. Dem Vorkaufsrecht der Gemeinden unterliegen jetzt nur noch bestimmte Grundstücke; damit ist auch eine Einschränkung der Mitteilungspflichten verbunden.

Bereits das Bundesbaugesetz sieht zur Ermittlung von Grundstückswerten selbständige, unabhängige

Gutachterausschüsse vor (§§ 136 ff. BBauG). Wichtiges Hilfsmittel für deren Arbeit ist die von ihnen zu führende sog. Kaufpreissammlung. Hierfür muß die beurkundende Stelle dem Gutachterausschuß Abschriften von allen Verträgen übersenden, die Grundstücksverkäufe oder die Begründung eines Erbbaurechtes zum Gegenstand haben (§ 143a BBauG). Wenn unterstellt wird, daß eine solche Beschränkung des Rechts auf informationelle Selbstbestimmung der Betroffenen im überwiegenden Allgemeininteresse zulässig ist, so muß doch die Verwendung der erhobenen Daten normenklar und zweckgerichtet geregelt werden. Insofern bringt die einschlägige Vorschrift des Baugesetzbuches (§ 195) gegenüber dem geltendem Recht einen Fortschritt. So wird z.'B. klargestellt, daß die Kaufpreissammlung nur dem zuständigen Finanzamt und nur für Zwecke der Besteuerung übermittelt werden darf. Gemäß § 195 Abs. 3 Baugesetzbuch dürfen Auskünfte aus der Kaufpreissammlung bei berechtigtem Interesse nach Maßgabe landesrechtlicher Vorschriften erteilt werden. Die Begründung zum Gesetzentwurf geht im übrigen — in Übereinstimmung mit der bisherigen Verwaltungspraxis — davon aus, daß solche Auskünfte stets nur in einer anonymisierten Form gegeben werden, so daß der Eigentümer des betreffenden Grundstücks nicht erkennbar ist. Dies müssen die zur erlassenden Ausführungsbestimmungen sicherstellen.

6.2 Datenschutzkontrolle der Bundesbaudirektion

Im Mai des Berichtsjahres nahmen meine Mitarbeiter bei der Bundesbaudirektion gemäß § 19 Abs. 1 BDSG eine Datenschutzkontrolle vor. Mit Schreiben vom 15. Juli 1986 informierte ich den Bundesminister für Raumordnung, Bauwesen und Städtebau über das Ergebnis und wies auf einige Problempunkte, namentlich bei der Verarbeitung der Personaldaten der Bediensteten und beim Einsatz von Personal Computern hin.

So ist beispielsweise die Bearbeitung von Anträgen auf Beihilfe in Krankheitsfällen m. E. organisatorisch und personell nicht ausreichend von der Bearbeitung der Personalangelegenheiten getrennt, wodurch die Gefahr von Interessenkonflikten besteht. Auch die automatisierte Registrierung und Verarbeitung von Telefonverbindungsdaten der Bediensteten gab Anlaß zur Kritik.

Bei der Bundesbaudirektion werden Personal Computer in nicht unerheblichem Umfang auch zur Verarbeitung personenbezogener Daten eingesetzt.

Dies birgt für die schutzwürdigen Belange der Betroffenen Risiken, die sich weitgehend einer Begrenzung entziehen (vgl. 8. TB S. 56 ff. und unten 20.1). Der vom BDSG geforderten Organisationskontrolle kommt dadurch besondere Bedeutung zu. Ich habe dem Bundesminister für Raumordnung, Bauwesen und Städtebau meine Auffassung mitgeteilt, daß die Organisation der Bundesbaudirektion den besonderen Risiken der Verarbeitung personenbezogener Daten mit Hilfe von Personal Computern noch nicht Rechnung trägt.

Die Stellungnahme der Bundesbaudirektion zu den von mir aufgeworfenen Fragen hat mich erst kurz vor Abschluß des vorliegenden Tätigkeitsberichts erreicht. Ich habe sie noch nicht auswerten können.

7. Personalwesen

7.1 Konventionelle Personaldatenverarbeitung

7.1.1 Personalaktenrecht

Nachdem ich bereits in meinem Dritten (S. 26, 27) und Fünften Tätigkeitsbericht (S. 27) auf die Unvollständigkeit des Personalaktenrechts des Bundes hingewiesen hatte, hat die Bundesregierung in den Jahren 1983 und 1984 Initiativen zu einer Neuregelung des Personalaktenrechts des Bundes ergriffen. Hierüber habe ich in meinem Sechsten (S. 18) und Siebenten Tätigkeitsbericht (S. 20) berichtet. Die Planungs- und Prüfungsarbeiten der interministeriellen Arbeitsgruppe beim Bundesminister des Innern wurden im Berichtsjahr intensiviert. Daran nehme ich in beratender Funktion teil. Bereits jetzt zeichnet sich ab, daß zahlreiche Forderungen, die ich in früherer Zeit gestellt hatte, wie beispielsweise die gesetzliche Verankerung des Personalaktengeheimnisses oder die Regelung des notwendigen Inhalts der Personalakten, hier insbesondere Inhalt und Behandlung der Personalbögen, der Bewerbungsunterlagen wie auch der personalärztlichen Vorgänge und Beihilfeakten, Berücksichtigung finden sollen.

Ich begrüße die beabsichtigte umfassende Regelung des Personalaktenrechts auch deshalb, weil mir durch zahlreiche Eingaben die Dringlichkeit dieses Vorhabens deutlich geworden ist.

7.1.2 Beihilfe

— Wiederholt habe ich in meinen Tätigkeitsberichten auf die Notwendigkeit einer *Abschottung der Beihilfestelle* von der Personalverwaltung hingewiesen (6. TB S. 19 f. und 8. TB S. 13 f.). In der Neufassung der allgemeinen Verwaltungsvorschriften über die Gewährung von Beihilfen in Krankheits-, Geburts- und Todesfällen vom 19. April 1985 (GMBl. 1985, S. 290 f. — BhV —) ist zwar festgelegt, daß die bei der Bearbeitung von Beihilfen bekanntgewordenen Angelegenheiten geheimzuhalten sind. Durch die organisatorische Einbindung der Beihilfestellen in die Personalverwaltung können jedoch, wie mir aufgrund von Eingaben deutlich geworden ist, insbesondere im Rahmen der Dienst- oder Fachaufsicht oder im Rahmen eines Widerspruchsverfahrens dann Probleme entstehen, wenn dem Leiter einer Organisationseinheit sowohl die Beihilfebearbeitung wie auch die allgemeine Personalverwaltung unterstehen. Die Mitarbeiter in den Beihilfefestsetzungsstellen sind verpflichtet, über die ihnen bei der Bearbeitung oder der Entgegennahme der Beihilfeanträge anvertrauten oder zur Kenntnis gelangten persönlichen Angelegenheiten auch im dienstlichen

Verkehr Stillschweigen zu bewahren. Es ist nicht auszuschließen, daß in den genannten Fällen ein auch für die Personalverwaltung zuständiger Vorgesetzter eines Beihilfesachbearbeiters Einblick in die Beihilfeunterlagen nimmt. Dieses Problem kann nicht isoliert gelöst werden, sondern nur im Zusammenhang mit der Forderung nach einer strikten Abtrennung der Beihilfestellen von der allgemeinen Personalverwaltung. Eine den Anforderungen des Personaldatenschutzes genügende vertrauliche Behandlung von Beihilfedaten wird erst dann gewährleistet sein, wenn in allen Teilen der Verwaltung eine konsequente Trennung der Beihilfestellen von den Personalstellen durchgeführt ist. Diese Auffassung wird vom Landesarbeitsgericht Köln (Urteil vom 6. November 1984 — 6 Sa 1324/83) gestützt. Danach können sich die Angaben, die ein Arbeitnehmer im Beihilfeantrag über seinen Gesundheitszustand macht, negativ auf sein berufliches Fortkommen auswirken, wenn die Bediensteten, die mit der Bearbeitung der Beihilfeanträge beauftragt sind, derart in die allgemeine Personalverwaltung eingebunden sind, daß ihr Kenntnisstand möglicherweise künftige personelle Maßnahmen des Arbeitgebers beeinflußt. Diese Gefahr müsse aufgrund der bestehenden Fürsorgepflicht durch geeignete organisatorische Maßnahmen ausgeräumt werden. Solange solche Vorkehrungen nicht getroffen seien, dürfe die Bearbeitung nicht von der Angabe der ärztlichen Diagnose abhängig gemacht werden.

Ich habe in diesem Zusammenhang immer wieder vorgeschlagen, die Beihilfen für bestimmte Teile der Verwaltung zentral zu bearbeiten. Dies geschieht bereits heute beim Bundesverwaltungsamt für die Beihilfen von Ruhestandsbeamten des Bundes. Ich empfehle zu prüfen, ob diese oder eine ähnliche Lösung nicht auch für die Bearbeitung der Beihilfen aktiver Bundesbediensteter in Betracht kommt.

— Auch im Berichtsjahr wurde ich durch mehrere Eingaben darauf hingewiesen, daß wegen der als mangelhaft empfundenen Abschottung der Beihilfestellen innerhalb der Personalverwaltung erhebliche Bedenken von Bediensteten bestanden, bestimmte Rechnungen für ärztliche Leistungen zur Beihilfegewährung einzureichen.

Die Beihilfefestsetzungsstelle ist verpflichtet, die Notwendigkeit und Angemessenheit der in Rechnung gestellten ärztlichen Leistungen zu prüfen. Diesen Anforderungen an eine ordnungsgemäße Bescheidung des Beihilfeantrages kann die Beihilfefestsetzungsstelle nur genügen, wenn sie die Art der diagnostizierten Erkrankung mit der abgerechneten ärztlichen Leistung vergleichen kann. Die Angaben der Diagnosen auf den Arztrechnungen sind daher m. E. erforderlich. Ein Problem besonderer Art wirft in diesem Zusammenhang das seit Oktober 1985 praktizierte Antragsverfahren für die *Anerkennung der Beihilfefähigkeit psychotherapeutischer Maßnahmen* auf. Es gibt unter Aspekten des Personaldatenschutzes insoweit Anlaß zu Bedenken, als in dem „Bericht an den Gutachter" (Anlage 2 zu Hinweis Nr. 5.2 zu § 6 Abs. 1 Nr. 2 BhV) unter vollständiger Namensnennung Aussagen über Psychogenese und Psychodynamik der neurotischen Entwicklung und über die Prognose der Therapie gefordert werden. Für die Begutachtung durch den externen Gutachter sind nach meiner Auffassung weder der Name noch das Geburtsdatum des Patienten erforderlich. Es wäre ausreichend, wenn in diesem Falle eine Chiffre-Nummer sowie das Alter des Patienten angegeben würden. Hinsichtlich der übrigen geforderten Merkmale des Patienten könnten Bedenken wegen einer möglichen Reidentifizierung im Hinblick auf den ohnehin bestehenden Vertrauensschutz zurückgestellt werden. Im übrigen sollten derartige Gutachten nicht nur — wie vorgeschrieben — in verschlossenen Umschlägen verwahrt und versandt, sondern darüber hinaus deren Öffnung dokumentiert werden. Im Bereich der Krankenkassen wird in den entsprechenden Fällen bereits jetzt der gesamte Behandlungsfall unter einer Chiffrenummer — ohne Namensnennung — abgewickelt, die der behandelnde Arzt bereits beim Ausfüllen der Formblätter festsetzt. Meine datenschutzrechtlichen Bedenken sowie den Lösungsvorschlag habe ich bereits vor einiger Zeit dem Bundesminister des Innern mitgeteilt. Eine Entscheidung ist bisher nicht getroffen worden.

— Im Bereich der Deutschen Bundespost wird die Beihilfe für Berechtigte, die zugleich freiwilliges Mitglied der *Postbeamtenkrankenkasse* sind, von der Postbeamtenkrankenkasse festgesetzt und zusammen mit den zustehenden Kassenleistungen ausgezahlt. Die Ansprüche auf Beihilfe und auf Kassenleistungen sind mit einem einheitlichen Antragsvordruck bei der Postbeamtenkrankenkasse geltend zu machen. Der Antrag ist zusammen mit den Rechnungsbelegen bei der Personalstelle der Beschäftigungsdienststelle des Antragstellers einzureichen.

Wiederholt haben Berechtigte in Eingaben an mich die Befürchtung geäußert, daß durch dieses Antragsverfahren Angaben über ihre gesundheitlichen Verhältnisse bzw. über die Art ihrer Erkrankung in die Personalverwaltung der Bundespost gelangen und dort zu treffenden Personalentscheidungen beeinflussen könnten.

Meine Feststellungen haben ergeben, daß derartige Bedenken nicht gerechtfertigt sind. Die Beihilfe- und Erstattungsanträge, die bei den Beschäftigungsdienststellen einzureichen sind, enthalten neben den persönlichen Angaben eine Zusammenstellung der Aufwendungen, in der lediglich die laufende Nummer und der Rechnungsbetrag der beigefügten Rechnungen enthalten sind; für weitere Angaben wie z. B. Name und/oder Fachrichtung des behandelnden Arztes, Art der Behandlung oder Bezeichnung des verordneten Medikaments ist in dem Antrag kein Raum. Die Rechnungsbelege können dem Antrag in einem verschlossenen Umschlag beigefügt werden, der dann erst bei der Postbeamtenkrankenkasse geöffnet wird.

Nach meinem Eindruck ist allerdings die offene Beifügung der Belege die Regel. Dieser Ein-

druck resultiert auch aus der Tatsache, daß jedenfalls bei einer Beschäftigungsstelle ein Vordruck vorhanden ist und verwendet wird, mit dem einzelne fehlende Belege vom Antragsteller nachgefordert werden können. Daraus ergibt sich, daß die Betroffenen zumindest nicht hinreichend darüber informiert sind, daß sie die Belege im verschlossenen Umschlag beifügen können. Ich sehe auch verfahrensmäßig keine Notwendigkeit für eine offene Beifügung der Belege.

In einem Fall hat die Beschäftigungsstelle bei geltend gemachten Aufwendungen für eine Heilkur die *Vorlage eines ärztlichen Schlußberichts* nachgefordert. In Unkenntnis des für Beihilfezwecke erforderlichen Inhalts eines solchen Kurberichts hat der Betroffene eine Ablichtung des Arztbriefes, den der Kurarzt dem weiterbehandelnden Hausarzt geschrieben hatte, vorgelegt. Dieser Arztbrief, der ausführliche Angaben über Diagnosen, Befunde und Therapien enthielt, wurde vom Hausarzt — verständlicherweise — nur unter großen Bedenken herausgegeben.

Auf meine Anregung hin wurde dem Betroffenen dieser Arztbrief zurückgegeben. Außerdem wurden die Formblätter für die Bescheide über die Anerkennung der Beihilfefähigkeit der Aufwendungen für eine Sanatoriumsbehandlung und einer Heilkur geändert und mit dem Hinweis versehen, daß der nach Abschluß der Maßnahme vorzulegende ärztliche Schlußbericht lediglich bestätigen soll, daß die Behandlung ordnungsgemäß durchgeführt worden ist und darüber hinausgehende medizinische Angaben nicht erforderlich sind.

7.1.3 Besoldung/Versorgung

— Im Berichtsjahr habe ich festgestellt, daß im Bundesministerium des Innern und seinem Geschäftsbereich separate *Kindergeldakten* nicht geführt werden. Vielmehr werden die anfallenden Unterlagen dem Kostenteil der Personalakte zugeordnet. Dies ergibt sich aus einem Erlaß des Bundesministers des Innern vom 21. Juni 1966 (Z 2-001 002/1) an die Dienststellen im Geschäftsbereich betreffend die Anlage und Führung der Personalakten.

In einem gemeinsamen Rundschreiben des Bundesministeriums des Innern und des Bundesministeriums für Jugend, Familie und Gesundheit vom 26. Oktober 1983 (D II4-221 972) ist klargestellt, daß das Sozialgeheimnis (§ 35 Sozialgesetzbuch I — SGB I) es verbietet, Kindergelddaten an die mit der Bearbeitung von Personalsachen Betrauten weiterzugeben; wenn Kindergeld- und Personalsachen von derselben Stelle/Person bearbeitet werden, dürfen Kindergelddaten bei der Bearbeitung von Personalsachen nicht verwendet werden. Dieser Hinweis auf die bestehende Rechtslage entspricht einer Forderung der Datenschutzbeauftragten des Bundes und der Länder (vgl. 6. TB S. 32). Weitere Maßnahmen sind aber erforderlich um zu verhindern, daß im Zusammenhang mit der Kindergeldbearbeitung erhobene Daten zur Kenntnis der mit der Personalverwaltung im engeren Sinne befaßten Bediensteten gelangen. Ich vertrete die Auffassung, daß Kindergeldakten getrennt von den übrigen Personalvorgängen geführt werden müssen. Diese Vorgänge dürfen nur Bediensteten zugänglich gemacht werden, die mit der Festsetzung und Anordnung von Bezügen betraut sind. In dem Kostenteil der Personalakten soll lediglich die Tatsache und der Begünstigte der kindergeldrechtlichen Maßnahme sowie der Name und das Geburtsdatum des Kindes vermerkt sein.

Änderungsbedürftig ist auch das derzeitige Verfahren, Steuerbescheide zu den Kindergeldunterlagen zu nehmen, wenn ein Anspruch über den Sockelbetrag hinaus geltend gemacht wird. Bei den daraus ersichtlichen Angaben über die verschiedenen positiven und negativen Einkünfte eines Bediensteten handelt es sich um besonders sensible Daten, die gemäß §§ 10, 11 Bundeskindergeldgesetz (BKGG) für die Entscheidung über den geltend gemachten Anspruch nicht in vollem Umfang erforderlich sind. Bereits in meinem Siebenten Tätigkeitsbericht (S. 43, 44) ist meine Auffassung festgehalten, daß es für die Prüfung der kindergeldrechtlichen Einkommensgrenze auf die Summe der positiven Einkünfte ankomme und daß deshalb eine Aufteilung nach einzelnen Einkunftsarten nicht vorzunehmen sei. Das Verlangen der Besoldungsstellen, hier stets alle Einzeleinkünfte zu erhalten und im Steuerbescheid lesbar zu belassen, ist m. E. unzulässig, da es insoweit an der Erforderlichkeit für die Leistungsbemessung mangelt.

— Der Bundesminister des Innern hat in einem Rundschreiben vom 11. Oktober 1985 (Z 5-007 800/6) darauf hingewiesen, daß den förmlichen Kassenanweisungen bei Zahlung von *Unfallfürsorge* Arztrechnungen, Rezepte und sonstige Belege beizufügen sind. Er beruft sich dabei auf § 58 Reichsrechnungsordnung (RRO). Danach sind Schriftstücke, die einen der förmlichen Kassenanweisung zugrundeliegenden Vorgang betreffen, der Kassenanweisung beizufügen, soweit dies in den §§ 59 bis 65 RRO vorgesehen oder vom Rechnungshof besonders bestimmt oder sonst zur Begründung der Kassenanweisung notwendig ist. Ich halte dieses Verfahren unter Aspekten des Personaldatenschutzes für bedenklich. Die genannten Belege müssen zwar den Bearbeitern bekannt sein, die über die Gewährung der Leistungen entscheiden, für eine Beifügung der Belege zu den Auszahlungsanordnungen sehe ich jedoch keine Notwendigkeit. So erhält beispielsweise auch in Beihilfefällen der Bedienstete entsprechende Belege zurück. Der beihilfefähige Betrag wird vom bewilligenden Sachbearbeiter sachlich und rechnerisch festgestellt. Begründende Begleitunterlagen gibt es nicht. Ich vermag der Argumentation des Bundesrechnungshofes nicht zu folgen, daß im Hinblick auf die §§ 48 und 55 RRO auf die Beifügung der Belege nicht verzichtet werden könne, weil aufgrund einer Güter- und Interes-

senabwägung das Verfahren der Vorprüfung der Unfallfürsorge dem Persönlichkeitsrecht des Betroffenen an Geheimhaltung seiner Gesundheitsdaten vorgehe.

Die Daten in Arztrechnungen und Rezepten berühren die Intimsphäre eines Bediensteten und lassen sehr weitreichende, möglicherweise unzutreffende Rückschlüsse Dritter auf seinen Gesundheitszustand zu. Daß die Beifügung der Unterlagen für das Auszahlungsverfahren selbst nicht erforderlich ist, zeigt die Praxis des Beihilfeverfahrens. Der Bundeskasse sollte es ausreichen, daß ein Verantwortlicher die sachliche und rechnerische Richtigkeit festgestellt hat. Auch für Zwecke der Vorprüfung ist das bisherige Verfahren offenbar nicht zwingend. Der Bundesrechnungshof hat zugestimmt, daß von der Beifügung begründender Unterlagen abgesehen werden kann, wenn der Bedienstete die Originalbelege einem anderen oder weiteren Kostenträgern vorlegen muß (z. B. Beihilfe). Es überzeugt nicht, daß in den Fällen, in denen der Bund alleiniger Kostenträger ist, die Beifügung der Unterlagen erforderlich sein soll. Nach meiner Auffassung ist das auch vom Bundesminister der Finanzen in diesem Zusammenhang vorgeschlagene Verfahren, die begründenden Unterlagen bei der anordnenden Dienststelle zu belassen und dort für die Rechnungsprüfung bereitzuhalten, unter dem Gesichtspunkt des Persönlichkeitsschutzes die einzig vertretbare Lösung.

7.1.4 Einzelfälle

— Die Deutsche Bundespost räumt ihren Bediensteten bei der Benutzung des *Postgiroverfahrens* bestimmte Vergünstigungen ein. Das Verfahren im einzelnen regelt sich nach einer Dienstanweisung (DAGehaltskto), die im Amtsblatt des Bundesministers für das Post- und Fernmeldewesen Nr. 96 vom 15. Juli 1982, S. 1046 veröffentlicht ist. Für den Fall, daß ein Bediensteter sein Konto über ein bestimmtes Limit hinaus überzieht, ist eine Sperre zu veranlassen, durch die sichergestellt werden soll, daß künftige Zahlungen nur bei Deckung geleistet werden. Über die Sperren hat die Personalstelle eine Liste zu führen. Diese Aufzeichnungen dürfen nur zur Bearbeitung von Deckungsanfragen genutzt werden.

  Ich habe bei einem Postamt festgestellt, daß sich dennoch ein Sperrvermerk in den Personalpapieren eines Bediensteten befand. Es stellte sich heraus, daß bei dieser Personalstelle regelmäßig entgegen der bestehenden Dienstanweisung verfahren wurde. Ich konnte dieses Verfahren unter Hinweis auf die bestehende Regelung abstellen.

— Ein weiterer Fall der unberechtigten Weitergabe von Daten über wirtschaftliche Verhältnisse von Bediensteten wurde mir durch die Eingabe des Personalrates des Bundesgrenzschutzes (BGS) beim Grenzschutzamt Braunschweig bekannt. Im Rahmen der *Wohnungsfürsorge* verlangte die Bezirksregierung Braunschweig vom Grenzschutzamt Braunschweig, daß einem Belegungsvorschlag für eine Wohnung eine Stellungnahme zu den wirtschaftlichen Verhältnissen beizufügen sei, z. B. ob Pfändungs- bzw. Überweisungsbeschlüsse oder andere Belastungen des Einkommens eines Bewerbers vorlägen. Hintergrund dieser Anforderung ist, daß Bediensteten im Rahmen der Wohnungsfürsorge nur solche Wohnungen zugewiesen werden sollen, deren Miete sie voraussichtlich auch bezahlen können. Ich halte die Datenweitergabe in der vorgesehenen Form für unzulässig. Soweit die BGS-Dienststelle über Unterlagen verfügt, die über Belastungen des Einkommens Auskunft geben, gehören diese Unterlagen zu den Personalakten und sind besonders vertraulich zu behandeln. Eine gesetzliche Grundlage für die Übermittlung dieser Daten sehe ich nicht. Ich halte die Weitergabe daher nur dann für zulässig, wenn die Bediensteten im Einzelfall zugestimmt haben. Eine Verweigerung der Zustimmung kann zwar die Konsequenz haben, daß der Betreffende bei der Wohnungsbelegung nicht berücksichtigt wird. Ich meine aber, es sollte jeder selbst entscheiden, ob er die Geheimhaltung seiner persönlichen Daten der Zuweisung einer preisgünstigen Wohnung vorziehen will. Diese Auffassung habe ich gegenüber dem Personalrat beim Grenzschutzamt Braunschweig zum Ausdruck gebracht.

— Durch eine Eingabe wurde ich darauf aufmerksam, daß den Abteilungskommandeuren des Grenzschutzkommandos (GSK) Süd eine *Liste* aller Hundertschaftsführer *mit dienstlicher Bewertung* ausgehändigt wurde. Das vom Kommandeur des GSK Süd verfolgte Ziel bestand darin, in vertraulichen Erörterungen auf eine Beurteilungspraxis anhand einheitlicher Beurteilungsmaßstäbe innerhalb seiner Behörde hinzuwirken. Der Bundesminister des Innern hat sich meiner kritischen Bewertung des Vorganges unter Hinweis darauf angeschlossen, daß es der Herausgabe einer Listenübersicht nicht bedurft hätte, weil eine Vergleichsbewertung und eine statistische Darstellung unterschiedlicher Beurteilungsmaßstäbe auch möglich gewesen wäre, ohne den konkreten Personenbezug im Einzelfall herzustellen. Er hat deshalb den Kommandeur des GSK Süd angewiesen, diese Listen wieder einzuziehen und vernichten zu lassen. Darüber hinaus wurde mir versichert, daß eine derartige Listenverteilung keine im Bundesgrenzschutz gängige Praxis ist.

— Aufgrund einer Eingabe hatte ich die Hauptverwaltung der Deutschen Bundesbahn um Stellungnahme zu ihrem Verfahren bei der *Rücksendung der Lohnsteuerkarten* an die Mitarbeiter und Versorgungsempfänger der Deutschen Bundesbahn gebeten. Anlaß hierfür war, daß die Lohnsteuerkarten gegen Empfangsbestätigung durch die Dienst- oder Betreuungsstelle offen ausgehändigt wurden. In kleinen Organisationseinheiten (Meistereien) war sogar vorgesehen, daß der Meister und damit der unmittelbare Dienstvorgesetzte eines Beschäftigten diesem

die Lohnsteuerkarte unverschlossen aushändigt. Unter Hinweis darauf, daß auf der Lohnsteuerkarte hochsensible personenbezogene Daten aufgeführt sind, die nur einem Personenkreis zur Kenntnis kommen dürfen, der sie zur Erfüllung seiner Aufgabe benötigt, habe ich die Deutsche Bundesbahn gebeten, ihre Praxis zu überprüfen. Zur Verbesserung des Personaldatenschutzes in diesem Bereich wurde zwischenzeitlich die Weisung erteilt, daß künftig Lohnsteuerkarten nur aufgrund einer schriftlichen Anforderung des Mitarbeiters bzw. Versorgungsempfängers von der Hauptkasse unter Verwendung eines von dem jeweiligen Empfänger beigefügten Briefumschlages, dieser natürlich verschlossen, ausgehändigt werden dürfen.

— Ferner hatte ich mich mit der Frage zu befassen, inwieweit der Bundesminister für das Post- und Fernmeldewesen bei der *Prüfung der Kindergeldanträge* Schul- bzw. Abschlußzeugnisse bei den Bediensteten anfordern kann. Nach meiner Auffassung reicht eine Schlußbescheinigung der Bildungseinrichtung als Nachweis für die Kindergeldzahlung an Bedienstete der Deutschen Bundespost aus. Dieser Auffassung hat sich der Bundesminister für das Post- und Fernmeldewesen angeschlossen und alle Mittelbehörden seines Geschäftsbereiches angewiesen, entsprechend zu verfahren.

— Der Bundesminister der Finanzen hat in einem Erlaß die Veröffentlichung personenbezogener Daten von Verwaltungsangehörigen in Bezirksnachrichten oder Hausmitteilungen in einer Form geregelt, die datenschutzrechtlichen Anforderungen in umfassender Weise Rechnung trägt. Ich habe daraufhin die Bekanntgabe von *„Personalnachrichten" in den Hausmitteilungen des Bundesministers des Innern* überprüft. Der BMI gibt überwiegend Daten bekannt, die unmittelbar von dienstlichem Interesse sind. Neben dem Anlaß der Bekanntgabe werden Namen, Amtsbezeichnung, Organisationseinheit, Hausruf und Zimmernummer veröffentlicht. Der BMI hat mir versichert, daß Wünschen von Bediensteten, auf die Bekanntgabe ihrer Daten in den Hausmitteilungen zu verzichten, ausnahmslos nachgekommen werde. Unter diesem Gesichtspunkt sehe ich kein Erfordernis, die Praxis der Bekanntgabe von „Personalnachrichten" in den Hausmitteilungen des Bundesministers des Innern zu ändern. Allerdings halte ich die Information der Mitarbeiter darüber, daß sie die Möglichkeit haben, einer Veröffentlichung ihrer Daten zu widersprechen, für geboten. Der BMI sieht hierfür — im Gegensatz zum Bundesminister der Finanzen — allerdings keine Notwendigkeit.

7.2 Automatisierte Personaldatenverarbeitung

7.2.1 Personalinformationssysteme

— Im Mittelpunkt meiner Kontrolle der Personaldatenverarbeitung des *Deutschen Patentamtes* (DPA) stand das dort betriebene Personalinformationssystem. Nach meiner Feststellung erscheint der Inhalt der Datenbank (rund 40 Felder mit Angaben zur Person, Ausbildung, zu Kenntnissen usw.) weitgehend problemlos. Lediglich im Hinblick auf die Speicherung und Verarbeitung der Beurteilungsnoten habe ich Bedenken geäußert. Ich habe empfohlen, von der automatisierten Verarbeitung abzusehen, sofern sich diese nicht nur auf die Einzelanzeige am Bildschirm beschränkt. Die Gefahr, daß es bei einer maschinellen Verarbeitung (Reihung, Vergleich mit anderen Mitarbeitern, Auswahl) zu einer Entscheidung durch das maschinelle System kommt, ist nach meiner Auffassung nicht auszuschließen. Dies würde jedoch eine Gefährdung des Persönlichkeitsrechts bedeuten.

Die Auswertung der Datenbank erfolgt mit einer modernen Abfragesprache. Es wurden bisher rund 350 Abfragen entwickelt. Fast ein Drittel davon wurde spontan formuliert. Diese Anzahl erscheint ungewöhnlich hoch. Ich habe hiergegen Bedenken geäußert, weil es nach meiner Bewertung die Verfügbarkeit freier Abfragen ausschließt, daß die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme im Sinne des § 15 Nr. 2 BDSG gewährleistet werden kann.

Hinzu kommt, daß bei spontan formulierten Auswertungen die nach § 75 Abs. 3 Nr. 17 PersVG gebotene Beteiligung der Personalvertretung ebensowenig möglich ist wie die des internen Datenschutzbeauftragten. Ich habe eine Reihe von Verfahrensvorschlägen gemacht und darüber hinaus eine Verbesserung der Datensicherungsmaßnahmen empfohlen.

Daneben habe ich ein weiteres Verfahren zur Personaldatenverarbeitung festgestellt, das bis dahin im DPA nicht als solches erkannt worden war. Dabei melden die Prüfer die im Patentprüfungsverfahren von ihnen erledigten Fälle monatlich ihren Abteilungsleitern. Diese Meldungen werden vom Hauptabteilungsleiter zu namentlichen Jahresübersichten zusammengestellt. Zumindest in einem Fall wurde die monatliche Prüferdatei vom Abteilungsleiter auf einem „pocket computer" geführt und verschiedene Auswertungen ausgedruckt. Dieses Verfahren soll zum einen der Arbeitsdisposition der Prüfabteilungen dienen, es wird zum anderen aber auch zur Leistungsermittlung der Prüfer genutzt: die Zahl der erledigten Prüffälle ist ein Hauptkriterium bei der Beurteilung der Prüfer.

Das DPA erwägt, ein automatisiertes Dialogsystem für Prüfer zu entwickeln, in das auch das vorstehend beschriebene Verfahren integriert werden soll.

Ich habe gegen diese Ausbaupläne insoweit Bedenken erhoben, als ein vollständiges Abbild des Arbeitsverhaltens der Mitarbeiter und eine lückenlose Kontrolle ihrer Leistung ein unverhältnismäßiger und daher unzulässiger Eingriff in Persönlichkeitsrechte wäre. Unter Berücksichtigung dieses Grundsatzes habe ich für die Sy-

stementwicklung die Ausrichtung an folgenden Kriterien empfohlen:

- Vorrang konventioneller Dienstaufsicht vor maschineller Kontrolle
- Kontrollen nur in Form von Stichproben
- Vorrang für Kontrollen mit nicht personenbezogenen Daten (z. B. Abteilungsübersichten) vor individuellen technischen Kontrollen
- Festlegung angemessener Löschungsfristen.

Darüber hinaus habe ich darauf hingewiesen, daß ebenso wie der interne Datenschutzbeauftragte auch der Personalrat an der Entwicklung zu beteiligen ist, da derartige Verfahren der Mitbestimmung unterliegen.

Insgesamt habe ich den Eindruck gewonnen, daß bei der Personaldatenverarbeitung im DPA aus datenschutzrechtlicher Sicht noch ein erheblicher Regelungs- und Kontrollbedarf besteht. Hieraus ergibt sich ein entsprechend hoher Zeitbedarf für die Arbeit des internen Datenschutzbeauftragten. Gegenwärtig stehen ihm nur ca. 10 % seiner Dienstzeit für seine Datenschutzfunktion zur Verfügung. Dies erscheint angesichts der Größe des Amtes und der Vielzahl unterschiedlichster Datenschutzprobleme bei weitem zu wenig. Ich gehe davon aus, daß das Deutsche Patentamt bzw. das Bundesministerium der Justiz als zuständige oberste Bundesbehörde im Sinne des § 15 BDSG innerhalb angemessener Zeit die für die Gewährleistung einer hinreichenden Datenschutzorganisation erforderlichen Entscheidungen treffen wird.

In seiner Stellungnahme hat mir das Deutsche Patentamt mitgeteilt, auf die Speicherung und Verarbeitung der Beurteilungsnote könne wegen der Personalstärke des Deutschen Patentamtes nicht verzichtet werden. Diese Argumentation ist nicht überzeugend, zumal das Amt selbst ausführt, aus dem System erfolge nur eine Vorauswahl durch den Dienstvorgesetzten, der die vollständige Beurteilung (aus der Personalakte) kenne, und eine Entscheidung werde anhand der Personalakte getroffen. Trotzdem halte ich die Verarbeitung der Beurteilungsnote, nur um einen ersten Überblick zu gewinnen, für bedenklich, weil sich erfahrungsgemäß eine solche Vorentscheidung leicht verfestigt.

Meine Anmerkungen hinsichtlich des Einsatzes einer freien Abfragesprache haben das Amt veranlaßt, darauf künftig zu verzichten.

Bezüglich der Entwicklung eines Dialogsystems für Prüfer hat mir das Deutsche Patentamt versichert, eine lückenlose Kontrolle der Leistung, die ein vollständiges Abbild des Arbeitsverhaltens wiedergebe, werde weder angestrebt noch seien Überlegungen in diese Richtung angestellt.

Die von mir als gravierender Mangel in der Datenverarbeitung bewertete dienstliche Nutzung eines privaten PC wurde allen Mitarbeitern von der Amtsleitung inzwischen untersagt.

Auch weitere Anregungen hat das Amt aufgenommen, so daß ich den Eindruck habe, daß hier eine positive Entwicklung eingeleitet wurde. Weitere Gespräche sind erforderlich. So hat sich das DPA zu den von mir angesprochenen Kapazitätsproblemen des internen Datenschutzbeauftragten bisher noch nicht geäußert.

- Bei der *Deutschen Bundesbahn* wurden Planung und Entwicklung der Örtlichen Personaldatenverarbeitung (ÖPDV) fortgeführt (vgl. 8. TB S. 18). Voraussichtlich im Jahr 1987 wird die Einführung des Systems erfolgen. Dann besteht für die einzelnen Dienststellen der Bundesbahn keine Notwendigkeit mehr, eigene Mitarbeiterdateien im bisherigen Umfang fortzuführen. Lediglich einige wenige Daten werden dort (z. B. zur Entwicklung eines Bürokommunikationssystems) erforderlich sein.

  Zur Einführung der ÖPDV soll eine Datenschutzregelung getroffen werden, nach der die daneben bestehenden bzw. zu entwickelnden Dateien in zwei Klassen aufzuteilen sind. Bei der Klasse I handelt es sich um die in § 24 Abs. 2 BDSG genannten Daten — ihre Speicherung soll der Dienststellenleiter genehmigen. In Klasse II einzuordnen sind alle weiteren Daten — über ihre Speicherung entscheidet die Hauptverwaltung der Bundesbahn.

  Durch diese Maßnahme soll die Kontrollierbarkeit von PC erreicht werden. Zusätzlich habe ich ein Verknüpfungsverbot und eine Verwendungsbeschränkung (keine Anwendungen für Personalführung und -disposition) für Daten der Klasse I gefordert sowie auf die Mitbestimmungsbedürftigkeit bei Dateien der Klasse II hingewiesen.

  Der Vorstand der Deutschen Bundesbahn hat mir mitgeteilt, daß für die Realisierung des Projekts ÖPDV Bürocomputer (MDT) eingesetzt werden, die in ihrer Standardsystemfunktion den Anforderungen des Datenschutzes genügen. Die Verarbeitung mit PC werde eingeschränkt. Für sie würden technische Sicherungsmaßnahmen entwickelt, die insbesondere eine stärkere Benutzerführung (geschlossene Menüsteuerung) und -überwachung (Registrierung der Eingaben und Veränderung von Daten) ermögliche. Ein Softwareprodukt sei bereits einsatzbereit.

  Ein abgestuftes Melde- und Genehmigungsverfahren gewährleistet die Berücksichtigung der in meinem Achten Tätigkeitsbericht (S. 55 ff.) entwickelten Grundsätze beim Einsatz von PC.

  Insgesamt ist die Entwicklung der automatisierten Personaldatenverarbeitung der Deutschen Bundesbahn positiv zu bewerten.

- Im Laufe des Berichtsjahres habe ich mehrere Beratungsgespräche mit dem *Bundesminister der Finanzen* geführt, der die Einführung eines DV-gestützten Personalbetreuungs- und Personalverwaltungssystems plant.

  Ich habe es begrüßt, daß mich der Bundesminister für Finanzen bereits zu einem sehr frühen Zeitpunkt um eine Beratung gebeten hat, da sich Datenschutzanforderungen erfahrungsgemäß

nachträglich nur unter großen Schwierigkeiten in ein derartiges System implementieren lassen.

In dem geplanten Personalbetreuungs- und Verwaltungssystem wird eine Verarbeitung von Beurteilungsnoten erfolgen, die nach meiner Bewertung über das vertretbare Maß hinausgeht. Ich hatte in meinem Achten Tätigkeitsbericht empfohlen, von einer automatisierten Verarbeitung solcher Daten abzusehen, sofern sie sich nicht nur auf eine Speicherung zur Einzelanzeige am Bildschrim beschränkt (8. TB S. 16). Der Bundesminister der Finanzen plant für Beförderungen eine maschinelle Reihung nach dem Dienstalter, die einen Bonus aufgrund der Beurteilung berücksichtigt. Dieses Verfahren wird seit Jahren in der nichtautomatisierten Bearbeitung praktiziert, der BMF möchte es in das automatisierte Verfahren übernehmen.

Nach beamtenrechtlichen Grundsätzen sind Beförderungen nach Eignung, Befähigung und fachlicher Leistung vorzunehmen. Allein nach Beförderungsdienstalter und der Gesamtnote der Beurteilung eine Reihung vorzunehmen, wie dies im vorliegenden Fall geschieht, bedeutet die Entscheidung in bedenklicher Weise zu vereinfachen. Selbst wenn man alle in der Beurteilung vorhandenen Einzelbewertungen hinzuzöge, bliebe das Gesamtbild unzureichend. Eine gerechte Entscheidung kann nach meiner Einschätzung immer nur eine Einzelentscheidung auf breitestmöglicher Informationsbasis sein. Für eine Beförderungsentscheidung sollten Informationsbasis das Gespräch mit den Vorgesetzten des Aspiranten, eine Durchsicht der Personalakte sowie alle Angaben der Beurteilung sein. Deshalb darf die Entscheidung nicht einem Rechenwerk (herkömmlicher Art oder durch EDV) mit lediglich zwei Informationen überlassen werden.

Das BAG hat in anderem Zusammenhang ausgeführt (Urteil vom 24. März 1983 — 2 AZR 21/82), Rechenwerke aufgrund von Punktetabellen suggerierten nur eine objektive, voraussehbare und „gerechte" Prüfung. Tatsächlich finde nur eine oberflächliche Würdigung der sozialen Situation der vergleichbaren Arbeitnehmer statt, weil die individuellen Unterschiede in einem allzu groben Raster unkenntlich gemacht würden. Wenn im vorliegenden Fall nur Eignung, Befähigung und fachliche Leistung berücksichtigt werden und nicht auch die soziale Situation, so hielte ich den dieser Entscheidung zugrunde liegenden Gedanken für übertragbar.

Positiv ist zu bewerten, daß eine freie Abfragesprache nicht eingesetzt werden wird, sondern nur fest definierte Anwendungen vorgesehen sind (siehe dazu auch oben Deutsches Patentamt).

— Nach § 15 Abs. 2 GOBReg sind der Bundesregierung alle Vorschläge zur Ernennung von Beamten von der Besoldungsgruppe A 16 ab sowie die Einstellungen und Eingruppierungen von Angestellten nach Vergütungsgruppe BAT I und höher zur Beschlußfassung vorzulegen. Darüber hinaus sind die Ressorts nach § 18 GOBReg verpflichtet, alle Ernennungen, Einstellungen und Eingruppierungen von Beamten/Angestellten des höheren Dienstes dem Bundeskanzler nachträglich zur Kenntnis zu geben.

Dazu erhält das *Bundeskanzleramt* jeweils einen besonderen Personalbogen, der gegenwärtig in einer Akte abgelegt wird. Um diese Informationen besser zu erschließen, sollen künftig die erforderlichen Daten nach einem festgelegten Datenkatalog in eine Datenbank übernommen werden.

Außerdem ist geplant, daß Daten von Personen (in der Regel Beamte der Ministerien, aber auch Persönlichkeiten aus Politik, Wirtschaft und Wissenschaft), die der Bund in die Organe von Unternehmen und Institutionen entsendet, an denen er beteiligt ist, in einer weiteren Datenbank gespeichert werden.

Es ist zu begrüßen, daß das Bundeskanzleramt mich bereits zu einem sehr frühen Zeitpunkt der Planungen um eine Beratung gebeten hat. Nur auf diese Weise ist es möglich, datenschutzrechtliche Anforderungen bei der Verfahrensentwicklung zu berücksichtigen.

Beim gegenwärtigen Sachstand habe ich gegen die weitere Entwicklung dieser Verfahren keine Bedenken: Die Rechtsgrundlagen erscheinen ausreichend, der Umfang der Daten sowie deren Verarbeitung akzeptabel; freie Abfragesprachen sollen nicht eingesetzt werden, sondern nur fest definierte Anwendungen unter strikter Menüsteuerung.

Ich habe empfohlen, bereits beim gegenwärtigen Entwicklungsstand zu prüfen, wie eine Information der Betroffenen über die Art der gespeicherten Daten und deren Verarbeitung sichergestellt werden kann und meine weitere Beratung angeboten.

7.2.2 Telefondatenverarbeitung

In meinem Siebenten Tätigkeitsbericht (S. 19) habe ich darauf hingewiesen, daß zu Abrechnungszwekken gespeicherte Telefonverbindungsdaten für eine Verhaltenskontrolle verwendet werden können, und daß insofern eine Gefährdung des Persönlichkeitsrechts vorliegt. Ich habe Verfahrensvorschläge für die Speicherung und Verwendung der Daten dienstlicher und privater Telefongespräche gemacht.

Der Bundesminister der Finanzen hat mir Anfang 1986 den Entwurf einer Neufassung der Allgemeinen Verwaltungsvorschrift über die Einrichtung und Benutzung dienstlicher Fernmeldeanlagen für die Bundesverwaltung (Dienstanschlußvorschriften — DAV —) zugesandt. Dieser Entwurf berücksichtigt zwar eine Reihe datenschutzrechtlicher Anforderungen. Ich habe dem Bundesminister der Finanzen indessen als weitere Verbesserungen vorgeschlagen, daß die im Entwurf vorgesehene Speicherung der Zielnummer bei Privatgesprächen nicht bzw. nur verkürzt erfolgen soll, sofern der Bedienstete die Speicherung nicht ausdrücklich wünscht.

Darüber hinaus habe ich darauf hingewiesen, daß bei der Einführung des Verfahrens weitere Regelungen erforderlich sind, die den Umfang und das Verfahren der Dienstaufsicht, die Zweckbindung der gespeicherten Daten, ein Verknüpfungsverbot und die Bekanntgabe an die Bediensteten betreffen.

Der Bundesminister der Finanzen hat erwidert, eine verkürzte Speicherung würde eine Klärung von Streitfällen vielfach unmöglich machen oder wesentlich erschweren; er neige dazu, das konkludente Einverständnis des Bediensteten mit der Speicherung der Zielnummer anzunehmen. Die Erörterung hierüber ist noch nicht abgeschlossen.

7.2.3 Verhaltens- und Leistungskontrolle

Die *Deutsche Bundespost* ist eine Behörde mit hohem Automatisierungsgrad. Für die Erledigung vieler Aufgaben wird modernste Informationstechnik eingesetzt. Die Verfahren sind zum Teil auch geeignet, das Verhalten und die Leistung der Beschäftigten zu überwachen (vgl. 8. TB S. 16). Der Bundesminister für das Post- und Fernmeldewesen hatte zur Gewährleistung der Persönlichkeitsrechte der Mitarbeiter bei der Verarbeitung ihrer Daten den Abschluß einer Dienstvereinbarung vorgesehen.

Um mir einen Überblick darüber zu verschaffen, welche zur Verhaltens- und Leistungskontrolle geeigneten Verfahren die Deutsche Bundespost plant, habe ich um Gespräche gebeten. In dem bisher einzigen Gespräch habe ich deutlich gemacht, daß Verfahren zur Verhaltens- und Leistungskontrolle mit technischen Systemen nach meiner Auffassung der Mitbestimmung unterliegen, daß ein *vollständiges* Abbild des Arbeitsverhaltens und eine *lückenlose* Kontrolle der Leistung unzulässig sind und heimliche technische Kontrollen nach meiner Ansicht gegen das Recht auf informationelle Selbstbestimmung verstoßen.

Ich habe angeregt, bei der Entwicklung derartiger Systeme folgende Grundsätze zu berücksichtigen:

— Vorrang konventioneller Dienstaufsicht vor maschineller Kontrolle.

— Transparenz für den Betroffenen, deshalb vorherige Mitteilung des Zeitraums, in dem Kontrollen möglich sind.

— Kontrollen nur stichprobenweise und nur aus konkretem Anlaß.

— Individuelle Kontrollen nur, wenn Kontrollen mit nicht personenbezogenen Daten wirkungslos sind.

Obwohl ich weitere Gespräche mit den betroffenen Fachabteilungen und dem Hauptpersonalrat angeregt hatte, teilte mir der Bundesminister für das Post- und Fernmeldewesen zunächst überraschend mit, er sehe das geführte Gespräch als abschließend an. Er hat lediglich weitere schriftliche Informationen angeboten. Das zwischenzeitlich mit dem Hauptpersonalrat vereinbarte Gespräch wurde gleichwohl durchgeführt. Dabei zeigte sich, daß der Hauptpersonalrat *jegliche* Verhaltens- und Leistungskontrolle mittels technischer Systeme ausschließen möchte.

Auf meinen Wunsch, die Diskussion der Angelegenheit fortzuführen, hat mir der BMP u. a. geantwortet,

— ein vollständiges Abbild des Arbeitsverhaltens werde durch die vorgesehene Dienstvereinbarung ebensowenig ermöglicht wie eine lückenlose Kontrolle der Leistung,

— eine nur stichprobenweise Kontrolle sei aus datenschutzrechtlichen Gründen nicht geboten,

— eine stichprobenweise Kontrolle der Beschäftigten sehe der Entwurf der Dienstvereinbarung gerade vor,

— ob eine Vorschaltung von Kontrollen mit nicht personenbezogenen Daten in bezug auf den Kontrollzweck wirksam sein könne, sei keine Frage des Datenschutzrechtes. Dies gelte ebenso für Kontrollen bei Unterschreiten der Dienst- und Betriebsgütevorhaben,

— bei der DBP seien z. Z. keine automatisch betriebenen Verfahren zur Speicherung von Daten zur Leistungs- oder Verhaltenskontrolle in Betrieb.

Der BMP hat sich neuerdings bereiterklärt, die Gespräche über diesen Komplex wieder aufzunehmen. Allerdings bestünde nicht mehr die Absicht, eine Dienstvereinbarung abzuschließen. Dies ändert jedoch nichts an der Mitbestimmungsbedürftigkeit nach § 75 Abs. 3 Nr. 17 BPersVG.

Ich hoffe, daß es mir gelingt, eine Lösung durchzusetzen, die der Verwaltung eine Dienstaufsicht in angemessener Weise ermöglicht ohne die Persönlichkeitsrechte der Mitarbeiter zu verletzen.

8. Deutsche Bundespost

8.1 Probleme der Zusammenarbeit mit dem Bundesministerium für das Post- und Fernmeldewesen

Trotz unterschiedlicher Rechtsauffassungen in manchen Fragen gestaltet sich die Zusammenarbeit mit dem Bundesministerium für das Post- und Fernmeldewesen in einigen Bereichen positiv. So war es z. B. möglich, hinsichtlich der Nutzung der Anschriften der Fernsprechteilnehmer zu Werbezwecken einen Kompromiß zu erreichen. Künftig wird im Formular „Auftrag für Telefonanschluß" deutlicher als bisher auf diese Nutzung hingewiesen und auf die Möglichkeit aufmerksam gemacht, ihr durch Ankreuzen eines entsprechenden Feldes zu widersprechen.

In anderen Bereichen ist die Zusammenarbeit leider wesentlich schwieriger.

So erreichen mich nach wie vor zahlreiche Briefe von Bürgern, in denen sie mir von Problemen mit Stellen bzw. Diensten der Deutschen Bundespost

berichten. Der deutlich erkennbare Schwerpunkt liegt dabei im Bereich der Telekommunikation, insbesondere beim Telefondienst und neuen Techniken wie Bildschirmtext und Kabelfernsehen. In der Regel bitten mich die Bürger in solchen Schreiben um meine Bewertung der dargelegten Sachverhalte unter datenschutzrechtlichen Aspekten. Mir ist daran gelegen, vor einer solchen Äußerung von der Deutschen Bundespost eine Stellungnahme zu den vom Petenten vorgetragenen Beschwerden zu erhalten. Leider kommt es immer wieder dadurch zu verärgerten Reaktionen bei den betroffenen Bürgern und auch zu einer erheblichen Belastung meiner Dienststelle, daß die Bearbeitung der Stellungnahmen durch das Bundesministerium für das Post- und Fernmeldewesen oft mehrere Monate dauert. So ging mir erst kürzlich eine erbetene Äußerung erst nach 5 Monaten zu. Eine Beschleunigung wäre erreichbar, wenn ich mich mit Auskunftsersuchen direkt an die zuständige Stelle, d. h. unmittelbar an die jeweilige dem Ministerium nachgeordnete Postbehörde, wenden könnte.

Bereits wiederholt hatte ich Anlaß zur Klage, daß die Deutsche Bundespost mich über die bevorstehende Einführung neuer datenschutzrelevanter Dienstleistungen nicht oder aber erst sehr spät informiert. Werden in solchen Fällen im nachhinein unter Gesichtspunkten des Datenschutzes bzw. der Datensicherung Mängel oder Probleme erkannt, ist ihre Behebung bzw. Bewältigung oftmals wesentlich erschwert oder gar unmöglich, da inzwischen vielfach Festlegungen tatsächlicher oder rechtlicher Art getroffen sind. Der Bundesminister für das Post- und Fernmeldewesen hat gelegentlich darauf verwiesen, daß für ihn eine Verpflichtung zur Inanspruchnahme von Beratungen durch mich nicht bestehe. Das mag formal richtig sein, doch der Gesetzgeber hat im Bundesdatenschutzgesetz einen Schwerpunkt der Aufgaben des Bundesbeauftragten für den Datenschutz auch im Bereich *vorbeugender* Maßnahmen gesehen. Dies kommt z. B. in § 19 Abs. 1 Satz 2 zum Ausdruck, der dem Bundesbeauftragten nicht nur eine Beratungspflicht auf entsprechendes Ersuchen zuweist, sondern das Recht einräumt, in eigener Initiative Empfehlungen zur Verbesserung des Datenschutzes zu geben. Ein solches Initiativrecht zum Schutze personenbezogener Daten (vgl. § 1 Abs. 1 BDSG), namentlich zu vorbeugenden Maßnahmen zur Verhinderung von datenschutzrechtlichen Mängeln, kann jedoch nur greifen, wenn der Bundesbeauftragte — zumindest bezüglich automatisierter Verfahren — vor der ersten Speicherung personenbezogener Daten von neuen Verarbeitungsverfahren Kenntnis erhält.

Im übrigen ist daran zu erinnern, daß eine Behörde gem. § 12 Abs. 1 BDSG verpflichtet ist, *„unverzüglich* nach der ersten Einspeicherung" das betreffende Verfahren bekanntzugeben, im Falle der automatisierten Verarbeitung auch dem Bundesbeauftragten für den Datenschutz eine entsprechende Meldung zum Dateienregister zu machen (§ 19 Abs. 4 Satz 3 BDSG). Gerade aber die Anmeldung automatisch betriebener Dateien in neueren Telekommunikationsdienstleistungen ist von der Deutschen Bundespost wiederholt unterlassen worden. Ich gehe davon aus, daß dies bei Inanspruchnahme meiner Beratung im Vorfeld der Diensteinführung nicht geschehen wäre.

Auch von zwei — wegen der Verknüpfung mit Landesrecht — datenschutzrechtlich besonders problematischen Verfahren der Datenübermittlung durch Stellen der Deutschen Bundespost an Dritte erfuhr ich erst nach längerer Zeit und von dritter Seite. Ich verweise hierzu auf meine Ausführungen zur Weitergabe der Anschriften von Kabel- bzw. Satellitenfunkteilnehmern (siehe unten 8.3). Ich würde es sehr begrüßen, wenn die konstruktive und verständnisvolle Zusammenarbeit, die mit einigen Stellen der Deutschen Bundespost bereits besteht, weiter ausgedehnt werden könnte.

8.2 Telekommunikationsordnung

Die Telekommunikation in ihren vielfältigen Ausprägungen ist nicht nur für Wirtschaft und Verwaltung von großer Bedeutung, sondern auch für den privaten Lebensbereich der Bürger immer wichtiger geworden. So ist z. B. das Telefon — nicht nur für Behinderte und alte Menschen — weitgehend unverzichtbar geworden. Wie mir zahlreiche Eingaben von Bürgern immer wieder bestätigten, sind gerade dem Fernsprechteilnehmer seine Rechte und Pflichten gegenüber der Deutschen Bundespost nur unvollständig bekannt. Zwar ist die Fernmeldeordnung (FO), in der die Rechtsbeziehungen zwischen der Deutschen Bundespost und dem Teilnehmer geregelt sind, jedermann zugänglich. Die komplizierte Struktur und die schwierige „Lesbarkeit" sowohl der Fernmeldeordnung selbst als auch der zugehörigen anderen fernmelderechtlichen Benutzungsverordnungen werden aber nicht nur von Laien, sondern auch von Verwaltungsfachleuten als nachteilig empfunden. Hier knüpfte auch die datenschutzrechtliche Kritik an: Der Bürger kann das ihm grundgesetzlich zustehende Recht auf informationelle Selbstbestimmung auch in diesem Zusammenhang nur wahrnehmen, wenn er nicht nur über Rechte und Pflichten aus dem Teilnehmerverhältnis informiert wird, sondern wenn ihm auch die wichtigsten Verfahrensabläufe dargelegt werden.

Auch aus Sicht des Datenschutzes war es daher zu begrüßen, daß der Bundesminister für das Post- und Fernmeldewesen sich entschloß, die wichtigsten fernmelderechtlichen Benutzungsverordnungen — Fernmeldeordnung, Fernschreib- und Datexverordnung, Direktrufverordnung und Telegrammordnung — zusammenzufassen und neu strukturiert zu überarbeiten. Der so entstandene Entwurf einer „Verordnung über die Bedingungen und Gebühren für die Benutzung der Einrichtungen des Fernmeldewesens (Telekommunikationsordnung — TKO —)" wurde mir leider erst recht spät zugänglich gemacht. Ich hielt es daraufhin für dringend geboten, sowohl in schriftlichen Stellungnahmen als auch in mehreren gemeinsamen Besprechungen den Bundesminister für das Post- und Fernmeldewesen auf datenschutzrechtliche Probleme bzw. Defizite hinzuweisen und Änderungen und Ergänzungen anzuregen. Maßstab für meine

Überlegungen waren dabei nicht nur das Bundesdatenschutzgesetz und andere Vorschriften über den Datenschutz, sondern insbesondere auch die vom Bundesverfassungsgericht in seinem Urteil zum Volkszählungsgesetz 1983 herausgearbeiteten Grundsätze zur Zulässigkeit der Beschränkung des Rechts auf informationelle Selbstbestimmung. Hilfreich waren auch die Beratungen mit den Datenschutzbeauftragten der Länder, die ihren Niederschlag in einer gemeinsamen Entschließung zur TKO gefunden haben (siehe Anlage 5).

Einzelne meiner Anregungen fanden in einem überarbeiteten Entwurf der TKO Berücksichtungung, der dem Verwaltungsrat der Deutschen Bundespost zur Beschlußfassung am 30. Juni 1986 vorgelegt wurde. In den vorausgegangenen Gesprächen mit dem Bundesminister für das Post- und Fernmeldewesen waren für einige der noch offenen Probleme bereits Lösungen erkennbar geworden, die entweder in Ergänzungsverordnungen zur TKO eingehen sollen — so z. B. die Schutzvorschriften für Nachrichteninhalte — oder aber in Dienstanweisungen und Informationsschriften, z. B. zur Aufklärung der Teilnehmer über mögliche Datenschutzrisiken des betreffenden Dienstes.

In einer Reihe anderer Fragen konnte indes keine Annäherung der Standpunkte erreicht werden. Wegen ihrer grundsätzlichen datenschutzrechtlichen Bedeutung hielt ich es für erforderlich, den Verwaltungsrat der Deutschen Bundespost auf einige aus meiner Sicht besonders wichtige Probleme aufmerksam zu machen und anzuregen, diese im Rahmen der Beratungen des ihm vorliegenden Verordnungsentwurfes zu berücksichtigen. Dabei konnte ich auf meinen Achten Tätigkeitsbericht (S. 20 f.) Bezug nehmen, in dem ich zwei der angesprochenen Punkte — die Frage der Verordnungsermächtigung sowie die sogenannte „Zwangseintragung" ins Telefonbuch — bereits behandelt habe. Ich habe dort auf die Notwendigkeit einer Prüfung hingewiesen, ob die Verordnungsermächtigung des § 14 Postverwaltungsgesetz für den Erlaß einer Benutzungsverordnung wie der Telekommunikationsordnung ausreicht. Zumindest wenn es um die Regelung völlig neuartiger, das gesamte Kommunikationsverhalten der Menschen möglicherweise verändernder Dienstleistungen geht, erscheint es klärungsbedürftig, ob solche wesentlichen Entscheidungen der Gesetzgeber nicht selbst treffen muß. Ich gehe davon aus, daß mit dieser Rechtsfrage — wegen ihrer über das Post- und Fernmeldewesen hinausgehenden Bedeutung — auch der Bundesminister der Justiz befaßt war. Über das Ergebnis der Untersuchungen bin ich allerdings nicht informiert worden.

Die Eintragung der Teilnehmer ins Telefonbuch auch gegen ihren Willen ist unverändert Gegenstand zahlreicher Eingaben. Insbesondere die Eintragung in das sogenannte Elektronische Telefonbuch des Bildschirmtextdienstes wird als Beeinträchtigung empfunden. Dies bestätigt auch meine rechtliche Bewertung, nach der eine „Zwangseintragung" mit dem Recht auf informationelle Selbstbestimmung nur schwer zu vereinbaren sein dürfte. Da die bislang für die Beibehaltung der „Zwangseintragung" vorgetragenen Argumente diese Bedenken nicht ausräumen konnten, habe ich angeregt, den Telefonteilnehmern in der TKO ein Widerspruchsrecht gegen die Telefonbucheintragung einzuräumen.

In Fällen telefonischer Belästigung führt die Deutsche Bundespost auf Antrag technische Maßnahmen durch, die zur Registrierung von Verbindungsdaten der Telefongespräche — Zeitpunkt, Dauer und angewählte Telefonnummer — führen. Da hier das Recht auf informationelle Selbstbestimmung berührt sein kann, halte ich es für unverzichtbar, sowohl das Verfahren der Registrierung als auch der Auskunftserteilung über die so gewonnenen Daten in aller Deutlichkeit zu regeln. Auch dies ist in der TKO nicht geschehen.

Im Rahmen der Antragstellung auf Einrichtung eines Telefonanschlusses, aber auch in zahlreichen anderen Fällen werden von Stellen der Deutschen Bundespost personenbezogene Daten der Antragsteller registriert, die einem amtlichen Ausweis entnommen werden, in der Regel dem Personalausweis. Dabei wird der Rahmen der zur Identifizierung der Person erforderlichen Daten überschritten. Ich halte es für dringend geboten zu prüfen, ob — über die Ausweisvorlage zur Identifizierung hinaus — Datenregistrierungen dieser Art überhaupt erforderlich sind und welche einzelnen Angaben für den betreffenden Zweck benötigt werden. Abhängig vom Ergebnis dieser Prüfungen müßten Anlaß, Umfang und Zweck solcher Registrierungen verordnungsmäßig geregelt werden.

Im Funkfernsprechdienst („Autotelefon") registriert die Deutsche Bundespost nach wie vor und entgegen meinen Bedenken die Verbindungsdaten aller Telefongespräche (vgl. 7. TB S. 25 f.). Teilt man die Auffassung der Deutschen Bundespost, daß wegen der unzureichenden Mißbrauchssicherung des Funkfernsprechnetzes an einer Vollspeicherung festgehalten werden muß, bedarf diese einer ausdrücklichen und transparenten Regelung in der TKO.

Zu meinem Bedauern ist keiner dieser Punkte vom Verwaltungsrat der Deutschen Bundespost aufgegriffen worden; er hat sich zu meinen Bemerkungen und Besorgnissen auch nicht geäußert. Am 30. Juni 1986 stimmte er dem Verordnungsentwurf zu, der damit am 1. Januar 1988 in Kraft tritt.

8.3 Bekanntgabe der Daten von Kabel- bzw. Satellitenfunkteilnehmern

Die Deutsche Bundespost hat im Berichtszeitraum ihre Anstrengungen weiter verstärkt, den Ausbau der sog. Breitbandkabelnetze voranzutreiben und durch intensive Werbemaßnahmen die Anzahl der angeschlossenen Teilnehmer zu erhöhen. Die Bezeichnung „Breitbandkabelnetz" weist auf die Vielzahl der auf einem Kabel gleichzeitig übertragbaren Kommunikationsvorgänge hin. Die derzeit von der Deutschen Bundespost eingesetzte Technik gestattet die Übertragung von achtzehn Fernseh- und

vierundzwanzig UKW-Rundfunkprogrammen. In der Entwicklung befindet sich bereits ein Nachfolgesystem, das die Übertragung von fünfunddreißig Fernseh- und dreißig UKW-Rundfunkprogrammen ermöglicht. Besonderer Aufmerksamkeit unter Datenschutzaspekten bedarf der sog. Rückkanal: Ein Fernsehteilnehmer, der über ein entsprechendes Zusatzgerät verfügt, kann damit nicht nur als (passiver) Teilnehmer aus einer Vielzahl von Programmen auswählen, er kann vielmehr auch von sich aus in aktiver Weise Informationen an eine Zentrale geben. So kann er sich z. B. elektronisch zur Teilnahme an Spezialfernsehprogrammen anmelden, für die der Anbieter — unabhängig von der Rundfunkgebühr — Vergütungen verlangt. Denkbar sind auch elektronisch durchgeführte Umfragen, in denen etwa der Teilnehmer über Verbrauchsgewohnheiten oder politische Meinungen befragt wird. Nach den mir vorliegenden Informationen ist jedoch derzeit diese Möglichkeit der zweiseitigen Kommunikation nur in einem geringen Teil des vorhandenen Breitbandkabelnetzes realisiert. Ihre Erprobung erfolgt gegenwärtig in einigen von Bund und Ländern besonders geförderten Kabelpilotprojekten, wie z. B. in Dortmund (s. u. 8.4).

Breitbandkabel (BK)-Anlagen werden als Fernmeldeanlagen angesehen; sowohl die Regelungskompetenz für diesen Bereich als auch Errichtung und Betrieb der Infrastruktur liegen somit in der Zuständigkeit des Bundes. Dementsprechend sind die fernmelderechtlichen Bedingungen und Gebühren für BK-Anschlüsse in der Fernmeldeordnung geregelt. Soweit hingegen die in den BK-Netzen übertragenen Informationen als Rundfunk im Sinne des Art. 5 Abs. 1 Grundgesetz anzusehen sind, steht die Gesetzgebungs- und Verwaltungskompetenz den Ländern zu. So ist z. B. im Freistaat Bayern am 22. November 1984 das „Gesetz über die Erprobung und Entwicklung neuer Rundfunkangebote und anderer Mediendienste in Bayern" (MEG) beschlossen worden. Dieses Gesetz sieht die Möglichkeit vor, in die Kabelnetze außer den ortsüblich empfangbaren Rundfunksendungen auch besondere Programme einzuspeisen. Insbesondere ist vorgesehen, durch private Kabelgesellschaften sog. neue Rundfunkprogramme anzubieten. Möchte ein Fernsehteilnehmer ein solches Programm empfangen, muß er mit der zuständigen Kabelgesellschaft einen Vertrag abschließen und das geforderte Entgelt entrichten.

Zur Koordinierung und Abstimmung des fernmelderechtlichen und -technischen Verfahrens der Deutschen Bundespost mit den medienrechtlichen Regelungen des MEG schloß die Deutsche Bundespost mit der nach Landesrecht zuständigen Bayerischen Landeszentrale für neue Medien ein „Rahmenübereinkommen ... über Fragen der Zusammenarbeit aufgrund des Fernmelderechts und des MEG". In diesem verpflichtet sie sich nicht nur, Teilnehmer für den Kabelrundfunk zu werben, sondern auch den Kabelgesellschaften Namen und Anschriften derjenigen bereits an das BK-Netz angeschlossenen Fernsehteilnehmer mitzuteilen, die die erwähnten Sonderprogramme mit dem installierten Anschluß empfangen können. Die zunächst gelegten Anschlüsse enthielten nämlich nicht die Sperreinrichtung, die den Empfang der besonderen Programme verhindert.

Das Übereinkommen wurde mir erst durch den Hinweis eines Abgeordneten des Bayerischen Landtags im Oktober 1985 bekannt. Ich habe dies bedauert, da es angesichts der komplizierten verfassungs- und medienrechtlichen Fragen von Vorteil gewesen wäre, vor einer Entscheidung hierüber den für den Datenschutz zuständigen Stellen Gelegenheit zur Äußerung zu geben (vgl. oben 8.1).

Die Weitergabe von Namen und Anschrift der Kabelteilnehmer durch die Deutsche Bundespost an die privaten Kabelgesellschaften ist entweder mit Einwilligung der Betroffenen oder aufgrund einer Erlaubnisvorschrift des Bundesdatenschutzgesetzes oder einer anderen Rechtsvorschrift zulässig. Eine Einwilligung liegt nicht vor; als Erlaubnisvorschrift käme lediglich § 11 Satz 1 BDSG in Betracht. Danach wäre im vorliegenden Fall die Datenübermittlung zulässig, wenn die Kabelgesellschaft ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden.

Unter den betroffenen Kabelteilnehmern lassen sich drei Gruppen unterscheiden: Einmal diejenigen, die die Sonderprogramme im sog. Zusatzpaket empfangen möchten und daher auch entsprechende vertragliche Vereinbarungen mit den Kabelgesellschaften treffen wollen, ferner diejenigen, die dies nicht wollen und den Empfang entsprechend durch die Deutsche Bundespost sperren lassen sowie jene, die zwar ebenfalls den Empfang der Sonderprogramme nicht wünschen, jedoch nicht gewillt sind, durch die Bundespost nachträglich die — gebührenpflichtige — Sperre vornehmen zu lassen. Bezüglich der ersten Gruppe ist davon auszugehen, daß der Kabelteilnehmer bereit ist, seinem Vertragspartner selbst Namen und Anschriften mitzuteilen. Bezüglich der zweiten Gruppe ist weder Erforderlichkeit noch Zulässigkeit einer Datenübermittlung zu erkennen, da die Kabelgesellschaft an dieser Gruppe kein berechtigtes Interesse geltend machen kann. Bezüglich der dritten Gruppe hingegen ist ein berechtigtes Interesse der Kabelgesellschaften gegeben. Auch kann der betreffende Kabelteilnehmer keine schutzwürdigen Belange dahin gehend geltend machen, als „Schwarzseher" Fernsehprogramme sehen zu können, ohne den landesrechtlich hierfür erforderlichen Vertrag abgeschlossen zu haben. Lediglich bezüglich solcher Fernsehteilnehmer ist die Übermittlung ihrer personenbezogenen Daten auch gegen ihren Willen durch die Deutsche Bundespost an die Kabelgesellschaften als zulässig anzusehen. Ich gehe davon aus, daß die Deutsche Bundespost bei der Durchführung des Rahmenübereinkommens in diesem Sinne verfährt und im übrigen auch durch Aufklärung aller Betroffenen für hinreichende Transparenz des Verfahrens sorgt.

Ähnliche Probleme treten bei der Weitergabe von Daten über Satellitenrundfunkteilnehmer auf. Der Empfang von Satelliten-Fernsehprogrammen ist zwar mit einigem technischen Aufwand verbunden,

aber durchaus möglich: Bereits drei Satelliten strahlen Programme aus, der Start weiterer steht bevor. Die erforderliche Empfangsanlage wird von der Deutschen Bundespost als Fernmeldeanlage qualifiziert und bedarf dementsprechend einer fernmelderechtlichen Genehmigung. Wegen der hohen Kosten wird eine solche Anlage überwiegend zur Einspeisung der Satellitenprogramme in Gemeinschaftsantennenanlagen und von Fachgeschäften für Demonstrationszwecke, für ausschließliche Privatnutzung aber nur ausnahmsweise errichtet. Wird eine Satellitenfunkempfangsanlage nicht ausschließlich für privaten Einzelempfang oder für Demonstrationszwecke benutzt, sondern sollen die empfangenen Programme über Kabelanlagen weiterverbreitet werden, so unterliegt dies landesrechtlichen Vorschriften, z. B. in Bayern dem bereits erwähnten Medienerprobungs- und entwicklungsgesetz. Nach diesem bedarf die Weiterverbreitung dann einer Genehmigung durch die Bayerische Landeszentrale für neue Medien, wenn sie in Kabelanlagen mit mehr als hundert angeschlossenen Wohneinheiten erfolgen soll (Art. 35 Abs. 1 Satz 2 MEG).

Wie ich wiederum erst von dritter Seite erfahren habe, hat der Bundesminister für das Post- und Fernmeldewesen im Juni 1986 die Oberpostdirektionen angewiesen, den landesrechtlich zuständigen Stellen — in Bayern der Bayerischen Landeszentrale für neue Medien — Ablichtungen aller Genehmigungsurkunden für Satellitenfunkempfangsanlagen zu übermitteln. Ich bat das Ministerium daher mit Schreiben vom 11. Juni 1986, mir diese Information zu bestätigen und mich gegebenenfalls über die Rechtsgrundlage sowie über das Verfahren zu informieren. Erst am 11. November 1986 ging mir das Antwortschreiben zu, dessen Ausführungen zur Zulässigkeit der genannten Datenübermittlung mich noch nicht befriedigen und weiterer Erörterung bedürfen. Auch hier bleibt festzuhalten, daß eine frühzeitige Information über das vorgesehene Verfahren angezeigt gewesen wäre.

Wegen der späten Antwort konnte die Diskussion noch nicht abgeschlossen werden. Nach einer ersten von mir vorgenommenen Bewertung stellt sich jedoch die Datenschutzproblematik wie folgt dar:

Die Zulässigkeit der Weitergabe der Daten der Genehmigungsinhaber durch die Deutsche Bundespost an die Bayerische Landeszentrale ist gemäß § 10 BDSG zu beurteilen. Sie ist dann gegeben, wenn die Datenübermittlung zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Empfängers liegenden Aufgaben erforderlich ist. Da die in Frage stehende Datenübermittlung keine der Deutschen Bundespost zugewiesene Aufgabe betrifft, wäre sie nur in den Fällen zulässig, in denen sie für die Aufgaben der empfangenden Stelle erforderlich ist. Nach meiner Überzeugung ist dies nur bezüglich solcher Satellitenfunkteilnehmer der Fall, die die empfangenen Programme in Kabelanlagen mit mehr als hundert angeschlossenen Wohneinheiten einspeisen wollen, weil dann eine landesrechtliche Genehmigung verlangt wird. Diese Teilnehmer müssen daher eine Übermittlung der erforderlichen Daten durch die Deutsche Bundespost an die Bayerische Landeszentrale dulden. Ob diese nach Landesrecht auch in solchen Fällen tätig werden muß, in denen die Einspeisung in Kabelanlagen mit weniger als einhundert Wohneinheiten vorgesehen ist, erscheint mir zweifelhaft. Bezüglich derjenigen Satellitenfunkempfangsanlagen jedenfalls, die ausschließlich für privaten Individualempfang oder für Demonstrationszwecke — etwa im Geschäftslokal des Teilnehmers — errichtet werden, liegt m. E. keine Weiterverbreitung von Rundfunkprogrammen im Sinne des MEG vor, ein Tätigwerden der Bayerischen Landeszentrale ist mithin nicht veranlaßt. Eine Übermittlung personenbezogener Daten dieser Inhaber einer fernmelderechtlichen Genehmigung durch die Deutsche Bundespost an Dritte ohne Einwilligung wäre daher unzulässig.

In seiner Stellungnahme ist der Bundesminister für das Post- und Fernmeldewesen nicht darauf eingegangen, ob und in welcher Weise die Deutsche Bundespost bei der Übermittlung der in Frage stehenden Daten unter den dargelegten Gesichtspunkten differenziert.

8.4 Kabelpilotprojekt Dortmund

Am 20. Dezember 1983 beschloß der Landtag Nordrhein-Westfalen das „Gesetz über die Durchführung eines Modellversuchs mit Breitbandkabel (Kabelversuchsgesetz NW)". Dabei geht es darum, über die Breitbandkabelnetze der Deutschen Bundespost neben den vorhandenen Rundfunkprogrammen auch neue Programmangebote zu erproben. In den Modellversuch soll auch die Erprobung neuer Informations- und Kommunikationsdienste sowie des sog. Rückkanals (siehe oben 8.3) einbezogen werden. Zur Planung, Vorbereitung und Durchführung aller programmseitigen Maßnahmen hat der Westdeutsche Rundfunk eine Projektstelle eingerichtet („Kabelfunk Dortmund"). Die Oberpostdirektion Dortmund übernahm die Realisierung und den Betrieb der notwendigen kabeltechnischen Infrastruktur im Versuchsgebiet, also des eigentlichen Kabelnetzes, sowie der für Betrieb und Administration erforderlichen Zentralen. Sie stellt auch die Heranführung und Einspeisung der Satellitenprogramme und der normalen Fernsehprogramme sicher. Die Hausverkabelung zwischen dem postalischen Übergabepunkt des Kabelnetzes und dem Endgerät, an das der Fernsehapparat angeschlossen wird, besorgt das örtliche Fachhandwerk.

Die Einspeicherung der personenbezogenen Daten der Teilnehmer am Pilotprojekt in die zentralen Rechner des Fernmeldeamtes Dortmund begann am 1. Juni 1985. Damit war die speichernde Stelle gemäß §§ 12 Abs. 1, 19 Abs. 4 Satz 3 BDSG verpflichtet, die Datei zu veröffentlichen und zum Register der automatisch betriebenen Dateien anzumelden. Dies geschah jedoch erst im April 1986, nachdem ich auf diese Rechtspflichten aufmerksam gemacht hatte. Diese Verstöße gegen die genannten Vorschriften des BDSG habe ich gegenüber dem Bundesminister für das Post- und Fernmeldewesen gemäß § 20 Abs. 1 BDSG beanstandet.

Im März des Berichtsjahres habe ich die Verarbeitung personenbezogener Daten durch die Deutsche Bundespost im Rahmen des Kabelpilotprojektes Dortmund kontrolliert. Ansatzpunkte waren dabei die genannten zentralen Rechner des Fernmeldeamtes Dortmund, in denen die Daten der rund 8 000 Projekt-Fernsehteilnehmer verwaltet werden und die auch das besondere Breitband-Kabelnetz des Pilotprojekts steuern. Das Projekt weist zwei Besonderheiten auf: Zum einen ist dies der bereits erwähnte Rückkanal, der es dem Fernsehteilnehmer ermöglicht, mit den zentralen Rechnern zu kommunizieren, also etwa bestimmte entgeltpflichtige Sonderprogramme abzurufen. Ungewöhnlich ist ferner die Art, wie der Fernsehapparat an das postalische Netz angeschlossen wird: Beim normalen Breitbandkabelanschluß geschieht dies über eine nichtintelligente „Antennensteckdose", beim Pilotprojekt dagegen über einen sog. „fernadressierbaren Teilnehmerkonverter" (FAT), der im Haus des Teilnehmers installiert wird. Er enthält einen Mikroprozessor und wird nicht nur von den zentralen Rechnern der Bundespost gesteuert, sondern übermittelt diesen auch Informationen. Dies hatte in der Öffentlichkeit zu der Besorgnis geführt, mit Hilfe des FAT könnten die Fernsehgewohnheiten der angeschlossenen Teilnehmer ohne ihr Wissen und Zutun registriert werden (welches Programm wann und wie lange?). Meine Datenschutzkontrolle setzte daher insbesondere an diesem Punkt an; ein zweiter Prüfungsschwerpunkt war die Verwaltung der Teilnehmerdaten.

Hinsichtlich der auf die FAT gerichteten Besorgnis habe ich folgendes festgestellt: Das Betrachten „normaler", nicht entgeltpflichtiger Fernsehprogramme durch den Fernsehteilnehmer führt zu keiner Speicherung personenbezogener Daten. Anders ist dies, wenn der Teilnehmer ein entgeltpflichtiges sog. Spartenprogramm („Unterhaltungskanal", „Kulturkanal" usw.) ansehen möchte: Nachdem er diesen Wunsch mit Hilfe seines Bediengeräts dem zentralen Rechner elektronisch mitgeteilt hat, registriert der FAT die dafür anfallenden Entgelte. Diese werden laufend kumuliert und täglich vom FAT zum zentralen Rechner übertragen; im FAT selbst werden sie gelöscht. Bereits zu diesem Zeitpunkt lassen die Entgelte nicht mehr erkennen, durch welche Programme sie verursacht oder zu welchen Zeitpunkten die Programme gesehen wurden. In der weiteren Verarbeitung in der Zentrale werden die Entgelte über jeweils einen Monat addiert und dem Kabelfunk Dortmund — als Gläubiger — mitgeteilt. Zusammenfassend kann festgestellt werden, daß die Datenschutzkontrolle dieses Verfahrens keine Anhaltspunkte für eine Registrierung des „Fernsehverhaltens" der angeschlossenen Teilnehmer durch die Deutsche Bundespost ergeben hat.

Dagegen gab die Datenverarbeitung sowohl im Bereich der Teilnehmerverwaltung als auch beim Betrieb der zentralen Rechner über die bereits erwähnten Beanstandungen hinaus Anlaß zur Kritik. Der für den „Antrag auf Kabelanschluß und Teilnahme am Kabelpilotprojekt Dortmund" verwendete Vordruck ermöglicht dem Betroffenen nicht die Unterscheidung zwischen solchen Angaben, zu denen er verpflichtet ist, und solchen, die er darüber hinaus freiwillig macht. Die Gestaltung des Antragformulars als mehrteiliger Durchschreibesatz sieht Übermittlungen der Daten sowohl an den Kabelfunk Dortmund als auch den Handwerksbetrieb vor, der die hausseitige Installation des Kabelanschlusses vornimmt. Dabei wurde jedoch nicht durchgängig dem Grundsatz Rechnung getragen, daß nur die Übermittlung erforderlicher Daten zulässig ist.

Weder der Antrag selbst noch das vorgeheftete Merkblatt klärt den Antragsteller darüber auf, daß seine personenbezogenen Angaben in Listenform auch an die Handwerkskammern zur Abwicklung des landesrechtlich vorgesehenen Subventionsverfahrens weitergeleitet werden. Sowohl bezüglich der Erforderlichkeit einzelner in der Liste enthaltenen Daten als auch grundsätzlich zur Zulässigkeit der Übermittlung der Liste habe ich Bedenken geäußert. Die Übermittlung wurde inzwischen eingestellt.

Schwachpunkte waren im Bereich der technisch-organisatorischen Sicherheitsmaßnahmen festzustellen. Insbesondere waren die programmseitig zu treffenden Vorkehrungen nicht ausreichend, die sicherstellen sollen, daß ein Bediensteter im Bereich der automatisierten Datenverarbeitung nur solche Tätigkeiten vornimmt, z. B. Programme aufruft, die zur Durchführung der ihm geschäftsplanmäßig zugewiesenen Aufgaben erforderlich sind. Ich habe es begrüßt, daß meine zur Verbesserung gegebenen Empfehlungen Berücksichtigung finden sollen.

8.5. Anschriftenermittlung zu posteigener Werbung

Bereits in meinem Achten Tätigkeitsbericht (S. 23) habe ich zu dem Problem der Ermittlung von Anschriften Neugeborener durch Postzusteller Stellung genommen. Im Laufe des Berichtsjahres bin ich durch weitere Eingaben von Bürgern darauf aufmerksam gemacht worden, daß die Zusteller der Deutschen Bundespost auch angehalten sind, Anschriften von Konfirmanden und Kommunionkindern zu sammeln, um der Deutschen Bundespost eine gezielte Werbung für den Postsparkassendienst zu ermöglichen.

In diesem Verfahren sehe ich ebenfalls einen Anreiz, das Postgeheimnis im Einzelfall zu durchbrechen, da es für den Zusteller naheliegt, die Information den Postsendungen zu entnehmen. Außerdem ist zu bedenken, daß auch eine behördeninterne Informationsweitergabe zur Erledigung sachfremder Aufgaben nur dann zulässig ist, wenn die Zweckentfremdung gesetzlich erlaubt ist. Diese Voraussetzung ist in den geschilderten Fällen nicht gegeben.

Darüber hinaus bin ich der Meinung, daß der Amtsverschwiegenheit nicht nur solche Informationen unterliegen, die der Postzusteller zur Erfüllung seiner Amtspflichten benötigt, sondern auch solche, die er nur im Rahmen seiner Amtsausübung wahrnimmt. Abgesehen davon kann eine Informationsbeschaffung durch Postzusteller, die nicht ihrer ei-

gentlichen Aufgabe — nämlich der Postzustellung — dient, geeignet sein, das bestehende Vertrauensverhältnis zwischen Bürger und Zusteller als dem Behördenvertreter, der dem Bürger am häufigsten begegnet, zu beeinträchtigen.

9. Verkehrswesen

9.1 Fahrzeugregistergesetz (ZEVIS)

Das Gesetz zur Änderung des Straßenverkehrsgesetzes (StVG), das Regelungen über die Fahrzeugregister bei den örtlichen Kfz-Zulassungsstellen sowie beim Kraftfahrt-Bundesamt (KBA) vorsieht, ist vom Deutschen Bundestag am 5. Dezember 1986 verabschiedet worden und tritt am 15. Februar 1987 in Kraft.

Dieses Gesetzgebungsvorhaben sollte ursprünglich zusammen mit den übrigen von den Koalitionsfraktionen und von der Bundesregierung eingebrachten und sodann zurückgestellten Sicherheitsgesetzen beraten und beschlossen werden. Aus gegebenem Anlaß (siehe oben 1.2) wurde im Herbst 1986 auf Koalitionsebene beschlossen, das ZEVIS-Gesetz aus dem Paket der Sicherheitsgesetze herauszulösen und noch in der laufenden Legislaturperiode zu verabschieden. In diesem Zusammenhang wurden hauptsächlich folgende Änderungen gegenüber der ursprünglichen Entwurfsfassung vorgeschlagen:

- Es entfällt die Einschränkung, daß die Nachrichtendienste das Register für verkehrsfremde Zwecke nur nutzen dürfen, „soweit Anhaltspunkte vorliegen für eine sicherheitsgefährdende oder geheimdienstliche Tätigkeit oder Bestrebung, die darauf gerichtet ist, Gewalt anzuwenden oder Gewaltanwendung vorzubereiten".
- Die Aufgaben des Bundesnachrichtendienstes und des Militärischen Abschirmdienstes, zu deren Erfüllung die Nutzung des Registers zulässig sein soll, werden bis zum Inkrafttreten gesetzlicher Aufgabenbestimmungen in einer Übergangsvorschrift umschrieben.

Über die Hauptpunkte des Gesetzentwurfs, meine grundsätzlichen Positionen hierzu und die noch bestehenden Bedenken habe ich schon früher berichtet (7. TB S. 27 ff., 8. TB S. 23 ff.). Bei der Beratung des Gesetzentwurfs im Innenausschuß des Deutschen Bundestages konnte ich meine Auffassung zu den einzelnen Vorschriften darlegen, jedoch leider nur noch marginale Änderungen erreichen. Da es sich um das erste bereichsspezifische Gesetz handelt, in dem — laut seiner Begründung — die Folgerungen aus den vom Bundesverfassungsgericht aufgestellten datenschutzrechtlichen Grundsätzen gezogen werden sollen, sind folgende allgemeine Bemerkungen angebracht:

1. Bisher wurde nie schlüssig dargelegt, daß die Bekämpfung des Terrorismus durch datenschutzrechtliche Hemmnisse beim Zugang zu Daten der Kraftfahrzeugzulassung behindert worden wäre, wie dies jetzt als Begründung für die vorgezogene Verabschiedung des Gesetzes angegeben wurde. In den Beratungen wurde auch eingeräumt, daß die erwähnte Erweiterung der Datennutzung durch die Nachrichtendienste weniger für die Terrorismusbekämpfung als für den Extremismusbereich bringt, wobei die Grenze zwischen beiden Bereichen fließend sei. Diese Entwicklung ist deshalb bedenklich, weil sie einen Kernpunkt der Sicherheitsgesetze betrifft, deren Entwürfe bislang von einer Trennung zwischen gewaltfreien und gewaltätigen Demonstrationen ausgehen und unter diesem Gesichtspunkt zwischen Extremismus und Terrorismus unterscheiden.

2. Entsprechend den von mir im Achten Tätigkeitsbericht (S. 24) aufgestellten Grundsätzen zur Datennutzung habe ich vorgeschlagen, den Speicherungszweck eindeutiger zu definieren; er muß sich an der spezifischen Verantwortung des Fahrzeughalters für die von seinem Fahrzeug ausgehenden verkehrs- und umweltbezogenen Gefahren orientieren.

   Für sie hat der Fahrzeughalter einzustehen; nur wegen dieser besonderen Haftung kann von ihm verlangt werden, das Fahrzeug mit einem Kennzeichen zu versehen und registrieren zu lassen, wodurch seine Identifizierung ermöglicht wird. Jede andere Nutzung der Registerdaten bedeutet eine Zweckentfremdung, die besonders zu rechtfertigen ist. Die vom Gesetz gewählte Definition des Speicherzwecks ist m. E. unklar, weil sie weitere Zwecke mit einbezieht, und zwar auch solche, bei denen ein überwiegendes Allgemeininteresse für eine zwangsweise Erhebung und Speicherung gerade dieser Daten nicht ohne weiteres erkennbar ist.

3. So ist m. E. ein praktisches Bedürfnis für die Zulassung der zweckfremden Nutzung des Registers für die Erfüllung der gesetzlichen Mitteilungspflichten zur Sicherung des Steueraufkommens nach § 93 der Abgabenordnung nicht dargetan. Die Datenübermittlung zur Sicherung des Kfz-Steueraufkommens ist anderweitig geregelt. Ich halte es aber nicht für gerechtfertigt, das Fahrzeugregister zu einem allgemeinen Daten-Service für die Finanzverwaltung werden zu lassen. Ähnliches gilt auch für andere nicht verkehrsbezogene Datennutzungen.

4. In den bisherigen Verhandlungen hatte ich deutlich gemacht, daß eine effektive Datenschutzkontrolle bei Abrufen im automatisierten Verfahren nur möglich ist, wenn im Protokoll auch der konkrete Anlaß des Abrufs und die für den Abruf verantwortliche Person festgehalten werden. Das daraufhin in den Gesetzentwurf eingearbeitete und nunmehr beschlossene Stichprobenverfahren sieht zwar vor, daß für einen vom Kraftfahrt-Bundesamt ausgewählten Teil der Abrufe weitere Aufzeichnungen dieser Art gefertigt werden. Dies soll aber in der Weise geschehen, daß die geforderten zusätzlichen Angaben nur für einen vorher ausgewählten Teil der Abrufe erfragt werden. Ich halte dieses Stichprobenverfahren für Kontrollzwecke für wenig geeignet. Wer das Abrufsystem unbefugt benutzen

will, bleibt so lange ohne Entdeckungsrisiko, bis er einmal vom System zur Angabe des Abrufanlasses aufgefordert wird; geschieht dies, kann er einen im Einzelfall schwer widerlegbaren, abstrakt zulässigen Abfragegrund angeben. Systematisches Fehlverhalten kann damit nicht erkannt werden, solange der Benutzer sich geschickt verhält.

Ich hatte statt dessen vorgeschlagen, stets alle notwendigen Daten zu erheben und erst *bei der Speicherung* mit einem Auswahlverfahren zu arbeiten. Die Auswahl sollte nicht allein zufallsbestimmt, sondern auch nach sachlichen Gesichtspunkten gesteuert werden, die sich aus der Kontrollpraxis ergeben können (z. B. vollständige Aufzeichnung des Dialog-Verkehrs eines bestimmten Terminals, wenn sich dort Auffälligkeiten gezeigt haben). Unkorrekte bzw. unzulässige Abrufe würden mit einem solchen Verfahren schon durch die Ungewißheit, ob die Abrufe protokolliert werden, verhindert bzw. eingeschränkt.

5. Ein weiterer Mangel des Gesetzentwurfs bestand darin, daß eine Nutzungsbeschränkung im Sinne einer Zweckbindung für übermittelte Daten fehlte. Eine entsprechende übergreifende gesetzliche Regelung ist meiner Auffassung nach erforderlich, solange auf der Empfängerseite — vornehmlich bei der Polizei und den Diensten — keine Verwendungsbeschränkungen bestehen. Mein entsprechender Vorschlag wurde in das Gesetz zwar eingefügt, sein Regelungsgehalt jedoch dadurch entscheidend abgeschwächt, daß der Empfänger die für einen bestimmten Zweck übermittelten Daten auch für andere Zwecke nutzen darf, soweit ihm die Daten auch für diese Zwecke hätten übermittelt werden dürfen. Hierüber kann der Empfänger allein entscheiden; die Zweckentfremdung wird auch nicht protokolliert. Diese Regelung halte ich sowohl unter dem Gesichtspunkt der Zweckbindung der Daten, wie auch der Transparenz ihrer Nutzung und einer effektiven Datenschutzkontrolle für bedenklich.

6. Die Übergangsvorschrift mit der Aufgabenumschreibung für MAD und BND wurde nicht befristet. Ich hatte in den Beratungen vorgeschlagen, durch eine Frist (Ende der 11. Legislaturperiode) den politischen Willen zu verdeutlichen, in angemessener Zeit spezialgesetzliche Regelungen für den Bundesnachrichtendienst und den Militärischen Abschirmdienst zu schaffen.

Ich begrüße es, daß der Deutsche Bundestag die Bundesregierung um einen Erfahrungsbericht zu einigen umstrittenen Regelungen des Gesetzes (automatisiertes Abrufverfahren, Aufzeichnungspflicht, P-Anfrage, Einsichtnahme in örtliche Fahrzeugregister) gebeten hat. Der an mich gerichteten Bitte, mich an diesem Bericht zu beteiligen, werde ich gerne nachkommen, zumal damit die Möglichkeit gegeben ist, eventuelle Schwachstellen zu prüfen und dazu Korrekturen vorzunehmen. Ich muß allerdings darauf aufmerksam machen, daß die Aufnahme neuer arbeitsintensiver Projekte — bei denen auf der Verwaltungsseite eine Vielzahl von Mitarbeitern mehrerer großer Bundesbehörden beteiligt ist — eine bessere Personalausstattung meiner Dienststelle voraussetzt.

9.2 Verkehrszentralregister

9.2.1 Stand der Gesetzesvorbereitung

Bereits im Februar 1984 hatte der Bundesminister für Verkehr angekündigt, daß die Bundesregierung sobald als möglich den Entwurf eines Verkehrszentralregistergesetzes vorlegen wird. Durch ein solches Gesetz sollen die derzeit im StVG und in der Straßenverkehrs-Zulassungs-Ordnung (StVZO) verstreut untergebrachten Rechts- und Verwaltungsvorschriften zusammengefaßt, die Tilgungsvorschriften mit dem Ziel, den Bewährungscharakter stärker herauszustellen, geändert und den Anforderungen des Datenschutzes deutlicher als bisher Rechnung getragen werden. In meinem Siebenten Tätigkeitsbericht (S. 33) hatte ich auf die Notwendigkeit einer entsprechenden gesetzlichen Regelung hingewiesen, da die bestehenden Vorschriften zum Teil unklar, unvollständig und widersprüchlich sind und einigen darüber hinaus die notwendige gesetzliche Grundlage fehlt. In den Beratungen des Innenausschusses des Deutschen Bundestages zu meinem Sechsten und Siebenten Tätigkeitsbericht wurde ebenfalls hervorgehoben, daß es notwendig sei, eine differenzierte Regelung auch im Sinne des Beschlusses des Deutschen Bundestages in Drucksache 10/1719 (Beschlußempfehlung des Innenausschusses zum Fünften Tätigkeitsbericht) zu treffen. Mit diesem Beschluß wurde die Bundesregierung ersucht, darzustellen, wie entsprechend den Grundsätzen des Volkszählungsurteils für das Verkehrszentralregister sichergestellt werden kann, daß

— nur zwingend erforderliche Tatbestände eingetragen werden,

— Auskünfte nur im zwingend erforderlichen Rahmen erteilt werden und

— das Verfahren und die Fristen für die Tilgung den schutzwürdigen Belangen der Betroffenen und den praktischen Gegebenheiten entsprechend geregelt werden.

Auf eine entsprechende Anfrage teilte mir der Bundesminister für Verkehr im September 1986 mit, daß für die Erstellung eines neuen Entwurfs eines Verkehrszentralregistergesetzes derzeit eine längerfristig angelegte Bestandsaufnahme durchgeführt werde. In den Entwurf sollten auch Erkenntnisse aus der parlamentarischen Beratung der sog. Sicherheitsgesetze einfließen. Es werde angestrebt, den Entwurf in der nächsten Legislaturperiode einzubringen.

Das Bundesverfassungsgericht hat zur Frage des Übergangsbonus eindeutige Aussagen gemacht (siehe oben 1.3). Ich halte es nicht für angängig, daß trotzdem Regelungen längerfristig aufrechterhalten werden, die dem vom Bundesverfassungsgericht aufgestellten Gebot der Reduzierung der Eingriffsbefugnis auf das für einen funktionsfähigen Betrieb unerläßliche Maß zuwiderlaufen. Das gilt

umso mehr, als auch das fachlich zuständige Ministerium meine Bedenken teilt, nachdem ich im Jahre 1984 eine Beanstandung ausgesprochen hatte.

9.2.2 Auskunftserteilung nach § 30 StVG (Vollauskunft)

Über die datenschutzrechtlich unzulässige Praxis der Auskunftserteilung aus dem Verkehrszentralregister durch das Kraftfahrt-Bundesamt habe ich in meinem Siebenten Tätigkeitsbericht (S. 31) berichtet. Im März 1985 teilte mir der Bundesminister für Verkehr zwar mit, daß er meine Auffassung, Auskünfte dürften nur in dem tatsächlich erforderlichen Umfang erteilt werden, grundsätzlich anerkenne, daß zu seinem Bedauern ein Lösungsvorschlag zu dem Problem der Vollauskunft jedoch noch nicht habe erarbeitet werden können. In Zusammenarbeit mit den Bundesländern und meiner Dienststelle sollten die jetzige Eintragungspraxis überprüft, die denkbaren Auskunftsfälle aufgelistet und diesen die für die Auskünfte jeweils notwendigen Eintragungen zugeordnet werden. Das Ziel sollte sein, möglichst bald eine Teilauskunftsregelung zu finden, die sowohl dem Datenschutz als auch den Zielen und Zwecken des Verkehrszentralregisters gerecht wird. Erste Überlegungen hierzu sind mir im Oktober 1986 zugegangen. Meine Frage, wann mit einer Entscheidung über die Vorabregelung gerechnet werden könne, wurde vom Bundesminister für Verkehr nicht beantwortet.

Die schleppende Art der Entscheidungsvorbereitung ist meiner Meinung nach nicht mit dem Grundsatz vereinbar, daß bis zur Herstellung eines verfassungsmäßigen Zustandes durch den Gesetzgeber die Befugnis zu Eingriffen in verfassungsrechtliche Positionen auf das zu reduzieren ist, was im konkreten Fall für die geordnete Weiterführung eines funktionsfähigen Betriebs unerläßlich ist. Die vom Bundesminister für Verkehr geduldete fortgesetzte Praxis zu weitgehender Auskunftserteilung verstößt gegen verfassungsrechtliche Grundsätze und muß daher umgehend korrigiert werden.

9.3 Kfz-Zulassungsdaten

9.3.1 Zusatzerhebung bei Ausländern

§ 23 Abs. 1 der StVZO bestimmt die Daten, die der Verfügungsberechtigte eines Kraftfahrzeuges bei dessen Zulassung anzugeben hat.

Ein Landesbeauftragter für den Datenschutz hat festgestellt, daß die Mehrzahl der Zulassungsstellen bei Kfz-Anmeldungen von Ausländern über die nach § 23 Abs. 1 StVZO zu erhebenden Daten hinaus die Angabe der Paßdaten und der Heimatanschrift verlangt. Die Zulassungsstellen berufen sich dabei auf einen Beschluß des Bund-Länder-Fachausschusses für Angelegenheiten der Zulassung von Fahrzeugen im Straßenverkehr vom 5./6. November 1981, welcher besagt,

— daß Heimatanschrift und Paßdaten gefordert werden können und

— daß sich die Erfassung der Heimatanschrift bei Ausländern sehr positiv ausgewirkt habe.

Die Geschäftsführung dieses Ausschusses liegt beim Bundesminister für Verkehr. Er hat den Zulassungsstellen in einer sog. Verkehrsverlautbarung bereits im Jahre 1966 (Verkehrsblatt 1966 S. 535) empfohlen, die Paßdaten entweder bei der Anmeldung oder Umschreibung von Kraftfahrzeugen für Halter mit ausländischer Staatsangehörigkeit zu ermitteln und in der Karteikarte zu vermerken oder diese Daten bei der zuständigen Ausländerbehörde zu erfragen.

Der Bundesminister für Verkehr nahm meine Bitte um Stellungnahme zu der zusätzlichen Datenerhebung zum Anlaß, die Angelegenheit erneut im Bund-Länder-Fachausschuß zur Sprache zu bringen. Dieser bestätigte nach Mitteilung des Bundesministers für Verkehr die Notwendigkeit der Erfassung der Paßdaten und der Heimatanschrift bei ausländischen Fahrzeughaltern für Maßnahmen nach 29d STVZO (Außerbetriebsetzung von unversicherten Fahrzeugen), soweit das Fahrzeug ins Ausland verbracht wurde. Der Bundesminister für Verkehr verwies in diesem Zusammenhang darauf, daß es bei der Außerbetriebsetzung vor allem auch auf rasches Handeln ankomme; Daten müßten daher erforderlichenfalls sofort zur Verfügung stehen. Anfragen an die Ausländerbehörden seien mit erheblichen Zeitverzögerungen verbunden, die nicht hinnehmbar seien. Der Bundesminister für Verkehr vertritt daher die Auffassung, daß die Erhebung der Paßdaten und der Heimatanschrift bei Ausländern durch die Zulassungsstellen erforderlich sei. Er war nicht bereit, die erwähnte Verkehrsverlautbarung vom 19. September 1966 (s. o.) zu ändern. Gegen sie bestehen folgende datenschutzrechtliche Bedenken:

§ 23 Abs. 1 StVZO ist m. E. eine abschließende Regelung, die nicht zur Disposition der Verwaltungsbehörden steht. Da eine Auskunftspflicht bezüglich der erwähnten Daten mangels Rechtsgrundlage nicht besteht, könnten sie allenfalls unter ausdrücklichem Hinweis auf die Freiwilligkeit nach § 9 Abs. 2 BDSG erfragt werden. Was die Erforderlichkeit betrifft, stehe ich auf dem Standpunkt, daß es auch nach dem Volkszählungsurteil des Bundesverfassungsgerichts (Verbot der Datensammlung auf Vorrat) unzulässig ist, für Zwecke des Verwaltungsvollzugs im Rahmen des § 29 d StVZO zwangszweise Daten bei einer Vielzahl von Personen nur vorsorglich für den Fall zu erheben, daß die Außerbetriebsetzung eines Fahrzeugs im Inland nicht möglich ist und eine Ausfuhr ins Ausland unterstellt werden kann. Dieses Verfahren steht in keinem Verhältnis zu dem angestrebten Schutzzweck. Für die Außerbetriebsetzung eines Fahrzeugs müßten deshalb andere, weniger belastende und mit dem Verhältnismäßigkeitsgrundsatz in Einklang stehende Verfahren gefunden werden. Im übrigen sieht auch das inzwischen verabschiedete Gesetz zur Änderung des Straßenverkehrsgesetzes (ZEVIS) keine entsprechende Erweiterung des Erhebungskatalogs vor.

Ich habe die Landesbeauftragten für den Datenschutz von meiner Auffassung in Kenntnis gesetzt, da die Datenschutzkontrolle bei den Zulassungsstellen in ihre Zuständigkeit fällt. Wie ich erfahren habe, verzichten die Zulassungsstellen mehrerer Länder inzwischen auf die vorsorgliche Erhebung und Speicherung der zusätzlichen Daten. Der Bundesminister für Verkehr sollte — auch aus Gründen der Rechtsvereinheitlichung — nunmehr die Konsequenzen ziehen und auf eine verfassungskonforme Datenerhebung bei der Kfz-Zulassung für Halter mit ausländischer Staatsangehörigkeit hinwirken.

9.3.2 Übermittlung an die Automobilindustrie

Über die Praxis des Kraftfahrt-Bundesamtes, Zulassungsdaten an die Automobilindustrie zu liefern, habe ich in meinem Siebenten Tätigkeitsbericht (S. 30) berichtet. Aufgrund der im Jahre 1984 darüber geführten Verhandlungen mit dem Bundesminister für Verkehr unter Beteiligung des Kraftfahrt-Bundesamtes und dem Verband der Automobilindustrie bin ich zu folgender Rechtsauffassung gelangt:

— Die Übermittlung von Daten aus der Kfz-Zulassung an Kfz-Hersteller und -Importeure stellt — soweit sie nicht unmittelbar der Sicherheit des Straßenverkehrs dient — eine Zweckentfremdung dar; sie ist daher nur im überwiegenden Allgemeinintresse auf einer gesetzlichen Grundlage zulässig.

— Das Interesse von Teilnehmern am privaten Wirtschaftsverkehr, die Vertragstreue ihrer Partner überprüfen zu können, stellt kein derartiges überwiegendes Interesse dar, das die Übermittlung aus behördlichen Datenbeständen rechtfertigen könnte.

— Gegen die Übermittlung von Zulassungsdaten, soweit sie ausschließlich zahlenmäßig, nämlich zur Bildung mathematisch-statistischer Vergleichsgrößen verwendet werden, bestehen keine grundsätzlichen Bedenken, wenn die ausschließlich statistische Verwendung gesetzlich festgelegt und durch geeignete Maßnahmen einschließlich der Datenschutzkontrolle sichergestellt wird, daß eine Verwendung zu anderen Zwecken ausgeschlossen bleibt.

— Die Bedenken gegen die Übermittlungspraxis lassen sich für eine begrenzte Übergangszeit zurückstellen, wenn die Datenschutzanforderungen bis zu einer gesetzlichen Regelung durch vertragliche Abmachungen gewährleistet werden.

Der Bundesminister für Verkehr wies nach längeren Verhandlungen zwischen allen Beteiligten das Kraftfahrt-Bundesamt an, entsprechend meinen Forderungen zu verfahren.

Die vom Kraftfahrt-Bundesamt daraufhin erarbeitete Zusatzvereinbarung zu den mit den Automobilherstellern und Importeuren abgeschlossenen Verträgen sieht vor, daß Daten ausschließlich für statistische Feststellungn in bezug auf die Verkehrssicherheit der Fahrzeuge bereitgestellt werden. Daten, die sich auf eine bestimmbare Person, eine bestimmte Fahrzeug-Identifizierungsnummer oder auf eine bestimmte Fahrzeugbriefnummer beziehen (d. h. nicht anonymisierte Daten), sollen nur dann übermittelt werden, wenn der Empfänger glaubhaft darlegt, daß eine Verwendung der Daten für statistische Feststellungen auf andere Weise nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist und unter Berücksichtigung des Zwecks des Vorhabens kein Grund zur Annahme besteht, daß schutzwürdige Belange eventuell Betroffener beeinträchtigt werden. Aufgrund dieser vertraglichen Festlegungen konnte ich davon ausgehen, daß grundsätzlich nur anonymisierte Daten übermittelt werden.

Durch die Eingabe eines Petenten traten erste Zweifel auf, ob die Datenübermittlungen entsprechend den Vorgaben der Zusatzvereinbarung erfolgen und ob die Empfänger der Daten diese auch nur für die in der Zusatzvereinbarung festgelegten Zwecke nutzen. Die Auskunft des Kraftfahrt-Bundesamtes auf eine entsprechende Frage zu der Übermittlungspraxis bestätigte meine Befürchtungen. Die fortgesetzte gegen § 3 BDSG verstoßende Übermittlungspraxis durch das Kraftfahrt-Bundesamt habe ich daher gegenüber dem Bundesminister für Verkehr beanstandet.

Nunmehr hat sich herausgestellt, daß das Kraftfahrt-Bundesamt die in der Zusatzvereinbarung niedergelegten besonderen Datenschutzvorkehrungen generell nicht beachtet hat; gleichwohl betrachtet es seine Praxis als rechtmäßig und beabsichtigt auch weiterhin so zu verfahren.

Ich muß demnach feststellen, daß das Kraftfahrt-Bundesamt meinen datenschutzrechtlichen Bedenken nur formal, nämlich durch Abschluß der Zusatzvereinbarung, Rechnung getragen, die beanstandete Übermittlungspraxis jedoch unverändert fortgesetzt hat. Obwohl der Bundesminister für Verkehr meine Bedenken teilte, hat er sich weder davon überzeugt, daß das Kraftfahrt-Bundesamt auch entsprechend verfährt, noch hat er Schritte unternommen, die rechtswidrige Datenübermittlung zu unterbinden.

Nach § 19 Abs. 3 Bundesdatenschutzgesetz sind alle Behörden des Bundes verpflichtet, den Bundesbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen. Nach § 15 BDSG haben die Obersten Bundesbehörden jeweils für ihren Geschäftsbereich die Ausführung des Bundesdatenschutzgesetzes sowie anderer Vorschriften über den Datenschutz sicherzustellen. An beide Verpflichtungen hat sich der Bundesminister für Verkehr im vorliegenden Fall nicht gehalten.

9.4 Führerschein auf Probe

Mit dem vom Deutschen Bundestag am 20. März 1986 beschlossenen Gesetz zur Änderung des Straßenverkehrsgesetzes wurde der Führerschein auf Probe eingeführt und im Zusammenhang damit

auch eine neue zentrale Datenspeicherung beim Kraftfahrt-Bundesamt. Über die Grundzüge der inzwischen in Kraft getretenen Gesetzesänderung habe ich in meinem Achten Tätigkeitsbericht (S. 25) berichtet. Ich habe auch darauf hingewiesen, daß die Bundesregierung meinem Vorschlag, die Geltung des Gesetzes zu befristen, gefolgt war. Die vorgesehene Befristung von acht Jahren wurde jedoch aufgrund einer Empfehlung des federführenden Bundestagsausschusses für Verkehr, der diese Regelung für entbehrlich hielt, nicht in den Gesetzesbeschluß des Deutschen Bundestages aufgenommen. Mein Vorschlag bezweckte, zunächst Erkenntnisse über die Eignung des Gesetzes zur Erreichung des verfolgten Ziels zu gewinnen (wissenschaftliche Begleituntersuchung), um danach endgültig beurteilen zu können, ob eine zentrale Datei aller Fahranfänger verhältnismäßig und erforderlich ist. Ich bin nach wie vor der Meinung, daß aus Gründen des Datenschutzes und der Entbürokratisierung eine nur versuchsweise Einführung des Führerscheins auf Probe sachgerechter gewesen wäre.

Zur Durchführung des Gesetzes über die Fahrerlaubnis auf Probe hat der Bundesminister für Verkehr den Entwurf einer Sechsten Verordnung zur Änderung straßenverkehrsrechtlicher Vorschriften erstellt. Dieser sieht u. a. vor, daß der Betroffene die schriftliche Anordnung der zuständigen Behörde zu einer Nachschulung dem Kursleiter bei der Anmeldung vorzulegen hat. Dadurch muß er sensible persönliche Angaben (begangene Verkehrsverstöße, die zu der Anordnung führten) offenbaren. Das Gesetz sieht eine solche Information, die als Erhebung von Daten zu beurteilen ist, jedoch nicht vor. Es bestehen auch Zweifel, ob die Verordnungsermächtigung nach § 6 Abs. 1 Nr. 1 d StVG eine faktisch zwangsweise Erhebung personenbezogener Daten durch die Kursleiter rechtfertigt. Allerdings ist auch richtig, daß sich die Pflicht zur Mitteilung dieser Daten aus dem Sinngehalt des Gesetzes ergibt, weil sich danach die Gestaltung der Nachschulungskurse richtet. Meine Bedenken könnte ich daher unter der Voraussetzung zurückstellen, daß die Kursleiter (evtl. durch Auflagen) verpflichtet werden, die erforderlichen Datenschutz-Vorkehrungen (Schutz gegen Mißbrach, Sicherung gegen unbefugte Nutzung, Verwertungsverbot, Löschungsregelungen) zu treffen. Die Datenschutzgesetze reichen dazu wegen ihrer Beschränkung auf Dateien und mangels einer Zweckbindungsregelung nicht aus; die Dringlichkeit ihrer Novellierung wird hier wieder einmal deutlich.

Ich habe diese Bedenken dem Bundesrat mitgeteilt, der sich meiner Auffassung anschloß. Die von ihm vorgeschlagene Ergänzung der Verordnung sah vor, daß der Kursleiter die aus der schriftlichen Anordnung ersichtlichen personenbezogenen Daten Dritten nicht ohne Einwilligung des Betroffenen mitteilen und sie auch nicht für andere Zwecke als für die Durchführung des Nachschulungskurses verwenden darf.

Der Bundesminister für Verkehr sah sich wegen der vom Bundesrat vorgeschlagenen umfangreichen Gebührenerhöhungen nicht in der Lage, die Verordnung in der vom Bundesrat empfohlenen Fassung zu erlassen, und hat dem Bundesrat den Verordnungsentwurf erneut in der ursprünglichen Fassung zugeleitet; warum die Verbesserungsvorschläge zum Datenschutz nicht übernommen wurden, ist mir nicht bekannt.

Da der Bundesrat seinen ursprünglichen Beschluß hinsichtlich der datenschutzrechtlichen Erfordernisse nach erneuter Beratung bestätigte, gehe ich davon aus, daß der Bundesminister für Verkehr diesen Empfehlungen folgen wird.

9.5 Luftfahrt-Bundesamt (LBA)

Im Februar 1986 habe ich erneut die Aufgaben und Arbeitsbereiche des Luftfahrt-Bundesamtes (LBA) kontrolliert, die ich erstmals im Jahre 1984 geprüft hatte (vgl. 7. TB S. 36). Dabei mußte ich wiederum Datenschutzverstöße feststellen und erneut eine Beanstandung aussprechen.

9.5.1 Fehlende Rechtsgrundlagen

Immer noch fehlt es für eine Reihe von Datenverarbeitungsvorgängen des Luftfahrt-Bundesamtes an der erforderlichen gesetzlichen Grundlage. Die Angaben aus der Luftfahrzeugrolle, die vom Betroffenen unter Zwang auf der Grundlage der Luftverkehrszulassungsordnung (LuftVZO) erhoben werden, werden nach wie vor in den Nachrichten für Luftfahrer und im Registre Aéronautique International veröffentlicht. Auf die datenschutzrechtliche Unzulässigkeit der Datenübermittlung zum Zwecke der Veröffentlichung und den insoweit bestehenden Regelungsbedarf hatte ich bereits hingewiesen (7. TB a. a. O.).

Der Bundesminister für Verkehr hat mir jetzt mitgeteilt, daß er prüfen werde, ob und wie die betreffenden Bestimmungen des Luftverkehrsgesetzes und der Luftverkehrszulassungsordnung geändert werden können, damit die Veröffentlichungen auf eine datenschutzrechtlich tragfähige Grundlage gestellt werden.

Ebenfalls in meinem Siebenten Tätigkeitsbericht hatte ich auf die Notwendigkeit hingewiesen, die Datensammlungen über Luftfahrer (Positiv-Datei/Negativ-Datei) nach der Art der zu verarbeitenden Daten und den Zwecken, zu denen diese Verwendung finden sollen, in einer gesetzlichen Regelung präzise zu bestimmen. Obwohl der Bundesminister für Verkehr den Regelungsbedarf seinerzeit anerkannt hat, sind auch zwei Jahre danach noch keine konkreten Ansätze, geschweige denn Ergebnisse, vorhanden.

Die Negativ-Datei wird gegenwärtig nach den Bestimmungen eines internen, vom Luftfahrt-Bundesamt erarbeiteten Entwurfs einer Verfahrensvorschrift für die Aufnahme und Tilgung von Eintragungen geführt. Dabei werden u. a. rechtskräftige Verurteilungen sowie strafgerichtliche Entschei-

dungen, durch die von Strafe abgesehen worden ist, und Verfahrenseinstellungen nach § 153a StPO erfaßt, ohne daß ein Sachzusammenhang der diesen Entscheidungen zugrundeliegenden Handlungen des Betroffenen mit der Luftsicherheit bestehen muß. Ich habe deshalb den Bundesminister für Verkehr darauf hingewiesen, daß eine uneingeschränkte Speicherung strafrechtlicher Verurteilungen in einem Informationssystem über Luftfahrer unzulässig ist. Maßstab für die Speicherung von Negativangaben kann indes deren Aussagekraft für Zwecke der Luftsicherheit sein. Unter diesem Gesichtspunkt muß geprüft werden, wie sich die eintragungsfähigen Straftatbestände etwa auf bestimmte Gruppen von Straftaten eingrenzen lassen.

Auch für den Umgang mit personenbezogenen Informationen bei der Wahrnehmung der Aufgaben der Flugunfalluntersuchung durch die Flugunfalluntersuchungsstelle beim Luftfahrt-Bundesamt besteht gegenwärtig noch keine gesetzliche Grundlage. Eine Übermittlung personenbezogener bzw. personenbeziehbarer Daten aus diesem Bereich an Dritte erfolgt zum einen in der Weise, daß bei Anfragen von Versicherungen ein mit dem Luftfahrt-Bundesamt abgestimmter Fragebogen benutzt wird. Mit diesem Fragebogen erbitten die Versicherungen unter Angabe des Luftfahrzeugs, des Unfallorts und -zeitpunkts sowie der Personendaten des verantwortlichen Luftfahrzeugführers nähere Einzelheiten zum Flugunfall. Das Luftfahrt-Bundesamt beantwortet diese Anfragen aus der Unfalluntersuchungsakte. Zum anderen ist die automatisierte Kurzfassung des Unfalluntersuchungsberichts (EDV-Unfallbericht) auf Anforderung für jeden Dritten zugänglich. Trotz der unbestreitbaren Verbesserung, die das Fragebogenverfahren gegenüber dem früher geübten Aktenversand bedeutet (vgl. 7. TB S. 36), kann immer noch nicht ausgeschlossen werden, daß im Einzelfall auch bei dieser eingeschränkten Übermittlung schutzwürdige Belange des Betroffenen beeinträchtigt werden. Angesichts der Vielzahl zum Teil sehr sensibler Daten, die bei einer Flugunfalluntersuchung erhoben werden, halte ich es deshalb auch aus der Sicht der Flugunfalluntersuchungsstelle für wünschenswert, gesetzlich genau und präzise zu regeln, welche Daten im einzelnen an wen weitergegeben werden dürfen. Damit bis zum Inkrafttreten einer gesetzlichen Regelung Grundrechtsverletzungen vermieden werden, habe ich außerdem die Empfehlung ausgesprochen, einstweilen nur noch solche Angaben in den automatisierten Unfalluntersuchungsbericht aufzunehmen, die ausschließlich sachliche, flugtechnische Eigenschaften betreffen und die so aufbereitet sind, daß sie keiner natürlichen Person mehr zugeordnet werden können.

9.5.2 Technische und organisatorische Mängel

Die im Jahre 1984 festgestellten technischen und organisatorischen Mängel beim Luftfahrt-Bundesamt wurden inzwischen zu einem Großteil abgestellt. Wegen mangelhafter Maßnahmen zur Sicherung der Datenverarbeitung aufgrund fehlender Dokumentation und unzureichender Paßwortverwaltung mußte ich jedoch erneut eine Beanstandung aussprechen. Bei einer Reihe von manuell geführten Karteien mit personenbezogenen Angaben fehlten zum Zeitpunkt der Kontrolle Sicherungsmaßnahmen.

9.6 Deutsche Bundesbahn (DB)

9.6.1 Deutsche Bundesbahn als Teilnehmer an Verkehrsverbünden

Einige Bundesbahndirektionen sind Gesellschafter von Verkehrs- und Tarifverbünden, die für ihre Gesellschafter auf dem Gebiet des öffentlichen Personennahverkehrs Aufgaben der Verkehrsforschung und -planung, der Gestaltung und Abstimmung der Betriebsleistungen, der Festsetzung eines Gemeinschaftstarifs (Verbundtarif) und der Beförderungsbedingungen sowie des Marketing und der Verteilung von Einnahmen wahrnehmen.

Eine Petentin wandte sich gegen das von dem Verkehrs- und Tarifverbund Stuttgart GmbH (VVS) praktizierte Verfahren, die Abgabe von Wertmarken für bestimmte Wochen und Monate nach einem sog. Übergangstarif von der Abgabe eines vollständig ausgefüllten Fragebogens abhängig zu machen, mit dessen Hilfe personenbezogene Daten (Name, Anschrift, Verbundpaßnummer) erhoben und gespeichert werden. Nachdem die Bemühungen der Petentin um eine Änderung des Verfahrens sowohl bei dem Innenministerim Baden-Württemberg als der für den nicht-öffentlichen Bereich zuständigen Datenschutzaufsichtsbehörde (datenschutzrechtlich nicht zu beanstanden) als auch bei dem Landesbeauftragten für den Datenschutz Baden-Württemberg (fehlende Zuständigkeit) erfolglos geblieben waren, wandte sie sich an mich als der nach dem BDSG für die Deutsche Bundesbahn in Angelegenheiten des Datenschutzes zuständigen Stelle.

Ich habe festgestellt, daß der VVS im Namen seiner Gesellschafter mit anderen regionalen Verkehrsunternehmen Verträge abgeschlossen hat, nach denen der auf die einzelnen Unternehmen entfallende Anteil des Gesamterlöses aus den verkauften Wertmarken des sog. VVS-Übergangstarifs dadurch ermittelt wird, daß jährlich einmal eine schriftliche Befragung der Fahrgäste beim Verkauf der Wertmarken dieses Tarifs durchgeführt wird. Der Inhalt des entsprechenden Fragebogens ergibt sich aus einem sog. Informationsverzeichnis, das Bestandteil der Verträge ist.

Der Übergangstarif gilt nach Mitteilung der Deutschen Bundesbahn auch für sie, da auch Strecken der Deutschen Bundesbahn in seinen Geltungsbereich fallen. Die Deutsche Bundesbahn hat mir darin zugestimmt, daß sich ihe datenschutzrechtliche Verantwortung auch auf diese tarifrechtliche Regelung erstreckt.

Der VVS — und somit auch die einzelnen Gesellschafter nebst den mit dem VVS kooperierenden regionalen Verkehrsunternehmen — verwendet

Fragebögen, die entgegen den abgeschlossenen Kooperationsverträgen auch Fragen nach Name und Anschrift des Kunden enthalten. Meine Bitte um Stellungnahme zu dem beanstandeten Verfahren leitete die Bundesbahndirektion Stuttgart an den ihrer Meinung nach zuständigen VVS weiter. Dieser teilte mir daraufhin mit, daß vorgesehen sei, „dieses Mal auf die Namensangabe und die Angabe der Hausnummer zu verzichten". Diese sachgerechte Änderung des Verfahrens begrüße ich. Mir ist allerdings unverständlich, warum in den Jahren bis 1985 die Erhebung personenbezogener Angaben immer mit der Notwendigkeit zu Plausibilitätskontrollen begründet wurde; nunmehr reicht nach Auskunft des VVS die bereits früher ebenfalls erhobene Verbundpaßnummer aus, um diese Funktion zu erfüllen.

Angesichts anscheinend unterschiedlicher Rechtsauffassungen der Bundesbahndirektionen sollte die Deutsche Bundesbahn, soweit sie an Verkehrs- und Tarifverbünden beteiligt ist, darauf hinwirken, daß die vertraglichen Abmachungen den Anforderungen des Datenschutzes entsprechen, und — notfalls durch Wahrnehmung ihrer Gesellschafterrechte — erforderliche Änderungen veranlassen. Ferner sollte sie dafür sorgen, daß die Aufteilung des Erlöses auf die einzelnen Gesellschafter und die mit den Verkehrs- und Tarifverbünden kooperierenden Verkehrsunternehmen möglichst auf der Grundlage anonymer statistischer Erhebungen erfolgt.

Da es nicht ausgeschlossen ist, daß mit der in dem erwähnten Fragebogen erhobenen Verbundpaßnummer ein Personenbezug hergestellt werden kann, habe ich die Deutsche Bundesbahn um Mitteilung gebeten,

- ob, in welcher Form und von welchen Stellen Aufzeichnungen über die Inhaber der Verbundpässe geführt werden und gegebenenfalls welchen Löschungsregelungen sie unterliegen,
- in welche Elemente die Verbundpaßnummer gegliedert ist,
- welche Rückschlüsse von der Verbundpaßnummer auf die Inhaber von Verbundpässen möglich sind und
- welche Funktion die Verbundpaßnummer im Rahmen des Abrechnungsverfahrens einnimmt.

Eine Beantwortung der bereits im Juli dieses Jahres gestellten Fragen steht noch aus. Erst danach kann ich beurteilen, ob für die korrekte Aufteilung der Verbundeinnahmen die Kenntnis der Verbundpaßnummer erforderlich ist, ob mit ihrer Hilfe eine Personenzuordnung möglich ist und daher die §§ 3 und 23 BDSG Anwendung finden.

9.6.2 Videoaufzeichnungen

Über einzelne Methoden der Viedeoüberwachung durch die Deutsche Bundesbahn habe ich in meinem Achten Tätigkeitsbericht (S. 25 f.) berichtet, soweit mir hierüber Erkenntnisse vorlagen. Ich habe gleichzeitig darauf hingewiesen, daß mir ein vollständiges Bild des Umfangs der Video-Nutzung durch die Bundesbahn noch nicht vorlag. Inzwischen hat mir die Hauptverwaltung folgendes mitgeteilt:

„Es gibt im DB-Berich bereits Anwendungsgebiete für die Video-Technik. Dabei kommt es, über die bereits diskutierte „Fern-Beobachung" über Monitor (aus Gründen der Personalersparnis anstelle einer örtlichen Überwachung) hinaus auch zu gezielten, sporadischen und regelmäßigen Aufzeichnungen der aufgenommenen und übertragenen Bilder.

Abgesehen von der Verwendung

- für filmische Zwecke (Dokumentation, Werbung)
- als Lehrmittel (Schulungsseminare)
- zur Überwachung technischer Anlagen (Versuchsüberwachung, Fahrdrahtlageüberwachung)

hat sich die Aufzeichnung auf Magnetband als vorzügliche Hilfe insbesondere bei der Rekonstruktion und Beweissicherrung bei Unfällen und Unregelmäßigkeiten

sowie in der Verbrechensbekämpfung bewährt, z. B.

- bei der Gefahrraumüberwachung an fernbedienten Bahnübergängen und
- der Ihnen bereits näher erläuterten Überwachung der Bahnsteige bei der S-Bahn Hamburg,
- als Observationshilfe bei der Diebstahlbekämpfung (z. B. Überwachung nicht öffentlicher Lagerhallenteile, Schließfachanlagen usw.),
- als Beweismittel bei Tumulten, Schlägereien und Beschädigungen von DB-Einrichtungen, z. B. durch Rowdytum von Faußballfans u. ä.

Hierzu werden Kameras verdeckt angebracht, um mit Hilfe der Aufnahmen — soweit ein sofortiges Eingreifen durch Monitorüberwachung nicht möglich ist — eine Tat- und Täterbeschreibung und die Tatzeit zu erhalten sowie die Filme auch als Beweismittel vorlegen zu können.

Die DB hat auch bereits mehrfach der Rauschgiftfahndung der Länder auf Antrag entsprechende Amtshilfe geleistet.

Bei Einsatz für Überwachungsaufgaben (z. B. S-Bahn Hamburg, Bahnübergänge) werden die Bänder in der Regel nicht aufbewahrt, sondern wieder überspielt. Nur bei Unfällen oder Unregelmäßigkeiten werden die Bänder zur Beweissicherung ausgewertet und — soweit erforderlich — aufbewahrt.

Bei der Verbrechensbekämpfung ist die Handhabung ähnlich. Zum Teil werden die Bänder nach Auswertung gelöscht, z. T. werden sie als Beweismaterial bis zur gerichtlichen Klärung aufbewahrt."

Ich habe der Deutschen Bundesbahn daraufhin mitgeteilt, daß — abgesehen von der Gefahrraumüberwachung an den Bahnübergängen, der Überwachung der Bahnsteige bei der S-Bahn Hamburg und der Überwachung sonstiger technischer Anlagen —

Maßnahmen der Bahnpolizei mit Eingriffscharakter nach § 57 Eisenbahn-Bau- und Betriebsordnung sowie Maßnahmen im Rahmen der Strafverfolgung nach der StPO sich auf konkrete Einzelfälle zu beschränken haben. Gegen eine Aufzeichnung aller Personen ohne konkreten Anlaß, die in den Blickwinkel der Kameras geraten, bestünden grundsätzliche Bedenken, denn es würden personenbezogene Daten über jedermann erhoben und festgehalten, bis das Band entweder neu überspielt oder aufgrund einer Entscheidung des zuständigen Beamten ausgewertet wird.

Die Erhebung und gleichzeitige Speicherung dieser personenbezogenen Daten, die bis zu ihrer Löschung jederzeit auswertbar sind, beeinträchtigt das informationelle Selbstbestimmungsrecht der Betroffenen. Für diese bahnpolizeilichen Maßnahmen besonderer Art unter Einsatz technischer Mittel bedarf es m. E. einer speziellen Befugnisnorm im Bahnpolizeirecht (gegebenenfalls auch im Rahmen eines Bundespolizeigesetzes).

Zu meinen Bedenken hat die Deutsche Bundesbahn ergänzend mitgeteilt, daß sich lediglich die Bundesbahndirektionen Karlsruhe und Frankfurt des Einsatzes von Videoanlagen zur Überwachung bei der Verbrechensbekämpfung, und zwar nur in Einzelfällen, bedienen. Eine Überwachung mit Aufzeichnung bestimmter Örtlichkeiten durch fest installierte Anlagen erfolge in keinem Fall ständig oder zu bestimmten Zeiten. Die Aufzeichnungen würden im übrigen nach Abschluß des Strafverfahrens oder nach Auswertung gelöscht bzw. bei der nächsten Aufnahme überspielt.

Ich werde mich über die Video-Praxis der Bundesbahn bei nächster Gelegenheit an Ort und Stelle informieren.

10. Statistik

10.1 Bundesstatistikgesetz

Nachdem mit dem Mikrozensusgesetz und dem Volkszählungsgesetz 1987 schon zwei wichtige bereichsspezifische Statistikgesetze an das Volkszählungsurteil angepaßt worden waren, wurde im Berichtszeitraum auch das Bundesstatistikgesetz novelliert, das die allgemeinen Regelungen, die für alle Bundesstatistiken gelten, enthält. Zu dem Entwurf des Bundesministers des Innern für die Neufassung des Bundesstatistikgesetzes habe ich bereits in meinem Achten Tätigkeitsbericht (S. 28 f.) Stellung genommen. Inzwischen ist das neue Bundesstatistikgesetz verabschiedet worden und in Kraft getreten.

Der Verabschiedung ging eine Anhörung im Innenausschuß des Deutschen Bundestages voraus, in der ich — ebenso wie in den nachfolgenden Beratungen des Ausschusses — Gelegenheit hatte, auf die datenschutzrechtlich problematischen Vorschriften des Regierungsentwurfs hinzuweisen. Außerdem habe ich zu dem Entwurf gegenüber dem Innenausschuß ausführlich schriftlich Stellung genommen. Eine Reihe meiner Empfehlungen hat Eingang in das Gesetz gefunden. Gleichwohl konnte ich meine Vorstellungen in einigen wichtigen Punkten nicht durchsetzen.

Hervorzuheben sind zunächst folgende *Verbesserungen des Datenschutzes:*

- Der Katalog von Sachverhalten, über die der einzelne Bürger bei statistischen Erhebungen schriftlich zu unterrichten ist, wurde erweitert (z. B. Zweck, Art und Umfang der Erhebung, die verwendeten Hilfsmerkmale, Bedeutung und Inhalt von laufenden Nummern und Ordnungsnummern).

- Bei statistischen Erhebungen dürfen nur solche Erhebungsbeauftragte (z. B. Zähler, Interviewer) eingesetzt werden, bei denen Interessenkonflikte wegen ihrer beruflichen Tätigkeit oder aus anderen Gründen auszuschließen sind. Es besteht darüber hinaus das Recht, schriftlich zu antworten.

- Die Auskunftsverpflichtung gilt nicht mehr als Grundsatz, sondern sie muß in der eine Bundesstatistik anordnenden Rechtsvorschrift besonders angeordnet werden. Allerdings bleibt eine Auskunftsverpflichtung bestehen, wenn Bundesstatistiken bislang mit Auskunftspflicht durchgeführt wurden.

- Aufgrund von Rechtsverordnungen dürfen nur Wirtschafts- und Umweltstatistiken mit Auskunftspflicht durchgeführt werden.

- Neue statistische Rechtsgrundlagen müssen künftig bestimmen, welche Angaben nur der technischen Durchführung einer Bundesstatistik dienen („Hilfsmerkmale").

- Datenübermittlungen der Statistischen Ämter des Bundes und der Länder sind — mit Ausnahme der Übermittlung an ein anderes Statistisches Amt — zu protokollieren.

Einige Vorschriften des Gesetzes können indes unter datenschutzrechtlichen Gesichtspunkten nicht befriedigen, zumal sie den Anforderungen im Volkszählungsurteil nicht in vollem Umfang entsprechen und zum Teil sogar hinter dem Stand des BStatG 1980 zurückbleiben. Einige Beispiele:

Die *Übermittlungen an oberste Bundes- und Landesbehörden* hätten aufgrund des Volkszählungsurteils stärker eingeschränkt werden müssen:

- Es fehlt eine Beschränkung der Verwendung der übermittelten Angaben auf statistische Aufbereitungen, und es wird nicht gefordert, daß die empfangende Stelle innerhalb der Behördenorganisation abgeschottet ist. Nach den Ausführungen des Bundesverfassungsgerichts (a. a. O., S. 61) ist dies verfassungsrechtlich zumindest bedenklich. Zwar spricht die Neufassung von der Übermittlung von „Tabellen mit statistischen Ergebnissen"; diese dürfen aber nach ausdrücklicher Regelung Felder enthalten, die nur einen einzigen Fall ausweisen, so daß die Übermittlung auch einer Vielzahl von personenbeziehbaren Einzelangaben nicht ausgeschlossen wird.

— Für eine Übergangszeit von vier Jahren wird die Fortgeltung der nicht an das Volkszählungsurteil angepaßten Übermittlungsbestimmungen für statistische Einzelangaben festgeschrieben. Wegen der erheblichen verfassungsrechtlichen Vorbehalte, die im Volkszählungsurteil gerade gegen Übermittlungsregelungen für nicht statistische Zwecke geltend gemacht wurden, hatte ich die Aufhebung dieser Vorschriften empfohlen. Die jetzige Regelung führt dazu, daß nun Übermittlungen wieder aufgenommen werden, die wegen des Volkszählungsurteils außer Vollzug gesetzt worden waren (vgl. 8. TB, S. 29).

Das *Statistikgeheimnis* ist in mehrfacher Hinsicht eingeschränkt worden:

— Das Statistische Bundesamt darf künftig generell den Statistischen Ämtern der Länder Einzelangaben für regionale Sonderaufbereitungen übermitteln, was bisher nur in Ausnahmefällen bei einzelnen Statistiken zugelassen war.

  Die Weitergabe von Identifikationsmerkmalen ist nicht ausgeschlossen. Hinzu kommt, daß diese Übermittlungen nicht protokolliert werden, was die Datenschutzkontrolle erschwert.

— Für die Erstellung Volkswirtschaftlicher Gesamtrechnungen dürfen personenbeziehbare Einzelangaben zwischen den Statistischen Ämtern des Bundes und der Länder ohne Einschränkung ausgetauscht werden. Auch in diesem Fall wurde aus einer bisher — aus guten fachlichen Gründen — nur in einzelnen Gesetzen enthaltenen und auf wenige Merkmale beschränkten Befugnis eine Generalermächtigung, obwohl im Regelfall die Übermittlung von anonymisierten oder aggregierten Daten ausreicht. Was „Volkswirtschaftliche Gesamtrechnungen" sind, ist gesetzlich nicht definiert, so daß eine klare Verwendungsbeschränkung fehlt.

— Für Zwecke unabhängiger wissenschaftlicher Forschung dürfen nicht vollständig anonymisierte Daten übermittelt werden. Gegen diese Regelung habe ich vom Grundsatz keine Einwände. Ich hätte mir jedoch gewünscht, daß wegen des Reidentifizierungsrisikos und im Hinblick auf die Bedeutung, die das Bundesverfassungsgericht der Kontrolle der Datenverarbeitung durch unabhängige Datenschutzbeauftragte beimißt, auch privatrechtlich organisierte Forschungseinrichtungen ihrer Kontrolle unterworfen worden wären. Die Aufsichtsbehörden dürfen bekanntlich nach dem BDSG nicht von sich aus tätig werden.

Die gesetzliche *Bestimmung der Hilfsmerkmale* wird nicht gewährleistet.

— Die vom Bundesverfassungsgericht aufgestellte Forderung, daß in den eine Bundesstatistik anordnenden Rechtsvorschriften die zur Identifizierung der Befragten dienenden Hilfsmerkmale aufzuführen sind, wird nur bei neu zu erlassenden Gesetzen erfüllt. Ich habe dagegen die Auffassung vertreten, daß der Bürger bei allen Statistiken aus dem Gesetz erkennen können muß, welche Angaben von ihm als Hilfsmerkmale verlangt werden.

— Das Gesetz unterscheidet nicht mit der gebotenen Klarheit zwischen den (nur der technischen Durchführung von Bundesstatistiken dienenden) Hilfsmerkmalen und den (für die statistische Auswertung bestimmten) Erhebungsmerkmalen. Entgegen ihrer Definition dürfen Hilfsmerkmale auch für andere als technische Hilfszwecke genutzt werden. Eine deutlichere Unterscheidung schien mir erforderlich, damit die Befragten Klarheit erhalten, für welche konkreten Zwecke ihre Daten in personenbezogener Form verwendet werden und wann sie den Personenbezug verlieren.

— Die Umsetzung des Gebots der Trennung und Löschung von Hilfsmerkmalen, dem grundrechtssichernde Bedeutung zukommt (Bundesverfassungsgericht a. a. O., S. 60), wird durch die unklare Unterscheidung von Hilfs- und Erhebungsmerkmalen erschwert. Zudem wird hinter die Regelung des BStatG 1980 zurückgegangen. Die Identifikationsmerkmale waren danach zum frühestmöglichen Zeitpunkt zu löschen und sollten bis dahin von den übrigen Angaben getrennt unter Verschluß gehalten werden (vgl. BVerfG, a. a. O., S. 59). Nach neuem Recht genügt eine Trennung „zum frühestmöglichen Zeitpunkt". Zwar muß die Löschung grundsätzlich unmittelbar nach Abschluß der Überprüfung aller Angaben auf ihre Vollständigkeit und Schlüssigkeit erfolgen. Dieser Grundsatz wird jedoch wegen der weitreichenden Ausnahmeregelungen in der Praxis kaum Bedeutung erlangen.

  So darf z. B. die überwiegende Zahl der Hilfsmerkmale in eine Adreßdatei (siehe unten) eingestellt werden. Ihre Löschung erfolgt erst dann, wenn sie auch für die Zwecke dieser Datei nicht mehr benötigt werden. Ferner dürfen Anschriften vier Jahre lang für die Zuordnung zu Blockseiten genutzt werden.

  Insbesondere durch die Nutzung von Anschriften für die regionale Zuordnung der Erhebungsmerkmale zu der sehr kleinen räumlichen Einheit „Blockseite" wird die Durchschaubarkeit des Verfahrens erschwert. Während nämlich bei der Vollerhebung Volkszählung — aus der diese Regelung übernommen wurde — die Zahl der Betroffenen pro Blockseite regelmäßig groß und die Anonymität der Angaben dadurch relativ hoch sein dürfte, ist bei den meisten anderen Statistiken, da sie sich nur auf wenige ausgewählte Befragte stützen, mit Hilfe dieses Regionalmerkmals ein Personenbezug wesentlich leichter herstellbar. Der Befragte kann nicht voraussehen, wie lange aufgrund seiner Angaben ein Rückschluß auf seine Person möglich bleibt.

  Ich habe auch Zweifel, ob die auf Blockseiten bezogene Aufbewahrung aller Statistikangaben dem Gebot der frühzeitigen Anonymisierung genügt. Daher hatte ich empfohlen, die erforderliche regionale Gliederung differenziert in den einzelnen Fachgesetzen zu regeln.

Das Gesetz enthält schließlich einige *neue statistische Instrumente*, die für den Schutz der persönlichen Daten der Betroffenen nicht ohne Risiken sind und deren Umfang heute noch nicht genau abzuschätzen ist.

— Die Vorschrift über die sog. Adreßdatei, deren Errichtung ursprünglich mit der Möglichkeit der gleichmäßigen Heranziehung und Entlastung der Betroffenen statistischer Erhebungen begründet wurde, erlaubt es, Daten aus allen Wirtschafts- und Umweltstatistiken personenbezogen zusammenzuführen. In die Datei werden auch Angaben von Einzelkaufleuten aufgenommen. Es besteht daher die Gefahr, daß Teilabbilder dieses Personenkreises entstehen, die das Recht auf informationelle Selbstbestimmung berühren.

— Das Gesetz erlaubt den Statistischen Ämtern, ohne besondere gesetzliche Anordnung von sich aus Bundesstatistiken aus Daten zu erstellen, wenn diese aus allgemein zugänglichen Quellen oder aus öffentlichen Registern, zu denen die Ämter Zugang haben, entnommen sind. Es wäre falsch, solche Angaben als „belanglos" anzusehen, da jedenfalls durch ihre Verknüpfung neue sensible Informationen entstehen können.

  Da weder ein überwiegendes Allgemeininteresse noch ein aktueller Bedarf für eine so weitreichende Durchbrechung des Grundsatzes der gesetzlichen Anordnung von Bundesstatistiken nachgewiesen war, hatte ich die Streichung der Vorschrift empfohlen.

— Neu ist ferner die Möglichkeit, statistische Erhebungen zur Erfüllung eines kurzfristig auftretenden Datenbedarfs mit einer begrenzten Zahl von Befragten ohne spezielle gesetzliche Grundlage auf freiwilliger Basis durchzuführen. Gegen diese Erhebungsform sind aus datenschutzrechtlichen Gründen dann keine Einwände zu erheben, wenn die Regeln, die für sonstige Statistiken gelten, angewandt werden. Ich halte es allerdings für geboten, derart gewonnene Daten nicht mit anderen statistischen Angaben zu verknüpfen. Dem haben die an der Beratung des Gesetzentwurfs Beteiligten auch zugestimmt. Das Gesetz beantwortet die Frage aber leider nicht eindeutig.

10.2 Zweites Statistikbereinigungsgesetz

Das im Berichtszeitraum verabschiedete Zweite Gesetz zur Änderung statistischer Rechtsvorschriften (2. Statistikbereinigungsgesetz — 2. StatBerG) dient dem Zweck, Vereinfachungen und Einsparungen bei der Durchführung von Bundesstatistiken, die zum Teil bereits in den — überwiegend zeitlich befristeten — Regelungen der Statistikbereinigungsverordnung vom 14. September 1984 (BGBl. I S. 1247) enthalten waren, auf Dauer festzuschreiben. Darüber hinaus enthält das Gesetz auch Ergänzungen des statistischen Erhebungsprogramms, die zur Erfüllung politischer Aufgaben erforderlich erschienen. Schließlich sollen mit dem 2. Statistikbereinigungsgesetz weitere Anforderungen des Volkszählungsurteils des Bundesverfassungsgerichts an den Inhalt von Rechtsgrundlagen für statistische Erhebungen erfüllt werden.

Im Gesetzgebungsverfahren stellte sich die Frage, ob eine Teilnovellierung von statistischen Rechtsgrundlagen ohne deren vollständige Anpassung an die Vorgaben des Volkszählungsurteils zulässig ist. Mit anderen Worten: Ist der Umsetzungsbonus dann verbraucht, wenn der Gesetzgeber einzelne Vorschriften eines Gesetzes ändert? Ich habe mich in meiner Stellungnahme gegenüber dem Innenausschuß des Deutschen Bundestages auf den Standpunkt gestellt, daß bei jeder Änderung eines statistischen Gesetzes die nach dem Urteil des Bundesverfassungsgerichts erforderlichen Regelungen getroffen werden sollten (z. B. Benennung der Hilfsmerkmale, Präzisierung der Trennungs- und Löschungsregelungen, Sicherung der statistischen Geheimhaltung). Da eine vollständige Anpassung aller dreizehn statistischen Gesetze und der vier Verordnungen, die durch das 2. Statistikbereinigungsgesetz betroffen sind, in der auslaufenden Legislaturperiode nicht mehr möglich erschien, habe ich es im Hinblick auf den unbestreitbaren Bereinigungseffekt des Gesetzes für vertretbar gehalten, wenn zunächst auf eine vollständige Anpassung der betroffenen Rechtsvorschriften verzichtet und diese in der nächsten Legislaturperiode nachgeholt wird. Als Voraussetzung dafür hielt ich es allerdings für erforderlich, daß der Gesetzgeber sich auf bloße Bereinigungen beschränkt und zugleich alle Vorschriften, die die Übermittlung oder Veröffentlichung von statistischen Einzelangaben zulassen, aufhebt. Gerade die Regelungen zur Übermittlung statistischer Einzelangaben für nicht statistische Zwecke erscheinen im Hinblick auf das Volkszählungsurteil besonders problematisch. Aus diesem Grund hat das Statistische Bundesamt den Vollzug solcher Vorschriften zu Recht ausgesetzt (vgl. hierzu 8. TB S. 29).

Der Gesetzgeber ist meinen Empfehlungen im wesentlichen gefolgt. Die von dem verabschiedeten Gesetz betroffenen Rechtsgrundlagen enthalten mit einer Ausnahme, die aufgrund besonderer Umstände toleriert werden konnte, keine Übermittlungsregelungen mehr. Das Gesetz beschränkt sich ganz überwiegend auf Kürzungen des statistischen Programms, die Erweiterungen nehmen sich daneben bescheiden aus. Darüber hinaus hat der Deutsche Bundestag zu dem Gesetz eine Entschließung verabschiedet, mit der klargestellt wird, daß mit der Verabschiedung des 2. Statistikbereinigungsgesetzes „kein Präjudiz in der Frage verbunden ist, ob und in welchem Umfang eine weitere gesetzgeberische Anpassung einzelstatistischer Rechtsvorschriften erfolgen muß" (Bundestags-Drucksache 10/6612 — Nummer 2 der Beschlußempfehlung —).

Der Deutsche Bundestag erwartet hierüber nähere Aufschlüsse durch den von der Bundesregierung aufgrund des Bundesstatistikgesetzes zum 1. Januar 1988 zu erstattenden Bericht über Notwendigkeit und Umfang von weiteren Änderungen einzelstatistischer Rechtsvorschriften.

Gleichwohl fordert nach meiner Auffassung das Volkszählungsurteil auch schon vor diesem Termin die Vorbereitung von weiteren Gesetzesänderungen, die in einigen Bereichen, wie der Bevölkerungsstatistik, dringend erforderlich erscheinen. Ich halte darüber hinaus die Anwendung von einzelstatistischen Übermittlungsregelungen nur innerhalb des Rahmens für zulässig, den das Bundesverfassungsgericht vorgegeben hat. Das bedeutet für die Übermittlung von Einzelangaben aufgrund von Rechtsgrundlagen, die vor dem Volkszählungsurteil ergangen sind, daß diese nicht für Verwaltungszwecke erfolgen darf und bei den Datenempfängern eine wirksame Abschottung gewährleistet sein muß.

10.3 Volkszählung 1987

Im Jahr 1987 wird nach dem Stand vom 25. Mai eine Volks-, Berufs-, Gebäude-, Wohnungs- und Arbeitsstättenzählung, kurz: die Volkszählung 1987, durchgeführt.

Bereits in meinem Achten Tätigkeitsbericht (S. 27) habe ich ausgeführt, daß der Gesetzgeber mit den Regelungen des Volkszählungsgesetzes 1987 die Anforderungen, die das Bundesverfassungsgericht in seinem Volkszählungsurteil an statistische Erhebungen stellt, erfüllt hat.

Im Berichtsjahr wurde der rechtliche Rahmen für die Erhebungen weiter vervollständigt. So haben die Länder in Rechtsverordnungen die Erhebungsstellen bestimmt und Einzelheiten der Durchführung der Zählungen geregelt. Die Statistischen Ämter des Bundes und der Länder haben Anleitungen für Gemeinden und Erhebungsstellen sowie Zähleranleitungen erstellt. Einzelne Länder haben mit Musterdienstanweisungen für die Durchführung der Volkszählung konkrete Empfehlungen für die Einrichtung der Erhebungsstellen, die dort zu treffenden Sicherungsmaßnahmen sowie den Dienstbetrieb gemacht. Der Erlaß solcher Dienstanweisungen durch die Leiter der Gemeindeverwaltung ist in manchen Ländern ausdrücklich vorgeschrieben.

Zu einigen Teilaspekten des Datenschutzes bei der Volkszählung 1987 hat mich der Bundesminister des Innern um Beratung gebeten. In mehreren Gesprächen unter Beteiligung des Statistischen Bundesamtes konnten insbesondere Verbesserungen der „Informationen zur Volkszählung 1987", die allen Bürgern ausgehändigt werden sollen, erreicht werden. Weitere Beratungsgegenstände waren der Einsatz automatischer Datenverarbeitungsanlagen in den Erhebungsstellen sowie die Durchführung der Volkszählung in Anstalten.

Mitarbeiter meiner Dienststelle haben sich schließlich im Statistischen Bundesamt über den vorgesehenen Ablauf der Volkszählung, insbesondere im Hinblick auf die Sicherheit der Daten, unterrichtet. Danach gehe ich davon aus, daß im Statistischen Bundesamt alle Voraussetzungen für einen wirksamen Schutz der Daten erfüllt sein werden. Nach dem Zählungsstichtag, aber noch ehe Einzelangaben das Amt erreichen, soll das Sicherheitskonzept nochmals geprüft werden.

10.4 Wissenschaftlicher Beirat für Mikrozensus und Volkszählung

Das Mikrozensusgesetz sieht zur Vorbereitung des schrittweisen Übergangs von der Auskunftspflicht zum Prinzip der Freiwilligkeit der Antworterteilung bei statistischen Erhebungen die Durchführung von freiwilligen Testerhebungen vor, bei denen alternative Verfahren der Antwortgewinnung erprobt werden sollen. Für die Festlegung der alternativen Verfahren und die methodische Auswertung der Testerhebungen wurde die Mitwirkung eines wissenschaftlichen Beirats angeordnet, der sich aus zwei Hochschullehrern auf dem Gebiet der Statistik und zwei Vertretern der Sozialforschung zusammensetzt (vgl. 8. TB S. 27).

Bei der Arbeit des Wissenschaftlichen Beirats wurde deutlich, daß die Erprobung von alternativen Erhebungsverfahren mit datenschutzrechtlichen Vorschriften kollidieren kann. Der Wissenschaftliche Beirat hat mich daher gebeten, ihn in Datenschutzfragen zu beraten. Aufgrund dieser Besprechungen konnten in anstehenden Verfahren Lösungen gefunden werden, die sowohl dem wissenschaftlichen Anliegen des Beirats als auch dem Schutz der informationellen Selbstbestimmung der für die Testerhebung ausgewählten Bürger Rechnung tragen.

Es handelte sich dabei einmal um ein Befragungsverfahren, bei dem die Bürger zwar hinreichend darüber informiert werden, daß sie — ohne Rechtsnachteile befürchten zu müssen — auf eine Teilnahme verzichten können, eine plakative Hervorhebung der Freiwilligkeit, die sie von einer Antworterteilung abhalten könnte, aber vermieden wird.

In einem anderen Fall wurde eine Möglichkeit gefunden, wie die Reaktionen der Befragten auf das Erhebungsinstrument von den Interviewern erfaßt werden können, ohne daß damit den statistischen Ämtern zusätzliche personenbeziehbare Daten der Betroffenen offenbart werden. Nach Auffassung des Wissenschaftlichen Beirats stellt die Kenntnis der Reaktionen der Befragten in Abhängigkeit von Haushaltsgröße und Zählbezirksstruktur eine wesentliche Voraussetzung für die Entwicklung alternativer Erhebungsverfahren dar.

Auf Initiative des Deutschen Bundestages wurde der Wissenschaftliche Beirat auch mit der Mitwirkung an der Vorbereitung und Durchführung der Volkszählung 1987 betraut. Dabei soll es insbesondere seine Aufgabe sein, neue Erkenntnisse für die Weiterentwicklung des Verfahrens der Volkszählung zu gewinnen. Auch dabei werden der Wissenschaftliche Beirat und das Statistische Bundesamt von mir beraten.

10.5 Handels- und Gaststättenzählung und Steuergeheimnis

In meinem Achten Tätigkeitsbericht (S. 27 f.) habe ich über datenschutzrechtliche Probleme bei der Handels- und Gaststättenzählung 1985 berichtet. Dabei blieb die Frage offen, ob die Übermittlung der

Steuer- und Finanzamtsnummer der von der Erhebung betroffenen Unternehmen durch die Finanzbehörden an die statistischen Landesämter gegen das Steuergeheimnis nach § 30 Abgabenordnung (AO) verstieß.

Meine in der Zwischenzeit vorgenommene Prüfung hat ergeben, daß die Übermittlung das Steuergeheimnis verletzt hat. § 30 AO schützt bereits die Tatsache, daß sich eine bestimmte Finanzbehörde mit einem bestimmten Steuerpflichtigen befaßt, was in der Vergabe einer Steuernummer zum Ausdruck kommt. Die Steuernummer stellt darüber hinaus ein personenbezogenes Datum dar, das die Verknüpfung mit anderen personenbezogenen Daten eines Betroffenen erlaubt. Einzelangaben von Steuerpflichtigen, die zu einem früheren Zeitpunkt ohne deren Namen und Anschriften, aber mit deren Steuernummern — scheinbar anonym — übermittelt wurden, können bei späterer Übermittlung von Steuernummern mit Namen und Anschriften den Steuerpflichtigen nachträglich unmittelbar zugeordnet werden. Die Auffassung des Bundesministers der Finanzen, beide Vorgänge seien getrennt zu betrachten und das Steuergeheimnis daher nicht tangiert, ist bedenklich, da sie zu einer Lücke im Geheimnisschutz führen würde.

Der durch die rechtswidrige Datenübermittlung eingetretene Schaden dürfte im vorliegenden Fall allerdings von geringem Ausmaß sein, da die Steuernummern nach Auskunft des Statistischen Bundesamtes in den Statistischen Landesämtern alsbald wieder gelöscht wurden und zudem die Mitarbeiter der Statistischen Ämter ihrerseits zur Wahrung des Steuergeheimnisses verpflichtet sind.

10.6 Agrarberichterstattung — Zusatzprogrammverordnung —

Ein Landesbeauftragter hat mich darauf aufmerksam gemacht, daß der Bundesminister für Ernährung, Landwirtschaft und Forsten plane, auf der Grundlage einer Verordnung im Jahr 1987 sensible Daten im Agrarbereich zu erheben. Ich habe daraufhin den Bundesminister für Ernährung, Landwirtschaft und Forsten gebeten, mir den entsprechenden Entwurf zur datenschutzrechtlichen Überprüfung zur Verfügung zu stellen.

Der mir daraufhin vorgelegte Entwurf einer Verordnung zur Durchführung des Zusatzprogramms nach § 5 Abs. 1 des Gesetzes über die Agrarberichterstattung (Agrarberichterstattung — Zusatzprogrammverordnung — AgrBZV) wies Mängel auf, über die ich den Bundesminister für Ernährung, Landwirtschaft und Forsten unterrichtet habe. Gleichwohl leitete der Bundesminister den Entwurf unverändert dem Bundesrat zur Zustimmung zu. Ich habe darauf meine Bedenken dem Präsidenten des Bundesrates für die weiteren Beratungen mitgeteilt. Die Beratungen führten im Ausschuß für Innere Angelegenheiten zu dem Votum, der Verordnung nicht zuzustimmen, während der federführende Agrarausschuß die Zustimmung mit zwei Änderungen empfahl. Der Bundesrat schloß sich der Empfehlung des Agrarausschusses an.

Bei der datenschutzrechtlichen Beurteilung der Agrarberichterstattung — Zusatzprogrammverordnung — ging es u. a. um das bereits im Zusammenhang mit dem 2. Statistikbereinigungsgesetz (vgl. oben 10.2) angesprochene Problem, ob die Ausweitung einer statistischen Erhebung die Anpassung des zugrundeliegenden Gesetzes an die Anforderungen des Volkszählungsurteils voraussetzt (z. B. Regelungen über den Einsatz von Zählern und die Übermittlung von Einzelangaben).

Ich habe auch in diesem Fall die Auffassung vertreten, daß eine vorherige Anpassung angebracht sei. Der Bundesminister für Ernährung, Landwirtschaft und Forsten hat daraufhin zugesagt, die Anpassung des Agrarberichterstattungsgesetzes sowie der sonstigen seinen Geschäftsbereich betreffenden Statistikgesetze nach Verkündung des Bundesstatistikgesetzes vorzunehmen. Bis zur Novellierung der Gesetze werde den Anforderungen des Volkszählungsurteils durch entsprechende Vorkehrungen bei der Durchführung statistischer Erhebungen Rechnung getragen.

Meine Bedenken richteten sich ferner gegen die Tragfähigkeit der Ermächtigungsgrundlage des Agrarberichterstattungsgesetzes für die in der Verordnung vorgesehenen Merkmale sowie die Ausgestaltung der mir vorgelegten Entwürfe der Erhebungsvordrucke, die die kombinierte Erhebung mit anderen Landwirtschaftsstatistiken vorsehen.

Auch wenn nicht alle meine Empfehlungen aufgegriffen wurden, trägt die erlassene Verordnung aufgrund der vorgenommenen Änderungen dem Recht auf informationelle Selbstbestimmung der Betroffenen deutlich besser Rechnung als der ursprüngliche Entwurf. So ist nun sichergestellt, daß — entsprechend den Ausführungen des Bundesverfassungsgerichts zur Volkszählung und im übrigen auch der zugrundeliegenden Ermächtigung des Agrarberichterstattungsgesetzes — jeder Betroffene über die seine Person betreffenden Sachverhalte, wie sein „außerbetriebliches Einkommen", selbst und unter Ausschluß der Möglichkeit zur Einsichtnahme durch den Betriebsinhaber Auskunft erteilen kann. Ferner wurde der Kreis der von der Erhebung Betroffenen um die „im Betrieb beschäftigten Familienangehörigen" reduziert. Damit wurde dem Gesichtspunkt entsprochen, daß die außerbetrieblichen Einkommen der Familienangehörigen, auch wenn sie im landwirtschaftlichen Betrieb der Eltern beschäftigt sind, wohl kaum unter das gesetzliche Merkmal „wirtschaftliche Verhältnisse des Betriebes" zu subsumieren sind.

Ich werde mich bemühen, durch eine frühzeitige Beratung der Bundesstellen, die an der Durchführung der im Frühjahr 1987 stattfindenden Agrarberichterstattung beteiligt sind, dazu beizutragen, daß trotz des Fehlens der eingangs erwähnten Rechtsanpassung eine verfassungskonforme Durchführung der Erhebung möglich ist.

10.7 Veröffentlichung von Statistikdateien

Der Bundesminister des Innern meldete bislang Dateien des Statistischen Bundesamtes mit perso-

nenbezogenen Statistikdaten nur dann gemäß § 12 BDSG für eine Veröffentlichung im Bundesanzeiger an, wenn die Daten nicht auf der Grundlage eines Gesetzes erhoben wurden. Der Bundesminister des Innern und das Statistische Bundesamt vertraten die Auffassung, die Veröffentlichung von Dateien mit statistischen Daten, die aufgrund eines Statistikgesetzes erhoben werden, sei deshalb entbehrlich, weil die mit § 12 BDSG bezweckte Publizität der Datenverarbeitung bereits durch das jeweilige statistische Fachgesetz hergestellt sei.

Ich konnte mich dieser Rechtsauffassung nicht anschließen. Nach meiner Ansicht läßt sich eine solche Ausnahme von der Veröffentlichungspflicht aus § 12 BDSG nicht ableiten.

Der Bundesminister des Innern hat nunmehr seine Vorbehalte gegen die Veröffentlichung der betreffenden Statistikdateien aufgegeben. Er hat auch die von mir vorgeschlagenen Regeln für die Veröffentlichung von Statistikdateien akzeptiert, durch die insbesondere verhindert werden soll, daß der Inhalt der Bekanntmachungen durch eine undifferenzierte Aufführung aller gespeicherten Datenarten das Ziel verfehlt, die wesentlichen Datenverarbeitungsprozesse transparent zu machen. Ich habe daher empfohlen, den Inhalt der Veröffentlichung am Umfang der Datei und der Sensibilität des Datenmaterials zu orientieren. Danach sollen die Datenarten, soweit sie weniger sensible Merkmale betreffen, wie beispielsweise im Rahmen von Wirtschaftsstatistiken zu erhebende Material- und Warenbestände, nicht genauso detailliert beschrieben werden wie sehr persönliche Daten, die aufgrund eines Merkmals wie „Angaben zur Person" erhoben werden.

11. Sozialwesen

Im Achten Tätigkeitsbericht (S. 29) habe ich über den Stand der Vorarbeiten zur Regelung der Verwendung der *Rentenversicherungsnummer* berichtet. Im Berichtsjahr konnte mit dem Bundesminister für Arbeit und Sozialordnung (BMA) über den Inhalt und die Form der beabsichtigten Regelungen weitgehend Einigung erzielt werden. Ein Problem bedarf allerdings noch besonderer Prüfung, nämlich die Verwendung der Versicherungsnummer durch die Arbeitsmedizinischen Dienste der Berufsgenossenschaften:
Die Verwendung der Versicherungsnummer durch die Träger der Sozialversicherung (und einige weitere in § 35 Abs. 1 SGB I genannte Stellen) steht nach dem Entwurf grundsätzlich unter dem Vorbehalt der Erforderlichkeit für die Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch (einschließlich seiner besonderen Teile, u. a. der RVO). Die Arbeitsmedizinischen Dienste der Bau-Berufsgenossenschaften, bei denen die Verwendung der Rentenversicherungsnummer ursprünglich der Anlaß für meine Forderung einer gesetzlichen Regelung war (vgl. 5. TB S. 68), werden zwar aufgrund des § 719 a RVO von den Berufsgenossenschaften eingerichtet. Sie erfüllen jedoch nach den jeweiligen Satzungen der Berufsgenossenschaften Aufgaben nach dem Arbeitssicherheitsgesetz. Es ist deshalb nach meiner Auffassung zweifelhaft, ob diese Arbeitsmedizinischen Dienste nach Inkrafttreten der konzipierten Regelungen die Versicherungsnummer zur Ordnung und Erschließung ihrer Untersuchungsdateien verwenden dürfen.

Es bereitet offensichtlich nach wie vor große Schwierigkeiten, die Vorschrift des § 9 Abs. 2 BDSG, daß der Betroffene bei der *Datenerhebung* auf die Rechtsgrundlage der Auskunftspflicht bzw. auf die Freiwilligkeit seiner Angaben hinzuweisen ist, in die Praxis umzusetzen (vgl. 5. TB S. 51). Immer wieder habe ich mich aufgrund von Bürgereingaben mit dem Problem zu befassen, daß in den vielfältigsten Zusammenhängen vom Bürger Angaben verlangt oder erbeten werden, ohne daß klar und deutlich auf bestehende Auskunftspflichten oder auf die Freiwilligkeit der Angaben hingewiesen wird.

Zwar haben viele Stellen der Sozialverwaltung in den letzten Jahren eine generelle Vordruckbereinigung unter datenschutzrechtlichen Gesichtspunkten in Angriff genommen und durchgeführt. Häufig wird aber der gesetzlichen Hinweispflicht nur rein formal Genüge getan und das datenschutzrechtliche Anliegen, das der Vorschrift des § 9 Abs. 2 BDSG zugrundeliegt, nach meinem Eindruck nicht verstanden.

So ist z. B. im Bereich der gesetzlichen Krankenversicherung der Hinweis im Vordruck, daß die Angaben über die persönlichen und sachlichen Verhältnisse aufgrund des § 318 a RVO erhoben werden, formal zutreffend, denn nach dieser Vorschrift haben die Versicherten „die zur Meldung sowie zur Durchführung der Versicherung und der der Krankenkasse übertragenen Aufgaben erforderlichen Angaben zu machen". Da den Betroffenen aber in der Regel ein Gesetzestext nicht zur Verfügung steht, bleibt es für ihn unklar, ob er verpflichtet ist, die verlangten Angaben zu machen, oder ob er dies freiwillig, also ohne rechtliche Verpflichtung, tut. Um die gesetzgeberische Absicht auch inhaltlich zu verwirklichen, sollte deshalb den Betroffenen die im konkreten Fall bestehende Auskunftspflicht deutlich gemacht werden, etwa durch den Zusatz: „Danach sind Sie verpflichtet, die erforderlichen Angaben zu machen."

Andere — auch neu konzipierte — Vordrucke enthalten statt des Hinweises auf die Rechtsvorschrift über die Auskunftspflicht immer noch einen Hinweis auf die Aufgabennorm, zu deren Erfüllung die Angaben erforderlich sind.

Manche Vordrucke enthalten zwar einen einwandfreien Hinweis gemäß § 9 Abs. 2 BDSG. Eine nähere Prüfung ergibt aber, daß von der angegebenen Auskunftspflicht nur ein (geringer) Teil der verlangten Angaben abgedeckt oder daß die Erforderlichkeit einzelner Angaben zumindest zweifelhaft ist.

Schließlich wird häufig übersehen, daß die Hinweispflicht für jede Form der Datenerhebung gilt, also nicht nur bei der Erhebung mittels vorgedruckter Fragebogen, sondern auch bei allen unformatierten Aufforderungen zu bestimmten Angaben.

Die Aufklärung des Bürgers über seine Rechte und Pflichten gegenüber der öffentlichen Verwaltung, die zur Erfüllung ihrer Aufgaben seine Mithilfe und in vielen Fällen Angaben über seine persönlichen und sachlichen Verhältnisse braucht, ist keine formale oder überflüssige Pflicht. Nach dem Volkszählungsurteil des Bundesverfassungsgerichts sind die Transparenz der Datenverarbeitung und die Beteiligung des Bürgers bei der Datenerhebung vielmehr als wesentliche Instrumente zur Verwirklichung des informationellen Selbstbestimmungsrechts anzusehen. Ich werde deshalb auch in Zukunft ein besonderes Augenmerk auf die Erfüllung dieser „lästigen" Pflicht durch die meiner Kontrolle unterstehenden Stellen richten und unzureichende oder fehlende Hinweise gemäß § 9 Abs. 2 BDSG gegebenenfalls bemängeln.

11.1 Arbeitsverwaltung

11.1.1 Arbeitsvermittlung/-beratung

— Aufgrund mehrerer Eingaben habe ich mich erneut mit der bereits im Achten Tätigkeitsbericht (S. 30) angesprochenen *Weitergabe von Bewerbungsunterlagen* von Arbeitssuchenden durch die Arbeitsämter an geeignet erscheinende Arbeitgeber auseinandergesetzt. Nach meiner Auffassung kann die Befugnis zur Übermittlung von Bewerbungsunterlagen an potentielle Arbeitgeber nicht auf § 69 Sozialgesetzbuch X (SGB X) in Verbindung mit §§ 13, 14 Arbeitsförderungsgesetz (AFG) gestützt werden. Diese gesetzliche Offenbarungslegitimation betrifft nur die für die Vermittlung erforderlichen Daten. Hierzu gehören der Name, die Anschrift und gegebenenfalls die Telefonnummer sowie die Bezeichnung der beruflichen Qualifikation des Arbeitssuchenden. Der potentielle Arbeitgeber wird dadurch in die Lage versetzt, mit dem Arbeitsuchenden in Kontakt zu treten und die entsprechenden Bewerbungsunterlagen von ihm selbst anzufordern. Ich verkenne nicht, daß Fälle denkbar sind, in denen aufgrund der Eilbedürftigkeit der Vermittlung eine unmittelbare Weitergabe der Bewerbungsunterlagen durch das Arbeitsamt an den Arbeitgeber zweckmäßig wäre. Auch in diesem Fall ist die Weitergabe jedoch nur mit Einwilligung des Betroffenen gemäß § 67 Nr. 1 SGB X zulässig, d. h. sie darf nur nach Rückfrage des Arbeitsamts bei dem Arbeitssuchenden vorgenommen werden. Eine solche Rückfrage wäre allerdings dann nicht erforderlich, wenn die nach § 67 Nr. 1 SGB X erforderliche Einwilligung, gegebenenfalls eingeschränkt durch Sperrvermerk, schon während des Beratungsgespräches bei dem Arbeitsvermittler schriftlich erteilt würde.

  Das gleiche gilt für die Vermittlung von Auszubildenden in berufliche Ausbildungsstellen gemäß § 29 AFG.

— Aufgrund einer Eingabe wurde ich auf ein Sonderproblem im Bereich der Arbeitsvermittlung aufmerksam, nämlich das Verfahren der Weiterleitung der *Bewerbungsunterlagen* bei der Vermittlung von Arbeitssuchenden *zu internationalen Organisationen*. Nach bisheriger Praxis wurde zur offiziellen Unterstützung deutscher Bewerbungen das Auswärtige Amt bzw. ein sonst zuständiges Bundesressort eingeschaltet, ohne daß für die damit verbundene Weiterleitung der Unterlagen der Bewerber eine entsprechende Rechtsnorm oder die schriftliche Einwilligung der Betroffenen vorhanden war. Ich halte diese Praxis für unzulässig und habe daher dem für diese Fachvermittlung zuständigen „Büro Führungskräfte zu Internationalen Organisationen" in der „Zentralstelle für Arbeitsvermittlung" empfohlen, bei künftigen Bewerbungen ein entsprechendes Einwilligungsformular zu verwenden, das der Bewerber unterzeichnet zurücksenden soll.

— In einer Eingabe wurde die Frage angesprochen, ob das Arbeitsamt berechtigt ist, den genauen *Grund einer Kündigung* des Arbeitnehmers zu erfragen. Eine Überprüfung hat ergeben, daß die Arbeitsämter nach dem AFG verpflichtet sind, sowohl dem gekündigten Arbeitnehmer wie auch dem kündigenden Arbeitgeber die Frage nach dem genauen Kündigungsgrund zu stellen. Die Verpflichtung des Arbeitsamtes, beim Arbeitnehmer den Kündigungsgrund zu erfragen, ergibt sich aus den Regelungen des AFG zum Vermittlungs- und Leistungsverfahren.

  Das Arbeitsamt hat nach § 14 AFG die Eignung des Arbeitssuchenden und dessen persönliche Verhältnisse angemessen zu berücksichtigen. Aus dieser Vorschrift läßt sich entnehmen, daß Gründe der Auflösung eines früheren Arbeitsverhältnisses zumindest dann, wenn diese in der Person des Arbeitnehmers zu suchen sind, dem Arbeitsamt bekannt werden müssen. Um eine erfolgreiche Vermittlung zu gewährleisten, muß das Stellenangebot durch das Arbeitsamt so gewählt werden können, daß ein neues Arbeitsverhältnis nicht aus den gleichen Gründen scheitert.

  Zur Durchführung des Leistungsverfahrens ergibt sich die Verpflichtung des Arbeitsamtes, nach dem Kündigungsgrund zu fragen, aus § 119 Abs. 1 Nr. 1 AFG. Hat der Arbeitslose das Arbeitsverhältnis selbst gelöst oder durch ein vertragswidriges Verhalten Anlaß für die Kündigung des Arbeitgebers gegeben und hat er dadurch vorsätzlich oder grob fahrlässig die Arbeitslosigkeit herbeigeführt, ohne für sein Verhalten einen wichtigen Grund zu haben, tritt eine Sperrzeit mit der Folge des Ruhens seines Leistungsanspruches ein.

  Im Falle der fristlosen Kündigung ist das Arbeitsamt zusätzlich im Hinblick auf § 117 Abs. 1 AFG berechtigt, nach dem Kündigungsgrund zu fragen. Danach ruht der Anspruch des Arbeitnehmers auf Arbeitslosengeld in der Zeit, für die der Arbeitslose Arbeitsentgelt erhält oder zu beanspruchen hat. Hat ein Arbeitgeber eine fristlose Kündigung ausgesprochen, ohne daß ein entsprechender Kündigungsgrund gegeben ist, so ist er bis zum Ablauf der ordentlichen Kündigungsfrist zur Leistung des Arbeitsentgeltes

verpflichet. Die Beurteilung dieses Sachverhalts setzt voraus, daß der Arbeitnehmer den Kündigungsgrund angibt.

Der erforderliche Umfang der Auskunftspflicht des Arbeitnehmers läßt sich jedoch nur anhand des Einzelfalles beurteilen. Generell wird man sagen können, daß ein Arbeitnehmer, der die Leistungen des Arbeitsamtes in Anspruch nimmt, zur wahrheitsgemäßen Auskunft über die Umstände der Kündigung verpflichtet ist, die für das Tätigwerden der Arbeitsämter erforderlich sind. Die Verpflichtung zur Auskunftserteilung findet jedoch in jedem Falle ihre Grenzen dort, wo die Antwort des Arbeitnehmers zu einer unzumutbaren Preisgabe intimer Angaben oder zu einer Selbstbezichtigung führen würde.

Der Arbeitgeber ist ebenfalls zur wahrheitsgemäßen Beantwortung der vom Arbeitsamt gestellten Fragen verpflichtet. Im Hinblick auf das sich aus § 14 AFG ergebende Fragerecht des Arbeitsamtes ist er wegen der nachwirkenden Fürsorgepflicht aus dem Arbeitsverhältnis im Interesse des ausgeschiedenen Arbeitnehmers verpflichtet, Auskünfte über diesen nur in einer Form zu erteilen, die einen unzumutbaren Eingriff in die Individualsphäre und damit eine Verletzung des Persönlichkeitsrechts des gekündigten Arbeitnehmers vermeidet. Auch bei Auskunftserteilung in den Fällen der §§ 117 Abs. 1 und 119 Abs. 1 Nr. 1 AFG hat ein Arbeitgeber in sachlicher Form wahrheitsgemäß zu antworten und damit zur Aufklärung des Sachverhaltes beizutragen.

Unter Beachtung dieser Grundsätze habe ich keine Bedenken gegen eine entsprechende Datenerhebung durch die Arbeitsämter.

— Die Bundesanstalt für Arbeit führt im Hinblick auf die Resozialisierung von Strafgefangenen *Arbeitsberatungen in Justizvollzugsanstalten* durch und schlägt gegebenenfalls Maßnahmen zur beruflichen Bildung oder zur Verbesserung der Vermittlungsaussichten vor. In diesem Zusammenhang wurde mir durch eine Eingabe bekannt, daß die Niederschrift eines Arbeitsamtes über die Beratung eines Strafgefangenen dem Bediensteten einer Justizvollzugsanstalt in Kopie überlassen worden ist. Eine solche Weiterleitung ist nur nach Prüfung des Einzelfalles im Rahmen des § 69 Abs. 1 Nr. 1 SGB X in Verbindung mit § 15 AFG zulässig, beispielsweise dann, wenn die Teilnahme an einer Maßnahme der geschilderten Art außerhalb der Justizvollzugsanstalt ins Auge gefaßt wird. In diesem Falle ist unter Umständen die Offenbarung einzelner Daten, wie z. B. der zeitlichen Inanspruchnahme des Betroffenen durch die Maßnahme, gegenüber der Justizvollzugsanstalt erforderlich. Es ist jedoch unverhältnismäßig, dem Bediensteten einer Justizvollzugsanstalt die gesamte Beratungsniederschrift zu überlassen. Die Bundesanstalt für Arbeit hat mir mitgeteilt, daß sie meine Auffassung in diesem Punkt teilt. Sie hat das betreffende Arbeitsamt und die Landesarbeitsämter darauf hingewiesen, daß unbeschadet der Notwendigkeit einer engen Kooperation mit der Leitung einer Justizvollzugsanstalt die ungeprüfte Weiterleitung von Beratungsniederschriften durch Arbeitsämter an die Justizvollzugsanstalt nicht zulässig ist.

11.1.2 Leistungsverwaltung

— Auch im Berichtsjahr hatte ich aufgrund zahlreicher Eingaben Veranlassung, mich mit der Problematik des Verfahrens bei der Gewährung von *Arbeitslosenhilfe* zu befassen. Einen Teilerfolg bei der Verbesserung des Datenschutzes in diesem Bereich konnte ich dadurch erzielen, daß nach Mitteilung der Bundesanstalt Einkommensnachweise von unterhaltspflichtigen Angehörigen der Antragsteller auf Arbeitslosenhilfe nunmehr unmittelbar den Arbeitsämtern vorgelegt werden können (vgl. 8. TB S. 30).

Nach wie vor hält die Bundesanstalt für Arbeit jedoch an ihrem Standpunkt fest, daß alle Angaben, die zur Entscheidung über die Arbeitslosenhilfe geführt haben, auch in dem Bescheid an den Antragsteller aufgeführt werden müssen. Sie leitet ihre Auffassung aus dem Begründungserfordernis schriftlicher Verwaltungsakte ab. Im Falle einer Leistungsminderung durch Anrechnung eines Unterhaltsanspruches müsse auch die Einkommenshöhe des unterhaltspflichtigen Angehörigen im Bescheid nachgewiesen werden, da sie Grundlage für die Berechnung des Anrechnungsbetrages sei.

Nach meiner Auffassung könnte diesem Erfordernis auch in anderer Form Rechnung getragen werden, ohne daß die Einkommensverhältnisse des Unterhaltsverpflichteten so ausführlich, wie dies derzeit geschieht, dargestellt werden müssen. So würde ich die Angaben nur des Anrechnungsbetrages für ausreichend halten. Erst in einem Widerspruchsverfahren könnten weitere Angaben erforderlich werden.

Wie bereits in meinem Siebenten Tätigkeitsbericht (S. 43) ausgeführt, entfallen beispielsweise nach § 50 Abs. 2 Bundesausbildungsförderungsgesetz (BAföG) im Bewilligungsbescheid auf begründetes Verlangen eines Elternteils oder eines Ehegatten die Angaben über dessen Einkommen mit Ausnahme des Betrages des angerechneten Einkommens. Dies gilt ausdrücklich auch für den Fall, daß der Antragsteller ein berechtigtes Interesse an der Kenntnis dieser Daten hat. Ich sehe keinen rechtlichen Grund, der einer sinngemäßen gesetzlichen Regelung im AFG entgegenstünde, wenn sichergestellt wird, daß der Antragsteller im Falle eines Verwaltungsstreites um die Höhe des anrechenbaren Einkommens des Unterhaltspflichtigen weitere Angaben zu dessen Einkommen erhält.

— Aufgrund einer Eingabe hatte ich zu prüfen, inwieweit die Bundesanstalt für Arbeit berechtigt ist, im Falle der Klageerhebung eines Leistungsberechtigten gegen die Bundesanstalt Leistungsakten einschließlich der *ärztlichen Gutachten* an die *Sozialgerichte* zu übersenden. Nach meiner Auffassung erfordert das in § 76

Abs. 2 Satz 2 SGB X gesetzlich festgelegte Widerspruchsrecht eines Betroffenen gegen eine entsprechende Aktenübersendung, daß der Betroffene durch die Bundesanstalt für Arbeit über eine beabsichtigte Aktenversendung aufgeklärt wird, um sein Recht wahrnehmen zu können. Ich würde es insoweit als ausreichend ansehen, wenn die Rechtsmittelbelehrung bei der Ablehnung eines Widerspruches gegen einen Leistungsbescheid der Bundesanstalt für Arbeit um den Hinweis ergänzt würde, daß die Leistungsakten einschließlich der ärztlichen bzw. psychologischen Gutachten im Falle eines Gerichtsverfahrens an das Sozialgericht übersandt werden und daß die Möglichkeit besteht, der Übersendung ärztlicher Unterlagen zu widersprechen. Dadurch würde auch der Beschlußempfehlung des Innenausschusses des Deutschen Bundestages vom 4. Mai 1984 Rechnung getragen, wonach der Deutsche Bundestag die Auffassung des Bundesbeauftragten für den Datenschutz teilt, daß das nach § 76 Abs. 2 Satz 2 SGB X mögliche Widerspruchsrecht des Betroffenen nur wahrgenommen werden könne, wenn dieser von einer beabsichtigten Offenbarung wisse (Bundestags-Drucksache 10/1719).

11.1.3 Ärztlicher/Psychologischer Dienst

— Die Bundesanstalt für Arbeit war auch im Berichtszeitraum bemüht, die Regelungen zur Erstellung und Behandlung ärztlicher und psychologischer Gutachten zusammenzufassen und transparenter zu gestalten. Ich habe zu diesem Thema mit der Bundesanstalt Gespräche geführt, die allerdings bisher nicht zu einem Abschluß gebracht werden konnten. Ein Schwerpunkt weiterer Verhandlungen muß u. a. die Regelung einer strengeren Trennung zwischen Arbeitsvermittlung bzw. Leistungsverwaltung einerseits und dem Ärztlichen und Psychologischen Dienst andererseits sein.

— In diesem Zusammenhang hatte ich mich insbesondere mit dem Problem der sog. *Teamberatung* zu befassen. Gemäß Runderlaß 88/85 handelt es sich bei der Teamberatung um eine Problembearbeitung durch den Psychologen und den Arbeits- oder Berufsberater gemeinsam mit dem Ratsuchenden, gegebenenfalls unter Beteiligung weiterer Mitarbeiter der Abteilungen Arbeitsvermittlung, Arbeitsberatung und Berufsberatung. Ich verkenne nicht, daß — wie in dem Runderlaß weiter ausgeführt — eine Zeitersparnis gegenüber anderen Vorgehensweisen eintreten kann. Zu bedenken ist jedoch, daß die Protokolle über die Beratungen üblicherweise von dem Psychologen des jeweiligen Arbeitsamtes verfaßt und in voller Länge zu den Vermittlungsakten genommen werden. Es ist häufig nahezu unvermeidlich, daß der Psychologe bei Erstellung des Protokolls bereits eine fachliche Bewertung des Verhaltens des Ratsuchenden vornimmt. Damit gehen in das Teamberatungsprotokoll Elemente eines psychologischen Gutachtens ein, die für die weitere Beratung oder Vermittlung des Ratsuchenden in dieser Form nicht erheblich sind. So fand ich beispielsweise in einem Teamberatungsprotokoll den Hinweis, daß aus psychologischer Sicht „Verdacht auf eine neurotische Fehlentwicklung mit verringerter Belastbarkeit und Ausweichverhalten in Belastungssituationen" bestehe. M. E. hätte es für die weitere Tätigkeit der Vermittlungsabteilungen in diesem Falle ausgereicht, wenn ohne nähere Begründung eine nervenfachärztliche Begutachtung empfohlen worden wäre.

  Ich halte daher eine Überprüfung des Verfahrens bei der Teamberatung unter Beteiligung eines Psychologen für angebracht und habe die Bundesanstalt für Arbeit um eine entsprechende Berücksichtigung meiner Auffassung in weiteren Runderlassen gebeten.

11.1.4 Berufsförderung

Aufgrund einer Eingabe habe ich die Erhebungsbögen überprüft, anhand deren die Dienststellen der Bundesanstalt für Arbeit die Förderungswürdigkeit von Maßnahmen nach § 34 Abs. 1 Nr. 1 AFG feststellen. Für die Förderungswürdigkeit eine Maßnahme sind u. a. Ausbildung und Berufserfahrung des Leiters und der Lehrkräfte einer beruflichen Bildungsmaßnahme maßgebend. In diesem Zusammenahng wird für die genannten Personen die Frage nach der Lehrbefähigung bzw. Anerkennung durch die Schulaufsichtsbehörde für die von ihnen wahrgenommenen Unterrichtsfächer gestellt. Aus den Erhebungsunterlagen ist nicht ersichtlich, daß der Träger einer Bildungsmaßnahme die gesamten Zeugnisse und Qualifikationsnachweise der in Lehrgängen eingesetzten Mitarbeiter einreichen muß. Die Bundesanstalt für Arbeit bestätigte meine Auffassung, daß ihre Dienststellen grundsätzlich nur die in den Vordrucken vorgesehenen Angaben zur Qualifikation der Lehrkräfte benötigen. Sie beabsichtigt, eine entsprechende Klarstellung in ihre Dienstanweisungen an die örtlichen Arbeitsämter aufzunehmen. Darin soll es wie folgt heißen: „Grundsätzlich sind die Angaben des Trägers zur Qualifikation der Lehrkräfte bei der Prüfung der Voraussetzungen nach § 34 Abs. 1 Satz 2 Nr. 1 AFG ausreichend. Die Einsichtnahme in entsprechende Nachweise ist nur dann zu fordern, wenn begründete Zweifel bestehen. Kopien von diesen Unterlagen, insbesondere von Zeugnissen sind nicht zu den Akten zu nehmen (Datenschutz)."

11.2 Krankenversicherung

11.2.1 Kontrollen

— Bei der *„Krankenversorgung der Bundesbahnbeamten (KVB)"* wurde eine datenschutzrechtliche Kontrolle durchgeführt.

  Die KVB ist nicht Träger der gesetzlichen Krankenversicherung, sondern eine betriebliche Sozialeinrichtung der Deutschen Bundesbahn (DB) in der Rechtsform einer bundesunmittelbaren Körperschaft des öffentlichen Rechts mit Selbstverwaltung. Die KVB erfüllt im Auftrag der DB

Fürsorgepflichten des Dienstherrn in Krankheits-, Geburts- und Todesfällen und bei Maßnahmen zur Früherkennung von Krankheiten, die der DB insbesondere nach § 79 BBG obliegen. Sie gewährt ihren Mitgliedern Leistungen im Sinne der Beihilfevorschriften des Bundes und darüber hinausgehende Leistungen nach Satzung und Tarif aufgrund eigener Beitragsleistungen der Mitglieder.

Die KVB ist organisatorisch eingegliedert in das Sozialamt der DB. Die Selbstverwaltungsorgane der KVB — Vertreterversammlung und Vorstand — bestehen jeweils aus einer bestimmten Anzahl von durch die Personalvertretungen gewählten Mitgliedervertretern und einem Vertreter der DB mit gleicher Stimmenzahl. Der Vertreter der DB in den Organen ist Abteilungspräsident des Sozialamtes und gleichzeitig Geschäftsführer der Hauptverwaltung der KVB.

Das Personal der KVB wird von der DB zur Verfügung gestellt. Die Mitarbeiter der KVB sind dienstrechtlich Angehörige der für die jeweilige Bezirksleitung zuständigen Bundesbahndirektion.

Diese Personalsituation macht die KVB insoweit vergleichbar mit einer Betriebskrankenkasse. Bei den Betriebskrankenkassen ergeben sich daraus regelmäßig datenschutzrechtliche Probleme, insbesondere dadurch, daß der Vertreter des Arbeitgebers in den Organen in aller Regel der Personalabteilung des Unternehmens angehört und damit gleichzeitig Personalvorgesetzter der Mitarbeiter und Mitglieder der Betriebskrankenkasse ist.

Bei der KVB ist demgegenüber der Vertreter des Dienstherrn in den Organen Angehöriger der besonderen Organisationseinheit „Sozialamt der Deutschen Bundesbahn"; er hat in dieser Funktion keine personalrechtlichen Befugnisse hinsichtlich der Mitarbeiter und der Versicherten der KVB, außer bei Mitarbeitern des Sozialamtes selbst, die auch Mitglieder der KVB sein können.

Insofern treten die Probleme, die sich aus der engen Verbindung von Personalverwaltung und Krankenkasse ergeben, bei der KVB nicht in gleicher Schärfe zutage wie bei den Betriebskrankenkassen. Konkrete Probleme aus dieser Aufbauorganisation sind bei der Kontrolle jedenfalls nicht bekannt geworden.

Die Kontrolle bei der Bezirksleitung Rosenheim der KVB diente in erster Linie der Klärung dieser rechtlichen und organisatorischen Struktur der KVB. Die Klärung war Voraussetzung für die Beurteilung der Organisation des Datenschutzes und der Datenverarbeitung und des sonstigen Umgangs mit personenbezogenen Daten in der KVB. Während dieses ersten Kontrollbesuchs wurde u. a. festgestellt, daß der KVB von der Datenverarbeitungsstelle regelmäßig verschiedene Listenausdrucke zur Verfügung gestellt werden. Diese Listen erscheinen als erforderlich und datenschutzrechtlich unbedenklich. Eine Ausnahme bildet die „Zusammenstellung nach Belegnummern". In dieser Liste wird die Arbeitsleistung jedes Mitarbeiters für jeden Tag ausgedruckt. Sie enthält für jeden Bearbeiter die Angabe des Tages, die Zahl der erledigten Anträge, die Anzahl der gelesenen Zeichen, die Zahl der Bildschirmkorrekturen bei jeder der eingetragenen Kennziffern (0—9) sowie die Zahl der zurückgewiesenen Anträge. Dieses Verfahren schafft einen Überblick über die Tagesleistung jedes Mitarbeiters und ermöglicht eine Leistungskontrolle über einen längeren Zeitraum sowie einen Vergleich mit der Arbeitsleistung der anderen Mitarbeiter. Ein solcher Vergleich wird durch zusätzliche Aufschreibungen und Zusammenstellungen unter Berücksichtigung von Fehlzeiten auch durchgeführt. Eine derartige Leistungskontrolle mit Hilfe der ADV gefährdet nach der Rechtsprechung des Bundesarbeitsgerichts das Persönlichkeitsrecht des Betroffenen und unterliegt daher der Mitbestimmung. Eine lückenlose Leistungskontrolle wäre allerdings auch im Rahmen der Mitbestimmung nicht zulässig.

Vor einer abschließenden Beurteilung der Datenverarbeitung der KVB sind weitere Prüfungen sowie Gespräche mit der Hauptverwaltung der KVB, mit der Datenverarbeitungsstelle Köln der Deutschen Bundesbahn als programmentwickelnde Stelle für die automatisierte Datenverarbeitung und gegebenenfalls mit dem Bereich „Zentrale Datenverarbeitung" der DB erforderlich.

— Bei der *Betriebskrankenkasse des Bundesverkehrsministeriums* habe ich eine datenschutzrechtliche Kontrolle durchgeführt. Die Kontrolle erstreckte sich insbesondere auf die Organisation des Datenschutzes und auf die Verarbeitung der Versicherten- und der Personaldaten in der Hauptverwaltung und in einer Bezirksstelle.

Die organisatorischen Rahmenbedingungen für die Sicherung und den Schutz der Sozialdaten sind nach den getroffenen Feststellungen gut. Die Übersicht über die vorhandenen Daten (§ 79 Abs. 1 SGB X i. V. m. § 29 Nr. 1 BDSG) ist im allgemeinen sorgfältig erstellt und entspricht den gesetzlichen Vorgaben. Um die Übersichtlichkeit und die Aussagekraft der Dateibeschreibungen noch zu erhöhen, habe ich einige Ergänzungen angeregt.

Die Aufgabe, die Mitarbeiter der Kasse durch geeignete Maßnahmen mit den Vorschriften über den Datenschutz vertraut zu machen (§ 29 Nr. 3 BDSG), wird vom internen Datenschutzbeauftragten durch eine von ihm erstellte ausführliche Dienstanweisung, durch besondere und gezielte Hinweise aus gegebenem Anlaß und durch umfangreiche Schulungsveranstaltungen in vorbildlicher Weise erfüllt.

Die Verfahrensabläufe der Datenverarbeitung, soweit sie in der Kasse stattfindet, geben keinen Anlaß zu datenschutzrechtlichen Bedenken. Der BKK des BMV steht für ihre Datenverarbeitung derzeit keine eigene EDV-Anlage zur Verfügung. Die automatisierte Datenverarbeitung, z. B. die Mitgliederbestandsführung, erfolgt in ihrem

Auftrag durch den Bundesverband der Betriebskrankenkassen im Rahmen des Informationssystems Betriebskrankenkassen (ISBKK). Wie in anderen Fällen bestand auch hier Veranlassung darauf hinzuweisen, daß bei einer Auftragsdatenverarbeitung der Auftraggeber alleiniger Herr der Daten und damit für die Durchführung der Datenverarbeitung und die ordnungsgemäße Programmanwendung verantwortlich bleibt (§ 8 Abs. 1 Satz 1 i. V. mit § 29 Nr. 2 BDSG). Dessen muß sich die auftraggebende Stelle stets bewußt sein, um auch im Einzelfall gegebenenfalls erforderliche Weisungen an den Auftragnehmer zu erteilen (§ 8 Abs. 2 Satz 2 BDSG, § 80 Abs. 2 SGB X).

Das ISBKK und die Verfahren im einzelnen wurden bei dieser Kontrolle nicht geprüft.

Es besteht in der BKK des BVM die Absicht, ab 1989 eine eigene dezentrale Datenverarbeitung einzuführen. Konkrete Planungen liegen noch nicht vor. Ich habe angeboten, im Rahmen meiner Möglichkeiten die Kasse bei der weiteren Planung und Realisierung zu beraten.

Ein allgemeines krankenkassenspezifisches Problem, nämlich die Bearbeitung und Verwaltung der Sozialdaten der Mitarbeiter in der Krankenkasse, konnte bei der BKK des BMV im letzten Jahr befriedigend gelöst werden. Die Führung der Leistungskarten und die Leistungsgewährung für die Mitarbeiter der Kasse wurde in den Bezirksstellen jeweils einem Mitarbeiter in herausgehobener Funktion, der jedoch keine Personalführungsaufgaben hat, übertragen. Diese Lösung entspricht den datenschutzrechtlichen Erfordernissen und meinen in früheren Tätigkeitsberichten gemachten Vorschlägen.

Die besondere datenschutzrechtliche Aufmerksamkeit gilt bei Betriebskrankenkassen stets auch der Bearbeitung und sonstigen Behandlung von Personaldaten und -unterlagen der Kassenmitarbeiter.

Bei den Betriebskrankenkassen stellt der Arbeitgeber auf seine Kosten und Verantwortung die für die Geschäfte erforderlichen Personen (§ 362 Abs. 1 RVO). Hieraus folgt, daß allein der Arbeitgeber bzw. Dienstherr des Kassenpersonals pesonalrechtliche Befugnisse ausübt und nicht etwa der Vorstand oder der Geschäftsführer der Kasse.

Dienstvorgesetzter der Mitarbeiter der BKK des BMV ist der Präsident der zuständigen Wasser- und Schiffahrtsdirektion (WSD).

Im Hinblick auf diese Rechtslage hat die WSD Nord bereits mit Schreiben vom 9. November 1982 darauf hingewiesen, daß es keine Legitimation zur Führung von Personalakten bei der BKK gebe. Die WSD hat deshalb verlangt, daß die bei der BKK geführten Personalakten aufgelöst und die Unterlagen gegebenenfalls der personalaktenführenden Stelle bei der WSD übergeben werden. Das bei der BKK in Personalangelegenheiten anfallende Schriftgut sei, sofern es nicht in die Personalakten aufgenommen werden müsse, in Generalakten zu führen.

Die stichprobenartige Durchsicht dieser Generalakten hat allerdings ergeben, daß darin für einzelne Mitarbeiter immer noch umfangreiche Unterlagen abgelegt sind, die eindeutig zu den Personalakten gehören. Sie sind deshalb an die personalaktenführende Stelle abzugeben.

11.2.2 Einzelfragen

— Bei *Betriebskrankenkassen* ergeben sich aus der gesetzlichen Organisationsstruktur grundlegende Problem. Ich habe hierüber mehrfach berichtet (vgl. 5. TB S. 63, 6. TB S. 34, 7. TB S. 48). Immer wieder erhalte ich Eingaben einzelner Mitglieder von Betriebskrankenkassen, von Personal- und Betriebsräten und auch von Ärzten, die ihrer Befürchtung Ausdruck geben, daß infolge der Personalhoheit der Trägerfirma über die Mitarbeiter der Kasse in unzulässiger Weise Einzelheiten über die gesundheitlichen Verhältnisse und die Art von Erkrankungen und der durchgeführten Behandlungen und Therapien an die personalverwaltende Stelle gelangen und dort zu treffende Personalentscheidungen beeinflussen können. Solche Befürchtungen sind nicht von der Hand zu weisen, ein konkreter Beweis gelingt jedoch kaum, da — wie in einer Eingabe ausgedrückt — „es dazu keiner Korrespondenz bedarf".

Hinzu kommt noch die ebenfalls problematische Zusammensetzung der Selbstverwaltungsorgane der Betriebskrankenkassen. Nach §44 Abs. 2 SGB IV gehören den Organen außer den Vertretern der Versicherten mit gleicher Stimmenzahl der Arbeitgeber oder sein Vertreter an. Nach meiner Erfahrung hat der Arbeitgebervertreter im allgemeinen eine — herausgehobene — Funktion in der Personalverwaltung des Unternehmens. Auf diesem Wege gelangen „dem Arbeitgeber" in der Person des Personalvorgesetzten in vielen Fällen personenbezogene Daten der Arbeitnehmer aus dem Bereich der Krankenkasse zur Kenntnis, die dem Arbeitgeber nach den Geheimhaltungsvorschriften des SGB wie auch nach arbeitsrechtlichen Grundsätzen nicht offenbart werden dürfen. Dazu bedarf es nicht einmal einer förmlichen Behandlung von Einzelfällen im Vorstand der Kasse. Allein die institutionalisierte enge Verbindung des Arbeitgebers zur Kasse und die zwangsläufige, funktionsbedingt intensive Befassung mit Kassenangelegenheiten widerspricht nach meiner Auffassung den Grundsätzen und Vorschriften über die Wahrung des Sozialgeheimnisses.

Ich habe bereits im Jahre 1982 den Bundesminister für Arbeit und Sozialordnung auf diese Problematik hingewiesen. In den Erörterungen mit dem Bundesarbeitsminister und dem Bundesverband der Betriebskrankenkassen hatte ich eine Ergänzung der Vorschrift des §44 Abs. 2 SGB IV dahin gehend vorgeschlagen, daß der Vertreter des Arbeitgebers in den Selbstverwaltungsorganen nicht der Personalverwaltung des Unternehmens angehören darf. Eine derartige gesetzliche Regelung wurde damals abgelehnt, jedoch hat der Bundesverband der Betriebskrankenkassen in einem Rundschreiben an

seine Mitgliedskassen auf die unterschiedlichen Zuständigkeiten zwischen dem Geschäftsführer der Kasse und den Selbstverwaltungsorganen hingewiesen und dazu festgestellt, daß die Weitergabe personenbezogener Daten über gesundheitliche Verhältnisse der Mitglieder von Krankenkassen an den Vorstand oder einzelne Mitglieder des Vorstandes grundsätzlich unzulässig ist, da weder der Vorstand noch dessen einzelne Mitglieder solche Daten im Rahmen der Wahrnehmung ihrer Aufgaben benötigen. Ich habe darüber in meinem Fünften Tätigkeitsbericht (S. 63) berichtet. Das Rundschreiben bezeichnet die Weitergabe von Kassendaten „grundsätzlich" als unzulässig und „regelmäßig" als nicht erforderlich, schließt also die Zulässigkeit in Einzelfällen nicht aus. Auch aus meiner Sicht kann es erforderlich sein, im Rahmen einer ordnungsgemäßen Aufgabenerfüllung in bestimmten Einzelfällen auch personenbezogene Einzelheiten im Vorstand zu erörtern oder zu entscheiden. Darüber hinaus ist es auch nicht völlig auszuschließen, daß solche Einzelheiten infolge der notwendigerweise engen Zusammenarbeit zwischen Geschäftsführer und Vorstand der Kasse „gesprächsweise" erörtert werden. Die Zweckbindung offenbarter Sozialdaten und die Geheimhaltungspflicht des Empfängers (§78 SGB X) ist aber dann kein ausreichender Schutz, wenn Personalunion zwischen dem Vorstandsmitglied und dem Personalvorgesetzten besteht. Die Interessenkollision ist in diesem Fall offensichtlich. Schon um den Anschein zweckwidriger unzulässiger Verwendung von Sozialdaten für Personalmaßnahmen zu vermeiden und entsprechenden Befürchtungen zu begegnen, die von Petenten immer wieder an mich herangetragen werden, komme ich auf meine frühere Anregung zurück, gesetzlich zu regeln, daß der Arbeitgebervertreter in den Selbstverwaltungsorganen der Betriebskrankenkassen nicht der Personalverwaltung des Unternehmens angehören darf.

— Im Rahmen der *Krankenhilfe* kann die Krankenkasse satzungsmäßige Zuschüsse zu den Kosten für Kuren gewähren, wenn diese nach vertrauensärztlicher Begutachtung erforderlich und geeignet sind, eine Schwächung der Gesundheit, die in absehbarer Zeit voraussichtlich zu einer Krankheit führen würde, zu beseitigen.

Wenn die Begutachtung durch den Vertrauensarzt nicht aufgrund einer körperlichen Untersuchung des Betroffenen, sondern nach ärztlichem Ermessen aufgrund der „Aktenlage" erfolgt, benötigt der Vertrauensarzt dazu von der Krankenkasse diese „Akten", d. h. alle Unterlagen, die für die Begutachtung geeignet und erforderlich sind.

Diese Unterlagen unterliegen bei der Krankenkasse dem Sozialgeheimnis (§35 SGB I). Sie dürfen einem Dritten nur unter den Voraussetzungen der §§67 bis 77 SGB X offenbart werden. Nach §69 Abs. 1 Nr. 1 SGB X ist eine Offenbarung zulässig, soweit sie für die Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch erforderlich ist. Die Offenbarungsbefugnis ist jedoch durch §76 Abs. 1 SGB X eingeschränkt bei Daten, die der Krankenkasse von einem Arzt zugänglich gemacht worden sind; in diesen Fällen ist die Offenbarung nur unter den Voraussetzungen zulässig, unter denen der Arzt selbst offenbarungsbefugt wäre.

Eine Krankenkasse hat im Rahmen des Gutachterverfahrens dem Vertrauensärztlichen Dienst zusammen mit anderen Unterlagen auch den Entlassungsbericht eines Krankenhauses zur Verfügung gestellt, in dem der Betroffene sich ein Jahr zuvor einer Herzoperation unterzogen hatte. Zur Zulässigkeit der Übersendung des Entlassungsberichts hat die Krankenkasse zunächst auf die Offenbarungsbefugnis nach §69 Abs. 1 Nr. 1 SGB X verwiesen und ergänzend ausgeführt, daß sie als Auftraggeber eines Gutachtens verpflichtet sei, den Vertrauensarzt über das Vorhandensein verwertbarer früherer Untersuchungsergebnisse zu unterrichten und diese vom Amts wegen oder auf Anforderung zu übermitteln. Dieser Rechtssatz sei zwar nicht ausdrücklich formuliert, ergebe sich aber aus den Vorschriften über die Zusammenarbeit der Leistungsträger (§86 SGB X) und über die Verwertung vorliegender Untersuchungsergebnisse (§96 Abs. 2 SGB X). Die Einschränkung der Offenbarungsbefugnisse gemäß §76 SGB X stehe im Hinblick auf diese Vorschriften der Offenbarung nicht entgegen.

Diese Auffassung ist m. E. nicht zutreffend. Nach §35 Abs. 2 SGB I sind die in §§67 bis 77 SGB X getroffenen Offenbarungsregelungen abschließend. Somit können die angegebenen Vorschriften der §§86 und 96 SGB X eine Offenbarungsbefugnis nicht begründen, sondern setzen diese voraus. Die Bedingungen, unter denen der Krankenhausarzt bei Berücksichtigung der ärztlichen Schweigepflicht gegenüber dem Vertrauensarzt offenbarungsbefugt wäre (§76 Abs. 1 SGB X), liegen nicht vor. Die Übermittlung eines Krankenhaus-Entlassungsberichts und anderer ärztlicher Unterlagen, die nicht selbst Gegenstand der Begutachtung sind (§369b RVO), an den gutachtenden Vertrauensarzt ist deshalb nur mit Einwilligung des Betroffenen zulässig.

— Die in meinem Siebenten Tätigkeitsbeicht (S. 52) beschriebene Praxis von Krankenkassen, zur *Beitragsbemessung* bei der Einkommensermittlung im Bedarfsfall Einkommensteuerbescheide vorlegen zu lassen, hat auch in diesem Berichtsjahr zu einer Reihe von Eingaben geführt. Zur Lösung dieses Problems hat die Deutsche Angestellten Krankenkasse (DAK) festgelegt, daß „von Selbständigen einschließlich Angehöriger freier Berufe, die eine befristete Einstufung in eine beitragsgünstigere Versicherungsklasse beantragen, keine Einkommensteuererklärung bzw. kein Einkommensteuerbescheid mehr vorzulegen ist". Die Kasse erkennt vielmehr als Nachweis der monatlichen Einnahmen die Erklärung des Mitgliedes auf einem Vordruck in Verbindung mit einer Bestätigung eines Steuerberaters an.

Ich halte dies für ein erfreuliches Beispiel dafür, daß nicht immer amtliche Bescheide verlangt werden müssen, die oft eine Fülle nicht benötigter Angaben enthalten, sondern daß es einfachere und datenschutzfreundlichere Verfahrensweisen gibt.

— Durch eine Eingabe ist mir bekannt geworden, daß eine bundesweit tätige Leiharbeitsfirma bei der *Einstellung von Mitarbeitern* von diesen die Unterschrift unter einen schon vorgedruckten Brief verlangt, mit dem der Mitarbeiter seine Krankenkasse „um eine Bescheinigung über die letzten zwölf Monate, aus der meine bisherigen Krankzeiten zu ersehen sind", bittet und sich gleichzeitig damit einverstanden erklärt, „daß diese Auskunft direkt an meine Firma ... weitergeleitet wird". Die in dem Einzelfall zuständige Krankenkasse hat bestätigt, daß sie „auf Wunsch" der Betroffenen der betreffenden Firma eine entsprechende Bescheinigung übersandt hat.

Nachdem ich die für die Leiharbeitsfirma zuständige Datenschutz-Aufsichtsbehörde eingeschaltet und diese die obersten Aufsichtsbehörden der Länder und die Landesbeauftragten für den Datenschutz beteiligt hatte, ist eine grundsätzliche Erörterung über die Rechtswirksamkeit solcher Einwilligungserklärungen unter Berücksichtigung des eingeschränkten Fragerechts des Arbeitgebers in Gang gekommen. Als überwiegend einheitliches Ergebnis ist festzustellen:

Die Übermittlung/Offenbarung von Krankheitsdaten durch eine Krankenkasse an den Arbeitgeber ist auch mit Einwilligung des Arbeitnehmers grundsätzlich unzulässig. Das in Artikel 1 und 2 GG verankerte allgemeine Persönlichkeitsrecht und das daraus abgeleitete informationelle Selbstbestimmungsrecht, wie es vom Bundesverfassungsgericht entwickelt wurde, führt im Sozialrecht zum Schutz des Sozialgeheimnisses und im Arbeitsrecht zur Einschränkung des Fragerechts des Arbeitgebers. Ein effektiver Schutz des informationellen Selbstbestimmungsrechts erfordert, daß bei Anwendung der sozialrechtlichen Vorschriften auf die arbeitsrechtlichen Grundsätze — wie auch umgekehrt — Rücksicht genommen wird. Bei der Frage, ob die Einwilligung des Versicherten die Übermittlung von Sozialdaten an den Arbeitgeber rechtfertige, ist daher auch zu prüfen, ob diese Einwilligung nicht aus arbeitsrechtlichen Erwägungen unwirksam ist. Die Beschaffung von Krankheitsdaten durch den Arbeitgeber von der Krankenkasse darf nicht zu einer Umgehung des arbeitsrechtlichen Verbots einer unmittelbaren Frage an den Arbeitnehmer führen. Das Fragerecht des Arbeitgebers ist nach ständiger Rechtsprechung in diesem Zusammenhang im Grundsatz beschränkt auf die gesundheitlichen Verhältnisse, die für den konkret zu besetzenden Arbeitsplatz von Bedeutung sind. Genausowenig darf eine abverlangte oder faktisch erzwungene Einwilligung zu einer Umgehung des Schutzes der Sozialdaten führen. Was die Krankenkasse dem Arbeitgeber nicht offenbaren darf und was der Arbeitgeber aus arbeitsrechtlichen Gründen den Arbeitnehmer nicht fragen darf, darf auch nicht über den Betroffenen als „(un)freiwilligen Mittler" in die Verfügung des Arbeitgebers gelangen.

Da jedoch die Krankenkasse die aus arbeitsrechtlichen Gründen bestehende Unwirksamkeit der Einwilligung in vielen Fällen kaum erkennen kann, ist eine Lösung nur von einer bereichsspezifischen Regelung des Datenschutzes für Arbeitnehmer zu erwarten, die von der Bundesregierung vorbereitet wird (vgl. Bundestags-Drucksache 10/1719 zu II 13).

— Wiederholt bin ich in Bürgereingaben, aber auch von Krankenkassen selbst auf *Werbemaßnahmen* anderer *Krankenkassen* und auf datenschutzrechtliche Bedenken gegen solche Maßnahmen angesprochen worden. Dabei ging es beispielsweise um folgende Fälle:

  — Stellungsuchende, deren Bewerbung bei verschiedenen Krankenkassen erfolglos blieb, erhielten kurze Zeit nach Ablehnung der Bewerbung Besuch von Außendienstmitarbeitern dieser Kasse, die für einen Eintritt in ihre Kasse warben.

  — Krankenkassen verwenden die ihnen als Einzugsstellen für die Rentenversicherungsbeiträge bekanntgewordenen Adressen von Nichtmitgliedern zu Werbezwecken.

  — Kassenmitglieder werden gezielt aufgefordert, auf einer beigefügten Antwortkarte Namen und Anschriften von Arbeitskollegen — auch ohne deren Wissen — mitzuteilen.

  — Arbeitgeber werden aufgefordert, Namen, Anschriften von Berufsanfängern und neu einzustellenden Mitarbeitern mitzuteilen.

  — Schulabgänger, die sich um einen Ausbildungsplatz bei einer Krankenkasse beworben haben, werden aufgefordert, Adressenlisten der Mitschüler zu übersenden.

In den Fällen der „Einzugsstellen" herrscht allgemein die Auffassung vor, daß Daten von Nichtmitgliedern wegen der Zweckgebundenheit dieser Daten nicht für Werbezwecke genutzt werden dürfen. Ein Landesverband der Ortskrankenkassen hat diese Auffassung ausdrücklich bestätigt.

Die Zweckbindung greift m. E. grundsätzlich auch bei Bewerberdaten ein.

Der Bundesminister für Arbeit und Sozialordnung hat in einem Rundschreiben an die zuständigen Minister (Senatoren) der Länder festgestellt, daß die Übermittlung von Anschriften der Auszubildenden vor dem Beginn des Ausbildungsverhältnisses an die Krankenkasse aus datenschutzrechtlichen und arbeitsrechtlichen Gründen unzulässig ist.

In anderen Fällen ist die Rechtslage leider nicht so klar. Häufig liegt ein Verstoß gegen konkrete Rechtsvorschriften nicht vor. Die Ersatzkassen verweisen in ihren Stellungnahmen auf ihr Recht auf Werbung, das ihnen vom Bundesso-

zialgericht in zwei Urteilen von 1983 und 1984 bestätigt worden sei. Dieses Recht wird von mir auch nicht bestritten; das Recht auf Werbung besagt jedoch nichts darüber, wie geworben wird.

Bestritten wird von einigen Kassen allerdings, daß es sich hier überhaupt um eine Frage des Datenschutzes handele. Dem kann ich jedoch nicht folgen. Denn in allen Fällen geht es um eine Erhebung und Verwendung personenbezogener Daten durch öffentliche Stellen. Wenn es sich hier auch nicht um eine zwangsweise Datenerhebung handelt, so sind doch die wesentlichen Grundsätze des Rechts auf informationelle Selbstbestimmung, d. h. hier der „Befugnis des einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen", zu beachten. Die Preisgabe und Verwendung seiner Daten beruht aber dann nicht auf einer freien Entscheidung des Betroffenen, wenn sie ohne sein Wissen geschieht. Mit dem Recht auf informationelle Selbstbestimmung ist deshalb eine Datenerhebung durch Befragung Dritter z. B. Arbeitskollegen, Mitschüler, nicht zu vereinbaren. Diese sind zwar nicht Adressaten des Grundrechtsanspruchs ihrer Mitbürger; sie selbst sind rechtlich nicht gehindert, (unaufgefordert) Anschriften an ihre Krankenkasse bekanntzugeben. Die Krankenkasse als Träger öffentlicher Rechte und Pflichten sollte aber dazu nicht auffordern, sondern im Gegenteil darauf hinwirken, daß die Anschriftenübermittlung nicht ohne Wissen des Betroffenen erfolgt.

12. Öffentliche Sicherheit

12.1 Probleme und Hindernisse

Bei der Erfüllung meiner Aufgaben im Sicherheitsbereich mußte ich mich im Berichtsjahr mit verschiedenen Schwierigkeiten und Komplikationen auseinandersetzen.

Der seit dem Volkszählungsurteil allgemein anerkannte Mangel an ausreichenden datenschutzrechtlichen Vorgaben für die personenbezogene Datenverarbeitung im Sicherheitsbereich soll durch eine Reihe von Gesetzen behoben werden, für die die Bundesregierung und die Koalition Entwürfe eingebracht haben und deren parlamentarische Behandlung begonnen hat. Eine Verbesserung des Datenschutzes ist dadurch allerdings noch nicht eingetreten — einerseits weil es, vom ZEVIS-Gesetz abgesehen, nicht zu Gesetzesbeschlüssen gekommen ist, andererseits weil von den Gesetzentwürfen in ihrer inhaltlichen Ausgestaltung kaum Signale ausgehen, die zu einer stärkeren Orientierung der Verwaltungspraxis am Recht des Bürgers auf informationelle Selbstbestimmung beitragen. Bestehende Verfahrensweisen und auch geplante Änderungen, die ich kritisiert habe, werden zunehmend mit dem Argument verteidigt, die Gesetzentwürfe erlaubten solche Maßnahmen.

Der Ausbau der Datenverarbeitungsverfahren schreitet unvermindert fort. Die Sicherheitsbehörden haben in den vergangenen Jahren für die automatisierte Datenverarbeitung große personelle Kapazitäten eingesetzt und erhebliche Sachinvestitionen getätigt. Die in den vergangenen Jahren entwickelten Systeme wollen jetzt auch eingesetzt sein, und neue Verfahren, die sich auf speziellen begrenzten Gebieten bewährt haben, „verlangen" nach breiterer Anwendung. Die Aufgabe des Datenschutzes, entsprechend dem Verhältnismäßigkeitsgrundsatz dafür zu sorgen, daß Systeme mit tiefgehenden Eingriffen in den Persönlichkeitsbereich nur bei entsprechend gravierenden Vorgängen — etwa schwersten Straftaten oder Spionage — angewendet werden, ist schwieriger geworden. Für den Datenschutz ist es daher dringend notwendig, daß der Gesetzgeber die ihm nach der Verfassung obliegenden Regelungsaufgaben wahrnimmt und dabei klare Markierungen für die informationstechnische Ausgestaltung setzt.

Mein Bericht über die Lage des Datenschutzes bei den Sicherheitsbehörden wäre unvollständig ohne einen deutlichen Hinweis auf die Behinderung meiner Kontrolltätigkeit beim Bundesamt für Verfassungsschutz, die auf Interventionen der Geheimschutzbeauftragten der Mehrheit der von Bundesministerien zurückging. Ich kann zwar mit Befriedigung feststellen, daß der Innenausschuß des Deutschen Bundestages, an den ich mich daraufhin gewandt habe, die Angelegenheit im Sinne des Datenschutzes behandelt und daß der Bundesminister des Innern mir daraufhin die Erfüllung meiner gesetzlichen Aufgaben wieder ermöglicht hat. Ich kann es aber nicht als ermutigendes Zeichen ansehen, daß auch im zehnten Jahr nach Verabschiedung des Bundesdatenschutzgesetzes einige Bundesministerien den koordinierten Versuch unternommen haben, dem Bundesbeauftragten den Zugang zu Unterlagen zu versperren, die ihm nach dem klaren Wortlaut des Gesetzes zur Erfüllung seiner Aufgaben vorzulegen sind. Ein klärendes Wort der Bundesregierung an die zuständigen Stellen könnte die Aufgeschlossenheit für den Datenschutz sicher fördern.

Erstmals haben sich in diesem Jahr auch bei der Veröffentlichung meines Tätigkeitsbereichs Schwierigkeiten ergeben. Sie haben dazu geführt, daß der Bereich des Bundesamtes für Verfassungsschutz aus diesem Bericht ausgeklammert bleibt (vgl. unten 14.). Die Geheimhaltungspflicht bei den Sicherheitsbehörden und meine Verpflichtung, jährlich einen öffentlichen Tätigkeitsbereich vorzulegen, stehen in einem gewissen Zielkonflikt zueinander. Daß ich die Geheimhaltungsbedürftigkeit bestimmter Sachverhalte und Verfahrensweisen im Sicherheitsbereich respektiere, ergibt sich aus meiner Berichtspraxis der vergangenen Jahre. Umgekehrt muß ich von den Bundesbehörden aber auch erwarten, daß sie auf meine Berichtspflicht Rücksicht nehmen. Ich bin darauf angewiesen, daß die Geheimhaltung nicht überzogen wird, weil sonst — gewollt oder ungewollt — das Recht des Bundesbeauftragten geschmälert wird, sich mit seiner Auf-

fassung öffentlich Gehör zu verschaffen, wenn dies aus seiner Sicht zum Schutz der Rechte des einzelnen geboten ist.

12.2 Gesetzgebungsvorhaben

Die von der Bundesregierung und der Koalition vorgelegten Gesetzentwürfe (Drucksachen 10/4737, 10/5343 und 10/5344), die weithin als Paket der „Sicherheitsgesetze" bezeichnet werden, sind für die Zukunft des Datenschutzes im Sicherheitsbereich von zentraler Bedeutung. Bereits bei der Vorlage der ersten Entwürfe Anfang 1986 habe ich erklärt, daß es höchste Zeit ist, den im Volkszählungsurteil formulierten datenschutzrechtlichen Grundsätzen Geltung zu verschaffen. Leider hat der Gesetzgeber den Entwürfen nicht die Priorität gegeben, die notwendig gewesen wäre, um die Gesetzgebungsverfahren noch vor Ende der Legislaturperiode abzuschließen. Zwar wurden Anhörungen anberaumt, in deren Rahmen ich auch meine Auffassung dargelegt habe, doch ist es zu einer Auswertung der Ergebnisse und zur Aufnahme der Beratungen in den Ausschüssen — vom ZEVIS-Gesetz abgesehen — nicht mehr gekommen.

Die in der 10. Legislaturperiode vorgelegten Gesetzentwürfe sind in datenschutzrechtlicher Hinsicht in zentralen Punkten unzureichend (vgl. dazu auch die Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. Januar und vom 18. April 1986, Anlagen 1 und 4). Die wichtigsten Punkte meiner Kritik sind folgende:

a) Informationelle Selbstbestimmung durch den einzelnen setzt voraus, daß er die Auswirkungen der Rechtsvorschriften auf die Verarbeitung seiner personenbezogenen Daten im voraus hinreichend sicher einschätzen kann. Dies erfordert ein hohes Maß an Normenklarheit, das in den Entwürfen häufig nicht erreicht wird. So werden etwa bei der Beschreibung von Aufgaben der Sicherheitsbehörden so allgemein gehaltene Formulierungen verwendet, daß die konkreten Grenzen der Behördentätigkeit nicht deutlich werden. Das gilt beispielsweise für Begriffe wie „Bestrebungen, die gegen die freiheitliche demokratische Grundordnung gerichtet sind" oder „Mitwirkung" an der Überprüfung von Personen. Auch der zentrale Begriff des „nachrichtendienstlichen Mittels" müßte näher präzisiert werden, um für den Bürger auch nur in Umrissen kalkulierbar zu sein.

b) Die Entwürfe besagen, daß die für die Aufgabenerfüllung erforderlichen Maßnahmen getroffen werden dürfen. Geregelt werden müßte aber auch, welche Maßnahmen der Datenverarbeitung für welche der sehr unterschiedlichen Aufgaben der Sicherheitsbehörden, insbesondere des Verfassungsschutzes und des Militärischen Abschirmdienstes, eingesetzt werden dürfen.

c) Die Gesetzentwürfe entsprechen in verschiedenen Punkten nicht dem Grundsatz der Verhältnismäßigkeit. So dürfte eine Befugnis zur gegenseitigen Unterrichtung und zur Einrichtung gemeinsamer Dateien nicht undifferenziert, sondern nur unter Berücksichtigung der einzelnen Aufgaben und der Bedeutung der Datenverarbeitung für die Betroffenen erteilt werden. Als unverhältnismäßig betrachte ich z. B. eine Befugnis zur Übermittlung personenbezogener Daten, ohne daß deren Richtigkeit und Aktualität geprüft wurde.

d) Der Grundsatz der Zweckbindung ist nur unzureichend berücksichtigt. Die verschiedenen Aufgaben einer Behörde können nicht einfach zu einem gemeinsamen Zweck zusammengefaßt werden, mit der Folge, daß innerhalb der Behörde der Zweckbindungsgrundsatz keine Rolle mehr spielt. Beispielsweise dienen Daten, die bei der Durchführung von Sicherheitsüberprüfungen mit der Zusage der vertraulichen Behandlung erhoben werden, nicht demselben Zweck wie Daten, die im Rahmen der Beobachtung von verfassungsfeindlichen Bestrebungen anfallen.

e) Sofern Daten aus dem engeren Persönlichkeitsbereich verarbeitet werden sollen, hat der Gesetzgeber die Voraussetzungen, den Zweck und den Umfang zu regeln und auch die Frage zu entscheiden, ob daraus Persönlichkeitsprofile hergestellt werden dürfen.

f) Das Gebot der Trennung von Polizei und Verfassungsschutz betrifft nicht nur den Behördenaufbau, sondern auch die Art und Weise der Zusammenarbeit. Ein Datenaustausch ist danach nicht schlechthin unzulässig, wohl aber eine pauschale Ermächtigung zum Informationsaustausch, die auf die unterschiedlichen Formen der Datengewinnung und die unterschiedlichen Verwendungszusammenhänge keine Rücksicht nimmt.

12.3 Neufassung der Sicherheitsüberprüfungsrichtlinien

Spätestens seit dem Volkszählungsurteil ist es evident, daß für die Durchführung von Sicherheitsüberprüfungen keine ausreichenden Rechtsgrundlagen vorhanden sind. Weder das Beamten- noch das Dienst-, Arbeits- oder Tarifrecht noch § 3 Abs. 2 des Bundesverfassungsschutzgesetzes, der nur die Mitwirkung des BfV anordnet, sind Rechtsgrundlagen, die den heutigen verfassungsrechtlichen Anforderungen entsprechen. Bei Sicherheitsüberprüfungen werden personenbezogene Daten über den zu Überprüfenden systematisch gesammelt, ausgewertet, bewertet und gespeichert. Die Daten werden insofern „zwangsweise" erhoben, als der Betroffene praktisch keine Möglichkeit hat, sich dem zu entziehen, wenn er von seinem Dienstherrn bzw. Arbeitgeber für eine sicherheitsempfindliche Tätigkeit vorgesehen ist. Die im Rahmen einer Sicherheitsüberprüfung erhobenen und ausgewerteten Daten sollen ein Bild von der Zuverlässigkeit des Überprüften vermitteln. Sie entstammen zu einem großen Teil der Privatsphäre des Betroffenen. Durch die Sicherheitsüberprüfung entstehen damit hochsensible Datensammlungen, die ein mehr oder weniger vollständiges bzw. zutreffendes Bild der Persönlichkeit einer Vielzahl von Betroffenen liefern.

Die Erhebung und Verwendung derartiger Daten ist nur zulässig, wenn dies in einer bereichsspezifischen und präzisen Rechtsgrundlage normenklar geregelt ist. Daran fehlt es derzeit. Nach der Rechtsprechung des Bundesverfassungsgerichts zum „Übergangsbonus" (siehe oben 1.3) können für eine angemessene Übergangsfrist noch Sicherheitsüberprüfungen auch ohne eine entsprechende Rechtsgrundlage durchgeführt werden, sofern dies im Einzelfall zur Wahrung der Staatssicherheit unabdingbar ist. In vielen Fällen einer Sicherheitsüberprüfung wird davon auszugehen sein, daß diese Voraussetzungen vorliegen. Allerdings dürfen unter Berufung auf den Übergangsbonus nur solche Eingriffsmaßnahmen vorgenommen werden, die unabdingbar sind und die sich auch in ihrer Ausgestaltung im einzelnen strikt am Erforderlichkeitsprinzip orientieren. Nach meiner Auffassung ist deshalb jedenfalls bis zur Schaffung einer einwandfreien Rechtsgrundlage für Sicherheitsüberprüfungen folgendes zu beachten:

— Die Durchführung einer Sicherheitsüberprüfung muß im Einzelfall erforderlich sein. Die pauschale Einbeziehung ganzer Behörden oder von Beamten bestimmter Laufbahngruppen steht mit diesem Erfordernis regelmäßig nicht im Einklang.

— Die Einbeziehung von Verwandten des Betroffenen in die Überprüfung muß sich auf das unverzichtbare Maß beschränken. Über Verwandte dürfen nicht allein wegen einer durchgeführten Sicherheitsüberprüfung Daten in Dateien gespeichert werden.

— Die im Rahmen der Sicherheitsüberprüfung erhobenen Daten dürfen nur für Zwecke der Sicherheitsüberprüfung verwendet werden. Ausnahmen sind allenfalls für die dem gleichen Zweck dienende Spionageabwehr sowie für mit § 7 Abs. 3 G 10 vergleichbare Fallgruppen möglich.

Der Bundesminister des Innern beabsichtigt, die seit vielen Jahren laufenden Bemühungen um eine Neufassung der Sicherheitsüberprüfungsrichtlinien nunmehr zum Abschluß zu bringen. Er hat mich in einer Reihe von Vorgesprächen an der Erarbeitung dieser Richtlinien beteiligt. Die Sicherheitsüberprüfungsrichtlinien können die fehlenden Rechtsgrundlagen jedoch nicht ersetzen; allerdings wird auch ein normenklares Sicherheitsüberprüfungsgesetz nicht alle Einzelheiten des Verfahrens regeln können. Deshalb werden in jedem Fall noch untergesetzliche Regelungen notwendig sein. Ich habe daher keine grundsätzlichen Bedenken dagegen, daß die Sicherheitsüberprüfungsrichtlinien jetzt neu gefaßt werden, sofern dabei die bindenden Vorgaben des Volkszählungsurteils beachtet werden.

Der mir bekannte Entwurf für die neuen Sicherheitsüberprüfungsrichtlinien enthält eine Reihe datenschutzrechtlicher Fortschritte. Ich unterstütze die Absicht, die Zahl der Sicherheitsüberprüfungen zu reduzieren. Das vom Bundesminister des Innern angestrebte Ziel, Quantität durch Qualität zu ersetzen, deckt sich mit dem datenschutzrechtlichen Anliegen, nur solche Personen einer Sicherheitsüberprüfung und den damit verbundenen Belastungen für das Persönlichkeitsrecht zu unterziehen, bei denen dies wirklich erforderlich ist. Durch die Transparenz des Verfahrens soll vor allem die Rechtsstellung des Betroffenen verbessert werden. Danach scheint es mir für die Zukunft praktisch ausgeschlossen zu sein, daß Sicherheitsüberprüfungen ohne Wissen des Betroffenen eingeleitet werden. Auch das rechtliche Gehör bei etwaigen Sicherheitsbedenken und nach Abschluß des Sicherheitsüberprüfungsverfahrens soll spürbar verbessert werden. Als positiv erachte ich es ferner, daß beim Bundesminister des Innern eine weitere Dienstvorschrift über die Datenverarbeitung im Zusammenhang mit Sicherheitsüberprüfungen erarbeitet werden soll. Von ihr erwarte ich die datenschutzrechtlich gebotene Klärung, unter welchen Voraussetzungen die im Rahmen einer Sicherheitsüberprüfung anfallenden personenbezogenen Daten verwendet werden dürfen.

In einigen Punkten ist der Entwurf allerdings nicht befriedigend. Insbesondere wird der Grundsatz der Zweckbindung der im Rahmen einer Sicherheitsüberprüfung erhobenen Daten zwar ausdrücklich festgeschrieben; zugleich sind aber Ausnahmen in derart weitem Umfang vorgesehen, daß das Prinzip in nicht akzeptabler Weise ausgehöhlt wird. Verbesserungen in diesem Punkt halte ich für vordringlich.

Verbessert werden muß auch die Regelung der Datenübermittlung zwischen den an der Sicherheitsüberprüfung beteiligten Stellen. Daraus muß sich präzise ergeben, welche Informationen die Personalverwaltung an den Geheimschutzbeauftragten übermitteln darf und welche Daten zwischen dem Geheimschutzbeauftragten und dem BfV ausgetauscht werden dürfen.

12.4 Neufassung der Richtlinien für die Sicherheitsüberprüfung von Personal in kerntechnischen Anlagen

Vom Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit werden derzeit neue Richtlinien für die Sicherheitsüberprüfung von Personal in kerntechnischen Anlagen erarbeitet. Hieran habe ich mich in Gesprächen und mit Stellungnahmen beteiligt. Ein Teil meiner Vorstellungen wurde bereits berücksichtigt. Dies gilt insbesondere für die Transparenz des Verfahrens gegenüber dem Betroffenen sowie für die Zweckbindung der im Rahmen solcher Überprüfungen gesammelten Daten. Über andere datenschutzrechliche Anliegen wird weiter beraten:

— In den Richtlinien muß definiert werden, aus welchen Tatsachen ein Sicherheitsrisiko folgt. Nur so ist es möglich zu präzisieren, in welchem Umfang die Sicherheitsbehörden den atomrechtlichen Genehmigungsbehörden personenbezogene Daten übermitteln dürfen.

— Damit hängt auch die Frage zusammen, aus welchen Informationssystemen die Sicherheitsbe-

hörden Daten übermitteln dürfen. Ich habe vorgeschlagen, im Rahmen dieser Überprüfung lediglich die zentralen Aktennachweissysteme abzufragen, nicht aber Spezialdateien wie PIOS- oder SPUDOK-Verfahren.

Der Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit hat zugesagt, dem Datenschutz im Zuge der weiteren Beratungen soweit wie möglich Rechnung zu tragen.

13. Bundeskriminalamt

13.1 Datenschutzrechtliche Kontrolle im Bereich der Bekämpfung der Rauschgiftkriminalität

Im Achten Tätigkeitsbericht (S. 35) habe ich über meine Kontrolle der Datenverarbeitung des Bundeskriminalamts im Bereich der Bekämpfung der Rauschgiftkriminalität und die nicht befriedigende Stellungnahme des Bundesministers des Innern berichtet. Inzwischen hat dieser ergänzend Stellung genommen und in einigen Punkten datenschutzrechtliche Verbesserungen zugesagt:

— Die Datensätze von Personen, die im Rahmen einer Telefonüberwachungsmaßnahme bekanntgeworden sind, werden besonders gekennzeichnet. Dadurch können künftig nach Abschluß der Abhörmaßnahme die Daten Unbeteiligter gelöscht werden, wie es von den §§ 100a und 100b StPO gefordert wird, aber bisher nicht gewährleistet war.

— Durch spezielle Unterweisungen und organisatorische Maßnahmen soll sichergestellt werden, daß in Zukunft justizielle Entscheidungen nicht als Anlaß für eine Verlängerung der Speicherfrist genommen werden. Ich hatte festgestellt, daß in Einzelfällen sogar die Mitteilung eines Freispruches zu einer Fristverlängerung von zehn Jahren geführt hatte.

— In einigen konkret von mir beanstandeten Fällen hat das Bundeskriminalamt die Speicherfrist erheblich verkürzt.

Zum überwiegenden Teil bleibt die Stellungnahme des Bundesministers des Innern jedoch weiterhin unbefriedigend. Die meisten meiner Vorschläge wurden abgelehnt. Für die Zukunft muß befürchtet werden, daß in den folgenden Bereichen Datenschutzbestimmungen nach wie vor verletzt werden:

— Nach Ziffer 8.1 der Dateienrichtlinien sind zu löschende Daten auf dem jeweiligen Datenträger unkenntlich zu machen. Außerdem sind die zu den gelöschten Daten geführten Unterlagen des Bundeskriminalamts zu vernichten. Um dem Amt in der praktischen Arbeit entgegenzukommen, habe ich vorgeschlagen, daß Unterlagen, die sowohl zu löschende als auch weiterhin zu speichernde Daten (anderer Personen) enthalten, weiter aufbewahrt werden dürfen, wenn durch einen Vermerk sichergestellt wird, daß Angaben, die in der Datei gelöscht sind, nicht mehr verwertet werden.

  Obwohl die oben zitierte Vorschrift der Dateienrichtlinien die Vernichtung derartiger Unterlagen verlangt, hat das Bundeskriminalamt meinen Kompromißvorschlag abgelehnt. Es will lediglich seine Mitarbeiter im dienstkundlichen Unterricht darauf hinweisen, daß gelöschte Daten nicht mehr verwertet werden dürfen. Dies reicht aus meiner Sicht nicht aus. Wenn in einer Akte noch dateimäßig gespeicherte Daten neben solchen, die in der Datei bereits gelöscht sind, ohne nähere Kennzeichnung nebeneinander stehen, kann nicht ausgeschlossen werden, daß auch die Daten derjenigen Personen weiter verwertet und übermittelt werden, deren Unterlagen nach den Dateienrichtlinien auszusondern wären, weil die entsprechenden Daten in den Dateien bereits gelöscht sind.

— Im Rahmen der Bekämpfung der Rauschgiftkriminalität werden — abweichend vom KAN-Konzept — alle Straftaten zentral gespeichert, auch wenn es sich nur um Kleinkriminalität im Zusammenhang mit Rauschgift handelt. Aus meiner Sicht ist dagegen nichts einzuwenden, solange der Zugriff auf diese Daten nur den Dienststellen offensteht, die für die Bekämpfung der Rauschgiftkriminalität zuständig sind. Dies ist durch die derzeitige Datenverarbeitungsstruktur nicht gewährleistet. Der Bundesminister des Innern hat entsprechende Änderungen abgelehnt.

— Im vergangenen Jahr habe ich über die Problematik der personengebundenen Hinweise berichtet (8. T B S. 44f.). Dabei habe ich u. a. ausgeführt, daß nach meiner Auffassung personengebundene Hinweise wegen ihrer stigmatisierenden Wirkung („bewaffnet", „gewalttätig", „Ausbrecher", „geisteskrank", „Prostituierte", usw.) nur in den Fahndungsdateien verwendet werden dürfen. Für die Speicherung derartiger Daten in einem Aktennachweissystem fehlt es meines Erachtens an der Erforderlichkeit. Häufig konnte auch nicht belegt werden, aufgrund welcher Tatsachen dem Betroffenen eine bestimmte Eigenschaft zugeschrieben wurde.

  Ich habe vorgeschlagen, soweit die weitere Speicherung von personengebundenen Hinweisen überhaupt für notwendig gehalten wird, kurze Überprüfungsfristen speziell für diese Daten einzuführen. Dies hat der Bundesminister des Innern abgelehnt. Er hat statt dessen erklärt, daß es sich bei den personengebundenen Hinweisen regelmäßig um Merkmale handele, die einer Person für einen längeren Zeitraum, auf jeden Fall für viele Jahre, zugeordnet werden könnten. Im Ergebnis bedeutet dies, daß Hinweise so lange gespeichert werden, wie eine Akte über die betreffende Personen existiert. Dies ist nach meiner Auffassung nicht vertretbar, weil damit die Speicherung auch unrichtiger Daten in Kauf genommen wird. Eine Person, die einmal bewaffnet war, bleibt dies nicht notwendig solange, wie eine Kriminalakte existiert. Ich halte deshalb daran fest, daß die Richtigkeit von personengebundenen Hinweisen in angemessenen Abständen überprüft werden muß.

— Bei der Kontrolle der Arbeitsdatei PIOS-Rauschgift (APR) habe ich festgestellt, daß dort Daten von insgesamt ca. 67 000 Personen gespeichert waren, davon aber nur ca. 500 „andere Personen", die überwiegende Zahl aber als „Verdächtige". Ich habe Zweifel geäußert, ob diese Relation zutreffend ist, und vermute, daß — unter Umgehung der strengeren Datenschutzvorschriften für „andere Personen" — möglichst viele Personen als Verdächtige eingestuft werden. Da es sich hier aber häufig um Abgrenzungsfragen handelt, für die sich nur schwer exakte Regeln aufstellen lassen, habe ich vorgeschlagen, für die Verdächtigen eine kürzere Speicherfrist als für die Beschuldigten einzuführen. Dies hat der Bundesminister des Innern abgelehnt; bei der Einstufung von Personen als „andere Personen" oder Verdächtige werde nicht schematisch, sondern inhaltlich und bezogen auf den einzelnen Fall entschieden.

— Kritik habe ich auch an der Art und Weise geübt, wie beim Bundeskriminalamt Kriminalakten angelegt und dazugehörige Personendatensätze gespeichert werden. Dies geschieht durch eine zentrale Serviceeinheit, die weitgehend formalistisch vorgeht. Als Ausgangspunkt für den Lauf der Wiedervorlagefrist wird in aller Regel das Datum der Anlegung des Datensatzes gewählt.

Ich stehe demgegenüber auf dem Standpunkt, daß die Entscheidung über die Anlegung oder Nichtanlegung einer Kriminalakte in den einzelnen Fachbereichen selbst getroffen werden muß und daß, orientiert am Sachverhalt, dort auch das Aussonderungsprüfdatum festgesetz werden muß. Um jedoch den organisatorischen Gegebenheiten beim Bundeskriminalamt entgegenzukommen, habe ich vorgeschlagen, daß zwar die Anlage von Kriminalakten und die Speicherung von Personendatensätzen auch weiterhin zentral erfolgt. Die Datensätze sollen aber nur mit einer kurzen Frist versehen werden, innerhalb der eine Bestätigung der Speicherung durch die Fachbereiche notwendig ist.

Der Bundesminister des Innern hat dies abgelehnt. Er vertritt statt dessen die Auffassung, daß sich das Aussonderungsprüfdatum in der überwiegenden Zahl der Fälle an dem Tag der Bearbeitung zu orientieren habe und dies sachgerecht sei. Durch verstärkten dienstkundlichen Unterricht soll darauf hingewirkt werden, daß in den Fachbereichen das Aussonderungsprüfdatum nachträglich noch überprüft und gegebenenfalls korrigiert wird.

Ich halte dies nicht für ausreichend. Nach Angaben des Bundeskriminalamtes werden von der zentralen Einheit täglich durchschnittlich 750 Kriminalakten angelegt und entsprechende Datensätze gespeichert. Bei einer derartigen Informationsmenge kann es nicht ausbleiben, daß schematisch vorgegangen wird. Stichproben belegen, daß dabei tatsächlich Fehler unterlaufen. Das Aussonderungsprüfdatum wird als Funktion des Tagesdatums automatisch festgesetzt. Die Orientierung nach dem Datum des Ereignisses erfordert dagegen eine besondere manuelle Eingabe.

Die festgestellten Mängel sind auch darauf zurückzuführen, daß die vorläufige Errichtungsanordnung zum Bundeskriminalamt-Aktennachweis (BKA-AN) in dieser Hinsicht zu vage ist und kaum konkrete Anhaltspunkte dafür gibt, wann eine Kriminalakte anzulegen ist. Ich habe dies und weitere datenschutzrechtliche Mängel der Errichtungsanordnung im Oktober 1985 gegenüber dem Bundesminister des Innern geltend gemacht. Eine Antwort steht immer noch aus. Wegen des außerordentlichen Volumens der täglichen Dateneingabe erscheint es mir dringlich, eine einwandfreie und präzise formulierte Erfassungsrichtlinie zu erlassen.

13.2 Weitere Zunahme der SPUDOK-Anwendungen

In den vergangenen Jahren habe ich über den weiteren Ausbau der automatisierten Datenverarbeitung beim Bundeskriminalamt und ihre Auswirkungen auf die polizeiliche Arbeit berichtet (vgl. 7. TB S. 67 ff., 8. TB S. 41 f. und S. 45 f.). Ich habe dabei insbesondere dargelegt, wie der zunehmende Einsatz von PIOS- und SPUDOK-Verfahren dazu führt, daß beim Bundeskriminalamt neben Beschuldigten und Verdächtigen immer stärker auch „andere Personen", d. h. solche Personen erfaßt werden, denen keine strafbaren Handlungen vorzuwerfen sind. Diese Tendenz hält unvermindert an. Das Bundeskriminalamt hält auch an seiner Praxis fest, in neuen Errichtungsanordnungen für SPUDOK-Dateien vorzusehen, daß eine Unterrichtung dieser „anderen Personen" pauschal unterbleibt, zumeist mit der formelhaften Begründung, daß es sich um ein laufendes Ermittlungsverfahren handele und die Ermittlungen durch die Unterrichtung gefährdet würden. Die Erfassung „anderer Personen" nimmt also weiter zu, während die besonderen Schutzvorkehrungen, die für diese Personengruppe gelten, kontinuierlich vernachlässigt werden.

Im vergangenen Jahr sind mir fünfzehn Errichtungsanordungen für neue SPUDOK-Dateien zugegangen. Einige wurden inzwischen wieder gelöscht. Nachdem ich das Bundeskriminalamt in den vergangenen Jahren mehrfach mahnen mußte, seiner Meldepflicht nach § 19 Abs. 4 Bundesdatenschutzgesetz nachzukommen, habe ich in diesem Jahr in zwei Fällen wegen versäumter Meldung eine Beanstandung ausgesprochen.

Neue SPUDOK-Dateien einzurichten und zu betreiben ist für das Bundeskriminalamt inzwischen zur Routine geworden. SPUDOK-Dateien werden nicht mehr nur zum Zweck der Aufklärung umfangreicher Straftaten errichtet, wofür sie ursprünglich entwickelt wurden, sondern zunehmend auch zur Bewältigung polizeilicher „Großlagen", zur Gefahrenabwehr oder auch zur Fahndung nach ausgebrochenen Straftätern. Die Entscheidung über die Errichtung einer SPUDOK-Datei scheint mitunter so kurzfristig zu fallen, daß für eine sorgfältige Errich-

tungsanordnung keine Zeit bleibt. Zunehmend erhalte ich vorgefertigte Texte, in die jeweils nur das Aktenzeichen und eventuell einige wenige Besonderheiten des einzelnen SPUDOK-Verfahrens eingetragen wurden.

Bei einigen Errichtungsanordnungen fällt es schwer, ihnen einen vernünftigen Sinn zu entnehmen. So soll z. B. mit Hilfe der SPUDOK-Datei „FREDI 86" nach einem ausgebrochenen Häftling gefahndet werden. Unter Ziffer 4.2 der Errichtungsanordnung ist geregelt, unter welchen Voraussetzungen verdächtige Personen in diese Datei aufgenommen werden dürfen. Der entsprechende Text lautet: Erfaßt werden dürfen „verdächtige(n) Personen, die nicht Beschuldigte sind, bei denen aber Anhaltspunkte dafür vorliegen, daß sie Täter oder Teilnehmer einer Straftat ... sind oder bei denen zu vermuten ist, daß sie Mitglieder oder Unterstützer einer Gruppe ... sind." Danach könnten die Daten beliebig vieler Bürger gespeichert werden, sofern sie irgendwann einmal irgendeine Straftat begangen haben oder Mitglieder oder Unterstützer irgendeiner Gruppe sind. Ich nehme nicht an, daß das Bundeskriminalamt dies beabsichtigt, kann aber auch nicht nachvollziehen, wie eine Anordnung dieses Inhalts erlassen werden kann, ohne bei den vorgesetzten Instanzen Reaktionen hervorzurufen. Es handelt sich im übrigen nicht um einen Einzelfall.

Bei mehreren Errichtungsanordnungen neueren Datums ist zu bemängeln, daß die „verdächtigen Personen" in einer Weise umfassend definiert werden, daß kaum noch feststellbar ist, was diesen Personenkreis von den „anderen Personen" unterscheiden soll.

Beispielsweise ist in der Errichtungsanordnung für die Datei „BILLET" vorgesehen, daß als „verdächtige Personen" auch solche zu bezeichnen und damit zu speichern sind, „bei denen zu vermuten ist, daß sie Mitglied oder Unterstützer einer Gruppe im Zusammenhang mit dem unter Nummer 2.1 genannten Ermittlungsverfahren sind". Es bleibt offen, was eine „Gruppe im Zusammenhang" mit einem Ermittlungsverfahren im Einzelfall sein soll. Bei der erwähnten Datei „BILLET" hatte das Bundeskriminalamt zunächst gemeldet, daß unter dieser Bezeichnung eine SPUDOK-Datei zur Aufklärung von Einbruchsdiebstählen in Postämtern im gesamten Bundesgebiet betrieben werden soll. Etwa zwei Monate später wurde dann gebeten, die beiden ersten Blätter der Errichtungsanordnung auszutauschen; die Datei werde nunmehr zur Bearbeitung eines Ermittlungsverfahrens gegen eine deutsche Tätergruppierung wegen Verdachts des Verstoßes gegen das Betäubungsmittelgesetz betrieben. Das Austauschen zweier Blätter genügt also für den Wechsel zum Betrieb einer völlig anderen Datei. Was mit den bis dahin gespeicherten Personendaten geschehen ist oder geschehen soll, wurde nicht mitgeteilt. Der Vorgang zeigt recht anschaulich, wie sehr die praktischen Vorteile der Datenverarbeitung im Vordergrund stehen und wie leicht dabei die datenschutzrechtlichen Ziele, wie z. B. das Erfordernis aussagefähiger Errichtungsanordnungen, vernachlässigt werden.

Der zunehmende Einsatz von SPUDOK-Dateien ist auch unter dem Blickwinkel zu betrachten, daß nach Ziffer 4.2.10 der für das Bundeskriminalamt gültigen Dateienrichtlinien Daten über Anzeigeerstatter, Hinweisgeber und Zeugen nur in SPUDOK-Dateien gespeichert werden dürfen. Die Wahl des SPUDOK-Verfahrens eröffnet dem Anwender die Möglichkeit, einen erweiterten Personenkreis zu erfassen. Was in den Dateienrichtlinien als Restriktion gemeint war, wirkt sich heute umgekehrt aus. Das Ergebnis ist die immer weiter ausgreifende Erfassung von Anzeigeerstattern, Hinweisgebern und Zeugen, d. h. von Personen, gegen die kein strafrechtlicher Verdacht besteht.

Die Rechtsordnung hat mit den technischen Veränderungen nicht Schritt gehalten. Während die automatisierte Datenverarbeitung vor allem im Bereich der PIOS- und SPUDOK-Anwendungen ständig ausgeweitet wird, lassen präzise gesetzliche Grundlagen, die auch die notwendigen datenschutzrechtlichen Schutzvorschriften enthalten, weiter auf sich warten. Die Datenverarbeitung schafft immer mehr Fakten, deren spätere Korrektur durch den Gesetzgeber immer schwieriger sein wird.

Mit meiner Personalausstattung bin ich nicht in der Lage, jede mir übersandten Errichtungsanordnung zu prüfen. Eine praktische Kontrolle der jeweiligen Datenverarbeitung ist mir angesichts der wachsenden Zahl von neuen Anwendungen allenfalls noch punktuell möglich.

13.3 Inbetriebnahme der Datei APIS

Am 2. Januar 1986 wurde der Betrieb der „Arbeitsdatei PIOS-Innere Sicherheit" (APIS) beim Bundeskriminalamt aufgenommen. Es handelt sich um eine Verbunddatei, an der die Landeskriminalämter über Direktverbindungen teilnehmen. Sie wirft verschiedene gravierende datenschutzrechtliche Probleme auf (vgl. 5 TB S. 85 f., 6. TB S. 46 f., 7. TB S. 68), die bis zur Aufnahme des Betriebs von APIS nicht gelöst wurden.

— In der Errichtungsanordnung für APIS ist vorgesehen, daß sowohl Staatsschutzdelikte im engeren Sinne dort erfaßt werden, als auch jede andere Straftat, sofern wegen der Angriffsrichtung, dem Motiv des Täters oder dessen Verbindung zu einer Organisation der Verdacht besteht, daß mit der Tat ein gegen die freiheitliche demokratische Grundordnung gerichtetes Ziel verfolgt wird. Nach meiner Auffassung müßte ausgeschlossen werden, daß auch Kleinkriminalität (z. B. Sachbeschädigung durch „wildes Plakatieren") in APIS erfaßt wird.

— Sehr problematisch erscheint auch, daß in APIS die Datei PIOS-Terrorismus mit den Datensammlungen des polizeilichen Staatsschutzes zusammengeführt wird. Damit werden schwere terroristische Straftaten und allgemeine Kriminalität bis hin zur Kleinkriminalität in einen Topf geworfen; Formen der Datenverarbeitung, die speziell für die Bekämpfung des Terrorismus

entwickelt worden sind, werden auf die gesamte Staatsschutzkriminalität ausgeweitet.

— Ein typisches Beispiel für die dadurch bedingte Verwischung von Datenverarbeitungsmaßstäben sind die Daten der sog. „L-Gruppe". Dies sind personenbeschreibende Merkmale; sie können mehrere hundert Einzelinformationen umfassen. Der Sache nach handelt es sich dabei um erkennungsdienstliche Daten. Eine genaue Körper- und Verhaltensbeschreibung hat im Bereich der Terrorismusbekämpfung sicher ihren guten Sinn. Im Bereich der vorher erwähnten einfachen Staatsschutzkriminalität sind derartige Daten aber regelmäßig weder erforderlich noch verhältnismäßig. Die Errichtungsanordnung für APIS aber sieht die Speicherung von Daten der L-Gruppe unterschiedslos für alle Personen vor. Selbst über „andere Personen", d. h. Kontakt- und Randpersonen, können danach Persönlichkeitsprofile gespeichert werden.

— Daten solcher „anderen Personen" wurden bisher im Bereich des polizeilichen Staatsschutzes überhaupt nicht gespeichert. Die Einführung von APIS, d. h. die Entscheidung für ein neues DV-Verfahren, führt somit im Staatsschutzbereich zur Erfassung neuer Personenkreise.

— Als Verbunddatei erlaubt APIS den angeschlossenen Kriminalämtern, Daten einzuspeichern und abzurufen. Allerdings werden die unterschiedlichen Teilmengen nicht nur additiv zusammengestellt. APIS geht vielmehr von der Konzeption der redundanzfreien Informationserfasssung aus. Dies bedeutet, daß alle bei den verschiedenen Teilnehmern zu einer Person vorhandenen Informationen miteinander „verschmolzen" werden. Keine Angabe wird mehrfach gespeichert. Dies setzt zwingend voraus, daß jeder Teilnehmer befugt (und verpflichtet) ist, an von anderen Teilnehmern eingestellten Datensätzen unmittelbar Veränderungen oder Ergänzungen vorzunehmen. Damit ist das föderative Prinzip berührt. Ich halte es für bedenklich, daß damit auch nach dem Erlaß des Volkszählungsurteils ein System in Betrieb genommen wurde, das die strukturellen Grundlagen der Datenverarbeitung im Verhältnis von Bund und Ländern nachhaltig verändert, ohne daß der Gesetzgeber tätig geworden ist.

Die Einführung neuer DV-Systeme darf nicht allein der schnelleren und umfassenderen Information der Behörden dienen, sondern muß auch Anlaß sein, durch die neue Technik mögliche datenschutzrechtliche Verbesserung auszuschöpfen. Dieser Grundsatz wurde bei der Einführung von APIS in zwei wesentlichen Punkten nicht beachtet.

a) Das Bundeskriminalamt hat die datenschutzrechtlichen Mängel, die bei seiner auf papiergebundenen Meldungen beruhenden Informationsverarbeitung bestanden, nicht beseitigt. Die papiergestützte Verarbeitung geht unverändert weiter. So sollen die Landeskriminalämter auch in Zukunft verpflichtet bleiben, ihre Informationen neben der Einspeicherung in APIS weiterhin in Schriftform an das Bundeskriminalamt zu übermitteln. Dies bedeutet, daß das Bundeskriminalamt auch in Zukunft mit Hilfe derartiger Zweitschriften, Einzelmeldungen und sonstiger Informationsfragmente Kriminalakten anlegen und auf dieser Basis zusätzlich eigene Aktenfundstellen in APIS speichern wird. Wie bereits mehrfach dargelegt (vgl. 8. TB S. 46 f.), wird das Bundeskriminalamt oft lediglich über die Einleitung eines Ermittlungsverfahrens bzw. über die Entstehung eines Verdachts unterrichtet, nicht aber über den weiteren Fortgang. Dadurch sind beim BKA häufig nur bruchstückhafte Informationen vorhanden. Meine Vorschläge, durch geeignete Verfahrensvorschriften wenigstens sicherzustellen, daß derartige unvollständige Informationen nicht auch noch weiterübermittelt werden, hat der Bundesminister des Innern bislang abgelehnt. Mein letztes diesbezügliches Schreiben vom November 1985 blieb bis jetzt unbeantwortet.

Wenn die Polizei sich mit APIS modernster Datenverarbeitungstechnik bedient, muß sie zugleich auch bereit sein, die mit den bisherigen Formen der Datenverarbeitung verbundenen Risiken abzubauen. Dies geschieht jedoch nicht. Dadurch tritt eine weitere Steigerung der datenschutzrechtlichen Gefahren ein.

b) Das Bundeskriminalamt hat die Nutzung des nachrichtendienstlichen Informationssystems NADIS als Aktennachweis für seine Abteilung Staatsschutz nicht eingestellt. Bereits im Sechsten Tätigkeitsbericht (S. 46 f.) habe ich dargelegt, daß die (schon damals geplante) Einführung von APIS immerhin den Vorteil bietet, diese bereichsüberschreitende technische Hilfe einzustellen. Die Benutzung von NADIS durch das BKA hat den datenschutzrechtlich bedenklichen Effekt, daß die anderen Teilnehmer an NADIS (Bundesamt für Verfassungsschutz, Landesämter für Verfassungsschutz; MAD und BND im Wege des Bandabgleichs) direkten Zugriff auf die Fundstellen des Bundeskriminalamtes haben. Ursprünglich war auch geplant, mit der Einführung von APIS die Speicherung von BKA-Fundstellen in NADIS entfallen zu lassen, weil sie dann nicht mehr erforderlich ist. Der Bundesminister des Innern hat mir nun aber mitgeteilt, daß trotz der Speicherung in APIS weiterhin auch Speicherungen in NADIS erfolgen. Zur Begründung hat er angeführt.

— Es sei davon auszugehen, daß die Erkenntnisse des Bundeskriminalamtes über Beschuldigte oder Verdächtige im Staatsschutzbereich regelmäßig auch verfassungsschutzrelevant seien.

— Das Bundesamt für Verfassungsschutz sei darauf angewiesen, Informationen über diesen Personenkreis möglichst schnell zu erfahren.

— Als Alternative bleibe lediglich der Anschluß des Bundesamtes für Verfassungsschutz an APIS oder eine „umfassende Datenanlieferung in anderer geeigneter Form".

— Zu einer Trennung zwischen der Abteilung Staatsschutz des BKA und dem Bundesamt für Verfassungsschutz bestehe auch aus rechtlichen Gründen keine Veranlassung. § 10 Abs. 1 Satz 1 BDSG könne so verstanden werden, daß die Übermittlung personenbezogener Daten auch zur rechtmäßigen Erfüllung der in der Zuständigkeit des Empfängers liegenden Aufgaben zulässig sei. Das Trennungsgebot sei durch den Zugriff des Bundesamtes für Verfassungsschutz auf die Daten des Bundeskriminalamtes nicht verletzt, da es nur organisatorischer Natur sei.

Ich habe daraufhin die weitere Einspeicherung von personenbezogenen Daten durch das Bundeskriminalamt in die NADIS-PZD beanstandet. Hierbei habe ich mich von folgenden Überlegungen leiten lassen:

— Zur Erfüllung der Aufgaben des Bundeskriminalamtes ist die Speicherung personenbezogener Daten in der NADIS-PZD nicht mehr erforderlich. Mit der Einführung von APIS besitzt das Bundeskriminalamt ein eigenes Aktennachweissystem, so daß es auf NADIS nicht mehr angewiesen ist. Damit ist die Begründung für die bisherige Praxis entfallen. Eine Fortsetzung der schon bisher rechtswidrigen Praxis (vgl. 6. TB S. 47) ist nicht länger hinnehmbar.

— Eine Übermittlung der Daten aller Beschuldigten und Verdächtigen, die bei der Abteilung Staatsschutz des Bundeskriminalamtes bekannt werden, an das Bundesamt für Verfassungsschutz ist unzulässig. Meine bisherigen Kontrollen haben viele Fälle ergeben, in denen zur Staatsschutzkriminalität auch Straftaten gezählt wurden, die Bagatellen darstellen oder bei denen nicht zu vermuten war, daß sie Teil einer Bestrebung gegen die verfassungsmäßige Ordnung waren.

— In jedem Falle hat das Bundesamt für Verfassungsschutz, wenn ihm Daten übermittelt werden, anhand seiner eigenen Verkartungspläne zu prüfen, ob und mit welchen Fristen Daten in NADIS-PZD zu speichern sind. Diese Entscheidung kann das Bundeskriminalamt nicht für das Bundesamt für Verfassungsschutz treffen. Es ist dafür nicht zuständig. Ihm fehlen auch die Kriterien, die hierbei zu berücksichtigen sind; selbst wenn das Bundeskriminalamt — was gegenwärtig nicht der Fall ist — die Verkartungspläne des Bundesamtes für Verfassungschutz zugrunde legen würde, könnte es bei der Entscheidung über die Speicherung und bei der Festlegung von Aussonderungsfristen nicht etwaige schon vorhandene Daten berücksichtigen.

— Mit der Speicherung von Informationen aus dem polizeilichen Staatsschutzbereich in NADIS-PZD ist auch die ständige Weiterübermittlung dieser Daten an den Militärischen Abschirmdienst und an den Bundesnachrichtendienst verbunden. Beide haben in Form des regelmäßigen Bandabgleichs Zugriff auf die in NADIS-PZD gespeicherten Daten.

— Wie bereits dargelegt, verfügt das Bundeskriminalamt im Staatsschutzbereich sehr häufig nur über unvollständige Informationen, hat aber bislang meine Vorschläge abgelehnt, mit denen sichergestellt werden könnte, daß es regelmäßig über den weiteren Fortgang von Verfahren unterrichtet wird. Dadurch besteht die Gefahr, daß in NADIS-PZD in großem Umfang Personendaten gespeichert werden, bei denen der zugrundeliegende Sachverhalt beim Bundeskriminalamt nicht vollständig bekannt ist.

14. Bundesamt für Verfassungsschutz (BfV)

Der Neunte Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz enthält keine Ausführungen über das Bundesamt für Verfassungsschutz. Dies ist ein Abgehen von der bisherigen Praxis, das ich um so mehr bedauere, als es zu besonderen Vorzügen unseres Datenschutzsystems zählt, daß es alle datenverarbeitenden Stellen einbezieht und datenschutzfreie Zone strikt vermeidet. Wenn ich mich in diesem Jahr gleichwohl dazu entschlossen habe, das Bundesamt für Verfassungsschutz aus diesem Bericht auszuklammern, dann nicht etwa deshalb, weil es über diesen Bereich nichts Berichtenswertes gibt, sondern weil ich nach reiflicher Prüfung zu dem Ergebnis gelangt bin, daß ich aus Gründen der Geheimhaltung keine andere Möglichkeit habe.

Wie schon in früheren Jahren habe ich bei der Vorbereitung des Jahresberichts einigen Sicherheitsbehörden Abzüge aus meinem Entwurf vorab mit der Bitte zugeleitet, mich gegebenenfalls darauf hinzuweisen, falls gegen eine Veröffentlichung bestimmter Sachverhalte Geheimhaltungsbedenken gesehen werden. Soweit ein Geheimhaltungsbedürfnis bestand, konnte ich dem bisher durch begrenzte Textänderungen Rechnung tragen. Der Konflikt zwischen meiner Pflicht zur öffentlichen Berichterstattung und der im öffentlichen Interesse gebotenen Geheimhaltung konnte dadurch konstruktiv gelöst werden. Dieses Verfahren hat es mir in den vergangen Jahren ermöglicht, einen informativen Bericht auch über die sicherheitsempfindlichen Bereiche vorzulegen.

In diesem Jahr ist dies nicht gelungen. Die vom Bundesminister des Innern und vom Bundesamt für Verfassungsschutz gegen die von mir beabsichtigten Ausführungen erhobenen Geheimhaltungsbedenken waren so umfangreich, daß bei ihrer Berücksichtigung für den Leser keine brauchbare Information mehr vermittelt worden wäre. Mich haben diese Einwände nicht von der Geheimhaltungsbedürftigkeit überzeugt, zumal mehrere Passagen meines Entwurfs als geheimhaltungsbedürftig bezeichnet wurden, obwohl sich Aussagen gleichen Inhalts in Veröffentlichungen — auch von Angehörigen des Verfassungsschutzes — finden.

Nach dem Bundesdatenschutzgesetz sind alle Behörden und sonstigen Stellen verpflichtet, den Bundesbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen (§ 19 Abs. 3). Zu diesen Aufgaben gehört der jährliche Tätigkeitsbericht (§ 19 Abs. 2). Dieser öffentliche Bericht ist, da dem Bundesbeauftragten keine Anordnungsbefugnisse übertragen sind, die entscheidende Grundlage seiner Wirksamkeit. Wenn jetzt Geheimhaltungsbedenken in einem Umfang erhoben werden, daß ganze Teile meines Berichts unterbleiben müssen, so besteht die Gefahr, daß die Datenschutzkontrolle in diesem Bericht nicht mehr die vom Gesetz vorgesehene Effektivität erreicht.

Bei der gegebenen Sachlage habe ich mich entschlossen, meinen Bericht über das Bundesamt für Verfassungsschutz als Verschlußsache einzustufen und ihn dem Innenausschuß des Deutschen Bundestages zuzuleiten. Ich würde es begrüßen, wenn die bewährte Praxis eines vollständigen und offenen Tätigkeitsberichts aufrechterhalten bzw. wieder hergestellt werden könnte.

15. Bundesnachrichtendienst (BND)

Im Frühjahr hat ein weiterer Kontrollbesuch beim Bundesnachrichtendienst stattgefunden. Auf verschiedenen, hier nicht näher zu beschreibenden Gebieten wurde die Frage erörtert, in welchem Umfang, mit welchen Daten und für welche Dauer Personen in der Datenverarbeitung des Dienstes erfaßt werden dürfen. Während abstrakt Einvernehmen darüber besteht, daß die Datenverarbeitung sich um so mehr zurückhalten muß, je weiter eine Person vom Zentrum der Aufgaben des Bundesnachrichtendienstes entfernt ist, treten bei der praktischen Anwendung dieses Grundsatzes auf verschiedene Fallgruppen Schwierigkeiten auf. In einigen Punkten wurden schonendere Verfahrensweisen gefunden, denen ich zustimmen konnte; in anderen scheint eine Annäherung der Standpunkte möglich. Der Bundesnachrichtendienst hat nunmehr — entsprechend meiner Anregung (vgl. 8. TB S. 37) — den Entwurf einer Dienstvorschrift erstellt, durch die der von der Datenverarbeitung betroffene Personenkreis umschrieben und eingegrenzt werden soll; die Beratung des Entwurfs ist vorgesehen. Ich hoffe, daß damit ein Beitrag mit großer Breitenwirkung geleistet werden kann.

Die Aufstellung präziser Abgrenzungskriterien für die datenmäßige Erfassung von Personen ist bei einem Nachrichtendienst allerdings besonders schwierig. Nicht alle Details der Datenverarbeitung lassen sich durch Dienstvorschriften steuern. Um so wichtiger ist es, die Praxis aus Datenschutzsicht fortlaufend zu kontrollieren.

Um im Einzelfall beurteilen zu könne, ob die Speicherung — teils sehr privater — personenbezogener Daten erforderlich und angemessen ist, bedarf es der Kenntnis der Akten oder sonstigen Vorgänge, die der Datenspeicherung zugrundeliegen. Deshalb gewährt mir das Bundesdatenschutzgesetz entsprechende Auskunfts- und Einsichtsrechte, die gegenüber allen Stellen des Bundes und in bezug auf alle relevanten Unterlagen gelten. Gleichwohl sind in diesem Punkt bei meinem Kontrollbesuch Schwierigkeiten aufgetreten. Nachdem die Frage meiner Informationsbefugnisse im Innenausschuß des Deutschen Bundestages aus anderem Anlaß zu meiner Zufriedenheit geklärt worden ist (vgl. oben 17.1) hat der Staatssekretär beim Bundeskanzleramt mitgeteilt, daß er den BND angewiesen habe, mir die Einsichtnahme in Sicherheitsakten in einem Umfang zu ermöglichen, wie ich dies verlangt hatte. Nunmehr besteht die Möglichkeit, die Kontrolle fortzusetzen und die Beratung in den noch offenen Fragen wieder aufzunehmen.

16. Bundesgrenzschutz

16.1 Grenzaktennachweis (GAN)

Im Berichtsjahr wurde die Errichtungsanordnung für den GAN des Bundesgrenzschutzes in Kraft gesetzt. Meine datenschutzrechtlichen Bedenken blieben weitgehend unberücksichtigt:

— Amtshilfsersuchen der Nachrichtendienste werden als ausreichende Grundlage für die Anlegung von Grenzakten und zur Speicherung im Grenzaktennachweis angesehen.

— Zwar sind nicht die sonst üblichen personengebundene Hinweise (vgl. 8. TB S. 44 f.) vorgesehen, dafür aber Hinweise neuer Art:
  — Urkundenfälscher (UFAE),
  — Schleuser (SCHL),
  — Ausweismißbraucher (AUWI),
  — Benutzer grüne Grenze (GRUN),
  — Arbeitnehmerüberlasser (ARBU).

  Die allgemeinen, gegen die Verwendung personenbezogener Hinweise bestehenden Bedenken, nämlich daß durch die notwendige Verkürzung häufig Fehler unterlaufen, bestehen auch hier.

— Neben den Grenzschutzämtern haben auch die Grenzschutzstellen Zugriff auf den GAN. Hierdurch kann es im Einzelfall bei der Grenzkontrolle zu Entscheidungen kommen, die allein auf abgerufene Daten aus dem GAN gestützt werden, obwohl diese dafür nicht geeignet sind.

— Die zunächst ausdrücklich vorgesehene Relevanzprüfung vor der Übermittlung von Daten und die Pflicht zum Nachbericht sind entfallen. Dem Sachbearbeiter ist also nicht mehr vorgeschrieben, vor der Übermittlung von Daten gesondert zu prüfen, ob diese richtig und vollständig sind; es besteht auch keine besondere Verpflichtung mehr, nach erfolgter Übermittlung später bekannt werdende wesentliche Änderungen nachzuberichten.

Diese datenschutzrechtlichen Mängel wurden in der endgültigen Fassung der Errichtungsanord-

nung für den GAN nicht behoben. Dies wenigstens hätte erwartet werden könne, nachdem der Gesetzgeber noch keine bereichsspezifischen Vorschriften für die Datenverarbeitung beim BGS geschaffen hat.

16.2 Restriktive Datenschutzpraxis beim Grenzschutzkommando Nord

Im Juli 1986 demonstrierten jugendliche Mitglieder des Deutschen Alpenvereins auf dem Gebiet der DDR gegen die Nutzung der Atomkraft in Ost und West. Der BGS stellte die Namen der Teilnehmer fest und fertigte Fotos. Anschließend wurde dem Deutschen Alpenverein, Sektion Hannover, eine Teilnehmerliste übermittelt. Dies geschah nach Auskunft des BGS, damit der Alpenverein auf die Gefahren derartiger Demonstrationen hinweisen könne. Teilnehmer der Demonstration haben in einer Eingabe geltend gemacht, sie seien bereits während der Aktion von den BGS-Beamten ausgiebig belehrt worden. Sie haben darauf hingewiesen, daß eine Warnung des Deutschen Alpenvereins keine Übermittlung von Namen durch den BGS voraussetze, was auch meine Auffassung ist. Ich habe das Grenzschutzkommando Nord ersucht, die Liste mit den Demonstranten aus dem bei dieser Gelegenheit angelegten Sachvorgang zu entfernen, da sich die Betreffenden nicht strafbar gemacht haben.

Dies hat das Grenzschutzkommando Nord abgelehnt. Eine rein sachbezogene Dokumentation ohne personenbezogene Angaben in den Vorgangsakten des BGS sei nicht möglich, „da dieses Ereignis ohne die Angehörigen des DAV nicht denkbar ist". Die gefertigten Fotos seien keine Portraitaufnahmen. Sie erfaßten lediglich „die Demonstration, die Versammlung und die verschiedenen Lagesituationen an sich, nicht aber Einzelpersonen". Im übrigen unterliege die Namensliste mangels Dateibezug weder meiner Kontrollkompetenz, noch sei erkennbar, aus welcher Rechtsgrundlage ich meine „Auffassung"/ Ermächtigung für eine Beurteilung der Erforderlichkeit und des Umfangs polizeilichen Handels herleite.

Der Vorgang zeigt, daß es an der notwendigen datenschutzrechtlichen Sensibilität bisweilen nach wie vor mangelt. Nach den Anforderungen des Bundesverfassungsgerichts an Eingriffe in das informationelle Selbstbestimmungsrecht betrachte ich es durchaus als meine Aufgabe, auf solche und vergleichbare Mißstände hinzuweisen, auch wenn mir die derzeitige änderungsbedürftige Rechtslage ein förmliches Einschreiten nicht ermöglicht.

17. Zollkriminalinstitut und Zollfahndungsdienst

Auch im vergangenen Jahr konnte ich keine datenschutzrechtliche Kontrolle im Bereich der Zoll- und Steuerfahndung durchführen, da mir die hierfür notwendigen Unterlagen weiterhin vorenthalten werden. Alle Kompromißvorschläge (vgl. z. B. 7. TB S. 73, 8. TB S. 40 f.) wurden vom Bundesminister der Finanzen unter Berufung auf das Steuergeheimnis abgelehnt. In der Fragestunde des Deutschen Bundestages hat der Parlamentarische Staatssekretär beim Bundesminister der Finanzen in diesem Zusammenhang u. a. ausgeführt, die im Rahmen der Bekämpfung der Rauschgiftkriminalität an die Polizei übermittelten Daten unterlägen auch dort noch dem Steuergeheimnis. Auch bei der Polizei selbst sei § 30 der Abgabenordnung zu beachten. Nach dem Ergebnis meiner Kontrollen beim Bundeskriminalamt ist jedoch nicht sichergestellt, daß lediglich die mit der Bekämpfung der Rauschgiftkriminalität befaßten Polizeidienststellen Zugriff auf diejenigen Daten haben, die von der Zollverwaltung zu diesem Zweck an die Polizei übermittelt werden (vgl. dazu auch 8. TB S. 40 f.). Darauf habe ich den Bundesminister der Finanzen hingewiesen.

Der Bundesminister der Finanzen hat hierzu erwidert, nach der Abgabenordnung komme es nicht darauf an, daß die für die Bekämpfung der Rauschgiftkriminalität übermittelten Daten nur zu diesem Zweck verwendet werden. Vielmehr sei es ausreichend, daß „die Polizeidienststellen die Informationen aus dem Zollbereich zur Durchführung nichtsteuerlicher Strafverfahren oder zur Verfolgung von Verbrechen und verschiedener schwerer Vergehen oder aus anderen Gründen eines zwingenden öffentlichen Interesses" verwenden. Diese Anforderungen seien nach seiner Auffassung bei der polizeilichen Datenverarbeitung erfüllt.

Diese Ausführungen erwecken den Eindruck, als werde hier die rechtliche Begründung für eine bereits vorhandene Datenverarbeitung nachgeschoben, nicht aber die Datenverarbeitung am Zweck der erfolgten Übermittlungen ausgerichtet. Ich habe auch Zweifel, ob selbst die nunmehr vom Bundesminister der Finanzen vorgenommene weite Zweckbestimmung bei der Polizei eingehalten werden kann.

Zwar bestimmt Ziffer 3.2 der KpS-Richtlinien, daß Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen und der die KpS führenden Dienststelle in Erfüllung von Berufs- oder Amtspflichten übermittelt worden sind, nur zur Erfüllung des gleichen Zwecks weiterübermittelt werden dürfen. Die Einhaltung dieser Vorschrift setzt jedoch voraus, daß im Falle der Weiterübermittlung solcher Daten noch erkennbar ist, daß es sich dabei um Daten der genannten Art handelt. In vielen Fällen fließen diese Daten aber mit anderen Daten ineinander und bilden eine einheitliche Informationsmenge zum betreffenden „Fall". Deshalb ist gegenwärtig keineswegs gewährleistet, daß die von der Finanzverwaltung an die Polizei übermittelten Daten nur eingeschränkt verwendet werden. So wurden mir bei einer Kontrolle im Bundeskriminalamt im Jahre 1985 ohne weiteres die dort befindlichen „Steuerdaten" zusammen mit den anderen Daten ohne Einschränkung vorgelegt.

18. Verteidigung

18.1 Fehlende Rechtsgrundlage für die Datenverarbeitung beim MAD

Da das MAD-Gesetz in der abgelaufenen Legislaturperiode nicht verabschiedet worden ist, werden beim MAD auch weiterhin personenbezogene Daten ohne ausreichende Rechtsgrundlage verarbeitet. Dieser Zustand ist nur noch für einen begrenzten Zeitraum hinnehmbar. Aus meiner Sicht ist es indes durchaus nicht unproblematisch, Rechtseingriffe durch den MAD auf die Grundsätze des sog. „Übergangsbonus" (siehe oben 1.3) zu stützen. Das Fehlen von Rechtsgrundlagen für die Verarbeitung personenbezogener Daten beim MAD war auch vor dem Volkszählungsurteil bereits bekannt. Ich habe in früheren Tätigkeitsberichten darauf immer wieder verwiesen. Das Volkszählungsurteil hat meinen Bedenken nur noch zusätzliches Gewicht verliehen.

Für einige Bereiche, in denen der MAD bislang seine Datenverarbeitung auf gesetzliche Vorschriften stützen konnte, hat das Volkszählungsurteil deutlich gemacht, daß diese den Grundsätzen der Normenklarheit entsprechen müssen. Soweit dies nicht der Fall ist, kann die Datenverarbeitung nur noch für eine Übergangszeit hingenommen werden. Ein besonders wichtiges Beispiel hierfür ist § 24 Abs. 6 Nr. 7 Wehrpflichtgesetz, wonach Wehrpflichtige während der Zeit der Wehrüberwachung „der zuständigen Wehrersatzbehörde die für eine erstmalige und für weitere Sicherheitsüberprüfungen erforderlichen Auskünfte zu erteilen" haben. Im Weigerungsfalle droht die Verhängung eines Bußgeldes gemäß § 45 Abs. 6 Wehrpflichtgesetz. § 24 Abs. 6 Nr. 7 genügt nicht den Anforderungen, die das Volkszählungsurteil an Rechtsnormen gestellt hat, auf deren Grundlage personenbezogene Daten zwangsweise erhoben werden sollen. Es ist nicht geregelt, welche Daten im Rahmen der Sicherheitsüberprüfung erhoben werden dürfen, ob und in welchem Umfang auch die Daten über Angehörige einbezogen werden können, wie diese Daten anschließend verarbeitet und verwertet und wie lange sie zu welchem Zweck gespeichert werden dürfen. Für Zeit- und Berufssoldaten fehlt es gänzlich an einer ausdrücklichen gesetzlichen Bestimmung über die Sicherheitsüberprüfung.

Da derzeit keine den Anforderungen des Volkszählungsurteils entsprechenden Rechtsgrundlagen für die Sicherheitsüberprüfung durch den Militärischen Abschirmdienst vorliegen, sind diese Überprüfungen nur noch für eine angemessene Übergangszeit zulässig. Nach den Rechtsgrundsätzen über den sog. „Übergangsbonus" muß sich die Verwaltung bis zum Erlaß einwandfreier Rechtsgrundlagen auf dasjenige beschränken, was unbedingt notwendig ist. Dies bedeutet, daß auch die Speicherung und Verwertung der im Rahmen einer Sicherheitsüberprüfung erhobenen Daten sich auf das unbedingt notwendige Maß beschränken muß. Eine zweckfremde Nutzung dieser Daten steht hiermit nicht in Einklang. Wie ich bereits in meinem Achten Tätigkeitsbericht (S. 50) dargelegt habe, ist derzeit aber die Zweckbindung der im Rahmen der Sicherheitsüberprüfung erhobenen Daten beim Militärischen Abschirmdienst nicht gesichert.

18.2 Neukonzeption für die Merkmalsspeicherung beim MAD

Der Militärische Abschirmdienst hat ein neues Konzept für die Speicherung von Merkmalen in seiner Zentraldatei vorgelegt. Es handelt sich dabei um Merkmale, die im Rahmen einer Sicherheitsüberprüfung ermittelt werden. Insbesondere geht es um Informationen, die auf ein Sicherheitsrisiko hindeuten. Derartige Merkmale wurden vom Militärischen Abschirmdienst schon bisher gespeichert. Dies habe ich 1982 beanstandet, soweit es um Informationen ging, die dem innersten Persönlichkeitskern zuzurechnen sind. Der Bundesminister der Verteidigung hat die Berechtigung dieser Beanstandungen anerkannt und die Löschung aller Merkmale dieser Kategorie angeordnet. Vom Vollzug habe ich mich überzeugt.

Im Rahmen der Neukonzeption sollen nunmehr derartige Merkmale in unwesentlich veränderter Form erneut gespeichert werden, ohne daß sich die Sach- oder Rechtslage geändert hätte. Ich habe dem Bundesminister der Verteidigung mitgeteilt, daß ich die Wiederaufnahme der Speicherung derartiger Merkmale beanstanden müßte.

Da sich der Militärische Abschirmdienst, wie dargelegt, im Bereich der Sicherheitsüberprüfung derzeit nur auf den „Übergangsbonus" berufen kann, muß er sich auf das unbedingt Notwendige beschränken. Dies bedeutet, daß die im Rahmen der Sicherheitsüberprüfung erhobenen Daten auch aus diesem Grund ausschließlich für diesen Zweck bzw. für die im Zweck gleichgerichtete Spionageabwehr verwendet werden dürfen. Ich habe deshalb den Bundesminister der Verteidigung gebeten, den Zugriff auf die gespeicherten Merkmale nur denjenigen Mitarbeitern zu ermöglichen, die sie für Zwecke der Sicherheitsüberprüfung oder Spionageabwehr brauchen.

18.3 Eignungs- und Verwendungsprüfung (EVP)

Nach § 20a Wehrpflichtgesetz (WPflG) können Wehrpflichtige, die wehrdienstfähig sind, vor ihrer Einberufung auf ihre Eignung für bestimmte Verwendungen geprüft werden. Die Eignungs- und Verwendungsprüfung (EVP) wird vom Psychologischen Dienst der Bundeswehr durchgeführt. Ihr Ergebnis wird in der EVP-Ergebniskarte festgehalten, die in einem Schutzumschlag in den Personalunterlagen des Wehrpflichtigen (sog. Klarsichthülle) aufbewahrt wird. Der Umschlag darf nur von Psychologen des Psychologischen Dienstes der Bundeswehr geöffnet und der Inhalt der Ergebniskarte nur von ihnen interpretiert werden. Das bedeutet, daß ein Wehrpflichtiger, der Auskunft über seine EVP-Einzeldaten verlangt, diese Auskunft nur über den Psychologen beim Kreiswehrersatzamt erhält.

Die Ergebnisse der EVP werden in der sog. EVP-Datei gespeichert, die Teil des Wehrersatzwesen-Informationssystems (WEWIS) ist. Wegen der Festlegung des Inhalts der EVP-Datei, deren Nutzung (insbesondere Zugriffsregelungen) und wegen der Maßnahmen zur Löschung der Daten führe ich Gespräche mit dem Bundesminister der Verteidigung.

Im Einvernehmen mit dem Verteidigungsausschuß des Deutschen Bundestages prüft der Bundesminister der Verteidigung, ob die EVP nicht durch Computerunterstützung verbessert, beschleunigt und mit der Musterung zusammengelegt werden kann. Der Wehrpflichtige brauchte dann nur noch an einem Tag zum Kreiswehrersatzamt zu kommen. Im Laufe des Jahres 1986 wurde in einem Kreiswehrersatzamt das „Computer Adaptive Testing" (CAT) genannte Verfahren versuchsweise installiert. Die Testpersonen füllen nicht mehr — wie bisher — Fragebogen aus, sondern bedienen ein Bildschirm-Terminal. Auf diesem erscheint gleichsam ein Abbild des jeweiligen Testformulars (Bildschirmmaske), das mittels Tastatur auszufüllen ist.

Als Text auf dem Bildschirm und über Sprachausgabe in einen Kopfhörer werden der Testperson die einzelnen Tests erläutert und Übungen angeboten. Diese Übungen kann der Proband beliebig wiederholen. Auch bestimmt er grundsätzlich das Tempo des Tests, es sei denn, „Zeit" ist ein Element des Tests, worauf er dann ausdrücklich hingewiesen wird. Die Testpersonen werden wie bisher von einem Testleiter beaufsichtigt, der von seinem Bildschirm-Terminal aus verfolgen kann, wie die Tests bei den Probanden ablaufen.

Jede der sog. CAT-Anlagen, die in den Kreiswehrersatzämtern eingesetzt werden sollen, wird aus zwei Computern mit Leit- und Datensammelfunktionen und mehreren Bildschirmarbeitsplätzen für die Testpersonen bestehen und als geschlossenes System ohne Anschluß an WEWIS oder sonstige Online-Zugangsmöglichkeit von außen arbeiten. CAT ist somit ein speziell aufgabenbezogenes System im sog. Stand-alone-Betrieb. Die Übergabe der Daten für die EVP-Datei in WEWIS erfolgt mit Datenerfassungsbeleg; eine Übergabe auf Disketten ist geplant.

CAT wird gegenwärtig mit Wehrpflichtigen getestet. Die Wehrpflichtigen werden ausdrücklich auf die Freiwilligkeit der Teilnahme an CAT hingewiesen; sie können zwischen „Papier und Bleistift" oder „Bildschirm und Tastatur" wählen. Auch werden sie über den Sinn und die geplante Verwendung des CAT-Verfahrens informiert. Hiervon habe ich mich an Ort und Stelle überzeugt.

CAT wird in einem der sensitivsten Bereiche personenbezogener Datenverarbeitung eingesetzt. Psychologische Tests per Computer ermöglichen eine weitaus differenziertere Verfolgung des Testablaufs und damit des Verhaltens des Probanden als im herkömmlichen Verfahren. Außer den bloßen Testergebnissen können beim computergestützten Test noch andere personenbezogene Daten gewonnen werden, die ebenfalls Aussagen über die Leistungsfähikeit und die Eignung ermöglichen. Die Anforderungen an CAT sind aus der Sicht des Datenschutzes deshalb besonders hoch.

Meine Empfehlungen an den Bundesminister der Verteidigung für die Durchführung von CAT, die übernommen sein sollten, bevor CAT verbindlich für alle Psychologischen Dienste bei den Kreiswehrersatzämtern eingesetzt und vorgeschrieben wird, beziehen sich u. a. auf

- die Information der Wehrpflichtigen über das Verfahren
- die Erprobung des Verfahrens
- die Dokumentation des Verfahrens u. a. mit einer Übersicht über das Gesamtsystem, Programme, Dateibeschreibungen und Datensatzbeschreibungen
- die Regelungen zur Wartung und Fehlersuche
- die Organisation der Datenausgabe
- die Kontrolle von Protokollen, die im Rahmen der Verarbeitung der Testdaten in CAT entstehen (logging)
- die Sicherungsmaßnahmen für die Arbeitsplätze und eventuell anfallende Ausgaben von Datenträgern aus CAT (z. Zt. nur Papier).

Insbesondere bei der Weiterverwendung der Ergebnisse muß im Detail festgelegt werden, welche Daten für die Bearbeitung des Einzelfalles (Ergebnisdaten zur Beurteilung des Wehrpflichtigen) und welche Daten für wehrpsychologische Analysen (z. B. zur Beurteilung/Validierung von Einzeltests) in welcher Weise verwendet werden sollen.

Ferner habe ich empfohlen, § 20 a WPflG zu novellieren. In der Vorschrift sollte präzise bestimmt werden, was vom Wehrpflichtigen für die EVP verlangt wird und welche Folgen das Ergebnis der Prüfung für ihn hat. Auch sollten die Aufgaben der wehrpsychologischen Forschung rechtlich abgesichert und für diesen Bereich eine Geheimhaltungspflicht ähnlich dem Statistikgeheimnis vorgesehen werden. Damit würde gewährleistet, daß diese personenbezogenen Daten der Wehrpflichtigen nur für Zwecke des wehrpsychologischen Dienstes und nicht für Verwaltungsangelegenheiten verwendet werden dürfen.

Der Bundesminister der Verteidigung hat bisher grundsätzlich Bereitschaft gezeigt, meinen Empfehlungen zu folgen. Zu einem Teil meiner Empfehlungen sind bereits entsprechende Erlasse ergangen. Zur Neufassung von § 20 a WPflG habe ich ebenfalls meine Beratung angeboten. Ich habe festgestellt, daß alle an den Beratungen zu EVP und CAT Beteiligten ein hohes Maß an Verständnis für mein Anliegen zeigten und meine Einschätzung teilen, daß die Verarbeitung der EVP-Daten der Wehrpflichtigen besonders sorgfältig und behutsam vorgenommen werden muß.

18.4 Verband der Reservisten

Die Verhandlungen mit dem Bundesminister der Verteidigung und dem Verband der Reservisten der

Deutschen Bundeswehr e. V. (VdRBw) mit dem Ziel, die gelegentlich vorgekommenen unzulässigen Verwendungen von Daten über Reservisten durch den VdRBw künftig zu vermeiden, haben zu positiven Ergebnissen geführt.

So wird künftig auf Anordnung des Bundesministers der Verteidigung von einer Auflistung von Daten entlassener Soldaten für die sog. Feldwebel für Reservisten bei den Verteidigungskreiskommandos abgesehen. Außerdem werden auch keine Adreßaufkleber mehr für die regionalen Organisationsleiter des VdRBw ausgedruckt. Statt dessen erhält das Generalsekretariat des VdRBw neun Monate nach dem Entlassungstermin der Soldaten/Reservisten Aufklebe-Etiketten mit deren Anschriften. Das Generalsekretariat übernimmt dann den Versand an seine Geschäftsstellen, wobei es an die Auflagen zum Umgang mit den Aufklebern erinnert, wie sie im Mitteilungsblatt des Verbandes festgehalten wurden (siehe unten). Aufgrund dieser klaren Neuregelung sind die Kreiswehrersatzämter nicht mehr an der Weitergabe von Daten der Reservisten an den VdRBw beteiligt, wodurch auch Mißverständnisse über die Art der zulässigen Unterstützung der Arbeit des VdRBw durch Datenweitergabe aus den Kreiswehrersatzämtern vermieden werden.

Zur Unterrichtung seiner Geschäftsstellen hat der VdRBw in seinem Mitteilungsblatt 4/86 den ordnungsgemäßen Umgang mit den personenbezogenen Daten von Reservisten beschrieben und insbesondere darauf hingewiesen, daß die Adreßaufkleber nur zum einmaligen Anschreiben der Betroffenen verwendet werden dürfen und sicher aufzubewahren sind. Wenn zugesandte Aufkleber innerhalb von drei Monaten für diese Werbeaktion nicht verbraucht wurden, sind sie zu vernichten. Das Generalsekretariat des VdRBw wird sich über die Durchführung der Werbeaktionen bzw. über die Vernichtung nicht verwendeter Aufkleber berichten lassen.

Sowohl die Maßnahmen des VdRBw als auch insbesondere die Neuorganisation der Datenübermittlung vom Bundesminister der Verteidigung an den VdRBw sichern einen datenschutzgerechteren Umgang mit den personenbezogenen Daten der Reservisten (Anschriften). Die getroffenen Maßnahmen entsprechen meinen Empfehlungen.

18.5 Umgang mit KDV-Unterlagen

Für die Kreiswehrersatzämter wurden zur Unterstützung ihrer Aufgaben aus dem „Wehrersatzwesen-Informationssystem" (WEWIS) folgende Listen erstellt, die auch Daten anerkannter Kriegsdienstverweigerer enthalten:

— eine Liste der Zugänge und Abgänge von Wehrpflichtigen in die bzw. aus der Überwachung eines Kreiswehrersatzamtes (hier: Bewegungsliste).

  Diese Liste dient vor allem der Eingangs- und Abgabekontrolle der vom Kreiswehrersatzamt aufzunehmenden oder abzugebenden Personalunterlagen von Wehrpflichtigen (sog. Klarsichthüllen) z. B. bei Umzügen oder beim Ausscheiden aus der Wehrüberwachung;

— eine Liste der aus der Wehrüberwachung eines Kreiswehrersatzamtes und aus der Wehrüberwachung ganz ausgeschiedenen Wehrpflichtigen (hier: Liste der ausgeschiedenen Wehrpflichtigen). Diese Liste diente dem Kreiswehrersatzamt als Hilfsmittel für Auskünfte an Betroffene. Wenn sich ehemalige Wehrpflichtige nach Beendigung der Wehrüberwachung noch mit Fragen an das zuletzt für sie zuständige Kreiswehrersatzamt wandten, konnte das Amt dann anhand dieser Liste feststellen, daß und warum keine Personalunterlagen mehr vorhanden waren.

Die Aufbewahrung und der Umgang mit den Listen waren unbefriedigend geregelt (vgl. 8. TB S. 51). So wurde einigen anerkannten Kriegsdienstverweigerern anhand dieser Listen die wenig plausible Auskunft gegeben, daß das Kreiswehrersatzamt keine Daten über den Betroffenen mehr speichere, weil er z. B. vor vier Jahren als Kriegsdienstverweigerer anerkannt worden sei. Die Betroffenen verstanden nicht, wozu das Kreiswehrersatzamt diese Information noch benötige und wieso es mitteilte, daß es keine Daten mehr speichere, wenn es gerade diese personenbezogenen Angaben noch habe.

Aufgrund meiner Anregungen hat der Bundesminister der Verteidigung das Verfahren zur Erstellung der Listen, deren Inhalt und den Umgang mit ihnen neu geregelt.

So wird künftig in WEWIS keine automatisierte Datei mehr geführt, mit der es möglich wäre, die *Bewegungsliste* zu erstellen und fortzuschreiben. Vielmehr wird diese Liste ausschließlich aus dem laufenden Änderungsdienst abgeleitet. Sie weist — wie auch bisher — die Aufnahme eines Datensatzes in und die Entnahme eines Datensatzes aus WEWIS nach und zwar getrennt für Ersatzreservisten und Reservisten und jeweils nur auf ein Kreiswehrersatzamt bezogen. Die Bewegungsliste wird künftig mit einem Vernichtungsdatum versehen. Da dieses Datum stets der 30. Juni des auf die Erstellung der Liste folgenden Jahres ist, wird die Liste längstens 18 Monate aufbewahrt und dann vernichtet.

Die Liste der ausgeschiedenen Wehrpflichtigen entfällt künftig. Auskünfte an ausgeschiedene Wehrpflichtige können nur noch aus der Bewegungsliste gegeben werden.

Mit diesen Neuregelungen ist meinem Anliegen entsprochen, daß Daten, die für die Aufgabenerfüllung nicht mehr benötigt werden, gelöscht werden sollten. Zugleich bleiben die Kreiswehrersatzämter in der Lage, denjenigen Wehrpflichtigen, für die sie einmal zuständig waren, einige Zeit danach noch sinnvolle Auskünfte erteilen zu können. Darüber, welche Daten in der Liste enthalten sein müssen, bin ich mit dem Bundesminister der Verteidigung noch im Gespräch.

Noch nicht endgültig festgelegt ist auch, wie mit Unterlagen aus einem Verfahren zur Anerkennung

als Kriegsdienstverweigerer umzugehen ist, das mit der Ablehnung des Antrags endete. Ich habe u. a. vorgeschlagen, die Unterlagen gesondert aufzubewahren sowie die Einsichtnahme und Löschung zu regeln. Dabei sollte der Fall einbezogen werden, daß Wehrpflichtige ihren Antrag auf Anerkennung zurückziehen oder notwendige Unterlagen (auch nach Mahnungen) nicht einreichen und damit eine Ablehnung bewirken; ein solcher Gesinnungswandel sollte nicht fast lebenslang festgehalten werden. Ich denke dabei besonders an Jugendliche, die sich z. B. unter dem Druck der Klassengemeinschaft entschließen, einen Antrag auf Anerkennung als Kriegsdienstverweigerer zu stellen, obwohl sie es nach sorgfältiger Überlegung eigentlich nicht wollen.

Der Bundesminister der Verteidigung erwägt, die Unterlagen aus dem Verfahren für die Dauer der Wehrüberwachung in einem verschlossenen Umschlag aufzubewahren, der in der Klarsichthülle verbleibt. Ein Teil der Unterlagen kann vernichtet werden, wenn die Wehrüberwachung endet. Zumindest der Bescheid über die Ablehnung und die Begründung des Antrags sollen jedoch weiter aufbewahrt werden, bis auch die Wehrpflicht des Betroffenen nach § 3 Abs. 3 bis 5 Wehrpflichtgesetz (WPflG) endet. Der Bundesminister der Verteidigung hält das für notwendig, weil nach § 4 Kriegsdienstverweigerungsgesetz (KDVG) ein Wehrpflichtiger jederzeit einen weiteren Antrag auf Anerkennung als Kriegsdienstverweigerer stellen kann und bei der Beurteilung eines erneuten Antrags die Unterlagen aus früheren Verfahren herangezogen werden sollen. Inwieweit dies wirklich erforderlich ist, wäre noch zu prüfen. Ich werde mich weiter darum bemühen, Regelungen zu erreichen, die dem Wehrpflichtigen ein hohes Maß an Persönlichkeitsschutz bieten.

Ein Petent hatte mir vor längerer Zeit ein Formular übersandt, das Soldaten ausfüllen müssen, die einen Antrag auf Anerkennung als Kriegsdienstverweigerer stellen. Viele der einzutragenden Angaben waren für den Zweck, für den das Formular benötigt wurde, nicht notwendig. Auf meine Empfehlung, das Formular neu zu fassen, hat der Bundesminister der Verteidigung mit Wirkung vom 1. Oktober 1986 das sog. Meldeverfahren (Erfassung von Anträgen auf Anerkennung als Kriegsdienstverweigerer, die von Soldaten gestellt werden) neu geregelt. Der jetzt einheitlich verwendete Vordruck enthält nur noch die für die Meldung erforderlichen Angaben. Die Neuregelung ist im Ministerialblatt des Bundesministers der Verteidigung vom 29. September 1986, Nr. 17, S. 327 ff. abgedruckt.

19. Nicht-öffentlicher Bereich

19.1 Kreditsicherung

Die Kreditwirtschaft hat mit Wirkung zum 1. Juli 1986 den Umgang mit personenbezogenen Informationen, die bei der Eröffnung und Führung von Girokonten oder der Einräumung und Abwicklung von Krediten über den Kontoinhaber oder den Kreditnehmer erlangt werden, auf eine neue Grundlage gestellt. Die „SCHUFA-Klauseln" wurden neu gefaßt, das Melde- und Auskunftsverfahren, kurz „SCHUFA-Verfahren" genannt, wurde neu gestaltet. Der Schutz der Kreditdaten des einzelnen wurde in einer Reihe von Punkten verbessert. Diese Verbesserungen sind das Ergebnis von Verhandlungen, die die obersten Datenschutzaufsichtsbehörden der Länder mit meiner Beteiligung mit dem Zentralen Kreditausschuß und der SCHUFA über die Konsequenzen aus dem Urteil des Bundesgerichtshofs vom 19. September 1985 (vgl. 8. TB S. 52 f.) geführt haben. Ziel der Datenschutzbehörden war es dabei vor allem, die seit längerem erkannten, jetzt vom Bundesgerichtshof bestätigten Defizite im Kreditdatenschutz aufzuarbeiten. Die wichtigsten Anforderungen waren folgende:

— Eine pauschale Einwilligung kann nicht verlangt werden.

— Vor der Übermittlung von Negativdaten an die SCHUFA ist eine einzelfallorientierte Abwägung vorzunehmen.

— Die Organisation des Kreditinformationssystems im ganzen muß datenschutzgerecht sein. (Transparenz des Systems, Vollständigkeit, Richtigkeit und Aktualität der Daten; Beschränkung der Systemnutzung auf Kreditgeber).

Die neue SCHUFA-Klausel (Text der Klausel für Kontoeröffnungsanträge und Kreditanträge ist als Anlage 6 abgedruckt) unterscheidet, anders als die alte Pauschaleinwilligung, klar zwischen Daten über die Aufnahme und vertragsgemäße Abwicklung einer Geschäftsverbindung (Positivdaten) und solchen über deren nicht-vertragsgemäße Abwicklung (Negativdaten). Sie setzt sich aus einem Einwilligungsteil und einem Informationsteil zusammen. Daß Positivdaten, etwa die Eröffnung eines Girokontos (Name, Anschrift, Geburtsdatum, Kontonummer) nur mit Einwilligung des Bankkunden an die SCHUFA übermittelt werden dürfen, kommt jetzt in der Klausel zum Ausdruck, ebenso wie der Umstand, daß Negativdaten nur dann an die SCHUFA weitergeleitet werden dürfen, wenn die Abwägung der schutzwürdigen Belange des Kreditnehmers mit den berechtigten Interessen des Kreditgebers zu dessen Gunsten entschieden werden muß. Ob allerdings diese Abwägung in der Praxis wirklich in jedem Einzelfall zutreffend erfolgen wird, bleibt abzuwarten. Entsprechende Erfahrungen liegen derzeit noch nicht vor. Die Kreditwirtschaft hat ihre Kontosachbearbeiter durch ein ausführliches Merkblatt mit dem Abwägungserfordernis bekannt gemacht und die Abwägung auch anhand von Beispielen erläutert; die Gefahr, daß auch weiterhin routinemäßig nach Schema übermittelt wird, ist aber nicht von der Hand zu weisen, zumal eine wirksame Kontrolle nicht vorgesehen ist.

Über die Änderung der Klauseln hat die Kreditwirtschaft die Inhaber von Girokonten mit einem Informationsschreiben unterrichtet und ihnen zugleich die Möglichkeit eingeräumt, der Datenweitergabe an die SCHUFA zu widersprechen. Eine Vielzahl

von Kontoinhabern, die von dieser Möglichkeit Gebrauch gemacht haben, mußte dann jedoch feststellen, daß gerade diese Ausübung ihres Rechts, grundsätzlich selbst über die Preisgabe und Verwendung ihrer persönlichen Angaben zu entscheiden, der SCHUFA gemeldet und dort als „Widerspruch zur SCHUFA-Klausel" auf ihrem Datenkonto vermerkt worden war.

Gegenüber dem Innenausschuß des Deutschen Bundestages, der sich mit dieser Problematik befaßt hat, habe ich darauf hingewiesen, daß der Widerspruch gegen eine Datenübermittlung aufgrund der alten, vom Bundesgerichtshof aufgehobenen Klausel dann nicht zu einer zusätzlichen Speicherung, sondern zur Löschung der bei der SCHUFA vorhandenen Daten führen muß, wenn der Giro- oder Ratenkreditvertrag vom Betroffenen bisher vereinbarungsgemäß erfüllt worden ist. Zwar kann das Kreditinstitut bei einem Girovertrag den Widerspruch zum Anlaß nehmen, die Kontoverbindung nur noch mit Einschränkungen (z. B. auf Guthabenbasis) fortzuführen; eine Übermittlung des Widerspruchs an die SCHUFA ist jedoch nur dann zulässig, wenn auf dem Datenkonto des Betroffenen bereits Negativmerkmale gespeichert sind und der Vermerk des Widerspruchs zur Information anderer Kreditgeber darüber dient, daß wegen des Widerspruchs Nachmeldungen zu diesem Konto nicht mehr erfolgen werden.

Von ebenso großer Bedeutung wie die präzise und konkrete Fassung der Klauseln ist eine Reihe von seit langem gebotenen Veränderungen im SCHUFA-Verfahren. So ist der recht umfangreiche Katalog der Melde- und Auskunftsmerkmale einer kritischen Revision im Hinblick auf die Aussagekraft einzelner Merkmale für die Kreditwürdigkeit unterzogen worden. Unscharfe Merkmale und Merkmale über einseitige Maßnahmen des Gläubigers werden künftig nicht mehr verwendet. Es ist also nicht mehr möglich, Kreditnehmer mit der Drohung unter Druck zu setzen, etwa die letzte außergerichtliche Mahnung der SCHUFA zu melden.

Die Auskunftserteilung durch die SCHUFA an den Betroffenen ist ebenfalls verbessert worden. Während der Kreditnehmer früher lediglich erfuhr, welche Daten die SCHUFA über ihn gespeichert hatte, erhält er jetzt auch Kenntnis davon, wer in der zurückliegenden Zeit bei der SCHUFA über ihn angefragt hat. Die SCHUFA hat zugesagt, Anfragen ihrer Vertragspartner künftig für ein Jahr in ihrem Datenbestand zu speichern und dem Betroffenen, der Auskunft verlangt, mitzuteilen. Die Betroffenen erhalten damit erstmals die Chance, bei entsprechendem Verdacht mißbräuchliche Nutzungen des SCHUFA-Systems aufzudecken.

Mit der Erweiterung der Selbstauskunft ist die Einbeziehung des Betroffenen jedoch noch nicht so weit erfolgt, wie dies m. E. erforderlich ist. Ich habe in meinem Achten Tätigkeitsbericht (S. 52, 53) darauf hingewiesen, daß die volle Einbeziehung des Betroffenen aus Gründen des Datenschutzes erforderlich ist, weil der Betroffene zum einen von sich aus die Möglichkeit haben muß, Richtigkeit, Aktualität und Vollständigkeit der gespeicherten Daten zeitnah zu überprüfen und Korrekturen zu veranlassen, noch ehe ein Schaden eingetreten ist. Zum anderen kann nur durch die volle Einbeziehung des Betroffenen geprüft werden, ob der jeweilige SCHUFA-Nutzer ein berechtigtes Interesse an der erbetenen Auskunft hat. Das Fehlen einer wirksamen Zulässigkeitskontrolle bei Übermittlungen durch die SCHUFA kann nur durch die Beteiligung des Betroffenen am Datenfluß ausgeglichen werden. Seine Einbeziehung sollte daher so aussehen, daß er von jeder Änderung des Datenbestands auf seinem Datenkonto und vor jeder Übermittlung durch die SCHUFA durch einen „Datenkontoauszug" unterrichtet wird. Die jetzt erfolgte Erweiterung der Selbstauskunft ist ein erster Schritt in diese Richtung.

Nachteilig für den Betroffenen ist es immer noch, daß die Kosten der Auskunft auf ihn abgewälzt werden, obwohl es sich dabei um eine datenschutzrechtlich gebotene Maßnahme des organisatorischen Betriebs handelt, die den Systemträgern zuzuordnen ist. Aus einer Vielzahl von schriftlichen Eingaben und telefonischen Anfragen ist mir bekannt, daß viele Betroffene durch die Kosten von der Einholung der Auskunft abgehalten werden. Aus diesem Grunde halte ich es für wichtig, bei der Novellierung des BDSG die Kostenfreiheit unmißverständlich zu bestimmen.

Eine weitere überfällige Änderung des SCHUFA-Verfahrens ist die mit dem Zentralen Kreditausschuß und der Bundes-SCHUFA vereinbarte Beschränkung des Kreises der SCHUFA-Anschlußnehmer auf Kreditgeber. Damit wird der seit langem erhobenen Forderung der Datenschutzbehörden und der Rechtsprechung des BGH Rechnung getragen, den Kreis der SCHUFA-Nutzer auf solche Anschlußnehmer zu beschränken, die ein berechtigtes Interesse an Informationen über die Kreditwürdigkeit anderer haben.

Neben den klassischen SCHUFA-Anschlußnehmern, wie Banken und Versandhäusern, waren bislang z. B. auch Handwerker, Heizöllieferanten, Auto- und Gerätevermieter und andere Gewerbezweige an die SCHUFA angeschlossen. Dabei liegt es auf der Hand, daß hier die Kreditgewährung nicht im Vordergrund der Geschäftstätigkeit steht. Entsprechend den getroffenen Absprachen hatte die Bundes-SCHUFA die Verträge mit diesen Anschlußfirmen zum 30. Juni 1986 gekündigt. Eine Reihe der von der Kündigung betroffenen Unternehmen hat dagegen wettbewerbsrechtliche Bedenken erhoben. Das Bundeskartellamt hat daraufhin ein Antidiskriminierungsverfahren gegen die SCHUFA eingeleitet und der SCHUFA aufgegeben, die ausgesprochenen Kündigungen zu suspendieren. Ein ganz wesentlicher Teil der Reform konnte dadurch noch nicht umgesetzt werden.

Im Rahmen meiner Beratungsaufgabe gemäß § 19 Abs. 1 BDSG habe ich in einem Gespräch mit der zuständigen Beschlußabteilung des Bundeskartellamts das Verhältnis von Wettbewerbsrecht und Datenschutzrecht erörtert und dabei die Auffassung vertreten, daß eine wettbewerbswidrige Diskriminierung seitens der SCHUFA dann nicht vorliegt,

wenn diese datenschutzrechtlich gehindert ist, den Unternehmen bestimmter Wirtschaftszweige den Zugang zu personenbezogenen Daten zu eröffnen. Geräte-, Auto- oder Wohnungsvermieter haben kein berechtigtes Interesse an Informationen über die Kreditwürdigkeit des Mieters, weil sie nur ein allgemeines wirtschaftliches Risiko, etwa der Beschädigung der Mietsache, aber kein Kreditrisiko eingehen. Eine strikte Beachtung dieser Trennung ist zur Wahrung der schutzwürdigen Belange der betroffenen Kreditnehmer erforderlich, denn auch im Privatrechtsverkehr muß der einzelne stets wissen können, wer was bei welcher Gelegenheit über ihn weiß. Dem dient der Grundsatz, daß Kreditdaten nur im Bereich der Kreditvergabe Verwendung finden.

19.2 Versicherungen

Über die Neufassung der Einwilligungsklauseln, die von den Versicherungsunternehmen im Rahmen ihrer Allgemeinen Geschäftsbedingungen gegenüber dem Versicherungsnehmer verwendet werden (Datenschutzklausel, Schweigepflichtentbindungsklausel; vgl. 8. TB S. 53 f.) haben weitere Gespräche zwischen den obersten Datenschutzaufsichtsbehörden der Länder und den Verbänden der Versicherungswirtschaft stattgefunden, an denen ich mich beteiligt habe. Eine Einigung über die Problematik — etwa, wie konkret die Einwilligung des Versicherten zur Übermittlung von Vertragsdaten an zentrale Dateien der Versicherungsverbände sein muß oder wie weit eine pauschale Erklärung zur Entbindung von der ärztlichen Schweigepflicht bei Kranken- oder Unfallversicherungen reichen kann — wurde jedoch noch immer nicht erzielt. Ich habe dies zum Anlaß genommen, das Bundesaufsichtsamt für das Versicherungswesen in diesen Fragen gemäß § 19 Abs. 1 BDSG zu beraten und die datenschutzrechtlichen Anforderungen zu erläutern, damit auch von seiten der Versicherungsaufsicht auf eine datenschutzgerechte Neugestaltung der Klauseln und, soweit nötig, auch des Umgangs mit den personenbezogenen Daten der Versicherten hingewirkt werden kann. Diese Beratung und die Beteiligung an den Gesprächen mit der Versicherungswirtschaft werde ich fortsetzen.

20. Datensicherung

Die Entwicklung der automatisierten Datenverarbeitung wird zur Zeit stark vom Angebot kleiner, preiswerter und zugleich leistungsfähiger und sehr flexibel einsetzbarer Datenverarbeitungsanlagen beeinflußt.

Damit können z. B. Speicherschreibmaschinen preiswert durch Systeme für Text- und Datenverarbeitung ersetzt werden, und es ist auch wirtschaftlich vertretbar, Datenverarbeitungskapazitäten an Arbeitsplätzen zur (freien) Verfügung zu stellen, an denen sie bei weitem nicht ausgelastet sind, aber doch eine sinnvolle Unterstützung der Arbeit leisten können, sei es durch die Führung und Verarbeitung eigener Datenbestände, sei es durch die Erschließung von großen, allgemein verfügbaren Informationssystemen wie z. B. JURIS. Bei dieser im Prinzip positiven Entwicklung darf jedoch nicht übersehen werden, daß Datenverarbeitung nicht einfach gekauft, sondern vom Anwender bewußt gestaltet werden muß, und daß eine Beschaffungsentscheidung über Geräte und Software sehr gründliche Vorarbeiten verlangt. Zu diesem Thema schreibt die Bundesstelle für Büroorganisation und Bürotechnik (BBB) in ihrem Bericht über ein Pilotprojekt im Bundesverwaltungsamt:

> „Es läßt sich nicht leugnen, daß die Anbieter im Bürokommunikations-Bereich „mit harten Bandagen kämpfen". Dies erklärt sich aus dem Überangebot und dem harten Wettbewerb.
>
> Die Anwender sollten aber auch ihr eigenes Vorgehen kritisch prüfen. Sie gehen meistens nicht ausreichend genug vorbereitet, mit mangelnder Fachkenntnis und weitgehend unklaren Vorstellungen in die Verhandlungen mit dem Anbieter.
>
> Es dürfte keinen anderen Bereich im privaten und beruflichen Leben geben (bei vergleichbarer finanzieller Größenordnung der zu beschaffenden Produkte), in dem der Anwender ähnlich geringe Vorstellungen, Kenntnisse und Beurteilungsfähigkeiten bei einer Beschaffung hat wie auf dem Gebiet der Bürokommunikation.

Entsprechend wenig beachtet sind dann oft die Vorschriften über den Datenschutz und die Notwendigkeit, technische und organisatorische Maßnahmen zur Datensicherung zu treffen. Erschwerend wirkt sich dabei aus, daß die von der Datenverarbeitung in Rechenzentren bewirkten oder zumindest begünstigten Funktionstrennungen, die eine erhebliche Schutzwirkung haben, nicht mehr erforderlich sind; im Gegenteil, gerade beim Einsatz von Arbeitsplatzcomputern liegt es nahe, Arbeitsgänge zusammenzufassen und Funktionstrennungen aufzuheben. Dann müssen aber kompensierende Sicherheitsmaßnahmen den Abbau dieses Schutzes ausgleichen.

20.1 Personal-Computer

Im Berichtsjahr setzte sich die Entwicklung zu leistungsfähigeren und billigeren Arbeitsplatzcomputern fort. Der dadurch verstärkte Einsatz dieser Geräte führt in einer erheblichen Zahl von Fällen zu je nach den Einsatzbedingungen unterschiedlichen Datenschutzproblemen. Dabei werden mir die auftretenden Schwierigkeiten oft nur zufällig, häufig wohl überhaupt nicht bekannt. Meine Dienststelle wäre auch überfordert, wenn sie in jedem Einzelfall eine an den besonderen Umständen orientierte Empfehlung aussprechen müßte. Meine Aufgabe kann hier nur darin bestehen, grundsätzliche Empfehlungen zu geben und anläßlich von Kontrollen festzustellen, ob die Möglichkeiten, Datenverarbeitung auf Personal-Computern (PC) sicher zu gestalten, angemessen genutzt werden, und ob diese Anlagen nur für solche Anwendungen eingesetzt werden, bei denen die mit angemessenem Aufwand

nicht ausschließbaren Restrisiken tragbar sind. Den Einsatz von PC ordnungsgemäß zu organisieren bzw. zu beschränken, ist dagegen Aufgabe der datenverarbeitenden Stellen selbst. Dazu ist es zunächst geboten, den Bestand an solchen Datenverarbeitungsanlagen zu erheben und die dabei festgestellten PC und ihren derzeitigen und geplanten Einsatz anhand der Kriterien des BDSG auf Zulässigkeit und Sicherheit zu prüfen. Darüber hinaus ist es aber auch aus Gründen der Wirtschaftlichkeit und der Berrschbarkeit der Organisation sinnvoll, den zukünftigen Einsatz von PC zu planen oder zumindest zu koordinieren, was auch die Gewährleistung des Datenschutzes erleichtert.

Die technischen Voraussetzungen für einen angemessen gesicherten PC-Einsatz haben sich im Berichtsjahr deutlich gebessert. So wird für viele Typen PC Sicherheits-Software angeboten, mit der man u. a. die Risiken mindern kann, die sich aus der Programmerstellung durch den Anwender selbst und den sonst nur schwer kontrollierbaren Routinen ergeben, wie z. B. Datenausgabe auf Disketten. Der Einsatz dieser Sicherheits-Software führt dazu, daß zwischen zwei Betriebszuständen unterschieden wird. Der eine Zustand erlaubt dem durch sein Paßwort ausgewiesenen privilegierten Benutzer die im wesentlichen unbeschränkte Programmierung der Anlage, die Einrichtung von Dateien und deren Schutz, den Aufbau von Menüführungen und die Definition von (weiteren) Benutzern und ihren (eingeschränkten) Berechtigungen. Der andere Zustand erlaubt den definierten und durch ihr Paßwort ausgewiesenen Benutzern die Nutzung des PC und die Arbeit mit den Daten und Programmen im Rahmen ihrer jeweiligen Berechtigung. Dabei können je nach Bedarf die Nutzung der Programme oder andere kontrollbedürftige Aktionen so protokolliert werden, daß sie dem jeweiligen Benutzer zugeordnet werden können. Zusätzlich zu diesen Sicherungsmaßnahmen bietet die Software oft die Möglichkeit, die Daten auf den Datenträgern so zu verschlüsseln, daß sie nur von den planmäßigen Programmen entschlüsselt werden können, oder die Daten wenigstens in einer Weise zu speichern, daß der verstehende Zugriff durch andere als die planmäßigen Programme erheblich erschwert wird.

Die allgemeine Beunruhigung über den oft unkontrollierten PC-Einsatz hat außer zu diesen mehr technisch orientierten Hilfen auch zu organisatorischen Hinweisen und Vorschlägen für Richtlinien u. ä. geführt. So hat z. B. die Arbeitsgemeinschaft für wirtschaftliche Verwaltung e. V. einen „Leitfaden Datenschutz und Datensicherung bei dezentraler EDV" herausgegeben (AWV-Schrift Nr. 400). Die im Bundesministerium des Innern angesiedelte Koordnierungs- und Beratungsstelle der Bundesregierung für die Datenverarbeitung in der Bundesverwaltung (KBSt) hat als Band 7 ihrer Schriftenreihe ausführliche Unterlagen für den Einsatz von Arbeitsplatzrechnern in der Bundesverwaltung veröffentlicht, in denen u. a. auf die Technik, die Nutzungsmöglichkeiten und Probleme sowie auf Auswahl- und Anschaffungsfragen eingegangen wird. Die oben erwähnte AWV-Schrift ist dort als Anhang beigefügt und zur Beachtung empfohlen. Ich begrüße diese Maßnahme, da sie hilft deutlich zu machen, daß sichere Datenverarbeitung Bestandteil korrekten Verwaltungshandelns ist.

Als Ergebnis dieser und anderer Bemühungen ist festzustellen, daß die Voraussetzungen für die Gewährleistung des Datenschutzes beim Einsatz von PC besser geworden sind. Es bleibt aber in den einzelnen Stellen noch viel zu tun, um diese Voraussetzungen auch zu nutzen. Dabei müssen die für die Datenverarbeitung und die für den Datenschutz verantwortlichen Instanzen berücksichtigen, daß die Arbeitseinheiten, in denen PC eingesetzt werden, oft nicht selbst über die notwendige Organisationskraft verfügen, um Einsatzbedingungen zu schaffen, die auch in datenschutzrechtlicher Hinsicht verantwortet werden können. Hier hilft sicher die Übersicht über alle eingesetzten PC. Denn die für den Datenschutz verantwortlichen Instanzen, aber auch die vorgesetzten Dienststellen, die für die Fachaufsicht zuständig sind, können aus der Übersicht und ihrem Wissen um Aufbau und Aufgaben der datenverarbeitenden Stelle ersehen, ob eine Stelle noch beraten werden muß oder ob sie in der Lage ist, selbst die Datenverarbeitung ordnungsgemäß zu organisieren.

Zu berücksichtigen ist auch, daß Stellen, die PC einsetzen wollen, in der Regel selbständig mit den Herstellern oder Verkäufern von PC verhandeln. Sie verfügen häufig aber nicht über das erforderliche Wissen, um alle Anforderungen formulieren zu können, die erfüllt sein sollten, um mit einem PC auch sicher arbeiten zu können. Nach meinen Erfahrungen sind die Hersteller oder Verkäufer von PC nicht sehr geeignet, einen Kunden auch über die ausdrücklich gestellten Fragen hinaus so zu beraten, daß dieser seine Aufgaben nicht nur effizient, sondern auch ordnungsgemäß und sicher erfüllen kann. Das Eingehen auf Forderungen des Datenschutzes oder gar das Hinweisen auf Sicherheitsprobleme wird wohl häufig als verkaufshemmend empfunden. Die Folge kann aber dann sein, daß eine Stelle z. B. einen PC mit optimal einsetzbarer Sicherheits-Software kauft, aber die Implementation voll dem Hersteller oder Verkäufer überläßt. Dieser programmiert in der Regel den „üblichen" Standard an Sicherheit, d. h. der PC kann in jeder Hinsicht flexibel genutzt werden. Der Kunde kann diesen Zustand mangels Wissen weder erkennen noch abstellen. Er hält dies häufig auch nicht für notwendig, weil er ja eine Sicherheits-Software gekauft hat und davon überzeugt ist, daß schon dadurch die Verarbeitung auch sicher sei. Diese Abhängigkeit vom Hersteller bzw. Verkäufer von PC kann sich derart zu Lasten des Käufers oder Anwenders auswirken, daß er die gesetzlichen Sicherheitsanforderungen nicht erfüllt, ohne daß er das weiß. Ich habe schon zahlreiche Gespräche insbesondere mit Herstellern genutzt, um an deren Mitverantwortung zu appellieren, daß gerade beim Verkauf oder Vermieten von PC die Beratung mit dem Ziel ordnungsgemäßer Datenverarbeitung erweitert werden sollte. Nur so kann m. E. langfristig vermieden werden, daß durch sonst notwendig werdende einengende Vorschriften die Organisationsfreiheit

von Behörden beschränkt wird. Auch trüge nach meinen Eindrücken aus Gesprächen mit Anwendern eine bessere Beratung zu einer höheren Akzeptanz von PC bei, was wohl letztlich im Sinne der Hersteller ist.

20.2 Bürokommunikation

Der Einsatz moderner Datenverarbeitungsanlagen kann die verschiedensten Bürotätigkeiten wirksam unterstützen. Dazu werden von vielen Herstellern Bürokommunikationssysteme angeboten, die Schreibdienst, Dateienverwaltung und Dateinutzungen, Mitteilungsdienste und die Verbindung zu externen Transportdiensten wie Telex, Teletex oder auch Bildschirmtext sowie zu Informationsdiensten wie z. B. JURIS integrieren. Die dabei erfolgende breite Streuung von Datenverarbeitungskapazität, sei es als Terminal ohne eigene Speicherungsmöglichkeit, sei es als Schreibsystem oder als frei programmierbarer Arbeitsplatzcomputer, ist jedoch nicht ganz problemlos. Denn dabei treten Organisations- und Datenschutzfragen etwa in derselben Art auf, wie beim Einsatz von Personal-Computern (vgl. 8 TB S. 56 ff.). Es kommt noch hinzu, daß durch die Versorgung möglichst aller Arbeitsplätze eines Bereichs mit Datenverarbeitung-Kapazität viele Benutzer mit diesen Geräten arbeiten können oder müssen, denen jedoch vom Aufgabengebiet her solche Anlagen und ihre Benutzung nicht vertraut sind. Damit verschärfen sich sowohl die Datenschutz- als auch die allgemeinen Sicherheitsprobleme, z. B. deshalb, weil in diesem Personenkreis stärker als bei den berufsmäßigen Datenverarbeitern die Tendenz besteht, Zugangsprozeduren einschließlich der Paßwörter aufzuschreiben und leicht greifbar aufzubewahren oder Disketten im nicht abgeschlossenen Terminal zu lassen.

Der Einsatz von Bürokommunikationssystemen in der öffentlichen Verwaltung des Bundes entwickelt sich nur langsam. Anders als bei der Nutzung isolierter Personal-Computer für bestimmte Aufgaben oder der Unterstützung von Schreibarbeiten durch nicht im Verbund arbeitende Textverarbeitungssysteme ist nämlich für den gesamten von einem Bürokommunikationssystem zu versorgenden Bereich eine integrierende Gesamtplanung erforderlich. Dabei stellt sich die Frage, welche Tätigkeiten außer den bereits automatisierten Massenarbeiten und der weitgehend automatisierten oder automatisierbaren Textverarbeitung durch ein Bürokommunikationssystem so wirksam unterstützt werden könnten, daß nicht nur die Anschaffungs- und Betriebskosten, sondern auch der erhebliche Einführungs- und Umstellungsaufwand gerechtfertigt sind. In der Regel läßt sich allerdings für jede einzelne solcher Tätigkeiten mit geringem Aufwand auch eine isolierte Lösung finden.

Trotzdem wird sich häufig herausstellen, daß bei zunehmendem Einsatz einzelner Computer für Bürotätigkeiten eine integrierte Lösung langfristig sinnvoller ist, und dementsprechend gibt es auch (Rahmen-)Planungen in verschiedenen Bereichen, die in den nächsten Jahren schrittweise verwirklicht werden sollen. Soweit mir solche Planungen bekannt sind, enthalten sie ausreichende Ansätze zur Berücksichtigung von Datenschutz und Datensicherheit. Bei der Realisierung der Planungen wird es darauf ankommen, durch Auswahl der Geräte und ihrer Sicherheitseinrichtungen, durch geordnete Verfahren zur Programmerstellung und zur gesicherten Programmanwendung sowie durch die intensive Schulung und Beratung aller Benutzer die Zulässigkeit und Sicherheit der Aufgabenerledigung auch unter den Bedingungen der Bürokommunikation zu gewährleisten. Dazu gehört, daß Verfahren zur Protokollierung kritischer Benutzeraktionen, wie Zugriffe auf besonders zu schützende Daten oder Veränderungen an wichtigen Texten, erprobt werden. Hierbei und bei den Verfahren zur Auswertung der entstehenden Protokolldaten ist die enge Zusammenarbeit mit den Personalvertretungen unverzichtbar, weil die für Datenschutz- und Datensicherheitskontrollen benötigten Aufzeichnungen zugleich Aussagen über Verhalten und Leistung der Mitarbeiter enthalten. Solche Kontrollen durch aktionsbegleitende Protokollierungen werden aber benötigt, weil auch ändernde Zugriffe — außer der oft nicht sofort zu entdeckenden Änderung selbst — keine Spuren und insbesondere keine Hinweise auf den Verursacher hinterlassen.

In diesem Zusammenhang ist darauf hinzuweisen, daß alle mir bekannten Textverarbeitungsprogramme auch im Rahmen von Bürokommunikationssystemen das Anbringen von Randnotizen an den einzelnen Textpassagen ebensowenig erlauben, wie nach Bearbeitern unterschiedlich gekennzeichnete Korrekturen. Eine Lösung dieser Fragen, die beim Zusammenwirken mehrerer Bearbeiter sowie bei der Abstimmung von Texten wesentlich sind, ist technisch möglich. Bevor sie aber nicht in einfach zu handhabender Form erreicht ist, wird in vielen Fällen die Bearbeitung und deren Dokumentation auf Papier nicht durch automatisierte Verfahren ersetzt werden können.

20.3 Vernetzung

Ein wesentliches Element der Bürokommunikation, aber auch anderer Datenverarbeitungssyssteme ist die Verbindung der einzelnen Anlagen der verschiedenen Benutzer untereinander und mit anderen Systemen über Datenkommunikationsnetze. Anders als etwa beim Telefonieren gibt es für diese Kommunikation keine „natürliche" gegenseitige Erkennung der Partner, etwa an der Stimme oder auch an einem dem sachbezogenen Informationsaustausch vorangehenden persönlichen Gespräch. Die Kommunikation wird vielmehr durch elektrische Impulse getragen, die keine individuelle Nuancierung aufweisen und deren Kombination weitgehend allgemein gültigen Festlegungen (Protokollvereinbarungen) folgt. Das Übermitteln einer Nachricht an einen Partner und das Stellen einer Frage einschließlich der Beantwortung durch den Partner setzen auch nicht mehr voraus, daß man den Partner persönlich erreicht, es genügt vielmehr, daß eine entsprechende Datenverarbeitungsanlage zu der jeweils gewünschten Kommunikation bereit ist.

Zu den sich daraus ergebenden Sicherheitsproblemen habe ich ausführlich in meinem Siebenten Tätigkeitsbericht (vgl. 7. TB Anlage 1, S. 98 ff.) Stellung genommen. Die dort gegebene Darstellung ist in erster Linie an Kommunikationsstrukturen orientiert, bei denen mehrere kleine Datenverarbeitungsanlagen, etwa abfrageberechtigte Terminals, auf eine zentrale Informationssammlung zugreifen können. In einer solchen Struktur ist es möglich und auch vertretbar, daß bei der Zentrale umfangreiche Sicherungsmaßnahmen gegen die unberechtigte Nutzung getroffen werden.

Dies gilt so nicht mehr, wenn kleinere Anlagen, wie etwa Personal-Computer, im Rahmen eines Bürokommunikationssystems miteinander so vernetzt werden, daß jeder mit jedem verbunden ist und im Extremfall viele Teilnehmer gegenseitig Nachrichten, Daten und Programme abrufen oder auch in die Anlage eines Partners hinein senden können. Mir ist zur Zeit kein Verfahren bekannt, mit dem man eine in dieser Weise offene Kommunikation mit zumutbarem Aufwand hinreichend sicher gestalten könnte, wenn sich die ermöglichten Zugriffe auch auf die zu schützenden Daten der einzelnen Teilnehmer in deren Anlagen beziehen sollen.

Zur Unterstützung des trotzdem sinnvollen Nachrichtenverkehrs zwischen den Teilnehmern in einem Kommunikationsnetz bzw. zur Beteiligung mehrerer Teilnehmer am Betrieb und/oder an der Nutzung von Datenbanken sollte deshalb jeweils die Möglichkeit zur Einrichtung zentraler Nachrichtenverteiler bzw. zentraler Datenbanken in einem Netz sonst überwiegend gleichartiger Teilnehmer genutzt werden, weil sich damit auch Datensicherheit erreichen läßt.

Nachrichtenverteiler (englisch: Message-Handling-Server) sind an ein Netz angeschlossene Datenverarbeitungsanlagen, die für jeden Teilnehmer ein bestimmtes „Fach" enthalten, in das andere ihre für diesen Teilnehmer bestimmten Nachrichten „ablegen" können. Die Leistung des Nachrichtenverteilers besteht zum einen darin, daß die notwendigen Sicherungs- und Kontrollmaßnahmen durchgeführt werden, die hier (zentral) in ausreichendem Umfang auch möglich sind. Dazu gehört die Sicherung, daß jeder nur auf die für ihn bestimmten Nachrichten zugreifen kann, was in der Regel durch Paßwortschutz erreicht wird (zur sicheren Gestaltung solcher Verfahren s. 6. TB S. 55 f.). Genauso kann der Verteiler dem Empfänger Klarheit über den Absender verschaffen, was ebenfalls zur Sicherheit der Kommunikation beiträgt. Eine weitere Leistung eines Nachrichtenverteilers kann die Betreuung eines „schwarzen Brettes" sein, z. B. dadurch, daß für eine Vielzahl von Teilnehmern ein Fach geführt wird, in das jeder Nachrichten für alle ablegen kann. Auch die Möglichkeit, Nachrichten an einen beschränkten Empfängerkreis zu senden, erleichtert die Kommunikation. Frage-Antwort-Dialoge zwischen zwei Teilnehmern bzw. deren Datenverarbeitungsanlagen können damit aber nur so durchgeführt werden, daß zunächst die Frage an den Nachrichtenverteiler gesandt wird, der Empfänger diese von dort abruft, über die Beantwortung entscheidet und seine Antwort auf demselben Weg zurückschickt. Die damit unvermeidbare Verzögerung ist der Preis für die Kontrolle des Vorgangs durch den jeweils fragenden oder antwortenden Teilnehmer.

Ist die Entscheidung und damit die Kontrolle durch den Datenbesitzer z. B. wegen der Häufigkeit solcher Vorgänge zu zeitaufwendig, zu umständlich oder wegen der abstrakten festgelegten Zugriffsberechtigungen auf bestimmte Daten auch nicht erforderlich, so kann eine Datenverarbeitungsanlage im Netz zentral zugreifbare Daten zur Verfügung stellen und die Zugriffe einschließlich der Zugriffsbeschränkungen verwalten. Weil auch in diesem Fall der Sicherungs- und Kontrollaufwand auf eine Stelle konzentriert ist, kann auch dafür die jeweils notwendige Sicherheit gewährleistet werden.

Zumindest dann, wenn der Schutzbedarf der Daten hoch ist, muß bei der Vernetzung vieler Anlagen miteinander außer der logischen Struktur des Nachrichtenverkehrs zusätzlich die technische Realisierung der Datenweiterleitung beachtet werden. Hier werden gerade für lokale Netze — wie in der Bürokommunikation oder auch für die Verbindung zwischen sonst selbständig arbeitenden Personal-Computern — besonders einfache Verfahren angeboten, die aber unter Sicherheitsaspekten nicht immer unproblematisch sind. Im wesentlichen ist zwischen drei Strukturtypen (Netztopologien) zu unterscheiden, die in größeren Netzen auch vermischt auftreten können:

— In einem sternartigen Netz sind alle Anlagen direkt an eine zentrale Vermittlungseinrichtung angeschlosssen. Alle Nachrichten laufen durch diese Stelle, weshalb hier nicht nur zur Sicherung der Verfügbarkeit, sondern auch aus Gründen der Vertraulichkeit besondere Sicherungsmaßnahmen geboten sind.

— In ringförmigen Netzen fehlt eine solche Zentrale, und jeder Teilnehmer ist mit zwei „Nachbarn" (einem Vorgänger und einem Nachfolger) so verbunden, daß insgesamt ein großer Ring entsteht. Darauf zirkulieren die von einem Absender auf den Weg gebrachten Nachrichten nach der Grundregel, daß jede Anlage, die von einem Nachbarn eine Nachricht erhält und anhand der Empfängeradresse erkennt, daß diese Nachricht nicht für sie selbst bestimmt ist, die Nachricht wiederum an ihren (anderen) Nachbarn unverändert weiterreicht, bis die auf diese Weise von Station zu Station laufende Nachricht schließlich bei ihrem adressierten Empfänger ankommt. In jeder Zwischenstation, die eine Nachricht empfängt und weitersendet, ohne der gewünschte Empfänger zu sein, sorgt Software dafür, daß die Nachricht weder verändert noch dem Benutzer dieser Station bekannt oder sonst verarbeitet wird. Deshalb ist bei der Benutzung von Ringnetzen zu prüfen, ob unbefugte Änderungen an dieser Software bei allen beteiligten Stationen mit hinreichender Sicherheit ausgeschlossen sind.

— Bei sog. Bus-Netzen sind alle angeschlossenen Geräte fest mit einer Kommunikationsleitung

verbunden. Wer etwas an einen anderen senden möchte, gibt seine Nachricht mit der Adresse des Empfängers auf diese Leitung. Alle Geräte empfangen (praktisch gleichzeitig) die Nachricht, und die Software in den einzelnen Geräten sorgt dafür, daß jedes Gerät nur die an seine Adresse gerichteten Nachrichten speichert und weiterverarbeitet. Damit ergibt sich auch hier bei jedem angeschlossenen Gerät die Notwendigkeit, die Kommunikationssoftware gegen Manipulation zu sichern.

Die beschriebenen Risiken schließen den sinnvollen Einsatz solcher Netze keineswegs aus. Es ist aber erforderlich, die Benutzer auf die Sicherheit bzw. die verbleibenden Manipulationsmöglichkeiten hinzuweisen, damit sie selbst entscheiden können, welche Daten sie dem Netz anvertrauen wollen und welche nicht. Der Benutzer sollte also die Sicherheit des Netzes, mit dem er arbeitet, grundsätzlich einschätzen können. Das gilt auch für Verbindungen „seines" Netzes über ein öffentliches Netz mit dem lokalen Netz eines fernen Partners. Je nach der Art der zu übermittelnden Daten oder der eingeräumten Zugriffsmöglichkeit kann es wichtig sein zu wissen, welche unterschiedlich konfigurierten und damit unterschiedlich sicheren Netze an der Kommunikation beteiligt sind. Die Pflicht des Benutzers, sich von der Sicherheit des Nachrichten-Transports zu überzeugen, ist vergleichbar mit der Notwendigkeit zu entscheiden, ob eine Nachricht auf einer Postkarte, im Brief, Einschreibe-Brief oder aber durch persönlichen Kurier transportiert werden soll.

Ein Benutzer von privaten (und öffentlichen) Netzen muß deshalb gewisse Grundkenntnisse über die Sicherheit der beteiligten Netze haben, um die Übermittlung zu schützender Daten verantworten zu können.

Dabei kann es auch geboten sein, für besonders schützenswerte Nachrichten andere Transportwege anzubieten oder vorzuschreiben.

20.4 Abstrahlung

Mit der Verbreitung elektronischer Datenverarbeitungsanlagen und elektrischer Einrichtungen zum Nachrichtentransport wächst auch die Bedeutung der „Kompromittierenden Abstrahlung", also jener Signale, die ungewollt ausgesandt werden und es anderen ermöglichen, mit mehr oder minder großem Aufwand Kenntnis von den verarbeiteten oder transportierten Informationen zu erlangen. Grundsätzlich gilt nämlich, daß alles, was elektrisch (oder elektronisch) betrieben wird, auch Strahlung verursacht, und zwar strahlt es Wellen aus, die ein Abbild des aktuellen Geschehens in dieser (Teil-)Einrichtung sind. Dieses Abbild ist aber eher ein „Schattenriß" als ein getreues Ebenbild, und je nach Art des Schattens kann man daraus mehr oder minder gut auf die Aktivitäten in einer Einrichtung schließen.

Die Strahlung der einzelnen Komponenten von Datenverarbeitugssystemen ist dabei sehr unterschiedlich, und auch eine eventuelle Postzulassung oder FTZ-Prüfnummer bedeutet nur, daß das Gerät den geregelten Funkverkehr nicht stört, garantiert aber keineswegs, daß man nicht gezielt die Abstrahlung auffangen und auswerten kann.

Übertragungsmedien strahlen eine je nach Art des Mediums stärkere oder schwächere Kopie der gerade übertragenen Zeichen aus:

— Einfache Kabel, insbesondere 2-Draht-Leitungen, haben eine gut analysierbare Strahlung, die auch in einigen Metern Abstand noch verwertbar ist.

— Mehradrige Kabel mit paralleler Übertragung strahlen jeweils die Summe der Einzelübertragungen aus, die aber nur schwer in ihre Einzelteile zerlegt werden kann.

— Koaxialkabel strahlen so wenig, daß man zum Auffangen verwertbarer Signale dicht oder direkt an das Kabel herangehen muß.

— Glasfasern strahlen so wenig, daß nicht nur der umhüllende Kabelmantel abgelöst, sondern das Kabel auch noch stark gekrümmt oder die Glasfaser angerauht werden muß, damit man die transportierten Nachrichten erkennen kann.

Bei diesen Abstrahlungen bedarf es je nach dem Übertragungsmodus und der Verkehrsbündelung z. T. recht komplizierter Analysen und Umsetzungen der aufgefangenen Signale in den Nachrichtentext, so daß Abstrahlungen dieser Art außerhalb des nachrichtendienstlich relevanten Bereichs wohl kaum eine Rolle spielen. Als Abwehr bietet sich in erster Linie die Verschlüsselung der Nachrichten an, weil die Auswahl des Übertragungsmediums oft nicht oder nur sehr schwer zu beeinflussen und eine ausreichende Kontrolle der Übertragungswege kaum möglich ist. Die Datenverarbeitungsanlagen selbst strahlen entsprechend der Verarbeitung viele schwache und kaum analysierbare Impulse aus. Am deutlichsten erkennbar dürften dabei die durch Elektromotoren gesteuerten Positionierungsvorgänge beim Schreiben und beim Lesen der Speichermedien (z. B. Magnetplatten und -bänder) sein. Inhalte des Speichermediums können dadurch aber nicht erkannt werden.

Besser auswertbar sind dagegen die Abstrahlungen der Druckausgabegeräte. So „sendet" z. B. jeder Typenraddrucker Informationen über die Drehung des Typenrades, über den Anschlag und über die Positionierungsschritte einschließlich des Rücklaufs in die Zeilenanfangsstelle. Weil die Belegung der Typenräder bekannt ist (es stehen nur relativ wenige zur Wahl), kann eine Analyse der Abstrahlung den geschriebenen Text erkennen lassen. Ähnlich sind die Bedingungen bei Kugelkopfdruckern, die wie Typenraddrucker in der Textverarbeitung weit verbreitet sind. Erheblich schwieriger ist dagegen die Analyse der Abstrahlung von Ketten- und Nadeldruckern. Stets ist aber über das Auffangen der Signale hinaus eine dechiffrierende Analyse erforderlich, wodurch die tatsächliche Nutzung dieser Möglichkeiten eher unwahrscheinlich ist. Weil sie aber offenbar nicht ausgeschlossen werden kann, verbietet die Verschlußsachenanweisung in Verbin-

dung mit den ergänzenden Richtlinien die Herstellung von geheimhaltungsbedürftigen Schreiben höherer Einstufung mit Hilfe bestimmter Druckertypen.

Prinzipiell anders sind die Verhältnisse bei der Abstrahlung von Bildschirmen mit den üblichen Kathodenstrahlröhren, die in der letzten Zeit zunehmend öffentlich diskutiert wird: Das Bild auf dem Schirm wird durch das Auftreffen eines Elektronenstrahls (Strom ohne Draht) auf einem präparierten Glasschirm erzeugt, der an der Stelle leuchtet, wo der Strahl auftrifft. Der Strahl überstreicht dabei mit seinem Ende zeilenweise den Bildschirm in ständig wiederkehrender Folge, und das Bild entsteht durch das passende An- und Ausschalten des Strahls, also durch „Strom" oder „Nicht-Strom". Dieser Strom bzw. sein An- und Ausschalten strahlt genauso wie Strom in einem Draht. Wenn es gelingt, das An- und Ausschalten zu registrieren, braucht man nur den gleichen Lauf des Strahls über einen Bildschirm nachzubilden und kann dann die Informationen ablesen. Den gleichartigen Lauf des Strahls erreicht man mit einem Monitor, bei dem die Zeilenfrequenz und die Zeilenfolge genauso eingestellt werden können, wie bei dem „abzuhörenden" Schirm. Dieses Synchronisationsproblem und das Problem des Umsetzens der aufgefangenen Signale in das An- und Ausschalten des Strahls kann man schon mit handelsüblichen Schwarz-Weiß-Fernsehgeräten in der Preislage von etwa DM 300,— lösen. Die dabei auftretende Schwarz-Weiß-Umkehrung läßt sich mit wenig Materialaufwand und mit Kenntnissen aufheben, über die auch ein Elektro-Bastler verfügen kann. Nach verschiedenen Berichten über Laborversuche ist es wahrscheinlich, daß je nach den „Sendeverhältnissen" mit einer einfachen Fernsehantenne auch in Entfernungen von ca. 100 Metern mit Geduld, Fingerspitzengefühl bei der Frequenzsuche und etwas Glück brauchbare Bilder erzeugt werden können.

Was diese Art von „Abhörangriffen" eher wahrscheinlich macht als die anderen Methoden, sind insbesondere

- die vergleichsweise einfachen Mittel,
- das geringe Entdeckungsrisiko, weil z. B. in der eigenen Wohnung empfangen werden kann,
- ermutigende Anfangserfolge beim Suchen, so daß man durch genauere Einstellung schrittweise ein optimales Ergebnis erreichen kann, und
- die öffentliche Diskussion über diese Methode, die seit einem grundlegenden Vortrag auf einer Sicherheits-Fachtagung immer breiter geworden ist.

Eine wirklich durchgreifende Abwehr ist schwierig, denn gerade die Verschlüsselung ist für die Ausgabe auf dem Bildschirm nicht geeignet. Es ist allerdings möglich, schützenswerte Informationen so auf dem Bildschirm anzuzeigen, daß ihre Bedeutung nicht für jeden Außenstehenden ohne weiteres erkennbar ist, wenngleich unter solchen Maßnahmen die Benutzerfreundlichkeit leidet. Auch die Abschirmung der Geräte z. B. durch Unterbringung in einem Spezialgehäuse ist aufwendig, sie macht die Geräte unhandlich, und außerdem befinden sich die Spezialgehäuse nicht im freien Handel. Ähnlichen Beschränkungen unterliegt auch der Einsatz von speziell gefertigten Geräten, die praktisch keine Abstrahlung aufweisen. Damit bleibt nur bei der Anschaffung die Wahl von Geräten, die tendenziell weniger Abstrahlung streuen, und bei der Aufstellung die Wahl von Orten, in deren unmittelbarer Nähe keine Gelegenheit zum unbemerkten Auffangen der Abstrahlung besteht. Wo möglich, sollte man sich dieser Mittel bedienen, denn wenn der Nutzen durch „Mitlesen" eines Bildschirms auch stets auf das beschränkt ist, was gerade auf dem Schirm zu sehen ist, so kann doch der Vertrauensschaden für den Betreiber der Datenverarbeitung erheblich sein.

Langfristig gesehen dürften diese Probleme aber dadurch geringer werden, daß sehr abstrahlarme Bildschirme entwickelt werden, oder Bildschirme mit anderen Verfahren der Bilderzeugung, z. B. mit Flüssig-Kristall-Anzeige (wie bei vielen Digitaluhren) eingesetzt werden können, die von Natur aus keine so einfach verwertbaren Signale abstrahlen.

21. Novellierung des Bundesdatenschutzgesetzes

In meinem Achten Tätigkeitsbericht (S. 59) habe ich eine vorläufige und summarische Bewertung des damals noch internen Gesetzentwurfs der Fraktionen der CDU/CSU und der FDP zur Änderung des BDSG vorgenommen. Der Entwurf ist als Bestandteil des sog. Sicherheitspakets (vgl. oben 1.2) im Laufe des Berichtsjahrs von diesen Fraktionen und gleichlautend von der Bundesregierung in den Deutschen Bundestag eingebracht worden. Außer einer eingehenden Anhörung von Sachverständigen, zu denen auch ich gehörte, am 21. April 1986 hat eine parlamentarische Beratung des Entwurfs nicht stattgefunden. Der Entwurf soll in der nächsten Legislaturperiode wieder in den Bundestag eingebracht werden. Ob dies in unveränderter Form geschieht, läßt sich noch nicht absehen, zumal nicht auszuschließen ist, daß sich die inzwischen fortentwickelte Datenschutzgesetzgebung in den Ländern auch auf die Bundesgesetzgebung auswirkt. Im gegenwärtigen Zeitpunkt erscheint es somit nicht angebracht, zu allen Einzelheiten des vorliegenden Gesetzentwurfs zur Novellierung des BDSG Stellung zu nehmen. Die nachfolgenden Bemerkungen beschränken sich deshalb auf Regelungsgegenstände, denen ich eine herausgehobene Bedeutung beimesse.

21.1 Anwendungsbereich

Nach dem Volkszählungsurteil des Bundesverfassungsgerichts gilt das Recht auf informationelle Selbstbestimmung für jeden Umgang mit personenbezogenen Daten, also auch für ihre Verarbeitung

außerhalb von Dateien. Insofern erweitert sich der datenschutzrechtliche Regelungsbedarf über den bisherigen Anwendungsbereich des BDSG hinaus. Es hätte nahegelegen, ähnlich dem Regelungsumfang des kürzlich verabschiedeten neuen hessischen Datenschutzgesetzes, die Datenverarbeitung außerhalb von Dateien in das BDSG einzubeziehen. Dies ist jedoch nicht vorgesehen, vielmehr soll der *Datenschutz für die Verarbeitung und Nutzung außerhalb von Dateien im Verwaltungsverfahrensgesetz* geregelt werden, für das ebenfalls ein Änderungsentwurf vorgelegt wurde. Dies hat zur Folge, daß wesentliche Verwaltungsbereiche den Schutzvorschriften nicht unterliegen, weil das Verwaltungsverfahrensgesetz u. a. in der Finanzverwaltung, bei der Post, bei der Verfolgung von Straftaten und Ordnungswidrigkeiten und in weiten Bereichen der Sozialverwaltung nicht gilt (§ 2 Abs. 2 und 3 VwVfG). Eine Einbeziehung der Datenverarbeitung außerhalb von Dateien in das umfassend geltende BDSG würde diese Schwierigkeiten beseitigen und zugleich zur Rechtsvereinheitlichung beitragen. Daß eine solche Zusammenfassung außerdem der Rechtsvereinfachung dienen würde, ergibt sich daraus, daß verschiedene Vorschriften in beiden Gesetzentwürfen im Wortlaut übereinstimmen. Dabei ist zu bedenken, daß die Ausweitung der automatisierten Datenverarbeitung in den Behörden, ihre Verlagerung an den Arbeitsplatz und der zunehmende Einsatz der Textverarbeitung dazu führen, daß die verschiedenen Formen der Datenverarbeitung einschließlich herkömmlicher Aktenbearbeitung mehr und mehr ineinander übergehen und die Unterschiede immer geringer werden. Es bedeutet aber eine erhebliche Erschwernis für den Verwaltungsvollzug, auf materiell gleiche Verwaltungsvorgänge unterschiedliche Vorschriften anwenden und diese auch noch verschiedenen Gesetzen entnehmen zu müssen.

Die Aufteilung der Rechtsmaterie auf zwei Gesetze halte ich auch aus rechtssystematischen Gründen für verfehlt. Spätestens seit dem Volkszählungsurteil des Bundesverfassungsgerichts steht fest, daß sich Datenschutzregelungen nicht in formalen Handlungsanweisungen an die Verwaltung erschöpfen, sondern als materiellrechtliche Ausformung des allgemeinen Persönlichkeitsrechts verstanden werden müssen. Während es für das Verwaltungsverfahrensrecht typisch ist, nur die Art und Weise der Ausführung von Gesetzen zu bestimmen, regelt das Datenschutzrecht eigenständig und inhaltlich die Informationsbeziehungen des Bürgers zum Staat im Sinne einer Legitimation staatlicher Eingriffsbefugnisse. Auch wegen dieser Unterschiedlichkeit im Regelungsansatz sollte das Datenschutzrecht einheitlich im BDSG geregelt und nicht mit den Regelungen im VwVfG vermengt werden.

Die Sonderregelung für die Informationsverarbeitung außerhalb von Dateien im VwVfG führt im übrigen zu Konsequenzen, die aus der Sicht des Datenschutzes zu kritisieren sind:

Die Regelungen im VwVfG weichen in manchen Punkten von den Zulässigkeitsvorschriften des BDSG auch dann ab, wenn dies durch die Verarbeitungsform außerhalb von Dateien keineswegs geboten ist. So wird das im BDSG bewährte Erforderlichkeitsprinzip z. B. bei Datenübermittlungen nach dem VwVfG ohne Not verlassen. Die Grundsätze der §§ 10, 11 BDSG sind indessen auch für die Informationsverarbeitung in Akten durchaus angemessen; das Problem, daß erforderliche Daten von nicht erforderlichen zuweilen nicht abtrennbar sind, ließe sich durch Sonderregelungen lösen.

Die Einhaltung der Vorschriften des VwVfG ist der Datenschutzkontrolle grundsätzlich entzogen, es sei denn, daß Anhaltspunkte für eine Rechtsverletzung (§ 19 Abs. 1 E-BDSG) vorliegen. Für die nur noch im VwVfG geregelte Datenerhebung würde aber auch diese Ausnahme nicht gelten (siehe unten 21.4).

Ungeachtet der stärker als im geltenden Recht vorgesehenen *Beschränkung des BDSG auf die Datenverarbeitung in Dateien*, die u. a. auch in der Bezeichnung und der Zieldefinition des Gesetzentwurfs zum Ausdruck kommt, ist auch die Neufassung des Dateibegriffs zu kritisieren. Sie ignoriert völlig die Technik der Bildverarbeitung, die zunehmend in der Form von Videoaufzeichnungen z. B. zum Zweck der Überwachung sicherheitsgefährdeter Objekte oder der Kontrolle von Produktionsvorgängen oder Verkehrsströmen angewendet wird. Hier fehlen Regelungen über die Eingriffe in das Persönlichkeitsrecht der Personen, deren Bilder aus solchen Anlässen gezielt oder zufällig aufgenommen, gespeichert und nach Bedarf verwertet werden.

Die zunehmenden Möglichkeiten der Vernetzung werden nur insoweit berücksichtigt, als durch neue Bedingungen für Online-Anschlüsse der Zulässigkeitsrahmen für Vernetzungen erweitert wird. Es fehlen jedoch Vorschriften über eine angemessene Transparenz für die datenverarbeitenden Stellen und über die Kontrollierbarkeit der tatsächlichen Nutzung der Verfahren, die insbesondere geboten ist, wenn die Vernetzung mittels Wählverbindungen über öffentliche (weltweite) Netze erfolgt.

Die wachsende Verbreitung preiswerter und leicht zu handhabender *Personal Computer (PC)* wird nur insoweit berücksichtigt, als die damit vermehrt mögliche Datenverarbeitung für private Zwecke natürlicher Personen von allen Beschränkungen dieses Gesetzes ausgenommen ist. Es fehlen jedoch Vorschriften, die den besonderen Risiken des Einsatzes von PC im öffentlichen Bereich Rechnung tragen. Diese Risiken bestehen darin, daß viele erprobte Prinzipien zur Gewährleistung des Datenschutzes — wie z. B. Vier-Augenprinzip, Funktionentrennung, kontrolliertes Auftragsverfahren, Programmfreigabe durch die Fachabteilung — beim Einsatz von PC entfallen, da sie nur im Zusammenwirken zwischen Aufgabenträger und Rechenzentrum realisiert werden können. Eine Sicherung gegen unbefugte Datenverarbeitung kann hier in erster Linie nur durch stärkere interne Kontrollen und Überwachungsmaßnahmen erfolgen.

21.2 Zweckbestimmung

Die Zweckbestimmung personenbezogener Daten hat das Bundesverfassungsgericht als tragendes

Prinzip des Datenschutzes hervorgehoben. Es stellt fest, daß ein Gesetz den Verwendungszweck bereichsspezifisch und präzise zu bestimmen hat und die Verwendung der Daten auf diesen Zweck begrenzt ist. Aus dem Leitsatz des Volkszählungsurteils, daß bei der Datenerhebung für statistische Zwecke eine enge und konkrete Zweckbindung nicht verlangt werden kann, folgt zweierlei: Außerhalb der Statistik besteht in der Regel eine enge und konkrete Zweckbindung, und die Zweckbestimmung ist auch auf die Datenerhebung bezogen. Das bedeutet, daß der Zweck — sofern die bereichsspezifische Erhebungsvorschrift ihn nicht konkret nennt — bei der Datenerhebung feststehen und dokumentiert sein muß, damit seine Einhaltung kontrolliert und die Zulässigkeit von Zweckänderungen daran gemessen werden kann. Wenn § 9 Abs. 1 E-BDSG die Datenspeicherung (und -veränderung) nur für „bestimmte" Zwecke zuläßt, so wird das Zweckbindungsprinzip nur unzureichend geregelt, weil unklar bleibt, wie diese Zwecke bestimmt und transparent gemacht werden. Das Fehlen einer Datenerhebungsvorschrift wirkt sich hier besonders nachteilig aus, weil nach meiner Auffassung dort die Pflicht zur Zweckfestlegung vorgeschrieben werden müßte.

Die Voraussetzungen für eine Zweckänderung in § 9 Abs. 2 Satz 3 E-BDSG sind sehr weit formuliert. Es handelt sich zum Teil um Verwendungszwecke, mit denen der Betroffene nicht ohne weiteres rechnen wird. Mit Rücksicht auf die Aufklärungspflichten, die das Bundesverfassungsgericht als verfahrensrechtliche Schutzvorkehrungen gefordert hat („jeder muß wissen können, wer was wann und bei welcher Gelegenheit über ihn weiß"), halte ich es deshalb für erforderlich, daß bei Zweckänderungen, die insbesondere bei Übermittlungen vorkommen, der Betroffene benachrichtigt wird. Eine solche Benachrichtigungspflicht kann generell im BDSG vorgeschrieben werden. Eine vergleichbare Unterrichtungspflicht ist in § 11 Abs. 2 Satz 1 E-BDSG für gewisse Datenübermittlungen an Stellen außerhalb des öffentlichen Bereichs bereits vorgesehen.

Für problematisch halte ich es auch, daß § 10 Abs. 5 Satz 2 E-BDSG auch vom Übermittlungszweck abweichende Nutzungen ermöglicht, nachdem der ursprüngliche Verwendungszweck bereits durch die Übermittlung durchbrochen ist. Ebenso sind Weiterübermittlungen durch den Datenempfänger an Dritte bedenklich, sofern damit wiederum Zweckänderungen verbunden sind. Wenn man solche beliebig oft zuließe, würde das Prinzip der Bindung an den ursprünglichen Datenerhebungszweck praktisch völlig aufgehoben, und von einer Transparenz für den Betroffenen könnte keine Rede mehr sein.

Die Regelungen im nicht-öffentlichen Bereich über Zweckbindung und Zweckänderungen sind wenig aussagekräftig. Sie geben dem Betroffenen keine Grundlage, um abschätzen zu können, wer wann was bei welcher Gelegenheit über ihn weiß. Es fehlt auch hier an einer Aussage, wie konkret und in welchem Verfahren der Zweck einer Datenspeicherung festgelegt und nachprüfbar dokumentiert werden soll. Weiterhin fehlt es an einer allgemeinen Zweckbindungsregel, die die weitere Nutzung und insbesondere Übermittlung davon abhängig macht, daß sie vom festgelegten Zweck abgedeckt ist. Eine Zweckbindung nur beim Übermittlungsempfänger genügt nicht. Mit dem Grundgedanken der Zweckbindung ist eine generalklauselartige Erlaubnis, die Daten auch für andere Zwecke zu verwenden, unvereinbar, so die vorgesehene Vorschrift des § 24 Abs. 3 Satz 2 E-BDSG, wonach eine Zweckänderung lediglich davon abhängig ist, daß kein Grund zur Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden.

21.3 Transparenz

Die Unentgeltlichkeit der Auskunft und die Erweiterung des Auskunftsanspruchs auf Herkunft und Empfänger sowie — allerdings nur im öffentlichen Bereich — auf den Zweck der Speicherung entsprechen dem Ziel, den Betroffenen darüber zu informieren, wer wann was bei welcher Gelegenheit über ihn weiß. Dieses Ziel wird kaum erreicht, wenn der Auskunftsanspruch der Betroffenen davon abhängig ist, ob die speichernde Stelle die Angaben über Herkunft und Empfänger in einer Datei speichert, und ob diese Angaben dort „zu seiner Person" gespeichert sind. Hierbei handelt es sich um Organisationsfragen, deren Regelung vollständig im Belieben der speichernden Stelle liegt. Ein Anspruch des Betroffenen auf Bekanntgabe von Herkunft und Empfängern sollte deshalb in jedem Fall normiert werden. Eine Notwendigkeit, diese Angaben festzuhalten, besteht für die speichernde Stelle ohnehin, weil anderenfalls die Zulässigkeit und Richtigkeit der Verarbeitung durch die Aufsichtsbehörden nicht nachprüfbar ist.

Das pauschale Auskunftsverweigerungsrecht für die Verfassungsschutzbehörden, den BND, den MAD und teilweise den BMVg ist weder sachlich geboten noch im Hinblick auf Artikel 19 Abs. 4 GG rechtlich vertretbar. Die Interessen dieser Behörden können durch eine Auskunftsregelung gewahrt werden, wie sie beispielsweise für Polizei und Staatsanwaltschaft vorgesehen ist, d. h. durch eine Abwägung des Interesses des Betroffenen an der Auskunftserteilung gegen die Geheimhaltungsinteressen der Behörden. Eine solche Regelung hat sich im Polizeibereich, wo sie schon praktiziert wird, bewährt.

Bei der Auskunftsverweigerung halte ich es auch nicht für angemessen, daß die Nachrichtendienste generell von der Begründungspflicht ausgenommen werden, wie dies im Gesetzentwurf vorgesehen ist. Denn zwischenzeitlich haben einige Gerichte einen Anspruch zumindest auf eine Ermessensentscheidung mit der Pflicht zur Begründung einer Auskunftsverweigerung anerkannt.

Bei der für den nicht-öffentlichen Bereich vorgesehenen Auskunftsregelung ist zu kritisieren, daß die Auskunft nicht den Zweck der Datenspeicherung umfassen soll. Auch erscheint es nicht gerechtfertigt, aus allgemein zugänglichen Quellen entnommene Daten von der Auskunft an den Betroffenen

auszunehmen. Dessen Informationsinteresse zielt gerade auf eine vollständige Information, da er die Entscheidungsgrundlagen der speichernden Stelle kennenlernen und deren Richtigkeit und Aktualität überprüfen möchte. Die Ausnahmevorschrift würde zu einer deutlichen Verunsicherung der Betroffenen führen, andererseits aber der speichernden Stelle kaum etwas bringen.

21.4 Kontrolle

Die Kontrollbefugnis des BfD soll nach der Begründung des Entwurfs ausgeweitet werden. Gemessen an der gegenwärtigen Kontrollpraxis ist diese Ausweitung minimal, für bestimmte Bereiche dürfte die Neuregelung sogar zu einer Verengung der Kontrollmöglichkeiten führen.

Bisher ergaben sich bei der Kontrolle der Einhaltung von Datenschutzvorschriften außerhalb des BDSG, wenn die Verarbeitung nicht in Dateien erfolgte, kaum Schwierigkeiten. Das gilt für die meisten Geheimhaltungsvorschriften, so insbesondere für das Sozialgeheimnis und die Offenbarungsbeschränkungen des SGB X, die auch für personenbezogene Sozialdaten gelten, die nicht in Dateien gespeichert sind. Hier habe ich bei den Leistungsträgern, die teilweise in großem Umfang personenbezogene Daten verarbeiten, z. B. bei der Arbeitsverwaltung, stets ungehindert systematische Kontrollen auch ohne besonderen Anlaß durchführen können. In Zukunft würde dies nach § 19 Abs. 1 Nr. 2 E-BDSG nur noch möglich sein, wenn der Betroffene hinreichende Anhaltspunkte dafür darlegt, daß er in seinen Rechten verletzt worden ist, oder dem BfD solche Anhaltspunkte bekannt sind. Schon die Forderung nach hinreichenden Anhaltspunkten, die für den Betroffenen angesichts der für ihn oft undurchschaubaren Datenverarbeitung nur schwer zu gewinnen sind, kann Anlaß zu Auseinandersetzungen mit der datenverarbeitenden Stelle geben. Das gilt auch für die weitere Einschränkung, daß die Kontrolle in solchen Fällen nur auf den Einzelfall beschränkt ist. Es ist unklar, ob dies bedeuten soll, daß beispielsweise bei Aktenfunden auf dem Müllplatz die Kontrolle nur auf diese konkreten Unterlagen beschränkt ist oder ob sie die Organisation der Aktenvernichtung insgesamt bei der betreffenden Stelle umfassen darf. Auf die Aktenverwaltung bezogene Datensicherungsmaßnahmen, die ich in der Vergangenheit nicht nur vereinzelt, sondern sehr häufig aus begründetem Anlaß vorgeschlagen habe und auch durchsetzen konnte, dürften in Zukunft ebenfalls nicht mehr Gegenstand von Empfehlungen sein, selbst wenn diesbezüglich einzelne Beschwerden Betroffener vorliegen. Die mit der modernen Bürotechnik immer stärker werdende Verflechtung zwischen den verschiedenen Formen der Datenverarbeitung macht den Dateibegriff ohnehin zunehmend fragwürdiger; ihn nunmehr auch in der vorgesehenen Weise für eine Beschränkung der Datenschutzkontrolle zu benutzen, halte ich für verfehlt, zumal das Bundesverfassungsgericht die von ihm hervorgehobene Bedeutung der Datenschutzkontrolle nicht vom Vorhandensein einer Datei abhängig gemacht hat.

Die Beschränkungen des § 19 Abs. 1 Nr. 1 und 2 E-BDSG sind auch aus einem anderen Grund abzulehnen. Die Datenerhebung, die den Bürger viel stärker als die ohne sein Zutun und häufig ohne sein Wissen ablaufende Datenverarbeitung berührt und bei der er tatsächlich sein informationelles Selbstbstimmungsrecht ausüben kann, würde künftig nicht mehr der Datenschutzkontrolle unterliegen, weil sie nicht mehr im BDSG, sondern nur noch im VwVfG geregelt werden soll. Datenschutzvorschriften außerhalb des BDSG sollen aber nur noch kontrollierbar sein, wenn sie die Verarbeitung oder Nutzung personenbezogener Daten betreffen. Die Datenerhebung gehört dazu nicht. Damit kann weder durchgesetzt werden, daß die vorgesehenen Hinweispflichten beachtet werden, noch können — wie bisher häufig mit Erfolg praktiziert — für Erhebungsformulare und die sonstigen Umstände einer Datenerhebung datenschutzgerechte Vorschläge gemacht werden. Ich halte dies im Interesse des Bürgers nicht für vertretbar.

Ich kann nicht abschätzen, welche Konsequenzen sich aus der in § 19 Abs. 1 enthaltenen Formulierung ergeben, daß der BfD seine Kontrolle unbeschadet der fachlichen Beurteilung und Verantwortlichkeit der speichernden Stelle ausübt. Nach der Begründung zum Gesetzentwurf soll dies zwar keine Einschränkung der Kontrollbefugnisse des BfD bedeuten, jedoch die Kontrolle der „rechtsfehlerfreien fachlichen Beurteilung" der zuständigen Stelle ausschließen. Datenschutzkontrolle kommt indessen ohne eine zumindest ansatzweise Betrachtung der Fachaufgabe nicht aus. Das tragende Prinzip des Datenschutzrechts ist die Erforderlichkeit der Datenverarbeitung zur rechtmäßigen Aufgabenerfüllung. Damit ist die rechtmäßige Aufgabenerfüllung der entscheidende Prüfungsmaßstab für die Zulässigkeit einer Datenverarbeitung. Wenn sie aus der Kontrolle ausgeklammert wird, würde sich diese auf rein formale, quantitative Aspekte eines behaupteten Datenbedarfs beschränken. Das kann m. E. nicht gewollt sein, auch weil es der vom Bundesverfassungsgericht den Datenschutzbeauftragten zugewiesenen Aufgabe, „im Interesse eines vorgezogenen Rechtsschutzes" tätig zu werden, nicht entspräche. Es ist selbstverständlich, daß der BfD nicht die Erfüllung jeder Fachaufgabe der von ihm kontrollierten Behörden und öffentlichen Stellen in allen Punkten nachvollziehen kann, um ihre Rechtmäßigkeit festzustellen und daran die Datenverarbeitung zu messen. Aber es muß ihm zumindest möglich sein, sich die Rechtmäßigkeit und die sonstigen Kriterien einer Verwaltungsentscheidung plausibel darlegen zu lassen und sich mit der zuständigen Stelle im Dialog darüber kritisch auseinanderzusetzen.

Es ist zu begrüßen, daß § 19 Abs. 5 E-BDSG bestimmt, daß grundsätzlich Berufs- oder besondere Amtsgeheimnisse der Datenschutzkontrolle nicht entgegengehalten werden können. Verfehlt scheint mir jedoch zunächst die Einschränkung, daß personenbezogene Daten, die der Kontrolle durch die Kommission nach § 9 des G 10 unterliegen, der Datenschutzkontrolle entzogen sind. Es geht dabei nicht um die Kontrolle der Überwachungsmaß-

nahme selbst, sondern um die weitere Verarbeitung der auf diese Weise gewonnenen Daten — möglicherweise bei Stellen, denen die Daten übermittelt worden sind. Das Bundesverfassungsgericht hat in seinem Beschluß vom 20. Juni 1984 Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses ausdrücklich nur unter der Voraussetzung für zulässig erklärt, daß eine Kontrolle durch die Datenschutzbeauftragten stattfindet. M. E. ist es deshalb schon unter verfassungsrechtlichen Aspekten nicht angängig, personenbezogene Daten dieser Art aus der Datenschutzkontrolle auszunehmen.

Das in § 19 Abs. 5 Nr. 3 E-BDSG in bestimmten Fällen vorgesehene Widerspruchsrecht gegen eine Kontrolle durch den BfD halte ich für problematisch. Selbstverständlich würde ich eine Kontrolle der Verarbeitung personenbezogener Daten eines Betroffenen, der Einsicht in seine Daten ausdrücklich ablehnt, nicht vornehmen und sein auch insoweit bestehendes Recht auf informationelle Selbstbestimmung respektieren. Die Institutionalisierung eines Widerspruchsrechts hielte ich allerdings deshalb für bedenklich, weil sich die datenschutzrechtliche Kontrolle nach § 19 Abs. 1 E-BDSG auf die Rechtmäßigkeit der Datenverarbeitung generell bezieht, ohne daß es insoweit darauf ankommt, ob durch eine Verletzung datenschutzrechtlicher Vorschriften auch das informationelle Selbstbestimmungsrecht eines einzelnen verletzt worden ist. Eine Regelung, daß datenschutzrechtliche Kontrolle nur insoweit möglich ist, als ihr der einzelne nicht widerspricht, führte daher wohl im Ergebnis zu einer anderen Qualität des Datenschutzes. Abgesehen von diesen grundsätzlichen Erwägungen wird in der vorgesehenen Bestimmung nicht geklärt, auf welche praktikable Weise dem Betroffenen Gelegenheit gegeben werden soll, von seinem Widerspruchsrecht Gebrauch zu machen. Ich würde es für verfehlt halten, wenn eine angekündigte Kontrolle zuvor allen Betroffenen bekanntgemacht werden müßte, um ihnen diese Gelegenheit zu verschaffen; abgesehen davon ist bei vielen datenverarbeitenden Stellen im Bereich des Bundes der Kreis der Betroffenen sehr groß. Eine besondere Anfrage bei den Betroffenen würde auf eine Einwilligung hinauslaufen, die auch vom Gesetzentwurf nicht gefordert wird. Schließlich könnte eine Datenschutzkontrolle verhindert werden, indem man die Betroffenen, z. B. Mitarbeiter, dazu veranlaßt, Widerspruch zu erheben, auch wenn diese daran gar kein persönliches Interesse haben.

Insbesondere im Falle der automatisierten Datenverarbeitung dürfte es praktische Schwierigkeiten bereiten, Datenträger mit einer Vielzahl personenbezogener Daten inhaltlich zu kontrollieren und dabei die Daten einiger weniger Betroffener, die Widerspruch erhoben haben, auszunehmen. Das Widerspruchsrecht darf aber nicht dazu führen, systematische Datenschutzkontrollen gänzlich unmöglich zu machen. Es sollte sich deshalb allenfalls auf solche Kontrollen beschränken, die gezielt zu bestimmten Personen vorgenommen werden.

Wie ich bereits in früheren Stellungnahmen ausgeführt habe, halte ich es für notwendig, daß der BfD über die Planung zum Aufbau oder zur wesentlichen Änderung automatisierter Informationssysteme, in denen personenbezogene Daten verarbeitet werden (sollen), so rechtzeitig unterrichtet wird, daß er darauf im Wege der Beratung noch Einfluß nehmen kann. Die Meldungen zum Dateienregister kommen dazu in der Regel zu spät. Ähnliches sollte für Gesetzgebungsvorhaben bzw. den Erlaß sonstiger Rechtsvorschriften gelten, die den Datenschutz berühren. Auch hier lehrt die Erfahrung, daß eine Einschaltung des BfD erst *nach* einem Kabinettbeschluß die Durchsetzung datenschutzrechtlicher Verbesserungen erheblich erschwert.

Ich hoffe, daß in den nach Wiedereinbringung des Gesetzentwurfs zur Änderung des BDSG anlaufenden parlamentarischen Beratungen Gelegenheit besteht, diese Kritikpunkte zu vertiefen und auch noch zu anderen Neuregelungen Stellung zu nehmen.

22. Ausland und Internationales

22.1 Europarat

Die Datenschutzkonvention des Europarats wurde mittlerweile von elf Ländern signiert. Die Zahl der Ratifikationen liegt weiterhin bei fünf; eine Ratifikation durch die Länder Dänemark, Luxemburg und Österreich wird erwartet. Das nach der Datenschutzkonvention zu bildende Beratende Komitee hat sich konstituiert. Es hat die Absicht geäußert, auch Nicht-Mitgliedstaaten zu beraten. Bekanntlich steht es auch dem Europarat nicht angehörenden Staaten frei, der Konvention beizutreten.

Die parlamentarische Versammlung des Europarates hat das Ministerkomitee aufgefordert, die wechselseitigen Bezüge des Datenschutzes und des freien Informationszugangs (freedom of information) zu untersuchen.

Im Expertenkomitee Datenschutz wurde die Beratung von Empfehlungen für die Sektoren Polizei, Arbeit und Technologie fortgesetzt. Das Komitee will sich danach den Problembereichen Chip-Karte, automatisierter Zahlungsverkehr und Verarbeitung von Daten über genetische Analysen zuwenden.

22.2 Entwicklung des Datenschutzes im Ausland

Auch außerhalb der Bundesrepublik Deutschland findet der Datenschutz weiterhin zunehmende Bedeutung. In den Ländern, die ein Datenschutzgesetz besitzen, wird die Praxis intensiv beobachtet, mit der Konsequenz, daß Lücken und Schwachstellen aufgedeckt und Verbesserungsvorschläge entwickelt werden. Dies führt in vielen Ländern zu besseren Datenschutzrechten für die Bürger, sei es daß die gesetzlichen Instrumente verfeinert, sei es daß der Anwendungsbereich der Datenschutzgesetze erweitert wird.

So hat beispielsweise der österreichische Bürger künftig Anspruch auf jährlich eine kostenlose Aus-

kunft über die ihn betreffenden Daten. In Kanada wurde vorgeschlagen, den privacy act auf staatliche Unternehmen, die im Wettbewerb stehen, wie etwa Air Canada, auszuweiten. In Dänemark soll der Betroffene Anspruch auf periodische Auskünfte erhalten; der Adressenhandel soll eingeschränkt werden. In Frankreich wurde die Verwendung der Sozialversicherungsnummer durch Arbeitgeber und Steuerverwaltung eingeschränkt bzw. untersagt. Island hat eine spezielle Gesetzesbestimmung für die Markt- und Meinungsforschung erlassen. In den Niederlanden wurde ein Datenschutzgesetzentwurf parlamentarisch eingebracht. In Norwegen sollen die Betreiber von Kreditinformationssystemen künftig dem Betroffenen auch Datenempfänger und Datenquelle benennen; die Datenschutzkommission soll das Recht erhalten, bestimmte Maßnahmen zur Datensicherheit und zur Datenqualität verbindlich vorzuschreiben. In Portugal hat der Justizminister einen Gesetzentwurf vorgelegt. In Schweden soll die Datenschutzbehörde durch Verwaltungsvereinfachung und EDV-Einsatz effektiver gemacht werden. In der Schweiz hat jetzt etwa die Hälfte der Kantone ein Datenschutzgesetz. In Großbritannien werden Verhaltensgrundsätze (codes of practice) für die Sektoren Polizei und Direktwerbung vorbereitet. Außereuropäische Länder, wie beispielsweise Argentinien, Japan und Australien, interessieren sich verstärkt für die europäischen Erfahrungen. Dies äußert sich für meine Dienststelle in Form von Anfragen und Besuchen von Regierungsdelegationen, Wissenschaftlern und Journalisten.

Wenn sich im abgelaufenen Jahr die Zahl der Länder mit einem nationalen Datenschutzgesetz nicht vergrößert hat, so liegt dies keineswegs an nachlassendem Interesse, sondern — eher im Gegenteil — an allzu hohen Ansprüchen. Natürlich sind die Länder, die den Datenschutz jetzt erst in Angriff nehmen, bemüht, aus den vorhandenen Erfahrungen zu lernen und direkt auf dem heute erreichten hohen Niveau einzusteigen. Diese begrüßenswerte Absicht hat offensichtlich in verschiedenen Ländern zu Rückschlägen geführt, und es zeichnet sich ab, daß ein schrittweises Vorgehen vielleicht doch mehr Erfolg verspricht, auch wenn dabei in Kauf genommen werden muß, daß manche Erfahrungen in jedem Land aufs neue gemacht werden müssen.

22.3 Zusammenarbeit der Datenschutz-Kontrollinstitutionen

Die Internationale Datenschutzkonferenz, die im September in Portugal stattfand, hatte folgende thematischen Schwerpunkte:

— Medizin/Forschung/Statistik,

— neue Technologien,

— maschinenlesbare Ausweise und Karten,

— Kreditinformation,

— öffentliche Sicherheit.

Die deutsche Delegation, der auch Ländervertreter angehörten, hat vier Fachvorträge zum Programm beigetragen.

23. Bilanz

In meinem Achten Tätigkeitsbericht habe ich über mehrere Datenschutzfragen berichtet, für die damals noch keine Lösung erreicht war. Wie die nachfolgende Aufstellung zeigt, war die weitere Entwicklung bei den verschiedenen Problemen sehr unterschiedlich. Zu vielen Punkten konnten gemeinsam mit den jeweils zuständigen Stellen gute oder zumindest tragbare Lösungen gefunden werden. Für einige Fragen, darunter auch für solche, die schon seit vielen Jahren in den Fachgremien diskutiert werden, stehen Lösungen noch aus, und zu einigen Problemen ist es mir nicht gelungen, eine nach meiner Auffassung gebotene Änderung der Praxis zu erreichen.

1. Zu einigen Punkten der Entwürfe eines Personalausweisgesetzes und eines Paßgesetzes habe ich Bedenken angemeldet (8. TB S. 8 f.). Die jetzt beschlossenen Gesetze tragen meinen Bedenken zum Teil Rechnung; siehe dazu Nr. 3.1 in diesem Bericht.

2. Für die Übermittlung der Daten von Beschäftigten im öffentlichen Dienst, die als Wahlhelfer geeignet erscheinen, an die örtlichen Wahlleiter habe ich eine Regelung durch Rechtsnorm angeregt (8. TB S. 11). Der Bundesminister des Innern ist meiner Anregung deswegen nicht gefolgt, weil nach seiner Kenntnis auch ohne die Übermittlung dieser Daten ausreichend viele Wahlhelfer gewonnen werden können; siehe dazu Nr. 3.4 in diesem Bericht.

3. Um im Fall einer Personenverwechslung oder sonst unrichtigen Auskunft durch das Bundeszentralregister den entstandenen Schaden möglichst eng zu begrenzen, habe ich empfohlen, hierfür auch die Protokolle über erteilte Auskünfte zu nutzen, solange diese zur Verfügung stehen (8. TB S. 12). Das Bundeszentralregister ist meiner Empfehlung gefolgt.

4. Zur Neuregelung des Verfahrens bei den Mitteilungen in Zivilsachen habe ich über meine Lösungsvorschläge zu verschiedenen Punkten berichtet (8. TB S. 12). Die Diskussion hierüber ist noch nicht abgeschlossen; siehe dazu Nr. 4.1 in diesem Bericht.

5. Zu einem Entwurf des Bundesministers der Justiz für die Neuregelung des Schuldnerverzeichnisses habe ich Empfehlungen gegeben (8. TB S. 12 f.). Der Bundesminister der Justiz hat seinen Entwurf zurückgezogen, weil er sowohl bei den Datenschutzbeauftragten als auch bei der Wirtschaft auf Kritik gestoßen ist; eine Lösung halte ich nach wie vor für dringlich.

6. Über intensive Beratungen der Datenschutzfragen des neuen Baugesetzbuches habe ich berichtet (8. TB S. 13). Der Bundesminister für

Raumordnung, Bauwesen und Städtebau hat einen wesentlichen Teil meiner Anregungen aufgegriffen, die auch vom Deutschen Bundestag beschlossen wurden; siehe dazu Nr. 6.1 in diesem Bericht.

7. Auf die Notwendigkeit, ein umfassendes Datenschutzkonzept zu erarbeiten, bevor die Verarbeitung von Personaldaten auf dezentralen Datenverarbeitungsanlagen bei der Deutschen Bundesbahn beschlossen und eingeführt wird, habe ich hingewiesen (8. TB S. 17 f.). Die Deutsche Bundesbahn hat inzwischen ein geeignetes Konzept erstellt; siehe dazu Nr. 7.2.1 in diesem Bericht.

8. Ich habe bedauert, daß Informationen aus dem Bereich der Deutschen Bundespost über neue automatisierte Verarbeitungen personenbezogener Daten bei mir oft verspätet eingehen und auch unzureichend sind (8. TB S. 19). Eine generelle Verbesserung des Informationsverhaltens der Post mir gegenüber ist nicht festzustellen; siehe dazu Nr. 8.1 in diesem Bericht.

9. Für das Verfahren, mit dem durch Fangschaltungen oder ähnliche Aufzeichnungen bei der Post belästigende Anrufer festgestellt werden sollen, habe ich mehr Transparenz gefordert (8. TB S. 22). Die Deutsche Bundespost hat die gebotenen Änderungen abgelehnt und auch in die neue Telekommunikationsordnung keine entsprechenden Verbesserungen aufgenommen; siehe dazu Nr. 8.2 in diesem Bericht.

10. Für die werbliche Nutzung der Telefonkundenanschriften habe ich Maßnahmen angeregt, mit denen der Widerspruch des Betroffenen schneller berücksichtigt werden soll (8. TB S. 22 f.). Durch eine Neuregelung des Verfahrens hat es der Bundesminister für das Post- und Fernmeldewesen ermöglicht, daß nicht mehr zu verwendende Anschriften schneller gesperrt werden.

11. Der Deutschen Bundespost habe ich empfohlen, nur dann eine Anschrift an die Deutsche Postreklame zur werblichen Verwendung weiterzugeben, wenn der Betroffene dem ausdrücklich zugestimmt hat (8. TB S. 23). Die jetzt zunächst schwerpunktmäßig verwendeten neuen Auftragsformulare machen die Weitergabe zwar nicht von der Zustimmung abhängig, sie weisen aber wesentlich deutlicher als bisher auf die beabsichtigte werbemäßige Nutzung und auf die Möglichkeit hin, ihr zu widersprechen.

12. Über meine Bedenken gegen die Erhebung der Berufs- und Gewerbeangaben bei der Kraftfahrzeug-Zulassung habe ich berichtet (8. TB S. 24). Im Rahmen der Beratung des Gesetzentwurfs zur Änderung des Straßenverkehrsgesetzes (ZEVIS) wurde erreicht, daß in Zukunft nur die Berufs- und Gewerbeangaben der Selbständigen erhoben und gespeichert werden. Die Gespräche mit dem Bundesminister für Verkehr über den Umfang der erforderlichen Daten aus der Kraftfahrzeug-Zulassung für Maßnahmen nach dem Bundesleistungsgesetz und dem Verkehrssicherstellungsgesetz werden fortgeführt.

13. Zu der im Handelsstatistikgesetz nicht vorgesehenen Übermittlung der Steuernummern der betroffenen Unternehmen von den Finanzbehörden an die Statistischen Landesämter habe ich Bedenken angemeldet (8. TB S. 28). Meine Prüfung hat ergeben, daß die Übermittlung unzulässig war, der Schaden aber gering blieb, weil die Steuernummern bei den Statistischen Landesämtern bald wieder gelöscht wurden; siehe dazu Nr. 10.5 in diesem Bericht.

14. Auf verschiedene datenschutzrechtliche Defizite im Entwurf der Neufassung des Bundesstatistikgesetzes habe ich hingewiesen (8. TB S. 28). Der Deutsche Bundestag ist bei der Verabschiedung dieses Gesetzes meinen Bedenken nur zum Teil gefolgt; siehe dazu Nr. 10.1 in diesem Bericht.

15. Zu den Regelungen über die geplante Verwendung der Rentenversicherungsnummer durch Sozialleistungsträger und durch außerhalb dieses Bereichs tätige Stellen und Personen habe ich Klarstellungen und Einschränkungen gefordert (8. TB S. 29 f.). Eine im wesentlichen tragbare Lösung zeichnet sich ab; siehe dazu Nr. 11. in diesem Bericht.

16. Über einen Modellversuch zur Durchführung des Arbeitslosenhilfeverfahrens, mit dem eine datenschutzgerechte Behandlung der Einkommensnachweise der für den Arbeitslosen unterhaltspflichtigen Personen erprobt werden sollte, habe ich berichtet (8. TB S. 30). Der Versuch wurde erfolgreich abgeschlossen mit dem Ergebnis, daß Einkommensnachweise von den Unterhaltspflichtigen den Arbeitsämtern direkt vorgelegt werden können; siehe dazu auch Nr. 11.1.2 in diesem Bericht.

17. Zur datenschutzgerechten Behandlung von Krankenhauserhebungen über die näheren Umstände von Entbindungen habe ich eine Lösungsmöglichkeit dargestellt (8. TB S. 34 und S. 64, Anlage 1). Der im 8. TB als Anlage abgedruckte Beschluß der Datenschutzbeauftragten des Bundes und der Länder wurde im Laufe des Jahres 1986 von der Bundesknappschaft (als einziger in meinem Zuständigkeitsbereich beteiligter Institution) in die Praxis umgesetzt.

18. Über Datenschutzprobleme bei der Übermittlung von Dialyse-Patienten-Fragebogen an die European Dialysis and Transplant Association (EDTA) habe ich berichtet (8. TB S. 34 f.). Die in Aussicht genommene einvernehmliche Lösung steht kurz vor ihrem Abschluß. In Abstimmung mit dem EDTA-Registry-Kommitee wurde eine Patienten-Einwilligungserklärung entwickelt, in der der Patient über Zweck und Ziel der Übermittlungen aufgeklärt und ausdrücklich auf die Freiwilligkeit seiner Teilnahme hingewiesen wird.

19. Für die Sicherheitsüberprüfung, bei der weit in die Privatsphäre eingreifende Datenspeicherungen erfolgen, habe ich eine klare gesetzliche

Grundlage gefordert (8. TB S. 39). Im Rahmen der Beratung über die Neufassung der Richtlinien zur Sicherheitsüberprüfung hat mir der Bundesminister des Innern mitgeteilt, daß er eine gesetzliche Regelung anstrebt.

20. Auf im wesentlichen organisationsbedingte Fehler bei der Festlegung von Löschungsfristen im Bundeskriminalamt habe ich hingewiesen (8. TB S. 42 f.). Meine Vorschläge zur Behebung dieser Mängel durch organisatorische Maßnahmen hat der Bundesminister des Innern abgelehnt. Ob lediglich der vorgesehene verstärkte dienstkundliche Unterricht ausreicht, diese Mängel abzustellen, ist zweifelhaft; siehe dazu Nr. 13.1 in diesem Bericht.

21. Gegen der Grundkonzeption des Kriminalaktennachweises nicht entsprechende Speicherungen von Daten beim Bundeskriminalamt habe ich Bedenken angemeldet (8. TB S. 43 f.). Der Bundesminister des Innern hat auf diese Bedenken bisher nicht geantwortet.

22. Auf die Notwendigkeit, die Verwendung von personenbezogenen Hinweisen in den INPOL-Datensätzen zu beschränken und ihre Richtigkeit durch planmäßige Überprüfungen sicherzustellen, habe ich hingewiesen (8. TB S. 44 f.). Zu beiden Problemen ist eine Verbesserung bisher nicht erfolgt; siehe dazu Nr. 13.1 in diesem Bericht.

23. Über die Nichtbeachtung der in den Dateienrichtlinien für das Bundeskriminalamt enthaltenen Verpflichtung, Personen, die weder Beschuldigte noch Verdächtige sind, zu benachrichtigen, wenn ihre Daten länger als ein Jahr in bestimmten Polizeidateien gespeichert werden, habe ich berichtet (8. TB S. 45 f.). Auch in diesem Berichtsjahr ist mir kein Fall bekannt geworden, in dem das BKA einen Betroffenen über eine solche Speicherung unterrichtet hat.

24. Für die Speicherung personenbezogener Daten insbesondere im Zusammenhang mit der Rauschgiftkriminalität habe ich eine Unterscheidung zwischen (formell) Beschuldigten und Verdächtigten vorgeschlagen, bei denen die Klärung des Verdachts nicht zur Beschuldigung geführt hat (8. TB S. 46). Der Bundesminister des Innern hat meinen Vorschlag abgelehnt.

25. Für die vielen Fälle, in denen die Abteilung Staatsschutz des BKA über den Verlauf eines gemeldeten Ermittlungsverfahrens lange Zeit keine weitere Nachricht erhält, habe ich angeregt, daß spätestens nach drei Jahren Erkundigungen über den Sachstand erfolgen sollten (8. TB S. 46 f.). Auch auf mein weiteres Vorbringen in dieser Sache hat der Bundesminister des Innern bisher nicht geantwortet.

26. Über verschiedene, datenschutzrechtlich problematische Datenverarbeitungen des Bundesamtes für Verfassungsschutz habe ich berichtet (8. TB S. 47 ff.). Wie unter Nr. 14 in diesem Bericht dargelegt, nehme ich dazu nicht öffentlich Stellung.

27. Auf die Notwendigkeit, mit dem Bundesminister der Verteidigung die Einzelheiten einer sinnvollen Neuregelung der personellen Vorbeugung durch den Militärischen Abschirmdienst zu erörtern, habe ich hingewiesen (8. TB S. 50). Nach Untersuchungen auch über die dabei notwendigen Tätigkeiten in den Kreiswehrersatzämtern hat der Bundesminister der Verteidigung zweckmäßige und datenschutzgerechte Regelungen getroffen.

28. Für die Daten, die im Rahmen der Sicherheitsüberprüfung vom Militärischen Abschirmdienst erhoben und gespeichert werden, habe ich eine konsequente Zweckbindung gefordert, und die Einhaltung der Zusicherung an die Betroffenen, daß ihre Daten „streng vertraulich" behandelt werden (8. TB S. 50). Die notwendige enge Zweckbindung wird beim MAD noch immer nicht eingehalten.

29. Zur Vermeidung unzulässiger Verwendungen von Anschriften der Reservisten durch den Verband der Reservisten der Deutschen Bundeswehr e. V. (VdRBw) habe ich Anregungen gegeben (8. TB S. 51 f.). Der Bundesminister der Verteidigung und der VdRBw haben entsprechende Maßnahmen ergriffen; siehe dazu Nr. 18.4 in diesem Bericht.

30. Über die Führung einiger Grunddaten von anerkannten Kriegsdienstverweigerern in Listen der Kreiswehrersatzämter habe ich berichtet (8. TB S. 51). Inzwischen hat der Bundesminister der Verteidigung das Verfahren so geregelt, daß Angaben über anerkannte Kriegsdienstverweigerer auch beim zuletzt zuständigen Kreiswehrersatzamt nur noch für eine kurze Zeit zur Kontrolle der korrekten Aktenübersendung an das Bundesamt für den Zivildienst und für Rückfragen zur Verfügung stehen; siehe dazu Nr. 18.5 in diesem Bericht.

31. Für die Aufbewahrung von Unterlagen aus Verfahren, die nicht mit der Anerkennung des Betroffenen als Kriegsdienstverweigerer abgeschlossen wurden, sowie für die Einsichtnahme in diese Unterlagen und ihre Vernichtung habe ich dem Bundesminister der Verteidigung empfohlen, ausdrückliche Regelungen zu erlassen (8. TB S. 51). Diese Regelungen stehen auch deswegen noch aus, weil über die Aufbewahrungsfristen für die einzelnen Teile der Unterlagen noch nicht entschieden wurde; siehe dazu Nr. 18.5 in diesem Bericht.

32. Auf die Notwendigkeit, das Melde- und Auskunftsverfahren der SCHUFA neu zu ordnen, habe ich hingewiesen (8. TB S. 53 f.). Die obersten Aufsichtsbehörden für den Datenschutz haben mit meiner Beteiligung in Gesprächen mit dem Zentralen Kreditausschuß und der SCHUFA neue Klauseln und Verbesserungen des SCHUFA-Verfahrens erreicht; siehe dazu Nr. 19.1 in diesem Bericht.

33. Über meine Bedenken gegen die noch immer zu pauschalen Schweigepflichtentbindungsklauseln in Versicherungsverträgen habe ich berichtet (8. TB S. 53 f.). Die Gespräche, die mit meiner Beteiligung zwischen den Datenschutzaufsichtsbehörden, dem Bundesaufsichtsamt für das Versicherungswesen und der Versicherungswirtschaft geführt wurden, haben bisher noch nicht zu einem Ergebnis geführt; siehe dazu Nr. 19.2 in diesem Bericht.

Bonn, den 28. Januar 1987

Dr. Baumann

Anlage 1 (zu 1.5)

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. Januar 1986

zu den Sicherheits- und Datenschutzgesetzen

Die Datenschutzbeauftragten erinnern an ihre Entschließungen zu den Auswirkungen des Volkszählungsurteils des Bundesverfassungsgerichts, zur Einführung eines maschinenlesbaren Personalausweises und zur Datenverarbeitung bei Polizei und Verfassungsschutz. Sie stellen fest, daß die angekündigten „Sicherheits- und Datenschutzgesetze" den von ihnen erhobenen Forderungen nur unzureichend Rechnung tragen und den Vorgaben des Bundesverfassungsgerichts nur teilweise entsprechen. Die geplanten Regelungen haben erhebliche Konsequenzen für die Datenverarbeitung in den Ländern und präjudizieren die Landesgesetzgeber in vielerlei Hinsicht.

Die Datenschutzbeauftragten sehen sich zu folgender ersten Bewertung veranlaßt:

1. Zum Bundesdatenschutzgesetz

— Das Recht auf informationelle Selbstbestimmung gilt für jeglichen Umgang mit personenbezogenen Daten. Daher ist es nicht gerechtfertigt, die Beschränkung des Bundesdatenschutzgesetzes auf Dateien festzuschreiben und die Datenerhebung auszugrenzen. Die vorgeschlagenen Regelungen im Verwaltungsverfahrensgesetz sind kein ausreichender Ersatz, weil wichtige Verwaltungsbereiche, wie z. B. die Finanzbehörden, ausgenommen sind und die Datenverarbeitung in Akten und anderen Unterlagen der Datenschutzkontrolle weitgehend entzogen wird.

— Eine wirksame Kontrolle durch die Datenschutzbeauftragten in Bund und Ländern ist nach wie vor nicht sichergestellt.

— Das Auskunftsrecht des Bürgers bleibt stark eingeschränkt.

— Unbefriedigend ist auch, daß der Datenschutz im nicht-öffentlichen Bereich insgesamt nicht verbessert wird.

2. Zum Personalausweisgesetz und Paßgesetz

— Die Einführung des maschinenlesbaren Ausweises verändert entscheidend die Bedingungen, unter denen Informationen über die Bürger im Sicherheitsbereich erhoben und verarbeitet werden. Mit seiner Hilfe soll die Polizei vorhandene Daten automatisiert abrufen und abgleichen sowie neue Datensammlungen anlegen können. Der behauptete Sicherheitsgewinn ist bis heute nicht dargetan.

— Darüber hinaus fehlt es an bereichsspezifischen Gesetzen, die den Umgang der Sicherheitsbehörden mit dem Ausweis regeln, wie sie auch der Deutsche Bundestag in seiner Entschließung vom 17. Januar 1980 gefordert hat. Die jetzt diskutierten Begleitgesetze einschließlich der Ergänzung oder Strafprozeßordnung genügen den Anforderungen nicht. Dies gilt um so mehr, als auch unverdächtige Bürger betroffen sind.

— Die Gefahren wachsen, wenn die gleichzeitig beabsichtigte automatisierte Nutzung des Verkehrszentralregisters in der vorgesehenen Form verwirklicht und der Datenverbund der Sicherheitsbehörden untereinander weiter ausgebaut wird.

3. Zum Bundesverfassungsschutzgesetz

Auch für den Verfassungsschutz gilt, daß seine Aufgaben im Gesetz klar in einer für den Bürger nachvollziehbaren Weise zu beschreiben sind. Gerade weil seine Tätigkeit weitgehend im Geheimen stattfindet, müssen die Bürger die Gewißheit haben, daß der Verfassungsschutz an eindeutige, eng umrissene und abschließend geregelte Aufgaben und Befugnisse gebunden ist. Der vorliegende Entwurf verfehlt dieses Ziel:

Weitere schwerwiegende Mängel kommen hinzu:

— Dem Bürger kann nach wie vor jegliche Auskunft verweigert werden.

— Es fehlen gesetzliche Fristen für die Löschung gespeicherter Daten.

— Dem Verfassungsschutz darf nicht das Recht zugestanden werden, in jedes amtliche Datenregister Einblick zu nehmen und jede Art von Daten anzufordern. Im Gesetzentwurf sind davon nicht einmal Gesundheits- und Steuerdaten ausgenommen.

— Während sich das nachrichtendienstliche Informationssystem (NADIS) bisher nur auf die Speicherung von Aktennachweisen beschränkte, sollen nach dem Gesetzentwurf auch Textzusätze über den Bürger automatisiert den Nachrichtendienst bundesweit zur Verfügung stehen. Damit werden zu Lasten des Bürgers Akteninhalte verkürzt und aus ihrem Entstehungszusammenhang herausgenommen.

4. Zur Zusammenarbeit von Nachrichtendiensten und Polizei

— Die rechtsstaatlichen Grenzen der Zusammenarbeit von Nachrichtendiensten und Polizei werden durch das Trennungsgebot bestimmt. Das Trennungsgebot erschöpft sich nicht in einer

bloßen organisatorischen Trennung zwischen Nachrichtendiensten und Polizei. Gerade wegen der automatisierten Datenverarbeitung kommt es mindestens ebenso auf eine strikte Trennung der Informationsbestände an. Das Trennungsgebot darf nicht durch einen umfassenden Informationsaustausch unterlaufen werden.

— Im übrigen darf eine Zusammenarbeit zwischen Polizei, MAD, Verfassungsschutz und BND erst erfolgen, wenn für die einzelnen Dienste eindeutige, auch den Datenschutz sichernde Rechtsgrundlagen geschaffen sind.

Anlage 2 (zu 1.5)

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14. März 1986

zur Änderung des Bundesdatenschutzgesetzes

Die Datenschutzbeauftragten beurteilen den Entwurf zur Novellierung des Bundesdatenschutzgesetzes (Drucks. 10/4737) nach den Grundsätzen des Volkszählungsurteils des Bundesverfassungsgerichts, den Notwendigkeiten, die sich aus der technischen Entwicklung der Informationsverarbeitung ergeben, und den Forderungen, die sie bereits in früheren Entschließungen formuliert haben. Sie messen ihn auch an der Erklärung der Bundesregierung, den Datenschutz im Interesse der Bürger zu verbessern und die Datenverarbeitung transparenter zu gestalten.

Die Datenschutzbeauftragten stellen fest, daß der Entwurf zwar Verbesserungen enthält (I), insgesamt die Erwartungen jedoch nicht erfüllt (II). Sie bemängeln insbesondere die Beschränkungen des Gesetzes auf Dateien, die Ausklammerung der Datenerhebung, die unzureichenden Kontrollbefugnisse des Datenschutzbeauftragten und die unbefriedigenden Regelungen für den nichtöffentlichen Bereich.

I.

1. Die Klarstellung, daß Datenschutz weder Schutz von Daten noch ausschließlich Schutz vor Mißbrauch, sondern Schutz des Bürgers vor Verletzungen seines Persönlichkeitsrechts ist, wird begrüßt.

2. Einige der vorgesehenen Änderungen entsprechen Forderungen, die die Datenschutzbeauftragten immer wieder erhoben haben. Das gilt — unbeschadet noch notwendiger Verbesserungen in Einzelheiten — für

   — die Einführung eines verschuldensunabhängigen Schadensersatzanspruchs, auch für Nichtvermögensschäden,

   — die Aufnahme einer Regelung der Datenverarbeitung für wissenschaftliche Zwecke,

   — die Abschaffung der Entgeltpflicht für die Auskunft über die eigenen Daten und die Ausdehnung der Auskunft auf Herkunft und Empfänger der Daten,

   — die Pflicht zur Löschung von Daten, die für den Speicherungszweck nicht mehr erforderlich sind,

   — die gesetzliche Anerkennung der Zweckbindung personenbezogener Daten,

   — die Klarstellung, daß Geheimhaltungsvorschriften der Kontrolle durch den Bundesbeauftragten nicht entgegengehalten werden können,

   — die Verstärkung der Befugnisse der Aufsichtsbehörden für den nichtöffentlichen Bereich und der Stellung des betrieblichen Datenschutzbeauftragten.

II.

Einzuwenden ist gegen den Entwurf vor allem:

1. Ein gravierender Mangel ist bereits die *Beschränkung auf die Datenverarbeitung in Dateien*, die schon in der neuen Gesetzesbezeichnung zum Ausdruck kommt und den gesamten Entwurf prägt (§ 1 Abs. 1). Das Recht auf informationelle Selbstbestimmung umfaßt jeden Umgang mit personenbezogenen Daten. Die dem Volkszählungsurteil folgende Einbeziehung der Datennutzung bleibt weitgehend wirkungslos, weil nur die Nutzung *unmittelbar* aus Dateien gewonnener Daten geregelt wird. Die zunehmende Verknüpfung von Akten-, Text- und Datenverarbeitung wurde ebensowenig berücksichtigt wie z. B. neue Formen der Bildverarbeitung, etwa durch Videoaufzeichnungen. Im übrigen ist auch der neue *Dateibegriff* zu eng.

2. Neue *Vorschriften im Verwaltungsverfahrensgesetz* des Bundes über den Schutz personenbezogener Daten bei ihrer Verarbeitung außerhalb von Dateien gleichen die Nachteile des auf Dateien beschränkten Anwendungsbereichs des BDSG nicht aus, zumal nach § 19 Abs. 1 ihre Einhaltung nur begrenzt kontrollierbar ist. Außerdem gilt das Verwaltungsverfahrensgesetz im Gegensatz zum BDSG nicht umfassend, sondern von seinem Anwendungsbereich sind große und wichtige Verwaltungsbereiche und -tätigkeiten, wie Finanzverwaltung, Post, Strafverfolgung, Verfolgung von Ordnungswidrigkeiten und weite Bereiche der Sozialverwaltung ausgenommen, ebenso die privatrechtliche Betätigung der öffentlichen Hand. Auch im nichtöffentlichen Bereich bleibt die Datenverarbeitung außerhalb von Dateien ungeregelt.

3. Der BDSG-Entwurf enthält keine ausdrückliche Regelung der *Datenerhebung*, obwohl gerade die Erhebung den Bürger unmittelbar belastet. Kein ausreichender Ersatz ist die Erhebungsvorschrift im Verwaltungsverfahrensgesetz. In ihr fehlt zudem die Verpflichtung der erhebenden Stelle, den Erhebungszweck ausdrücklich festzulegen, an den die gesamte weitere Verarbeitung und Nutzung grundsätzlich gebunden ist. Er müßte dem Betroffenen auch mitgeteilt werden, um ihm Kenntnis darüber zu verschaffen, wer was wann und bei welcher Gelegenheit über ihn weiß.

4. Die weitgehende Ausklammerung *„interner Dateien"* ist nicht hinnehmbar (§ 1 Abs. 3). Es ist verfassungsrechtlich bedenklich, die interne Datenverarbeitung von jeglicher Kontrolle durch die Betroffenen, die Datenschutzbeauftragten und die Aufsichtsbehörden freizustellen.

5. Da das Gesetz jede Datenverarbeitung zuläßt, wenn die *Einwilligung* des Betroffenen vorliegt, muß der Gesetzgeber durch besondere Regelungen den Betroffenen davor schützen, daß er durch soziale, wirschaftliche und psychische Zwänge (etwa als Mieter, Patient oder Arbeitsuchender) in seiner Entscheidungsfreiheit unangemessen eingeschränkt wird.

6. Die Regelung für die Datenverarbeitung zu Zwecken der *wissenschaftlichen Forschung* (§ 3 a) weist noch eine Reihe von Mängeln auf. Der Vorrang der Berufs- und besonderen Amtsgeheimnisse muß klargestellt werden. Auch muß — nach dem Vorbild des Sozialgesetzbuchs — ein Forschungsgeheimnis aufgenommen werden, das den Betroffenen vor jeder zweckfremden Nutzung der für ein Forschungsvorhaben zur Verfügung gestellten Daten schützt.

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

8. Die Regelung für *automatisierte Abrufverfahren (Online)* (§ 6 a) weist Mängel auf. Die inhaltlichen Anforderungen an die Zulassung solcher Verfahren sind weiter zu präzisieren. Die Risiken, die in der möglichen Selbstbedienung des Datenempfängers liegen, müssen zumindest durch wirksame Kontrollmechanismen gemindert werden. In der öffentlichen Verwaltung ist die Einführung von Online-Verfahren jedenfalls in besonders sensiblen Bereichen unter den Vorbehalt einer Rechtsvorschrift zu stellen.

9. Die *Datenspeicherung* sollte grundsätzlich nur für den bei der Erhebung festgelegten Zweck zugelassen werden, der dem Betroffenen bekanntzugeben ist (§ 9). Der Katalog erlaubter Zweckänderungen ist zu weit; soweit zweckfremde Datenspeicherungen und -nutzungen zugelassen werden, müßten sie den Betroffenen mitgeteilt oder in anderer Weise transparent gemacht werden. Das gilt auch für *Datenübermittlungen*, sofern damit eine Zweckänderung verbunden ist.

10. Das Recht des Bürgers auf *Auskunft* über seine Daten (§ 13) muß Herkunft und Empfänger umfassen, auch wenn diese Informationen nicht in Dateien gespeichert sind. Das Auskunftsrecht darf im übrigen nicht dadurch geschmälert werden, daß Nachrichtendienste ohne Verpflichtung zur Interessenabwägung im Einzelfall und ohne Begründung die Auskunft verweigern dürfen (§ 13).

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

    — daß eine Kontrolle der Einhaltung „anderer Vorschriften" über den Datenschutz bei einer Datenverarbeitung außerhalb von Dateien nur noch dann möglich ist, wenn durch eine Beschwerde oder auf andere Weise Anhaltspunkte für eine Rechtsverletzung vorliegen,

    — daß in solchen Fällen systematische Kontrollen des BfD — z. B. im Sozialleistungsbereich — entgegen der bisherigen Praxis ausgeschlossen sind, weil die Kontrolle auf den Einzelfall beschränkt wird,

    — daß die Formulierung in § 19 Abs. 1 Satz 1, wonach die Kontrolle der Behörden „unbeschadet ihrer fachlichen Beurteilung und Verantwortlichkeit" stattfindet, von den kontrollierten Stellen so verstanden werden könnte, als ob eine Datenverarbeitung künftig nicht mehr inhaltlich, z. B. nicht mehr auf ihre Erforderlichkeit, überprüft werden kann,

    — daß die Datenerhebung selbst dann nicht mehr kontrollierbar ist, wenn sie zur Dateispeicherung führt, weil sie nicht mehr im BDSG geregelt wird und auch nicht als Datenverarbeitung oder Nutzung im Sinne des § 19 Abs. 1 Nr. 1 und 2 gilt,

    — daß nach § 19 Abs. 5 Satz 3 Nr. 1 personenbezogene Daten durch besonderes Gesetz von der Kontrolle ausgenommen werden können, obwohl es nach dem Volkszählungsurteil keine kontrollfreien Räume geben darf,

    — daß nach § 19 Abs. 5 Satz 3 Nr. 2 personenbezogene Daten, die bei Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses nach dem G 10 anfallen, der Datenschutzkontrolle grundsätzlich entzogen sind, obwohl das Bundesverfassungsgericht im Beschluß vom 20. Juni 1984 die Kontrolle durch Datenschutzbeauftragte zur Voraussetzung für die Zulässigkeit solcher Maßnahmen erklärt hat.

    Schließlich ist festzustellen:

    — § 19 Abs. 5 Satz 3 Nr. 3 muß gestrichen werden, da es für die Datenschutzbeauftragten selbstverständlich ist, das informationelle Selbstbestimmungsrecht bei der Kontrolle zu wahren, und die geplante Regelung dazu führen kann, die Datenschutzkontrolle nachhaltig zu erschweren.

    — Die Klarstellung, daß (bundesrechtliche) Berufs- oder Amtsgeheimnisse der Datenschutzkontrolle nicht entgegengehalten werden können, muß auch die Kontrolle durch die Landesbeauftragten für den Datenschutz einbeziehen.

— Es fehlt eine zum Teil in früheren Gesetzentwürfen vorgesehene Verpflichtung der Behörden, den BfD über Planungen wichtiger Automationsvorhaben zu unterrichten und bei datenschutzrelevanten Gesetzgebungsvorhaben zu beteiligen.

12. Die *Datenschutzvorschriften für den nicht-öffentlichen Bereich* orientieren sich nicht am Grundsatz der Zweckbindung und räumen verfassungsrechtlich bedenkliche Verarbeitungsprivilegien ein. So kann die Personengruppe, über die listenmäßig bestimmte Daten übermittelt werden dürfen, beliebig festgelegt werden (§ 24 Abs. 1 Nr. 3). Für Zwecke der Markt- und Meinungsforschung und der Werbung können auch Vertragsdaten, beispielsweise aus einem Arbeitsverhältnis, ohne Einwilligung des Betroffenen und ohne Rücksicht auf seine schutzwürdigen Belange listenmäßig übermittelt werden.

13. Die *Auskunft an den Betroffenen* über seine Daten muß auch im nicht-öffentlichen Bereich den Speicherungszweck umfassen (§ 26). Gleiches gilt für die Benachrichtigung über die erstmalige Speicherung von Daten. Über Herkunft und Empfänger ist auch dann Auskunft zu erteilen, wenn diese Angaben nicht in Dateien gespeichert sind.

14. Der Empfänger übermittelter Daten muß strenger an den *Übermittlungszweck* gebunden werden. Zweckfremde Nutzungen dürfen nicht schon dann zulässig sein, wenn der Nutzer keinen Grund zur Annahme sieht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden (§ 24 Abs. 3).

15. Die Datenschutzbeauftragten halten eine Ergänzung des BDSG um Sonderregelungen für den *Adreßhandel* für erforderlich.

16. Im übrigen erinnern die Datenschutzbeauftragten an ihre früheren Forderungen nach bereichsspezifischen Regelungen nicht nur für den öffentlichen, sondern auch für den nicht-öffentlichen Bereich. Hierzu zählen insbesondere Regelungen für die Verarbeitung von *Arbeitnehmerdaten* sowie für den *Kredit- und Versicherungsbereich*.

Anlage 3 (zu 1.5)

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14. März 1986

zum Datenschutz im Krankenhaus

Die Datenschutzbeauftragten haben in ihrer Entschließung vom 27./28. März 1984 über die Auswirkungen des Volkszählungsurteils auf die Notwendigkeit hingewiesen, auch im Bereich des Gesundheitswesens bereichsspezifische gesetzliche Regelungen zu erlassen. Die ärztliche Schweigepflicht und die allgemeinen Datenschutzgesetze reichen nicht aus, alle Fälle, in denen im Bereich des Krankenhauses das Persönlichkeitsrecht des Patienten berührt wird, angemessen zu lösen. Konkrete Regelungen für diesen Bereich sind insbesondere deshalb notwendig, weil automatisierte Datenverarbeitung in immer stärkerem Maße im Krankenhausbereich auch für die Verarbeitung medizinischer Daten eingesetzt wird. Die zunehmende Komplexität der Verarbeitung und Nutzung von Patientendaten führt dazu, daß für den einzelnen Patienten der Umfang und die Zwecke der Verwendung seiner Daten undurchschaubar werden. Der Bürger muß aber auch künftig die Gewähr haben, daß das Vertrauensverhältnis zwischen Arzt und Patient (Arzt-/Patientengeheimnis) und sein Persönlichkeitsrecht gewahrt bleiben.

Bisher wird die Datenverarbeitung in Krankenhäusern vielfach aufgrund sehr weit gefaßter formularmäßiger Einwilligungen gerechtfertigt. Die Einwilligung kann jedoch in vielen Fällen keine ausreichende Grundlage für die Verarbeitung von Patientendaten sein, da für den Patienten die Informationsmöglichkeit und die Entscheidungsfreiheit häufig eingeschränkt sind.

Maßstab für den Umfang der Erhebung, Verarbeitung und Nutzung von Patientendaten muß stets die Behandlung des Patienten sein. Eine zusätzliche vom Behandlungszweck nicht gedeckte Datenerhebung, -verarbeitung und -nutzung bedarf einer besonderen Legitimation.

Auch die für die Behandlung verwendeten Vordrucke und Aufnahmeverträge müssen diesen Grundsätzen angepaßt werden. Die zuständigen Stellen werden aufgefordert, ihre Vordrucke und Aufnahmeverträge entsprechend zu überarbeiten.

Zur Wahrung des Patientengeheimnisses ist es geboten, im Krankenhaus den ärztlichen Bereich von der Verwaltung informationell abzuschotten. Daraus folgt, daß z. B. die Akten der Krankenhausverwaltung getrennt von denjenigen des ärztlichen Bereichs zu führen sind. Daraus folgt weiter, daß auch im ärztlichen Bereich nur vom jeweils behandelnden Arzt auf die Daten zugegriffen werden kann.

Läßt das Krankenhaus Patientendaten bei anderen Stellen im Auftrag verarbeiten, wird das Arztgeheimnis durchbrochen. Auch besteht die Gefahr einer Grundrechtsbeeinträchtigung durch Verknüpfung von medizinischen Daten und solchen aus anderen Bereichen und durch überregionale Konzentration medizinischer Daten. Die Verarbeitung medizinischer Daten außerhalb des eigenen Krankenhauses sollte daher — in eingeschränktem Umfang — allenfalls bei einem anderen Krankenhaus zugelassen werden.

Das Krankenhaus steht im Zentrum vielfältiger Informationsanforderungen, nicht zuletzt von Sozialleistungsträgern und anderen öffentlichen Stellen. Diese Informationsanforderungen sind häufig nicht normenklar festgelegt. Ihre Notwendigkeit muß überprüft, die gesetzlichen Grundlagen müssen präzisiert werden. Dies gilt insbesondere dann, wenn die Übermittlung zu belastenden Konsequenzen für den Patienten im Verwaltungsvollzug (z. B. Führerscheinentzug) führen kann.

Der Patient darf ohne sein Wissen und sein Einverständnis grundsätzlich nicht zum Objekt der Forschung mit Daten gemacht werden, die zu seiner Behandlung erhoben werden. Die Verarbeitung von Daten zu Forschungszwecken ohne Beteiligung des Patienten sollte nur zugelassen werden, wenn dies im Interesse der wissenschaftlichen Forschung unabdingbar ist und die Rahmenbedingungen der Verarbeitung durch den Gesetzgeber näher festgelegt sind. Dies gilt auch für gemeinsame Dokumentationssysteme mehrerer behandelnder Einrichtungen.

Das informationelle Selbstbestimmungsrecht umfaßt auch das Recht des Patienten, Einsicht in Patientenakten und ärztliche Unterlagen zu nehmen und Auskunft zu erhalten, sofern nicht überwiegende Geheimhaltungsinteressen anderer entgegenstehen.

Eine undifferenzierte, zeitlich unbefristete Aufbewahrung von Patientenunterlagen darf es auch im Krankenhaus nicht geben. Deshalb müssen die Krankenhäuser prüfen, wann welche Patientenunterlagen ohne Beeinträchtigung schutzwürdiger Belange der Patienten vernichtet werden können.

Anlage 4 (zu 1.5)

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. April 1986

zur Änderung des Bundesverfassungsschutzgesetzes

Die Datenschutzbeauftragten beurteilen den Entwurf zur Novellierung des Bundesverfassungsschutzgesetzes (Drs. 10/4737) nach den Grundsätzen des Volkszählungsurteils des Bundesverfassungsgerichts, den Notwendigkeiten, die sich aus der technischen Entwicklung der Informationsverarbeitung ergeben, und den Forderungen, die sie bereits in früheren Entschließungen formuliert haben. Sie messen ihn auch an der Erklärung der Bundesregierung, den Datenschutz im Interesse der Bürger zu verbessern und die Datenverarbeitung transparenter zu gestalten.

Der Entwurf wird den sich aus dem Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz ergebenden Anforderungen nicht gerecht. Seine Vorschriften müssen schon deshalb wesentlich präziser gefaßt werden, weil die Arbeit des Verfassungsschutzes vorwiegend unter Ausschluß der Öffentlichkeit und der Kontrolle der betroffenen Bürger stattfindet.

Hauptkritikpunkte sind:

1. Da sich der zulässige Umfang der Informationsverarbeitung maßgeblich nach den Aufgaben der datenverarbeitenden Stelle bemißt, bedarf es einer möglichst genauen gesetzlichen Beschreibung dieser Aufgaben. Die in § 3 Abs. 1 verwendeten Begriffe wie etwa „Bestrebungen gegen die freiheitlich-demokratische Grundordnung" oder „Gefährdung auswärtiger Belange" sind unpräzise.

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

   Auf jeden Fall ist es notwendig, die Voraussetzungen für die Erhebung, Speicherung und sonstige Verwendung personenbezogener Daten im Rahmen der Erfüllung dieser Aufgaben präziser und für den Bürger transparent zu regeln. Begriffe wie „Aufgaben des Verfassungsschutzes" und „Zwecke des Verfassungsschutzes" sind nicht hinreichend bestimmt.

   Die Mitwirkung der Verfassungsschutzbehörden an der Überprüfung von Personen durch andere Stellen muß im Verfassungsschutzgesetz abschließend geregelt werden. Sofern über die Sicherheitsprüfung (§ 3 Abs. 2) hinaus eine Mitwirkung an anderen Verfahren wie etwa bei Einbürgerungen, Asylverfahren, Ordensverleihungen oder der Überprüfung von Bewerbern für den öffentlichen Dienst für unabdingbar gehalten wird, sind diese im Gesetz ausdrücklich zu nennen. Auch die damit im Zusammenhang stehende Datenverarbeitung ist im Verfassungsschutzgesetz präzise zu regeln. Unabhängig davon ist für die Sicherheitsüberprüfung und jedes andere Verfahren zur Überprüfung von Personen eine bereichsspezifische Regelung erforderlich.

2. Der im Entwurf vorgesehene Informationsaustausch der Verfassungsschutzbehörden untereinander (§ 4 Abs. 1) ist zu umfassend und bedarf einer aufgabenbezogenen Einschränkung. Er ist nur zulässig, soweit Informationen für die jeweilige Aufgabenerfüllung der einzelnen Verfassungsschutzbehörden erforderlich sind. So dürfen beispielsweise die aus einer Telefonüberwachung gewonnenen Daten auch zwischen Verfassungsschutzbehörden nur unter den engen Voraussetzungen des § 7 Abs. 3 G 10 ausgetauscht werden.

   Besondere datenschutzrechtliche Risiken birgt die Aufnahme von Textzusätzen aus Akten der Verfassungsschutzbehörden in automatisierte Dateien. Damit werden zu Lasten des Bürgers Akteninhalte verkürzt und aus ihrem Entstehungszusammenhang herausgenommen. Sollten trotz dieser Bedenken Textzusätze in eingeschränktem Umfang zugelassen werden, ist es über die bereits im Entwurf getroffenen Beschränkungen und Schutzvorkehrungen hinaus unerläßlich, in der Datei die für die Bewertung und Überprüfung solcher Textzusätze maßgeblichen Unterlagen anzugeben. Entscheidungen dürfen auf diese Textzusätze allein nicht gestützt werden. Die im Gesetz gewollte Begrenzung auf Spionageabwehr und Terrorismusbekämpfung wird nicht erreicht, weil der Gewaltbegriff nicht einschränkend definiert ist.

3. Die in § 5 und § 6 Abs. 2 vorgesehene Befugnis, nachrichtendienstliche Mittel einzusetzen, entspricht nicht dem Grundsatz der Normenklarheit. Zumindest sind die wichtigsten Mittel im Gesetz aufzuzählen. Auch zum Zwecke der Datenschutzkontrolle sollte daneben die interne Festlegung der zulässigen Mittel und Dokumentation ihres Einsatzes im einzelnen vorgeschrieben werden. Angesichts der Schwere des mit der Anwendung nachrichtendienstlicher Mittel verbundenen Eingriffs in das Persönlichkeitsrecht darf sich ihr Einsatz grundsätzlich nur gegen konkret verdächtige Personen richten. Entsprechend den Regelungen über die Post- und Telefonüberwachung sind Verwertungsbeschränkungen und eine Verpflichtung zur nachträglichen Unterrichtung des Betroffenen vorzusehen.

4. Die in § 6 Abs. 1 geregelte Befugnis zur Datenerhebung entspricht wegen der Bezugnahme auf die zu weitreichende Klausel „zur Erfüllung der Aufgaben der Verfassungsschutzbehörden erforderlich" nicht im Grundsatz der Verhältnismäßigkeit. Die verfassungsrechtlich gebotene Güterabwägung im Einzelfall kann ergeben, daß vorrangige Individualrechte einer personenbezogenen Erhebung entgegenstehen, so beispielsweise bei der Ausübung des Demonstrationsrechts (vgl. Brokdorf-Beschluß des Bundesverfassungsgerichts). Dies gilt gleichermaßen hinsichtlich solcher Personen, die selbst keinerlei verfassungswidriger Bestrebungen verdächtigt sind.

5. Die in § 7 getroffene Regelung über die Speicherung, Veränderung und sonstige Nutzung personenbezogener Daten darf nicht — wie jetzt vorgesehen — auf Dateien beschränkt bleiben, zumal bei Verfassungsschutzbehörden ein Großteil der das Persönlichkeitsrecht der Bürger maßgeblich berührenden Daten in Akten geführt wird und komplexe Aktensammlungen bereits heute gezielt und mit Hilfe automatisierter Verfahren erschlossen werden können.

   Im Bereich der Beobachtungen verfassungswidriger Bestrebungen ohne Gewaltbezug sollte die personenbezogene Speicherungsbefugnis davon abhängig gemacht werden, daß der Extremismusbezug in der Person des zu Speichernden vorliegt.

   Überdies muß die Vorschrift um die Festlegung von Überprüfungs- und Löschungsfristen, differenziert nach den einzelnen Aufgabenbereichen, erweitert werden.

6. Der Entwurf will in § 8 die Verpflichtung anderer Behörden, den Verfassungsschutz über eigene Wahrnehmungen von sich aus zu unterrichten, auf Erkenntnisse aus den Bereichen Spionage und Terrorismus beschränken, ohne jedoch — wegen des zu weiten Gewaltbegriffs — dieses Ziel voll zu erreichen. Die darüber hinaus allen Behörden eingeräumte Befugnis, dem Verfassungsschutz auch Informationen über gewaltfreie extremistische Bestrebungen zuzuleiten, birgt in dieser uneingeschränkten Form die Gefahr in sich, daß ein Klima allgemeiner Verdächtigungen entsteht. Auch vermag der Bürger, der in Kontakt mit einer Verwaltungsbehörde tritt, nicht zu erkennen, was diese wann und bei welcher Gelegenheit an die Verfassungsschutzbehörde übermittelt.

   Schließlich fehlt in der Vorschrift eine Regelung, unter welchen Voraussetzungen Veränderungen des Sachverhalts der Verfassungsschutzbehörde nachzuberichten sind.

7. Die in §§ 9 und 16 des Entwurfs festgelegte Verpflichtung für alle übrigen öffentlichen Stellen, den Verfassungsschutzbehörden auf Ersuchen die zur Erfüllung ihrer Aufgaben erforderlichen Auskünfte zu erteilen, geht zu weit, da sie im Einzelfall z. B. der Zweckbindung widersprechen kann. Noch weniger hinnehmbar ist die vorgesehene pauschale Ermächtigung der Verfassungsschutzbehörde, in alle amtlich geführten Register Einsicht zu nehmen. Schließlich fehlt es auch an einer Regelung für die Übermittlung von Informationen durch andere Stellen, die diese aufgrund besonderer Eingriffsbefugnisse erlangt haben. Die in § 9 Abs. 2 vorgesehene Befreiung der Verfassungsschutzbehörde von der Verpflichtung, ihre Auskunftsersuchen zu begründen, kann nur für die Fälle hingenommen werden, in denen Sicherheitsinteressen oder schutzwürdige Belange des Betroffenen einer Begründung entgegenstehen.

8. Angesichts des weitreichenden Auftrags der Verfassungsschutzbehörden zur Sammlung von Informationen bedürfen die dabei anfallenden personenbezogenen Erkenntnisse einer besonders strengen Abschottung nach außen. Dem trägt § 10 Abs. 1 des Entwurfs nicht hinreichend Rechnung, der es für eine Weiterleitung verfassungsschutzbehördlicher Erkenntnisse an andere öffentliche Stellen genügen läßt, daß die Daten dort im Rahmen der Aufgabenerfüllung für Zwecke der öffentlichen Sicherheit benötigt werden.

   Die in § 10 Abs. 2 zugelassene Übermittlung von Daten der Verfassungsschutzbehörde an Dienststellen der Stationierungsstreitkräfte muß angesichts der unübersehbaren Folgewirkungen und wegen der fehlenden Geltung deutschen Datenschutzrechts an besonders enge Voraussetzungen geknüpft werden. Zumindest ist in jedem Fall eine Abwägung mit den schutzwürdigen Belangen der Betroffenen vorzuschreiben.

   Die Weitergabe von Erkenntnissen an private Stellen (§ 10 Abs. 3) muß auf die Fälle der Sicherheitsüberprüfung und der Spionage- bzw. Terrorismusabwehr beschränkt werden.

9. Die Übermittlung personenbezogener Daten durch das Bundesamt für Verfassungsschutz an die politische Führung (§ 11 Abs. 1) darf nur zugelassen werden, soweit dies für Zwecke der Aufsicht oder im Rahmen der politischen Berichtspflicht erforderlich ist. Darüber hinaus ist eine strenge Zweckbindung für die übermittelten Daten vorzusehen.

   Die nach § 11 Abs. 2 zugelassene Unterrichtung der Öffentlichkeit über personenbezogene Daten muß die Ausnahme bleiben.

10. Die in § 14 auf automatisierte Dateien beschränkte Verpflichtung, Errichtungsanordnungen zu erstellen, muß auf alle Datensammlungen ausgedehnt werden. Die Unterrichtung des Datenschutzbeauftragten vor Aufnahme des Dateibetriebes ist vorzusehen. Schließlich ist gesetzlich sicherzustellen, daß die Frage der Notwendigkeit zur Weiterführung oder Änderung einer Datei in bestimmten Zeitabständen aufgabenbezogen überprüft wird.

Anlage 5 (zu 1.5)

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. April 1986 zum Entwurf einer Telekommunikationsordnung

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen die Absicht des Bundesministers für das Post- und Fernmeldewesen, die Bedingungen für die Benutzung der Einrichtungen für das Fernmeldewesen in einer einheitlichen Telekommunikationsordnung (TKO) neu zu regeln und an einer Stelle zusammenzufassen. Damit soll auch der technischen Entwicklung Rechnung getragen werden: Die Digitalisierung der Telekommunikation führt zu einer bisher nicht gekannten Speicherung von Verbindungs-, Abrechnungs- und Benutzungsdaten. Auch der Inhalt der Kommunikation wird zunehmend elektronisch gespeichert.

Das Bundesverfassungsgericht hat gerade vor dem Hintergrund der zunehmenden elektronischen Datenverarbeitung in seinem Urteil zum Volkszählungsgesetz 1983 die Bedeutung des Rechts auf informationelle Selbstbestimmung unterstrichen und daraus Grundsätze abgeleitet. Diese sind auch für die TKO von Bedeutung, da die Bürger auf die Inanspruchnahme der einzelnen Dienste in zunehmendem Maße angewiesen sind. Der Entwurf trägt diesen Anforderungen nicht hinreichend Rechnung:

1. Jeder der Telekommunikationsdienste birgt technisch bedingte Risiken in sich, die vom Teilnehmer nicht ohne weiteres erkennbar sind, bei der Nutzung aber berücksichtigt werden müssen. Deshalb sollte in die TKO eine Vorschrift aufgenommen werden, die die Deutsche Bundespost verpflichtet, die Teilnehmer des jeweiligen Dienstes über dessen wesentliche technische Bedingungen und Risiken bei der Benutzung des Telekommunikationsnetzes zu informieren und sie auf sicherheitsförderndes bzw. sicherheitsgefährdendes Nutzungsverhalten hinzuweisen.
2. Die in § 4 TKO genannten öffentlichen Telekommunikationsdienste werden nicht hinreichend präzise umschrieben. Diese Dienste dürfen nur zugelassen werden, soweit sich aus den ihren Einsatz regelnden gesetzlichen Bestimmungen die Voraussetzungen und der Umfang der Einschränkung des Rechts auf informationelle Selbstbestimmung klar und für den Bürger erkennbar ergeben.
3. Durch Veränderung der technischen und betrieblichen Funktionsbedingungen ist eine inhaltliche Umgestaltung einzelner Dienste ohne Änderung der entsprechenden Bestimmungen in der TKO möglich (§ 5 TKO). Eine derartige Ermächtigung der Deutschen Bundespost ist mit den Forderungen des Bundesverfassungsgerichts nach Transparenz der Datenverarbeitung und nach Schaffung einer normenklaren gesetzlichen Grundlage für eine Einschränkung des Rechts auf informationelle Selbstbestimmung nicht vereinbar. Gleiches gilt für die Regelung des § 3 Abs. 1 Satz 3 TKO, nach der das öffentliche Telekommunikationsnetz für sonstige, in der TKO nicht geregelte Telekommunikationszwecke freigegeben werden kann.
4. Die im Zusammenhang mit den öffentlichen Telekommunikationsdiensten maßgeblichen datenschutzrelevanten Begriffe wie „Teilnehmer", „Anbieter", „Abrechnungsdaten", „Verbindungsdaten", „Benutzungsdaten" etc. sollten bei den nach § 2 TKO in einem Anhang zu dieser Verordnung festgelegten Begriffsbestimmungen aufgeführt werden. In einem Anhang sollten ferner die bei der Nutzung der einzelnen Dienste anfallenden personenbezogenen Daten erläutert werden. Nur so kann der Bürger als Nutzer der öffentlichen Kommunikationsdienste entsprechend einer Forderung des Bundesverfassungsgerichts wissen, welche personenbezogenen Daten die Deutsche Bundespost wann und bei welcher Gelegenheit über ihn verarbeitet.
5. Wiederholt wird die Zulässigkeit der Verarbeitung personenbezogener Daten damit begründet, daß sie aus „betriebsbedingten Gründen" erforderlich sei. Dieser Rechtsbegriff bedarf einer Definition in der TKO, aus der hervorgeht, welcher Art diese Gründe sein können, wobei die Eigenart der verschiedenen Dienste zu berücksichtigen ist.
6. Die Allgemeinen Vorschriften zum Datenschutz in Teil VII Abschnitt 2 TKO bedürfen der Ergänzung und Präzisierung:
   - Wann Bestandsdaten, Verbindungsdaten und Gebührendaten zu löschen sind, ist teils überhaupt nicht, teils nur unbestimmt geregelt. So dürfen Verbindungsdaten aus „betriebsbedingten Gründen" auf unbestimmte Zeit gespeichert werden. Gleiches gilt, wenn der Teilnehmer „eine andere Art der Verarbeitung" beantragt hat; die Voraussetzungen hierfür werden nämlich nicht festgelegt.
   - Auch die Bestimmungen über die Verarbeitung der Gebührendaten müssen so formuliert werden, daß keine unzulässigen Schlüsse auf ein Teilnehmerverhalten gezogen werden können.
   - Die Regelungen umfassen nicht alle bei der Post anfallenden Daten. Beispielsweise fehlen Regelungen zu den Inhalten der Informationen und den beim Betrieb der Dienste anfallenden Daten.
   - Die Vorschriften erlauben der Post, alle Daten zu beliebigen „Telekommunikationszwecken" zu verwenden. Unerläßlich ist eine Nutzungsbeschränkung auf die Zwecke der jeweils in Anspruch genommenen Dienste.

— Die Regelung der Befugnis, Daten weiterzugeben, ist zu umfassend und unklar. Insbesondere sollten Verbindungsdaten von jeder Übermittlung ausgeschlossen bleiben.

— Trotz der Fülle und der besonderen Sensitivität der bei der Post vorhandenen personenbezogenen Daten fehlen spezielle Vorschriften über die Datensicherung.

Insgesamt dürfen die allgemeinen Datenschutzregelungen nicht hinter dem Standard der neuen Mediengesetzgebung zurückbleiben.

7. Auch die Regelungen zu den einzelnen Diensten berücksichtigen die Interessen der Bürger nur unzureichend:

— Beim Telefondienst ist der „Zwangseintrag" der Teilnehmer im Telefonbuch vorgesehen. Insbesondere nach dem Volkszählungsurteil bestehen Zweifel, ob dies mit dem informationellen Selbstbestimmungsrecht noch vereinbar ist.

— Unter welchen Voraussetzungen die Post Daten über einzelne Telefonverbindungen, insbesondere die gewählte Rufnummer, registriert und an wen sie Auskunft darüber gibt, ist nicht geregelt. Das gleiche gilt für die sog. Fangschaltung. Beim Funktelefon speichert die Post ohne Rechtsgrundlage detaillierte Verbindungsdaten.

— Trotz seiner Annäherung an die Struktur der Datenschutzbestimmungen des Bildschirmtext-Staatsvertrages (Btx-StV) bleibt der Regelungsgehalt des § 387 TKO hinter Art. 9 Btx-StV zurück. Dies betrifft insbesondere die Regelung zu den Verbindungsdaten sowie Definition und Umfang der Vergütungsdaten. Ein klares Verbot der Übermittlung von Vergütungsdaten an Dritte fehlt. Ferner fehlt ein Verbot der Übermittlung von Daten, die im Zusammenhang mit der Übermittlung von Mitteilungs- und Antwortseiten anfallen. Unzureichend ist auch der Umfang der technischen und organisatorischen Maßnahmen zur Datensicherung geregelt.

8. Abgesehen von Kritik an Einzelbestimmungen des Entwurfs der TKO bleiben wesentliche Fragen offen:

— Eine auf den Netzbereich beschränkte Regelung, für die allein der Bund zuständig ist, muß wesentliche Aspekte der Medienordnung ungeregelt lassen. Auch die in die Länderkompetenz fallenden Nutzungs- und Anwendungsbereiche werfen Datenschutzprobleme auf, die von der jeweiligen Netzstruktur abhängig sind, und die bereits bei der Konzeption der Dienste berücksichtigt werden müssen.

— Auch bei der in Aussicht genommenen Regelung weiterer Dienste (z. B. Breitbandkommunikationsdienste, Fernwirkdienste) sind entsprechende spezielle Datenschutzregelungen in die TKO aufzunehmen.

— Zur Fortentwicklung der datenschutzrechtlichen Möglichkeiten der TKO wird die Post aufgefordert, bei der Neu- und Umgestaltung einzelner Telekommunikationsdienste datenschutzfreundliche Lösungen zu realisieren. So sollten Überlegungen angestellt werden, ob nicht z. B. ein Dienst zur Verschlüsselung der Nachrichten sowie Verfahren der Gebührenzählung bzw. -abrechnung beim Teilnehmer eingeführt werden können.

— In Anbetracht der Bedeutung einer künftigen Telekommunikationsstruktur und im Hinblick auf künftige Diensteinführungsentscheidungen sind nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder verfassungsrechtliche Zweifel angebracht, ob die Verordnungsermächtigung aus § 14 PostVwG für die Regelung solcher wesentliche Bereiche des öffentlichen Lebens bestimmender Sachverhalte noch als ausreichend anzusehen ist oder ob nicht vielmehr der Gesetzgeber die wesentlichen Entscheidungen treffen muß.

Anlage 6 (zu 19.1)

SCHUFA-Klausel für Kontoeröffnungsanträge

Ich/Wir willige(n) ein, daß die Bank der für meinen/unseren Wohnsitz zuständigen SCHUFA-Gesellschaft (Schutzgemeinschaft für allgemeine Kreditsicherung) Daten über die Beantragung, die Aufnahme und Beendigung dieser Kontoverbindung übermittelt.

Unabhängig davon wird die Bank der SCHUFA auch Daten aufgrund nicht vertragsgemäßen Verhaltens (z. B. Scheckkartenmißbrauch durch den rechtmäßigen Karteninhaber, Scheckrückgabe mangels Deckung, Wechselprotest, beantragter Mahnbescheid bei unbestrittener Forderung sowie Zwangsvollstrekkungsmaßnahmen) melden. Diese Meldungen dürfen nach dem Bundesdatenschutzgesetz nur erfolgen, soweit dies zur Wahrung berechtigter Interessen der Bank, eines Vertragspartners der SCHUFA oder der Allgemeinheit erforderlich ist und dadurch meine/unsere schutzwürdigen Belange nicht beeinträchtigt werden.

Soweit hiernach eine Übermittlung erfolgen kann, befreie(n) ich/wir die Bank zugleich vom Bankgeheimnis.

Die SCHUFA speichert die Daten, um den ihr angeschlossenen Kreditinstituten, Leasinggesellschaften, Einzelhandels-, Versandhandels- und sonstigen Unternehmen, die gewerbsmäßig Geld- oder Warenkredite an Konsumenten geben, Informationen zur Beurteilung der Kreditwürdigkeit von Kunden geben zu können. Sie stellt diese Daten ihren Vertragspartnern nur zur Verfügung, wenn diese ein berechtigtes Interesse an der Datenübermittlung glaubhaft darlegen. Die SCHUFA übermittelt nur objektive Daten ohne Angabe des kontoführenden Instituts; subjektive Werturteile, persönliche Einkommens- und Vermögensverhältnisse sind in SCHUFA-Auskünften nicht enthalten.

Ich kann/Wir können Auskunft bei der SCHUFA über die mich/uns betreffenden gespeicherten Daten erhalten. Die Adresse der SCHUFA lautet:

Ich/Wir willige(n) ein, daß im Falle eines Wohnsitzwechsels die vorgenannte SCHUFA die Daten an die dann zuständige SCHUFA übermittelt.

Weitere Informationen über das SCHUFA-Verfahren enthält ein Merkblatt, das auf Wunsch zur Verfügung gestellt wird.

SCHUFA-Klausel für Kreditanträge

Ich/Wir willige(n) ein, daß die Bank der für meinen/unseren Wohnsitz zuständigen SCHUFA-Gesellschaft (Schutzgemeinschaft für allgemeine Kreditsicherung) Daten über die Beantragung, die Aufnahme (Kreditnehmer, Mitschuldner, Kreditbetrag, Laufzeit, Ratenbeginn) und vereinbarungsgemäße Abwicklung (z. B. vorzeitige Rückzahlung, Laufzeitverlängerung) dieses Kredits übermittelt.

Unabhängig davon wird die Bank der SCHUFA auch Daten aufgrund nicht vertragsgemäßer Abwicklung (z. B. Kündigung des Kredits, Inanspruchnahme einer vertraglich vereinbarten Lohnabtretung, beantragter Mahnbescheid bei unbestrittener Forderung sowie Zwangsvollstreckungsmaßnahmen) melden. Diese Meldungen dürfen nach dem Bundesdatenschutzgesetz nur erfolgen, soweit dies zur Wahrung berechtigter Interessen der Bank, eines Vertragspartners der SCHUFA oder der Allgemeinheit erforderlich ist und dadurch meine/unsere schutzwürdigen Belange nicht beeinträchtigt werden.

Soweit hiernach eine Übermittlung erfolgen kann, befreie(n) ich/wir die Bank zugleich vom Bankgeheimnis.

Die SCHUFA speichert die Daten, um den ihr angeschlossenen Kreditinstituten, Leasinggesellschaften, Einzelhandels-, Versandhandels- und sonstigen Unternehmen, die gewerbsmäßig Geld- oder Warenkredite an Konsumenten geben,

Informationen zur Beurteilung der Kreditwürdigkeit von Kunden geben zu können. Sie stellt diese Daten ihren Vertragspartnern nur zur Verfügung, wenn diese ein berechtigtes Interesse an der Datenübermittlung glaubhaft darlegen. Die SCHUFA übermittelt nur objektive Daten ohne Angabe des Kreditgebers; subjektive Werturteile, persönliche Einkommens- und Vermögensverhältnisse sind in SCHUFA-Auskünften nicht enthalten.

Ich kann/Wir können Auskunft bei der SCHUFA über die mich/uns betreffenden gespeicherten Daten erhalten. Die Adresse der SCHUFA lautet:

Ich/Wir willige(n) ein, daß im Falle eines Wohnsitzwechsels die vorgenannte SCHUFA die Daten an die dann zuständige SCHUFA übermittelt.

Weitere Informationen über das SCHUFA-Verfahren enthält ein Merkblatt, das auf Wunsch zur Verfügung gestellt wird.

Sachregister

Abgabenordnung 20
Abstrahlung 74f.
Arbeitsmedizinische Dienste 47
Ärztliche Gutachten und Atteste 24, 49f., 53
Ärztliche Schweigepflicht 89
Akten 50, 53, 76, 78, 90f.
Akteneinsicht 19f.
Aktennachweis des BKA 59
Amtsgeheimnis 78
Anschriftenermittlung 34f.
Arbeitsberatung 48f.
Arbeitsdatei PIOS innere Sicherheit (APIS) 60ff.
Arbeitsgemeinschaft für wirtschaftliche Verwaltung e. V. (AWV) 10, 71
Arbeitslosenhilfe 49
Arbeitsvermittlung 48f.
Arztrechnung 24f.
Auskunftsverweigerungsrecht 77, 87
Ausländerzentralregister 15f.
Ausweisregister 14
Autotelefon 31

Baugesetzbuch 21f.
Beihilfe 22f.
Berufsförderung 50
Bestattungsunternehmen 17
Betriebskrankenkasse 51ff.
Beurteilungen 26ff.
Bewerbungsunterlagen 48
Bildschirmtext (Btx) 30, 31
Breitbandkabelnetz 31f., 34
Bürokommunikation 13, 70, 72, 73
Bundesamt für Verfassungsschutz 55, 57, 62f.
Bundesaufsichtsamt für das Versicherungswesen 70
Bundesbahn 27, 40f.
Bundesdruckerei 14
Bundesgrenzschutz 63f.
Bundeskanzleramt 28
Bundeskartellamt 69
Bundeskriminalamt 58ff.
Bundesnachrichtendienst 63
Bundespost 29ff.
Bundesverfassungsschutzgesetz 5f., 84, 90f.

Dateibegriff 76, 86
Dateiveröffentlichung 46f.
Datenschutzkonvention 79
Deutscher Bundestag 13
Deutsches Patentamt 26f.
Diagnose 23

Einkommensnachweis 49, 53
Einreisebedenken 16
Einwilligung 47f., 54, 70, 87
Erbschaftssteuer 16
Europarat 79

Fahndung 6, 14, 20
Fahrzeugregister 35f.
Fernadressierbarer Teilnehmerkonverter (FAT) 34
Fernmeldeordnung 30
Fernsehgewohnheiten 34
Fernsprechteilnehmer 29f.
Flugunfalluntersuchung 40
Freiwilligkeit der Angaben 47
Führerschein auf Probe 30f.

Grenzaktennachweis (GAN) 63f.
Grenzkontrolle 14

Handels- und Gaststättenzählung 45f.

Internationale Datenschutzkonferenz 80
ISDN 11, 13

JURIS 13, 20, 72
Justizmitteilungsgesetz 19

Kabelfernsehen 30, 31ff.
Kabelpilotprojekt Dortmund 33f.
Kfz-Zulassung 37f.
Kindergeld 24, 26
Kompromittierende Abstrahlung 74f.
Kontrollbefugnis des BfD 55, 78, 87
Kontrollmitteilungen 20f.
Koordinierungs- und Beratungsstelle der Bundesregierung für die Datenverarbeitung in der Bundesverwaltung (KBSt) 71
Krankenhausentlassungsbericht 53
Krankenhilfe 53
Krankenkasse 53ff.
Krankenversorgung der Bundesbahnbeamten 50f.
Kredit 68ff., 94
Kreiswehrersatzamt 66, 67
Kriegsdienstverweigerer 18, 67f.
Kündigungsgrund 48
Kur 53
Kurbericht 24

Leiharbeitsfirma 54
Leistungskontrolle 51
Lohnsteuerkarten 25f.
Luftfahrzeugrolle 39
Luftsicherheit 40

MAD-Gesetz 6
Medienerprobungs- und -entwicklungsgesetz 32f.
Melderegister 14, 16
Militärischer Abschirmdienst (MAD) 65
Mitbestimmung 51
Mitteilungen in Strafsachen (MiStra) 19
Mitteilungen in Zivilsachen (MiZi) 19

Nachlaßwert 16f.
NADIS 61f.
Netz 72ff.
Novellierung des BDSG 4ff., 69, 75ff., 86ff.

Online-Anschluß, -Zugriff 13, 76, 87

PARLAKOM 13f.
Paß 14, 84
Personal
-akten 22, 52
-informationssysteme 26ff.
-nachrichten in Hausmitteilungen 26
Personalausweis 14f., 31, 84
-gesetz 4
Personal-Computer (PC) 27, 70ff., 73, 76, 87
Personengebundene Hinweise 58
Personenstandsrecht 16
Persönlichkeitsprofil 56
PIOS 58, 59, 60
Polizeirecht 5
Postbeamtenkrankenkasse 23
Posteigene Werbung 34f.
Postgeheimnis 34, 87
Postgiroverfahren 25
Psychologische Tests 66

Rasterfahndung 20
Recht auf informationelle Selbstbestimmung 4ff., 75f., 89, 84f., 87, 89
Rentenversicherungsnummer 47
Reservisten 66f.
Rezept 24f.
Richterprofil 20
Rückkanal 32, 33f.

Sanierungsmaßnahmen 21
Satellitenfunk 31ff.
Schleppnetzfahndung 14
SCHUFA 68ff., 94
Schwarzseher 32
Schweigepflichtenbindungsklausel 70
Seriennummer 14
Sicherheitsbehörden 6
Sicherheitsgesetz 4f., 56, 84f.
Sicherheitsüberprüfung 56ff., 90
Soldaten 67, 88
Sozialdaten 52
Spionageabwehr 90, 91
Spurendokumentationssystem (SPUDOK) 58, 59f.
Standesbeamter 16f.
Statistik 4, 42ff.
Statistikbereinigungsgesetz 44f.
Steuerbereinigungsgesetz 20
Steuerbescheid 24, 53
Steuerdaten 16
Steuergeheimnis 45f.
Strafprozeßordnung 14, 15, 19f.
Straßenverkehrsgesetz 35f.

Telebox-Dienst der Post 13
Telefon 29ff.
Telefonbuch 31
Telefonverbindungsdaten 28, 31
Telekommunikationsordnung (TKO) 30, 92f.
Terrorismus 6, 35, 90f.
Transparenz 11, 48, 77
Totenliste 16f.

Übergangsbonus 6f., 57, 65
Unabhängigkeit des BfD 12
Unfallfürsorge 24

Verhaltenskontrolle 28f.
Verkehrs- und Tarifverbünde 40f.
Verkehrszentralregister 36
Versicherung 70
Verwaltungsverfahrensgesetz 5f., 76, 86
Videoaufzeichnung 41, 76, 86
Volkszählung 4, 45
Vorkaufsrecht 21

Wahlhelfer 17f.
Wehrpflichtiger 65f., 67f.
Werbung 34
Wohnungsfürsorge 25
Zivildienst 18f.
Zollkriminalinstitut 64
Zusammenarbeitsgesetz (ZAG) 6
Zwangseintrag 31
Zweckbindung 29, 53, 54, 56, 57, 77, 87f.

Abkürzungsverzeichnis

ADV	Automatisierte Datenverarbeitung
AFG	Arbeitsförderungsgesetz
AO	Abgabenordnung
APIS	Arbeitsdatei PIOS innere Sicherheit
AZR	Ausländerzentralregister
BAG	Bundesarbeitsgericht
BAT	Bundesangestelltentarifvertrag
BDSG	Bundesdatenschutzgesetz
BfD	Bundesbeauftragter für den Datenschutz
BfV	Bundesamt für Verfassungsschutz
BGBl	Bundesgesetzblatt
BGS	Bundesgrenzschutz
BKA	Bundeskriminalamt
BMA	Bundesminister für Arbeit und Sozialordnung
BMBau	Bundesminister für Raumordnung, Bauwesen und Städtebau
BMF	Bundesminister der Finanzen
BMFT	Bundesminister für Forschung und Technologie
BMI	Bundesminister des Innern
BMJ	Bundesminister der Justiz
BMJFFG	Bundesminister für Jugend, Familie, Frauen und Gesundheit
BMP	Bundesminister für das Post- und Fernmeldewesen
BMU	Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit
BMV	Bundesminister für Verkehr
BMVg	Bundesminister der Verteidigung
BND	Bundesnachrichtendienst
BRH	Bundesrechnungshof
BStatG	Bundesstatistikgesetz
Btx	Bildschirmtext
BVerfG	Bundesverfassungsgericht
BVerfGE	Bundesverfassungsgerichtsentscheidung
DB	Deutsche Bundesbahn
DBP	Deutsche Bundespost
DV	Datenverarbeitung
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
G 10	Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses
GAN	Grenzaktennachweis
GG	Grundgesetz
GMBl	Gemeinsames Ministerialblatt
GOBReg	Geschäftsordnung der Bundesregierung
INPOL	Informationssystem der Polizei
ISDN	Integrated Services Digital Network
JURIS	Juristisches Informationssystem
KAN	Kriminalaktennachweis
KBA	Kraftfahrt-Bundesamt
KDV	Kriegsdienstverweigerer
KpS	Kriminalpolizeiliche personenbezogene Sammlungen
MAD	Militärischer Abschirmdienst
MDT	Mittlere Datentechnik
MiStra	Mitteilungen in Strafsachen
MiZi	Mitteilungen in Zivilsachen
MRRG	Melderechtsrahmengesetz

NADIS	Nachrichtendienstliches Informationssystem
PC	Personal-Computer
PersVG	Personalvertretungsgesetz
PIOS	Auskunftssystem über Personen, Institutionen, Objekte und Sachen
PostVwG	Postverwaltungsgesetz
PZD	Personen-Zentral-Datei
RVO	Reichsversicherungsordnung
SCHUFA	Schutzgemeinschaft für allgemeine Kreditsicherung GmbH
SGB	Sozialgesetzbuch
SGB X	Sozialgesetzbuch Zehntes Buch
SPUDOK	Spurendokumentationssystem
STATIS	Statistisches Informationssystem
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
StVG	Straßenverkehrsgesetz
StVZO	Straßenverkehrs-Zulassungs-Ordnung
TB	Tätigkeitsbericht*)
TEMEX	Telemetry Exchange (Fernwirkdienst der DBP)
TKO	Telekommunikationsordnung
VwVfG	Verwaltungsverfahrensgesetz
WEWIS	Wehrersatzweseninformationssystem
ZEVIS	Zentrales Verkehrsinformationssystem

*) Erster Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 8/2460
Zweiter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 8/3570
Dritter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 9/93
Vierter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 9/1243
Fünfter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 9/2386
Sechster Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 10/877
Siebenter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 10/2777
Achter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 10/4690