Deutscher Bundestag
10. Wahlperiode

Drucksache 10/4690

17. 01. 86

Sachgebiet 204

Unterrichtung

durch die Bundesregierung

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

Gliederung

		Seite
1.	**Einleitung**	4
1.1	Überblick	4
1.2	Kooperation	8
1.3	Öffentlichkeitsarbeit	8
2.	**Innere Verwaltung**	8
2.1	Neue Personalausweise und Pässe	8
2.2	Melderecht	10
2.3	Ausländerzentralregister	10
2.4	Wahlrecht	11
2.5	Bundesamt für den Zivildienst	11
3.	**Rechtswesen**	11
3.1	Bundeszentralregister	11
3.2	Mitteilungen in Zivilsachen	12
3.3	Schuldnerverzeichnis	12
4.	**Bauwesen**	13
5.	**Personalwesen**	13
5.1	Konventionelle Personaldatenverarbeitung	13
5.1.1	Beihilfe	13
5.1.2	Umgang mit ärztlichen Unterlagen	14
5.1.3	Einzelfälle	15
5.2	Automatisierte Personaldatenverarbeitung	16
5.2.1	Personalinformationssysteme	16
5.2.2	Leistungs- und Verhaltenskontrolle	16
5.2.3	Dezentralisierung der automatisierten Personaldatenverarbeitung	17
5.2.4	Mitbestimmung und bereichsspezifische gesetzliche Regelung des Arbeitnehmerdatenschutzes	18
6.	**Deutsche Bundespost**	19
6.1	Zusammenarbeit mit dem Bundesminister für das Post- und Fernmeldewesen	19
6.2	Bildschirmtext	19
6.2.1	Stand der Entwicklung	19
6.2.2	Kontrollkompetenz; Regelungsdefizite	19
6.2.3	Datenschutzkontrollen	20
6.3	Telefon-Fernwirksystem TEMEX	20
6.3.1	Projektstand	20
6.3.2	Datenschutzbegleitgremium	20
6.3.3	Regelungsbedarf	21
6.4	Eintrag der Teilnehmer ins Telefonbuch	21
6.4.1	„Zwangseintragung"	21
6.4.2	Elektronisches Telefonbuch	21
6.5	Fernsprechauskunft	22
6.6	Registrierung der Verbindungsdaten von Telefongesprächen bei belästigenden Anrufen	22
6.7	Weitergabe von Telefonkundenanschriften zu Werbezwecken	22
6.8	Ermittlung von Anschriften Neugeborener durch Postzusteller	23
7.	**Verkehrswesen**	23
7.1	Fahrzeugregistergesetz (ZEVIS)	23
7.1.1	Datenerhebung	24
7.1.2	Datennutzung	24

Zugeleitet mit Schreiben des Bundesbeauftragten für den Datenschutz — I — 192 111/10 — vom 17. Januar 1986 gemäß § 19 Abs. 2 des Bundesdatenschutzgesetzes.

		Seite
7.1.3	Kontrolle der Datennutzung	24
7.1.4	Abruf im automatisierten Verfahren	24
7.2	Führerschein auf Probe	25
7.3	Video-Überwachung von Einrichtungen der Deutschen Bundesbahn (DB)	25
8.	**Bundesarchivgesetz**	26
9.	**Statistik**	27
9.1	Volkszählungsgesetz und Mikrozensusgesetz	27
9.2	Handels- und Gaststättenzählung	27
9.3	Hochschulstatistikgesetz	28
9.4	Bundesstatistikgesetz	28
10.	**Sozialwesen**	29
10.1	Bundeserziehungsgeldgesetz	29
10.2	Hinterbliebenenrenten- und Erziehungszeiten-Gesetz (HEZG)	29
10.3	Sozialversicherungsnummer	29
10.4	Arbeitsverwaltung	30
10.5	Krankenversicherung	31
10.6	Gesundheitswesen	32
10.6.1	Ärztliche Entlassungsberichte	32
10.6.2	Perinatologische Erhebungen	34
10.6.3	Dialyse-Patienten-Fragebogen	34
11.	**Öffentliche Sicherheit — Allgemeines**	35
11.1	Kontrollen und Ergebnisse	35
11.1.1	Bundeskriminalamt (BKA)	35
11.1.2	Bundesgrenzschutz	36
11.1.3	Bundesamt für Verfassungsschutz (BfV)	36
11.1.4	Militärischer Abschirmdienst (MAD)	36
11.1.5	Bundesnachrichtendienst (BND)	37
11.1.6	Zusammenfassende Würdigung	37
11.2	Gesetzgebungsvorhaben und deren datenschutzrechtliche Bewertung	37
11.3	Datenschutz bei der Sicherheitsüberprüfung	39
11.3.1	Die jüngsten Ereignisse und das Verlangen nach mehr Sicherheit	39
11.3.2	Forderungen des Datenschutzes	39
11.4	Internationale Zusammenarbeit der Sicherheitsbehörden und internationaler Datenschutz bei den Sicherheitsbehörden	39
11.4.1	Verstärkung der internationalen Zusammenarbeit	39
11.4.2	Verstärkung des internationalen Datenschutzes	40
11.5	Offene Fragen aus meiner Kontrolltätigkeit	40
12.	**Bundeskriminalamt (BKA)**	41
12.1	Probleme aus der Datenverarbeitungsstruktur beim BKA	41
12.2	Kriminalaktennachweis — Theorie und Praxis	43
12.3	Personengebundene Hinweise und Gefahr der sozialen Abstempelung	44
12.4	Das fortdauernde Problem der Speicherung „anderer Personen"	45
12.5	Ungelöste Probleme bei der Abteilung Staatsschutz	46
13.	**Nachrichtendienste**	47
13.1	Bundesamt für Verfassungsschutz (BfV)	47
13.1.1	Konsequenzen aus der datenschutzrechtlichen Kontrolle bei der Abteilung III	47
13.1.2	Die Weiterentwicklung der Datenverarbeitung beim BfV	49
13.1.3	Sonderdatei im Rahmen der Sicherheitsüberprüfung	49
13.2	Militärischer Abschirmdienst	50
13.2.1	Personelle Vorbeugung	50
13.2.2	Zweckbindung der Daten aus der Sicherheitsüberprüfung	50
14.	**Verteidigung**	50
14.1	Wehrersatzwesen	50
14.1.1	Umgang mit KDV-Unterlagen	51
14.1.2	Vorschriften zur Wehrerfassung	51
14.2	Verband der Reservisten	51
15.	**Nicht-öffentlicher Bereich**	52
15.1	SCHUFA-Klausel	52
15.2	Versicherungen	53
15.3	Fehlende Datenschutzkontrolle bei mittelbarer Datenverarbeitung	54
16.	**Datensicherung**	55
16.1	Beratung in Sicherheitsfragen	55
16.2	Der Beitrag von Kontrollen zur Datensicherung	55
16.3	Personal Computer	56
16.3.1	Datenschutzmaßnahmen für Anlagen, die nicht zur Verarbeitung personenbezogener Daten eingesetzt werden sollen	57
16.3.2	Sicherung gegen ungefugte Datenverarbeitung mit PC	57
16.3.3	Datenschutzrechtliche Überlegungen vor der Anschaffung und dem Einsatz von PC	58
17.	**Novellierung des Bundesdatenschutzgesetzes und Gesetzgebung im Bereich der öffentlichen Sicherheit**	59
18.	**Ausland und Internationales**	60
18.1	Europarat	60
18.2	Zusammenarbeit der Datenschutz-Kontrollinstanzen	60
19.	**Bilanz**	60
	Anlage 1 (zu Nr. 10.6.2): Datenschutz bei der Perinataldokumentation	64
	Anlage 2 (zu Nrn. 11.2 und 11.4.1): Anforderungen an Datenschutzregelungen im Polizeirecht	65
	Anlage 3 (zu Nr. 11.3.2): Anforderungen an Datenschutzregelungen für den Verfassungsschutz	68

Seite

Anlage 4 (zu Nrn. 11.4.2 und 18.2):
Beschluß der internationalen Datenschutzkonferenz zu Grundsätzen der polizeilichen Datenverarbeitung 71

Anlage 5 (zu Nr. 12.3):
Speicherung personengebundener Hinweise im INPOL-System 72

Seite

Anlage 6 (zu Nr. 18.1):
Empfehlung Nr. R (85) 20 des Ministerkomitees an die Mitgliedsstaaten zum Schutz personenbezogener Daten bei der Verwendung für Zwecke der Direktwerbung 73

Sachregister 76

Abkürzungsverzeichnis 78

1. Einleitung

1.1 Überblick

Der Datenschutz in der Bundesrepublik Deutschland hat im Berichtsjahr 1985 weitere Fortschritte gemacht, die insbesondere an zwei Erscheinungen deutlich werden. Die für die Gesetzgebung Verantwortlichen haben akzeptiert und in ihre Konzeptionsplanung aufgenommen, daß dort, wo der Gesetzesvollzug zur Verarbeitung personenbezogener Daten führt, dieser Eingriff in die informationelle Selbstbestimmung nur durch eine am überwiegenden Allgemeininteresse orientierte und dem Gebot der Normenklarheit genügende Rechtsvorschrift gerechtfertigt werden kann. Zahlreiche Gesetzgebungsaktivitäten sind darauf zurückzuführen oder wurden davon beeinflußt. Damit hat das Urteil des Bundesverfassungsgerichts vom 15. Dezember 1983 zum Volkszählungsgesetz 1983 nach anfänglicher „Denkpause" und sich anschließender Überprüfung der jeweils einschlägigen Rechtsgebiete sichtbare Früchte getragen. Ich nenne an abgeschlossenen Gesetzgebungsvorhaben das Mikrozensusgesetz und das Volkszählungsgesetz 1987; beide Gesetze wurden im Berichtsjahr nach intensiven parlamentarischen Beratungen verabschiedet, andere sind auf dem Weg. Der Deutsche Bundestag hat die endgültige Verabschiedung des neuen Personalausweisgesetzes, mit dem der gegenwärtige Personalausweis durch eine fälschungssichere und maschinell lesbare Identitätskarte abgelöst werden soll, bis zur Vorlage wesentlicher Neuregelungen für die Arbeit der Sicherheitsbehörden zurückgestellt. Dies führte zu entsprechenden Initiativen der Koalitionsfraktionen: Mit der notwendig gewordenen Änderung des Personalausweisgesetzes und der Änderung des Paßgesetzes wurden insgesamt sieben Gesetzentwürfe, zu denen auch die Novellierung des Bundesdatenschutzgesetzes gehört, vorbereitet und in intensiven Beratungen weitgehend fertiggestellt. Ich hatte Gelegenheit, mich zu den Entwürfen in einer bestimmten Beratungsphase zu äußern. Von einer eingehenden inhaltlichen Bewertung möchte ich jedoch an dieser Stelle absehen, da die Entwürfe im Berichtsjahr leider noch nicht endgültig abgeschlossen werden konnten, und ich auch keine Kenntnis davon habe, ob meine Empfehlungen berücksichtigt wurden (siehe unten Nrn. 7.1, 11.2, 17.). Diese gesetzgeberischen Anstrengungen machen aber deutlich, daß das Verständnis für den Datenschutz gewachsen ist und er inzwischen überall als ein verfassungsrechtliches Postulat begriffen wird, dem sich die für die Gesetzgebung Verantwortlichen nicht entziehen können, auch wenn dies den Abschied von manchen bequemen Gewohnheiten in der Verwaltungspraxis bedeuten könnte.

Die nachhaltige Berichterstattung in den Medien über diese Gesetzgebungsvorhaben, auch wenn sie den bekanntgewordenen Regelungsinhalt überwiegend kritisch würdigte, hat dazu beigetragen, das durch die Volkszählungsdiskussion ohnehin gestärkte Datenschutzbewußtsein in der Bevölkerung weiter zu verbreiten und zu vertiefen. Es ist zu hoffen, daß diese Tendenz anhält und dazu führt, Datenschutz als selbstverständlichen Bestandteil aller derjenigen Vorgänge in der öffentlichen Verwaltung und in der Wirtschaft zu begreifen, die sich auf den Umgang mit personenbezogenen Daten beziehen.

Ich gründe meine eingangs getroffene Feststellung von den Fortschritten des Datenschutzes noch auf eine weitere Erfahrung dieses Berichtsjahrs: Meine beiden letzten Tätigkeitsberichte (6. TB für 1983 und 7. TB für 1984) wurden in ungewöhnlich breit angelegten und eingehenden Beratungen in zahlreichen Bundestagsausschüssen, insbesondere aber in vielen Sitzungen des Innenausschusses erörtert. Für mich waren diese Beratungen — bei aller damit verbundenen zeitlichen Belastung — ein deutliches Zeichen dafür, daß Datenschutzfragen im Parlament auf ein überaus starkes Interesse stoßen und einen hohen politischen Stellenwert bei allen Fraktionen des Deutschen Bundestages erreicht haben. Nach meinem Eindruck machen sich immer mehr Parlamentarier in dieser komplizierten Materie sachkundig, was vertiefte und weiterführende Diskussionen ermöglicht und damit auch zur Stärkung der Rechte der Bürger beiträgt. Ich werte dies aber auch als erfreulichen Beweis für die Akzeptanz meiner Arbeit und berichte darüber vor allem auch deshalb, um den Bürgern die Gewißheit zu verschaffen, daß ihr „Recht auf informationelle Selbstbestimmung" als Ausfluß des verfassungsrechtlich verankerten allgemeinen Persönlichkeitsrechts in der politischen Arbeit beachtet und als unverzichtbare Voraussetzung des Zusammenlebens in einem freiheitlichen Gemeinwesen respektiert wird.

Die sich bereits im vergangenen Jahr (vgl. 7. TB S. 5) abzeichnende Tendenz, meine Dienststelle mehr und mehr für die Beratung in Datenschutzfragen in Anspruch zu nehmen, hat im Berichtsjahr erheblich zugenommen. Bundesministerien, nachgeordnete Behörden und insbesondere Abgeordnete, Ausschüsse und Fraktionen des Deutschen Bundestages haben mich in unerwartet starkem Maß um Stellungnahmen zu Gesetzgebungsvorhaben gebeten, bei der Vorbereitung anderer Vorschriften zu Rate gezogen oder über meine Auffassung zu Datenverarbeitungsprojekten befragt. Teils habe ich darauf mit schriftlichen Ausarbeitungen geantwortet, teils wurden mehr oder weniger intensive Beratungsgespräche geführt, die selbstverständlich stets sorgfältiger Vorbereitung innerhalb meiner Behörde bedurften; abgesehen hiervon habe ich im Berichtsjahr an insgesamt sieben öffentlichen Anhörungsverfahren teilgenommen, von denen fünf vom Innenausschuß und zwei von Fraktionen veranstaltet wurden. Ich bedauere, daß infolge solcher Inanspruchnahmen etwa ein Drittel der geplanten 46 Kontrollen bei Bundesbehörden zurückgestellt werden mußte, da die Arbeitskapazität meiner Behörde auf eine Beratungstätigkeit dieses Umfangs

nicht ausgelegt ist. In den Haushaltsberatungen für das Jahr 1986 wurde mir zwar eine weitere Stelle für einen Mitarbeiter des höheren Dienstes zugestanden. Ich erkenne diese Bemühung um die Verbesserung der Arbeitsfähigkeit meiner Dienststelle dankend an, halte aber weitere Personalaufstokkungen für notwendig (vgl. 7. TB S. 6). Da auch die Vorbereitung des Tätigkeitsberichts erhebliche Kräfte meiner Dienststelle über einen längeren Zeitraum bindet, hielt ich es für zweckmäßig, diesen Bericht gegenüber den früheren Berichten zu straffen und ihn in der Darstellung noch stärker auf das für die parlamentarische Beratung Wesentliche abzustellen. Ich gehe dabei davon aus, daß ich in den Ausschußberatungen, die dadurch möglicherweise konzentriert werden können, Gelegenheit zu weiteren Ausführungen haben werde.

Die nachfolgende Zusammenstellung soll eine Übersicht über die Beratungsersuchen des Jahres 1985 und ihre Erledigung geben:

Thema	Art der Erledigung
Novellierung des BDSG	Anhörung im Innenausschuß des Deutschen Bundestages mit schriftlicher Stellungnahme
— Entwurf der SPD-Fraktion	
— Entwurf der Fraktionen der CDU/CSU und der F.D.P.	Beratung der Koalitionsfraktionen des Deutschen Bundestages
Personalausweisgesetz/Paßgesetz	Anhörung im Innenausschuß des Deutschen Bundestages mit schriftlicher Stellungnahme, auch gegenüber dem BMI; Beratung der Koalitionsfraktionen des Deutschen Bundestages
Volkszählungsgesetz 1987	Anhörung im Innenausschuß des Deutschen Bundestages mit schriftlicher Stellungnahme
Mikrozensusgesetz	Anhörung im Innenausschuß des Deutschen Bundestages mit schriftlicher Stellungnahme
Bundesarchivgesetz	— Anhörung der SPD-Fraktion
	— Anhörung im Innenausschuß des Deutschen Bundestages mit schriftlicher Stellungnahme
Novellierung des Bundesstatistikgesetzes	Beratung und schriftliche Stellungnahme gegenüber dem BMI
Novellierung des Bundesverfassungsschutzgesetzes	Beratung der Koalitionsfraktionen des Deutschen Bundestages
Entwurf eines MAD-Gesetzes	Beratung der Koalitionsfraktionen des Deutschen Bundestages
Entwurf eines Gesetzes über die informationelle Zusammenarbeit der Sicherheits- und Strafverfolgungsbehörden des Bundes und der Länder in Angelegenheiten des Staats- und Verfassungsschutzes	Beratung der Koalitionsfraktionen des Deutschen Bundestages
Änderung des Straßenverkehrsgesetzes (Fahrzeugregistergesetzes), ZEVIS	Beratung der Koalitionsfraktionen des Deutschen Bundestages und Beratung des BMV
Einsichtsrecht in Umweltakten	Anhörung der Fraktion DIE GRÜNEN mit schriftlicher Stellungnahme
Beteiligung in einer Verfassungsbeschwerde	schriftliche Stellungnahme gegenüber dem BVerfG
Ausländerrecht	Beratung des BMI, schriftliche Stellungnahmen gegenüber dem BMI
— Ausländerzentralregister	
— Ausländergesetz	
Großversuch TEMPO 100	schriftliche Stellungnahme gegenüber dem BMV
Hinterbliebenenrenten- und Erziehungszeiten-Gesetz (HEZG) einschl. Rechtsverordnungen	Beratung und schriftliche Stellungnahme gegenüber dem BMA
Entwurf eines Gesetzes zur Beschränkung der Verwendungen von Versicherungsnummern	Beratung des BMA
Sicherheitsüberprüfungsrichtlinien	schriftliche Stellungnahme gegenüber dem BMI

Thema	Art der Erledigung
Hochschulstatistikgesetz	Anhörung beim BMBW und dessen Beratung
Entwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes und des Fahrlehrergesetzes (Fahrerlaubnis auf Probe)	Beratung und schriftliche Stellungnahme gegenüber dem BMV
5. Verordnung zur Änderung straßenverkehrsrechtlicher Vorschriften (u. a. Stufenführerschein, Datenübermittlungen zwischen Sonderfahrerlaubnisbehörden und allgemeinen Fahrerlaubnisbehörden).	schriftliche Stellungnahme gegenüber dem BMV
Steuerbereinigungsgesetz 1986 u. a. Änderung der Abgabenordnung, EG-Amtshilfegesetz, gesetzliche Regelung für das Zoll-Kriminal-Institut (ZKI)	schriftliche Stellungnahme gegenüber dem BMF
Änderung der Fernmeldeordnung wegen Btx und TEMEX	Beratung und schrifliche Stellungnahme gegenüber dem BMP
Postverwaltungsgesetz	Beratung des BMP
Verordnung zur Durchführung des Gesetzes über den Amateurfunker	schriftliche Stellungnahme gegenüber dem BMP
Elektronisches Telefonbuch	Beratung und schriftliche Stellungnahme gegenüber dem BMP
Baugesetzbuch	Beratung und schriftliche Stellungnahme gegenüber dem BMBau
SCHUFA-Klausel, SCHUFA-System	Beratung der Kreditwirtschaft
Datenzugang der Forschung	Beratung von Behörden und Forschungsinstituten
Bundeserziehungsgeldgesetz	schriftliche Stellungnahme gegenüber dem BMJFG
Bundeszentralregistergesetz	Beratung und schriftliche Stellungnahme gegenüber dem BMJ
Zivilprozeßordnung/Regelungen über das Schuldnerverzeichnis	Beratung und schriftliche Stellungnahme gegenüber dem BMJ
Mitteilung in Zivilsachen	schriftliche Stellungnahme gegenüber dem BMJ
Mitteilung in Strafsachen	schriftliche Stellungnahme gegenüber dem BMJ
Entwurf eines Gesetzes zur Bekämpfung der Wirtschaftskriminalität	schriftliche Stellungnahme gegenüber dem BMJ
Grundbuchordnung	schriftliche Stellungnahme gegenüber dem BMJ
Bundesrechtsanwaltordnung	schriftliche Stellungnahme gegenüber dem BMJ
Personenstandsgesetz/Verordnung über Mitteilungspflichten im Personenstandswesen/Ehegesetz	Beratung und schriftliche Stellungnahme gegenüber dem BMI
Bundeswahlgesetz und Bundeswahlordnung	Beratung und schriftliche Stellungnahme gegenüber dem BMI
Zivilschutzgesetz	Beratung und schriftliche Stellungnahme gegenüber dem BMI
Waffengesetz	Beratung und schriftliche Stellungnahme gegenüber dem BMI
Verkartungsplan der Abt. III des BfV	Beratung und schriftliche Stellungnahme gegenüber dem BMI
Regelung zur personellen Vorbeugung des MAD	Beratung und schriftliche Stellungnahme gegenüber dem BMVg
Modellprogramm „Aufsuchende Sozialarbeit"	Beratung des BMJFG

Thema	Art der Erledigung
Auswertung der Rechtsprechung nach dem Betäubungsmittelgesetz	Beratung des BMJFG und BMJ
Änderung der 2. Meldedatenübermittlungsverordnung	Beratung und schriftliche Stellungnahme gegenüber dem BMI
Personaldatenverarbeitung insbesondere wegen — Planung von Personalinformationssystemen — Leistungskontrollen	Beratung verschiedener Ressorts und Personalräte
Auswirkungen neuer Techniken (z. B. PC-Einsatz, Sachbearbeiterdialog)	Beratung von Ressorts, Krankenkassen, Personalräten
Mikroverfilmung z. B. von ärztlichen Unterlagen	Beratung bzw. schriftliche Stellungnahmen gegenüber BMI, BGS und BfA
Organisation von Beihilfestellen	Beratung verschiedener Stellen
Regelungen zum Umgang mit ärztlichen und psychologischen Gutachten	Beratung und schriftliche Stellungnahmen gegenüber der Bundesanstalt für Arbeit
Datenschutz im Krankenhaus	Beratung und Erarbeitung eines Gesamtkonzeptes mit den Landesbeauftragten für den Datenschutz mit dem Ziel einer Empfehlung an die Deutsche Krankenhaus-Gesellschaft

Die für das Kalenderjahr vorgesehenen Datenschutzkontrollen bei Behörden und anderen öffentlichen Stellen des Bundes werden unter Berücksichtigung feststehender Termine, beispielsweise für parlamentarische Beratungen, und der voraussichtlich jeweils verfügbaren Arbeitskapazität zum Beginn eines jeden Jahres in einem Gesamt-Arbeitsplan festgelegt. Dieser steht unter dem Vorbehalt der Änderungen, die durch unvorhersehbare Verpflichtungen ausgelöst werden können, beispielsweise durch Anforderungen von Stellungnahmen zu Gesetzentwürfen, durch Beratungsersuchen, durch unkalkulierbare Ereignisse (wie bekanntgewordene Datenschutzverstöße) und schließlich durch Eingaben und Beschwerden von Bürgern, die unvorhergesehene Einzelüberprüfungen notwendig machen. Das Aufkommen an Eingaben und Bürgerbeschwerden hat sich in den letzten Jahren konstant gehalten und lag im Berichtsjahr bei ca. 1 000 Zuschriften, wobei die Nachfragen nach Informationsmaterial und einfachere Rechtsauskünfte nicht mitgezählt sind.

Bei folgenden Behörden haben Mitarbeiter meiner Dienststelle im Berichtsjahr Kontrollen durchgeführt, Beratungen zur Verbesserung des Datenschutzes vorgenommen oder Informationsbesuche abgestattet, um die dort betriebene Datenverarbeitung kennenzulernen:

Bundesminister des Innern

Bundesminister der Verteidigung

Bundesminister für innerdeutsche Beziehungen

Bundesminister für das Post- und Fernmeldewesen

Generalbundesanwalt

Bundeszentralregister

Statistisches Bundesamt

Bundesgrenzschutz

Bundesnachrichtendienst

Bundesamt für Verfassungsschutz

Bundeskriminalamt

Zoll-Kriminal-Institut

eine Wehrbereichsverwaltung

ein Rechenzentrum der Bundeswehr

ein Kreiswehrersatzamt

Telebox-Zentrale

Btx-Leitzentrale

eine Btx-Vermittlungsstelle

mehrere Fernmeldeämter

Deutsche Bundesbahn

Kraftfahrt-Bundesamt

Bundeszentrale für politische Bildung

Bundesanstalt für Arbeit

Bundesversicherungsanstalt für Angestellte

Bundesdruckerei

Grenzdurchgangslager Friedland

Knappschaftsklinik Bad Neuenahr

eine Geschäftsstelle der Barmer Ersatzkasse

Die wichtigsten Ergebnisse dieser Überprüfungen und Kontakte werden in den einzelnen Abschnitten dieses Berichts näher dargestellt.

1.2 Kooperation

Die Zusammenarbeit mit den Datenschutzbeauftragten der Länder und der Datenschutzkommission Rheinland-Pfalz (§ 19 Abs. 5 BDSG) vollzog sich in gewohnter Weise in der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, die im Berichtsjahr unter dem Vorsitz des Hessischen Datenschutzbeauftragten mehrmals getagt hat. Einzelprobleme wurden in Arbeitskreisen der Konferenz vorberaten. Als wichtigste Diskussionsthemen sind zu nennen:

— die Postdienste Btx und TEMEX,

— Neuregelungen für die Statistik und die Volkszählung 1987,

— Anforderungen an Datenschutzregelungen im Polizeirecht und für den Verfassungsschutz.

Zur letztgenannten Problematik hat die Konferenz zwei umfangreiche Empfehlungen erarbeitet, die jeweils die datenschutzrechtlichen Anforderungen an entsprechende Neuregelungen katalogartig aufführen und inzwischen den zuständigen Stellen beim Bund und in den Ländern übergeben worden sind (siehe dazu unten Nummer 11.2 und Anlagen 2 und 3).

Daneben beteiligten sich Mitarbeiter meiner Dienststelle wiederum an den Beratungen des „Düsseldorfer Kreises", in dem die Aufsichtsbehörden der Länder für den Datenschutz im nichtöffentlichen Bereich gemeinsam interessierende Probleme behandeln.

Schließlich wurden auch die Kontakte zu anderen Stellen außerhalb der öffentlichen Verwaltung, die sich mit Datenschutzfragen befassen, fortgesetzt. Zu nennen sind hier, wie in den vergangenen Jahren, insbesondere die Arbeitsgemeinschaft für wirtschaftliche Verwaltung e. V. (AWV), eine Einrichtung, in der DV-Anwender, Hersteller von DV-Anlagen und betriebliche Datenschutzbeauftragte zusammenarbeiten, und das Deutsche Institut für Normung e. V. (DIN).

1.3 Öffentlichkeitsarbeit

Die zur Beantwortung allgemeiner Fragen zum Datenschutz wie zur Werbung für den Datenschutz von mir herausgegebenen Informationsschriften „Bürgerfibel Datenschutz", „Der Bürger und seine Daten" sowie „Der Bürger und seine Daten im Netz der sozialen Sicherung" sind nach wie vor in erfreulich hohen Stückzahlen von interessierten Bürgern oder Schulungs- und Fortbildungseinrichtungen angefordert worden. Ich habe 1985 jeweils auf Abruf insgesamt ca. 135 000 Exemplare dieser Schriften versandt. Auch meine Tätigkeitsberichte verteile ich als Sonderdruck an Interessenten; so wurden im Jahr 1985 etwa 6 000 Exemplare allein des Siebenten Tätigkeitsberichts an interessierte Bürger oder Stellen abgegeben.

Stark zugenommen hat im Berichtsjahr die Betreuung von Besuchergruppen, die auf eigenen Wunsch und durch Vermittlung des Bundespresseamts meine Dienststelle besuchen, um Näheres über den Datenschutz zu erfahren. Im Verlaufe des Berichtsjahrs konnte ich zwanzig Besuchergruppen in meinem Amt begrüßen. Ich werte auch dies als erfreuliches Zeichen für die zunehmende Akzeptanz des Datenschutzes.

Wie in den Vorjahren haben meine Mitarbeiter wie auch ich selbst in zahlreichen öffentlichen Veranstaltungen, in Seminaren oder in anderen Fortbildungsveranstaltungen insbesondere politischer Bildungseinrichtungen sowie in der Fortbildung der Bundesakademie für öffentliche Verwaltung durch Vorträge oder Fachreferate mitgewirkt.

2. Innere Verwaltung

2.1 Neue Personalausweise und Pässe

Eine Anhörung von Sachverständigen durch den Innenausschuß des Deutschen Bundestages vom 20. Mai 1985 zu dem im Oktober 1984 von den Fraktionen der CDU/CSU und FDP im Deutschen Bundestag eingebrachten Entwurf eines Fünften Gesetzes zur Änderung des Gesetzes über Personalausweise hat mir erneut Gelegenheit gegeben, zu Fragen der Einführung eines fälschungssicheren und maschinenlesbaren Ausweises Stellung zu nehmen. Zur Fälschungssicherheit vertrete ich die Auffassung, daß aus dem Recht auf informationelle Selbstbestimmung, wie es das Bundesverfassungsgericht festgestellt hat, auch die Pflicht des Staates folgt, bei der Gestaltung des Personalausweises den Bürger durch geeignete Vorkehrungen davor zu schützen, daß seine persönlichen Daten von einem anderen durch Fälschung oder Verfälschung seines Ausweises mißbraucht werden. Wo ein überwiegendes Allgemeininteresse Einschränkungen des Rechts auf informationelle Selbstbestimmung durch zwangsweise Datenerhebung rechtfertigt, sind auch Vorkehrungen geboten, die sicherstellen, daß Daten eines Betroffenen nicht einer anderen Person zugeordnet und dadurch in einen für ihn belastenden Verwendungszusammenhang gebracht werden. Technische Maßnahmen zur Verbesserung der Fälschungssicherheit werden von mir also ausdrücklich begrüßt. Die Frage der Verbesserung der Fälschungssicherheit ist aber deutlich von der Frage der Zulassung automatischen Lesens zu unterscheiden. Da es hierfür, d. h. für die Maschinenlesbarkeit des Ausweises und deren Erleichterung durch eine Lesezone, immer noch an einer überzeugenden Begründung fehlt, ist die Frage besonders wichtig, ob sich hieraus Beeinträchtigungen des Rechts auf informationelle Selbstbestimmung ergeben können. Ich habe hierzu die Auffassung vertreten (vgl. 6. TB S. 6 ff., 7. TB S. 7 ff.), daß der Bürger zwar bei der Prüfung seines Ausweises in seinem Recht nicht dadurch zusätzlich beeinträchtigt wird, daß an die Stelle der bisherigen visuellen Kontrolle oder der manuellen Eingabe der Ausweisdaten zum Zwecke der Abfrage des Fahndungsbestandes das maschinelle Lesen des Ausweises tritt. Die Eingriffsqualität wird aber dadurch erhöht, daß der Bürger ver-

pflichtet wird, einen Ausweis zu besitzen und diesen auf Verlangen vorzuzeigen, der nicht nur in herkömmlicher Weise, sondern multifunktional verwendbar ist und als praktisches Instrument vielfältiger automatischer Datenverarbeitung eingesetzt werden kann. Denn mit dem in dem Entwurf vorgesehenen Ausweis, seiner speziellen Lesezone, den dafür entwickelten Lesegeräten, der dahinter stehenden Datenverarbeitungsorganisation und den Festlegungen zur automatisierten Anwendung (einheitliche Struktur der Übermittlungsdatensätze, gleichförmige Verfahren der Datenverarbeitung) wird eine Infrastruktur für personenbezogene Datenverarbeitung geschaffen, die ohne nennenswerten zusätzlichen Aufwand auch ganz andere als die gegenwärtig beabsichtigten Nutzungen ermöglicht. Die Schwelle für die Zulassung weiterer Datenerfassungen und Datenverarbeitungen wird dadurch niedriger und neue Gefährdungen der Privatspähre des Bürgers sind nicht auszuschließen. Dies gilt nicht nur für die erhöhte Mißbrauchsgefahr, also nicht nur für Gefährdungen, die darin zu sehen sind, daß dieses Instrument gesetzwidrig verwendet werden könnte. Vielmehr ist davon auszugehen, daß sich der Gesetzgeber einem stetigen Druck für eine immer umfassendere Anwendung auf lange Sicht nicht entziehen kann. Entsprechende Anwendungsmöglichkeiten lassen sich unschwer ausmachen. Diese Möglichkeiten geben deshalb Anlaß zur Sorge, weil jede von ihnen für sich besehen durchaus plausibel und vernünftig erscheint, aber ihre in kleinen Schritten vollzogene Kumulierung die Gefährdung der Privatsphäre ausmacht.

Der Entwurf bedarf im übrigen in einer Reihe von Punkten einer Verbesserung; herausgehoben seien die folgenden:

— Der Umfang zulässiger Datenerhebung und der Speicherung im Personalausweisregister wie auch die Datenübermittlung an andere Behörden sollten in dem Gesetz selbst geregelt werden (§ 2 a Abs. 1 und § 2 b Abs. 2). Der Verweis auf andere Gesetze und Verordnungen (§ 2 b Abs. 1) müßte daher gestrichen werden.

— Was die Übermittlung an andere Behörden anbelangt, so sollte die subsidiäre Funktion des Personalausweisregisters dahin gehend festgelegt werden, daß Übermittlungen nur zulässig sind, wenn es auf die Seriennummer, das Lichtbild oder die Unterschrift besonders ankommt. Übermittlungen können danach nur in Betracht kommen, wenn für die Zwecke des Empfängers die Kenntnis der im Melderegister enthaltenen Daten nicht ausreicht oder die Anfrage unmittelbar die Ausgabe, den Besitz oder den Verlust des Ausweises betrifft. Die vorgesehene Übermittlungsregelung, die Übermittlungen an beliebige andere Behörden zuläßt, sollte daraufhin überprüft werden, an welche Behörden tatsächlich Übermittlungen erforderlich sind.

— Das vorgesehene Verbot, die Seriennummern so zu verwenden, daß mit ihrer Hilfe ein Abruf personenbezogener Daten aus Dateien oder eine Verknüpfung von Dateien möglich ist (§ 3 Abs. 4), ist zu begrüßen. Positiv ist auch zu bewerten, daß die Seriennummer nicht im Melderegister gespeichert werden darf. Um aber dem Umkehrschluß vorzubeugen, daß die Speicherung außerhalb des Melderegisters gestattet sei, sollte bestimmt werden, daß eine Speicherung der Seriennummer im übrigen unzulässig ist, wenn sie nicht im Personalausweisgesetz oder in einer bereichsspezifischen Rechtsvorschrift ausdrücklich vorgesehen ist. Zumindest für Speicherungen in automatisierten Verfahren sollte dies bestimmt werden.

— Besonders kritischer Betrachtung bedarf auch die Speicherung des automatischen Abrufs personenbezogener Daten aus dem polizeilichen Fahndungsbestand bei besonderen Sicherheitslagen (§ 3 a Abs. 2 bis 5 des Koalitionsentwurfs). Solche Speicherungen, die in der bisherigen Diskussion häufig auch als Protokollierung bezeichnet wurden, sind allenfalls in einer Ausnahmesituation hinnehmbar, in der eine so schwerwiegende Einschränkung des Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse notwendig ist. Einschränkungen müssen unter Berücksichtigung des Gebots der Normenklarheit und insbesondere des Grundsatzes der Verhältnismäßigkeit präzise bestimmt werden. Eingehenderer Begründung bedarf danach die umfassende Verweisung auf § 100 a StPO, durch die m. E. zu viele Straftatbestände einbezogen werden. Es muß geprüft werden, welche von ihnen wegen der Schwere der Tat wirklich unverzichtbar sind. Bei der beabsichtigten Protokollierung liegen die Voraussetzungen nämlich insofern anders als bei der Anwendung des § 100 a StPO, als hier der betroffene Personenkreis auf die Benutzer bestimmter Fernmeldeanschlüsse beschränkbar ist. In der vorliegenden Vorschrift dagegen ist unklar, wie die angestrebte Bezeichnung der Betroffenen bzw. die Festlegung des Personenkreises nach bestimmten Merkmalen oder Eigenschaften erfolgen und wie eine solche partielle Protokollierung technisch realisiert werden soll.

Aus den Koalitionsberatungen ist bekannt geworden, daß in dem Gesetz zur Änderung des Personalausweisgesetzes auf die eben genannte Speicherung des automatischen Abrufs personenbezogener Daten aus dem polizeilichen Fahndungsbestand (Protokollierung) verzichtet werden soll, dies allerdings mit dem ausdrücklichen Vorbehalt abweichender gesetzlicher Regelung. Die Frage, ob hiermit für den Datenschutz etwas gewonnen ist, hängt davon ab, ob die bisher im Personalausweisgesetz vorgesehene Regelung nunmehr in — möglicherweise mehrere — bereichsspezifische Gesetze übernommen werden soll. Ich würde in einer bloßen Umschichtung nicht nur keinen Vorteil, sondern eher einen Nachteil sehen. Im Interesse der Transparenz und Normenklarheit sollte der Bürger aus dem Personalausweisgesetz selbst eine abschließende Antwort darauf erhalten, ob der Vorgang des automatischen Lesens seines Ausweises der kontrollierenden Stelle lediglich etwa vorhandene Daten sichtbar macht oder selbst zur Speicherung von

Ausweisdaten führen kann — und wenn ja, unter welchen Voraussetzungen.

Von Beginn der Diskussion um den neuen Personalausweis an habe ich mit meinen Kollegen in den Ländern darauf hingewiesen, daß durch die vorgesehene Maschinenlesbarkeit datenschutzrechtliche Mängel und Lücken im Sicherheitsbereich verschärft werden; die Datenschutzbeauftragten haben entsprechende flankierende Maßnahmen gefordert (vgl. 6. TB S. 8; TB S. 8 f.). Bislang scheint mir nicht gesichert, daß die bestehenden Lücken und Mängel durch geeignete bereichsspezifische Regelungen behoben werden. Im einzelnen gehe ich hierauf im Rahmen meiner Ausführungen zu den vorliegenden Entwürfen zur Neufassung des Bundesverfassungsschutzgesetzes, zur Schaffung eines MAD-Gesetzes, eines Gesetzes über die informationelle Zusammenarbeit der Sicherheitsbehörden des Bundes und der Länder sowie über die Fortschreibung des Musterentwurfs eines einheitlichen Polizeirechts ein (siehe unten Anregungen für die Gesetzgebung im Sicherheitsbereich, Nr. 11.2).

Die Bundesregierung hat am 7. Mai 1985 den Entwurf eines Paßgesetzes im Deutschen Bundestag eingebracht. Der Entwurf lehnt sich weitgehend an den Entwurf der Koalitionsfraktionen zur Änderung des Personalausweisgesetzes an. In meiner Stellungnahme, zu der mir der Bundesminister des Innern schon auf der Grundlage des Referentenentwurfes Gelegenheit gegeben hat, konnte ich daher auf meine Stellungnahme zu dem Koalitionsentwurf Bezug nehmen.

Bei einem Besuch bei der Bundesdruckerei habe ich aus datenschutzrechtlicher Sicht einen positiven Eindruck vom Stand der Vorbereitungen zur Herstellung der neuen Personalausweise und der hierfür vorgesehenen technischen und organisatorischen Vorkehrungen gewonnen. Nach meiner Überzeugung bedürfen diese aber einer weiteren Überprüfung, ob sie den tatsächlichen Anforderungen eines Massenbetriebes standhalten. Als geeigneten Schritt habe ich daher besonders den geplanten Betriebsversuch empfohlen. Da nur im Zusammenspiel aller Beteiligten eine ordnungsgemäße Durchführung des vorgesehenen Herstellungsverfahrens zu erwarten ist, sollte der Betriebsversuch mehrere Wochen dauern und eine repräsentative Auswahl örtlicher Personalausweisbehörden einbeziehen.

2.2 Melderecht

Ende 1984 hat sich der frühere Präsident des Bundesverfassungsgerichts, Prof. Dr. Benda, zu dem damaligen Entwurf eines Meldegesetzes für das Land Berlin gutachtlich geäußert. In diesem Gutachten wird unter anderem angezweifelt, ob § 16 Melderechtsrahmengesetz (MRRG) nach dem Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz noch verfassungskonform ist. § 16 MRRG regelt die sogenannte Hotelmeldepflicht und die Krankenhausmeldepflicht. Die Vorschrift zwingt die Länder, bei der landesgesetzlichen Begründung einer Meldepflicht für Beherbergungsstätten und Krankenhäuser entsprechende Vorschriften in die Landesmeldegesetze aufzunehmen.

Ausgehend von der Gesetzgebungskompetenz des Bundes für das Meldewesen in Artikel 75 Nr. 5 GG stellt Benda in Frage, ob die Anmeldung für einen kurzfristigen Aufenthalt in einem Hotel oder in einer Krankenanstalt noch dem Meldewesen zuzuordnen ist, dessen Ziel es ist, die Identität und die Wohnungen der Einwohner festzustellen. Er äußert Zweifel, ob es zur Erreichung dieses gesetzlich festgelegten Zweckes erforderlich, geeignet und dem Bürger zumutbar ist, einen solchen kurzfristigen Aufenthalt zu melden, obwohl der Bürger in der Regel bereits an seinem Wohnort registriert ist.

Ich teile die in dem Gutachten vertretene Auffassung und habe dem Bundesminister des Innern empfohlen, § 16 MRRG zu überprüfen. Ich bin dafür eingetreten, eine eventuelle Änderung im Rahmen eines Rechtsbereinigungsgesetzes vorzunehmen. Der Bundesminister des Innern hat inzwischen in seiner Stellungnahme zu dem Gutachten dem Senat von Berlin mitgeteilt, daß er Änderungen des Melderechtsrahmengesetzes nicht beabsichtige. Ich bedauere diese Entscheidung und werde mit dem Bundesminister des Innern über die Angelegenheit weiter im Gespräch bleiben.

2.3 Ausländerzentralregister

Die vom Bundesminister des Innern zur Vorbereitung einer neuen Konzeption des Ausländerzentralregisters (AZR) eingesetzte Arbeitsgruppe, an der neben Vertretern der unmittelbar betroffenen Behörden (u. a. Ausländerbehörden, Grenzschutzdirektion) auch der BfD beteiligt war, hat im November 1985 ihre letzte Sitzung durchgeführt. Ihre Aufgabe war es, ein Konzept für die künftige Gestaltung des AZR zu entwickeln, das vorrangig auf die Interessen der Behörden ausgelegt ist, die ausländerrechtliche Einzelfallentscheidungen zu treffen haben. Dabei kam es wesentlich darauf an, das AZR von der bisherigen Überfrachtung zu entlasten. Erforderlichkeit der Datenspeicherung und deren Aktualität, Leistungsfähigkeit der Datenanlieferer und notwendiger Informationsbedarf der Datenbezieher waren daher die ausschlaggebenden Kriterien bei der Arbeit dieser Gruppe. Das eingeschlagene Verfahren, nämlich zunächst eine Darstellung der Datenfelder, die künftig im AZR geführt werden sollen, sodann die Kommunikationsstruktur, d. h. die Darstellung der Datenlieferung und Datenübermittlung, zu erarbeiten und auf dieser Basis eine gesetzliche Regelung vorzubereiten, wird von mir positiv bewertet.

Eine eingehende Bewertung des Arbeitsergebnisses der Gruppe wird auf der Basis ihres abschließenden Berichts erfolgen, der — wie vom Bundesminister des Innern angekündigt — auch die Grundlage für ihre offizielle Abstimmung mit den Bundesressorts und den Landesregierungen sein soll.

Meine positive Beurteilung des Verfahrens in der Arbeitsgruppe bedeutet kein Abgehen von meiner

von Anfang an erhobenen Forderung, klare Rechtsgrundlagen für das AZR zu schaffen. Der Bundesminister des Innern hat von Beginn der Arbeit an eingeräumt, daß das gegenwärtige AZR nicht nur in inhaltlicher und verfahrensmäßiger, sondern auch in rechtlicher Hinsicht den Anforderungen nicht mehr entspricht, und die Schaffung geeigneter Rechtsgrundlagen als einen unverzichtbaren Schritt im Rahmen der Neukonzeption anerkannt. Er hat in Aussicht gestellt, parallel mit dem Bericht der Arbeitsgruppe einen Entwurf bezüglich des Regelungsbedarfs zur Diskussion zu stellen. Ich hoffe, daß hiermit die Bemühungen um die Neukonzeption des AZR bald weitere Fortschritte machen.

2.4 Wahlrecht

Der Bundesminister des Innern hat meiner Anregung, auf das vollständige Geburtsdatum eines vorgeschlagenen Kandidaten in den Wahlvorschlägen zu verzichten und stattdessen nur das Geburtsjahr anzugeben oder jedenfalls die öffentliche Bekanntmachung hierauf zu beschränken (vgl. 7 TB S. 10f), zunächst ablehnend gegenübergestanden. Im Zuge der Änderung der Bundeswahlordnung habe ich jedoch erreichen können, daß in der Bekanntmachung der Wahlvorschläge künftig nur das Geburtsjahr angegeben wird.

Auf ein weiteres Problem im Zusammenhang mit Wahlen habe ich Anfang 1985 hingewiesen. So wenden sich in zunehmendem Maße Gemeinden bzw. örtliche Wahlleiter an Behörden mit der Bitte um Benennung von Beschäftigten zur Bestellung von Wahlvorständen. Ich halte ein solches Verfahren dann für sinnvoll, wenn sich nicht auf freiwilliger Basis geeignete Personen für diese Ehrenämter finden lassen. Da es sich bei einer solchen Benennungspflicht von Behörden jedoch um eine Einschränkung des Rechts auf informationale Selbstbestimmung handelt, habe ich empfohlen, eine Regelung durch Rechtsnormen im Bundeswahlgesetz oder in der Bundeswahlordnung vorzunehmen.

Der Bundesminister des Innern hat mir inzwischen mitgeteilt, daß er zur Zeit die Personalaktenführung in rechtlicher und tatsächlicher Beziehung überprüfe. Dabei spiele auch die Frage eine Rolle, welche Auskünfte aus den Personalakten und an wen erteilt werden dürfen. Nachdem ich bereits im Februar 1985 auf die vorstehend geschilderte Problematik hingewiesen habe, sollte meines Erachtens hierzu eine Regelung rechtzeitig vor den nächsten Bundestagswahlen erfolgen.

2.5 Bundesamt für den Zivildienst

In meinem Siebenten Tätigkeitsbericht (S. 10) habe ich darüber berichtet, daß ich mit dem Bundesamt für den Zivildienst und dem Bundesminister für Jugend, Familie und Gesundheit im Gespräch darüber bin, ob und mit welchen Mitteln ein zusätzlicher Schutz des Anerkennungsteils der Kriegsdienstverweigerer-Akte nach der Neuregelung des Kriegsdienstverweigerungsrechts erreicht werden kann. Es wurde Einvernehmen darüber erzielt, daß ein solcher Schutz geboten ist. Entsprechend werden daher die Anerkennungsunterlagen mit Ausnahme des Anerkennungsbescheids in einem besonderen verschlossenen Umschlag aufbewahrt. Der Verschlußstreifen dieses Umschlags trägt neben der Dienstpostenbezeichnung auch den Namen und das Datum desjenigen Bediensteten, der den Umschlag verschlossen hat.

Ich halte dieses Verfahren für sachgerecht. Die Bediensteten des Bundesamtes für Zivildienst können auf den Anerkennungsteil nur noch unter besonderen Voraussetzungen, dann jedoch nachprüfbar, zugreifen. Dazu kommt noch, daß in den seltenen Fällen einer Aktenübersendung an andere Stellen in jedem Einzelfall geprüft wird, ob der besonders verschlossene Teil der Zivildienstakte übersandt werden muß.

3. Rechtswesen

3.1 Bundeszentralregister

Beim Bundeszentralregister (BZR) als einem der bedeutendsten Datenverarbeitungssysteme im Bundesbereich habe ich auch 1985 einen Kontrollbesuch durchgeführt und hierbei erneut ein insgesamt erfreulich hohes Niveau des Datenschutzes in dieser Behörde festgestellt. Die im fortgesetzten Dialog über mögliche weitere Verbesserungen erreichten technischen und organisatorischen Vorkehrungen bieten wirksame Hilfen, um Bearbeitungsfehler zu vermeiden. Solange aber in bestimmten Bereichen der Bearbeitung von Auskunftsersuchen, z. B. bei der Identitätsprüfung, menschliche Entscheidungen unverzichtbar sind, wird eine gewisse Fehlerquote auch künftig nicht völlig auszuschließen sein, zumal es sich um ein Massenverfahren mit täglich knapp 30 000 Auskünften handelt. Über die Fehleranteile in den einzelnen Arbeitsschritten kann ich mir im Rahmen der zeitlich begrenzten Kontrollen durch meine Mitarbeiter allenfalls ein punktuelles Bild verschaffen. Die Besuche haben daher deutlich gemacht, daß die Tätigkeit der hausinternen Revisionsgruppe durch meine Kontrolltätigkeit nicht ersetzt werden kann und beide Bemühungen sich in sinnvoller Weise ergänzen müssen. Die Wirkung der bestehenden organisatorischen und technischen Vorkehrungen zur Gewährleistung des Datenschutzes bedarf einer kontinuierlichen Beobachtung und Analyse durch die Revisionsgruppe, um aus festgestellten Fehlern Erkenntnisse für mögliche weitere Verbesserungen zu gewinnen. Angesichts der Sensibilität und des Volumens der im BZR zu verarbeitenden Daten halte ich den Einsatz dieser Gruppe weiterhin für unerläßlich.

Wie in meinem Siebenten Tätigkeitsbericht (S. 12) angekündigt wurde, habe ich die Wirksamkeit von Anordnungen überprüft, die auf die Zurückweisung von Anträgen auf unbeschränkte Auskunft mit mangelhafter Zweckangabe abzielen. Die mir für

einen Zeitraum von vier Wochen zur Prüfung von Zweckangaben in Ersuchen von obersten Bundes- und Landesbehörden (§ 41 Abs. 1 Nr. 2 BZRG) und Finanzbehörden (§ 41 Abs. 1 Nr. 4 BZRG) erstellten Prüflisten haben Mängel in der Auskunftserteilung nicht erkennen lassen. Ich habe angeregt, die Prüfung in bestimmten Zeitabständen durch die Revisionsgruppe wiederholen zu lassen.

Einen weiteren Schwerpunkt der Erörterung bildete die Protokollierung von Auskünften (Speicherung von Auskunftsempfängern). Protokolle sind ein unerläßliches Instrument für Prüfungen der hausinternen Revisionsgruppe wie auch für meine Kontrollen. Zwar sind Fälle einer fehlerhaften Auskunft wegen mangelnder Indentität der in dem Auskunftsersuchen und in der Auskunft genannten Person oder wegen fehlerhafter Mitteilung an das BZR — etwa Mitteilung eines nicht rechtskräftigen Urteils — äußerst selten. Jedoch halte ich unter Gesichtspunkten der Schadensbegrenzung bzw. -minderung das BZR für verpflichtet, in solchen Fällen den Empfänger der Auskunft zu informieren, um die Auskunft „zurückzuholen". Ich habe empfohlen, die Protokolle auch hierfür zu verwenden. Es besteht im übrigen Einvernehmen darüber, daß es — auch ohne ausdrückliche Klarstellung im BZRG — Auskünfte des BZR über Protokollinhalte nicht geben darf.

In einem mit dem Bundesminister der Justiz geführten Gespräch habe ich außerdem erneut an meine Vorschläge zur Novellierung des Bundeszentralregistergesetzes (s. 5. TB S. 18, 6. TB S. 12, 7. TB S. 13) erinnert und hoffe, daß die notwendigen Vorarbeiten bald aufgenommen werden.

3.2 Mitteilungen in Zivilsachen

Vor dem Hintergrund des in meinem Siebenten Tätigkeitsbericht (S. 15) wiedergegebenen Beschlusses der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 6./7. Juni 1984 und der darin enthaltenen Empfehlungen begrüße ich die vom Bundesminister der Justiz im Zusammenwirken mit den Landesjustizverwaltungen eingeleitete umfassende Überprüfung der Mitteilungen in Zivilsachen (MiZi). Die Datenschutzbeauftragten haben sich erneut mit dieser Thematik befaßt und parallel zu den Bemühungen der Justizverwaltungen einzelne Abschnitte der MiZi unter datenschutzrechtlichen Gesichtspunkten untersucht. Das Ergebnis dieser Prüfung habe ich dem Bundesminister der Justiz übersandt und empfohlen, es bei den Beratungen der Justizverwaltungen und der Vorbereitung des Entwurfs einer gesetzlichen Regelung zu berücksichtigen.

Die Konferenz der Datenschutzbeauftragten hat in Anknüpfung an die in ihrem früheren Beschluß gegebenen grundlegenden Empfehlungen nochmals hervorgehoben, daß die Überprüfung der MiZi sich nicht nur auf die Erforderlichkeit und die Rechtsgrundlagen der Mitteilungen bezieht, sondern auch deren Umfang, Inhalt und Form einschließen sollte. Soweit für einzelne Mitteilungen von den Justizverwaltungen als „mittelbare Rechtsgrundlagen" bezeichnete Rechtsvorschriften vorhanden sind, die sich auf die Aufgaben des Empfängers der Mitteilungen beziehen, so können diese ein Indiz für die Erforderlichkeit der Übermittlung sein, jedoch notwendige bereichsspezifische Rechtsgrundlagen für die Zulässigkeit der Übermittlung nicht ersetzen.

In Ergänzung der schon gegebenen Empfehlungen halte ich folgende Punkte für wichtig:

— Die Übermittlungsvorgänge sollten transparenter gestaltet werden. Das Unbehagen vieler Bürger beim Umgang mit der öffentlichen Verwaltung rührt oftmals daher, daß diese über Kenntnisse verfügt, deren Herkunft den Betroffenen unbekannt ist. Wo es ohne unzumutbaren Aufwand möglich ist, sollte daher grundsätzlich vorgesehen werden, den Betroffenen von den Mitteilungen in geeigneter Weise zu unterrichten.

— Bei der Bestimmung der Empfängerbehörde sollte auf einen funktionalen Behördenbegriff abgestellt werden. Eine genaue Bezeichnung des Empfängers (z. B. Jugendamt, Straßenverkehrsamt) dient Anforderungen, die das Bundesverfassungsgericht an die präzise Bestimmung des Verwendungszwecks geknüpft hat.

— Der Eingriffscharakter von Mitteilungen tritt besonders bei solchen an die Finanzbehörde hervor. Die Notwendigkeit solcher nur im überwiegenden Allgemeininteresse zulässigen Eingriffe sollte unter dem Gesichtspunkt des in § 93 Abs. 1 Satz 3 Abgabenordnung verankerten Subsidiaritätsprinzips geprüft werden. Danach sind andere Personen bzw. Stellen als die Betroffenen selbst erst dann zu einer Auskunft (bzw. Mitteilung) heranzuziehen, wenn die Sachverhaltsaufklärung durch die Betroffenen nicht zum Ziele führt oder keinen Erfolg verspricht.

Der Bundesminister der Justiz hat mich inzwischen unterrichtet, daß die Mitteilungen in Zivilsachen (MiZi) — ebenso wie die Mitteilungen in Strafsachen (MiStra, vgl. hierzu meinem 7. TB S. 14) — im Gerichtsverfassungsgesetz eine gesetzliche Regelung finden sollen, und in Aussicht gestellt, einen Referentenentwurf in der ersten Hälfte des Jahres 1986 zu versenden. Ich gehe davon aus, daß mir hierzu Gelegenheit zur Stellungnahme gegeben wird. Um die Zeit bis zum Erlaß gesetzlicher Regelungen zu überbrücken, haben die Justizverwaltungen im April 1985 für die MiStra und im Dezember 1985 für die MiZi Übergangsregelungen in Kraft gesetzt, die bereits deutliche Abstriche von dem bisherigen Mitteilungsumfang enthalten. Ich sehe darin positive Voraussetzungen für die weiteren Bemühungen um eine gesetzliche Regelung.

3.3 Schuldnerverzeichnis

Schon vor dem Volkszählungsurteil des Bundesverfassungsgerichts habe ich in früheren Tätigkeitsberichten (vgl. 2. TB S. 18, 3. TB S. 20, 4. TB S. 44 f., auch 7. TB S. 15 f.) auf die Notwendigkeit hingewie-

sen, den Datenschutz bei der Übermittlung von Angaben aus dem Schuldnerverzeichnis zu verbessern, insbesondere den Umfang der praktizierten Datenübermittlungen kritisch zu überprüfen und auch die zugrundeliegende gesetzliche Regelung des § 915 ZPO zu überarbeiten. Inzwischen hat der Bundesminister der Justiz eine neue Konzeption dazu entwickelt, und im August 1985 einen Entwurf zur Änderung gesetzlicher Vorschriften über das Schuldnerverzeichnis sowie den Entwurf einer Verordnung über die Erteilung von Abdrucken aus dem Schuldnerverzeichnis vorgelegt. Die Entwürfe sollen den Schutz der Persönlichkeitssphäre des im Schuldnerverzeichnis eingetragenen Schuldners verstärken, ohne die berechtigten Interessen der Wirtschaft am Schutz des Geschäftsverkehrs zu beeinträchtigen. In die Diskussion der Entwürfe sind die Landesjustizverwaltungen und die Datenschutzbeauftragten der Länder einbezogen.

Ich teile die Zweifel mehrerer Landesbeauftragter, ob die vorgesehene Gebühr von 15,00 DM für jede Auskunft einen hinreichenden Schutz vor mutwilligen Anfragen bietet und habe zu dem vorgesehenen § 915 a ZPO empfohlen, zumindest eine Mißbrauchsklausel vorzusehen, die es ermöglicht, eine Auskunft jedenfalls dann abzulehnen, wenn erkennbar ist, daß der Antragsteller ein berechtigtes Interesse an der Auskunft nicht hat. Wesentliches Ziel der Neuregelung ist die nur durch eine Eingrenzung des Empfängerkreises erreichbare zweckgerichtete Kontrolle des Verbleibs der Abdrucke bzw. der Vervielfältigungen (Listen) und deren Aktualisierung. Ich begrüße es daher, daß der Entwurf von dem früheren Verfahren der Veröffentlichung der Listen abrückt. Ich habe aber Zweifel, ob nach der in § 915 b Abs. 2 Satz 1 des Entwurfs erlaubten Überlassung von Listen an die Mitglieder von Industrie- und Handelskammern, Handwerkskammern, Landwirtschaftskammern und anderen Körperschaften des öffentlichen Rechts, in denen Angehörige eines Berufes kraft Gesetzes zusammengeschlossen sind, noch hinreichend überschaubar ist, in welche Hände die Listen tatsächlich gelangen, und ob die Empfänger der Listen die vorgeschriebenen Löschungen tatsächlich vornehmen. Auch wenn man von der Gutwilligkeit der Empfänger ausgeht, ist zu befürchten, daß ein Teil von ihnen durch das Löschungsverfahren tatsächlich überfordert wird (s. besonders § 915 d Abs. 2 und 3). Ich neige zu der Auffassung, daß den Interessen der Körperschaftsmitglieder in hinreichender Weise auch dadurch Rechnung getragen werden kann, daß die Auskunftserteilung durch die Körperschaften erfolgt. Ein solches Verfahren würde an der angestrebten Entlastung der Geschäftsstellen der Gerichte nichts ändern, durch sachnähere Beurteilung des berechtigten Interesses der Auskunftssuchenden aber wesentlich zum Ausschluß von Mißbräuchen beitragen. Gegenüber dem Argument, dieses Verfahren erfordere möglicherweise bei den Körperschaften zusätzliches Personal, sollte berücksichtigt werden, daß es zugleich den Aufwand einer Vielzahl von Mitgliedern für die Aufbewahrung, Kontrolle, Löschung und Vernichtung der Listen entfallen läßt. Bislang ist nicht ersichtlich, daß der Informationsbedarf einzelner Mitglieder etwa so breit ist, daß er durch einen Auskunftsdienst der Körperschaft nicht befriedigt werden könnte. Für den Fall, daß eine eingehendere Prüfung dies jedoch ergeben sollte, könnte erwogen werden, ausnahmsweise einzelnen Mitgliedern unter bestimmten Voraussetzungen Listen zu überlassen. Die vorliegende Entwurfsfassung, die den Empfang von Listen allein mit der Mitgliedschaft in einer der genannten Körperschaften begründet, halte ich nicht für befriedigend.

Wenn ich auch die Schwierigkeiten nicht verkenne, zu einem sachgerechten Ausgleich zwischen Gläubigerschutz und Datenschutz zu gelangen, so hoffe ich doch, daß es noch in dieser Legislaturperiode zu einer gesetzlichen Neuregelung kommt.

4. Bauwesen

Im August des Berichtsjahres hat mir der Bundesminister für Raumordnung, Bauwesen und Städtebau (BMBau) den Entwurf eines Baugesetzbuches mit der Bitte um Stellungnahme zu zwei datenschutzrechtlich besonders relevanten Vorschriften zugesandt. Sie betreffen zum einen die Auskunftspflichten von Eigentümern, Mietern und Pächtern von Grundstücken und Gebäuden im Rahmen von städtebaulichen Sanierungsmaßnahmen, zum anderen die sogenannte Kaufpreissammlung. Die hierfür bestehenden gesetzlichen Regelungen im Städtebauförderungsgesetz bzw. im Bundesbaugesetz erscheinen aus der Sicht des Datenschutzes zu unbestimmt und lückenhaft. Besonders bezüglich der Erhebung personenbezogener Angaben im Zusammenhang mit Sanierungsmaßnahmen hat es in der Vergangenheit wiederholt Beschwerden von Bürgern gegeben. Diese bezogen sich z. B. auf Fragen nach der Konfession, der Häufigkeit des Kirchganges, der Zugehörigkeit zu Vereinen, der Qualität nachbarschaftlicher Kontakte („Nur Grüßen, kaum Kontakte, häufiger Streit") sowie auf die Höhe und Zusammensetzung des Einkommens.

Ich halte es für unerläßlich, daß in dem beabsichtigten Gesetz die Angaben, zu denen der Betroffene verpflichtet werden soll, einzeln ihrer Art nach oder zumindest hinreichend bestimmbar aufgeführt werden und hierfür eine Begründung gegeben wird. Die Vorschrift müßte verdeutlichen, daß personenbezogene Daten, soweit erforderlich, nur im Umfang eines so definierten Maximalrahmens abgefragt werden dürfen.

Ich habe dem BMBau meine Stellungnahme zu den genannten Problembereichen übermittelt und sie ihm auch in Besprechungen erläutert. Die Beratungen des Entwurfes dauern derzeit noch an.

5. Personalwesen

5.1 Konventionelle Personaldatenverarbeitung

5.1.1 Beihilfe

Bereits mehrfach habe ich in meinen Tätigkeitsberichten gefordert (so z. B. im 6. TB S. 19), daß Beihil-

feakten von den übrigen Personalakten getrennt zu führen und die Beihilfestellen von der übrigen Personalverwaltung abgeschottet werden müssen. In der Neufassung der Allgemeinen Verwaltungsvorschrift über die Gewährung von Beihilfen in Krankheits-, Geburts- und Todesfällen vom 19. April 1985 (GMBl. 1985, S. 290ff.) ist nunmehr ausdrücklich festgelegt, daß die bei der Bearbeitung von Beihilfen bekanntgewordenen Angelegenheiten geheimzuhalten sind.

Der Bundesminister für das Post- und Fernmeldewesen hat auf der Grundlage dieser Vorschrift sowie eines Gesprächs mit mir die Beihilfesachbearbeiter einer besonderen Schweigepflicht unterworfen, die sie auch gegenüber Vorgesetzten zu wahren haben. Die diesbezügliche Regelung hat folgenden Wortlaut:

Verpflichtung zur Verschwiegenheit

Die Kräfte der Beihilfefestsetzungsstellen und die mit der Entgegennahme von Beihilfeanträgen befaßten Kräfte der Personalstellen unterliegen im Rahmen der Rechtsordnung der Pflicht zur Amtsverschwiegenheit (§ 61 BBG, ggf. TV). Darüber hinaus sind sie verpflichtet, über die ihnen bei der Bearbeitung oder der Entgegennahme der Beihilfeanträge anvertrauten oder zur Kenntnis gelangten persönlichen Angelegenheiten auch im dienstlichen Verkehr — also auch gegenüber Vorgesetzten — Stillschweigen zu bewahren. Dies gilt nicht, soweit der Beihilfeberechtigte oder der Angehörige schriftlich von der Schweigepflicht befreit hat oder eine gesetzliche Berechtigung oder Verpflichtung zur Offenbarung besteht. Soweit eine Offenbarung nicht zulässig ist, besteht keine Auskunftspflicht und auch keine Zeugnispflicht. Unberührt von der Schweigepflicht bleibt die gesetzlich begründete Pflicht, Straftaten anzuzeigen (§ 61 Abs. 4 BBG).

Für Aussagen vor Gericht, der Polizei oder einer anderen Behörde bedarf es der Genehmigung des Dienstvorgesetzten. Im Strafprozeß und im Disziplinarverfahren gelten hinsichtlich des Zeugnisverweigerungsrechts die beamtenrechtlichen Vorschriften (§§ 61, 62 BBG), wonach die Aussagegenehmigung nur versagt werden darf, wenn das öffentliche Wohl gefährdet ist.

Von der vorstehenden Verpflichtung zur Verschwiegenheit habe ich Kenntnis genommen.

....., den .....

.....
Unterschrift (Vor- und Zunahme)

Diese beispielhafte Regelung sollte auch von den übrigen Bundesbehörden — je nach Organisationsstruktur gegebenenfalls modifiziert — übernommen werden.

Daß es nötig ist, auf dieses Problem zum wiederholten Male hinzuweisen, hat eine Prüfung bei der Bundesversicherungsanstalt für Angestellte (BfA) gezeigt. Dort sind für Beihilfesachen und allgemeine Personalangelegenheiten bislang dieselben Bearbeiter zuständig. Dies halte ich für bedenklich. Die BfA hat inzwischen zugesagt, nach einer noch nicht absehbaren Übergangszeit die organisatorischen Maßnahmen für eine Abschottung zu treffen. Ich halte demgegenüber eine kurzfristige Realisierung für dringlich.

5.1.2 Umgang mit ärztlichen Unterlagen

Anläßlich der Prüfung bei der BfA habe ich außerdem festgestellt, daß die Behandlung ärztlicher Unterlagen im Personalwesen nicht den datenschutzrechtlichen Anforderungen entsprach.

Ich nehme dies zum Anlaß, an dieser Stelle nochmals auf die Problematik einzugehen.

Nach den Ausführungen im 2. TB (S. 23) und im 7. TB (S. 20f.) soll sich der Inhalt der der personalbearbeitenden Stelle zugänglichen Gutachten auf das Untersuchungsergebnis beschränken, soweit es für die anstehende Personalentscheidung relevant ist. Der Begriff „Gutachten" wurde damals im Sinne von „Zeugnis" gebraucht.

Ärztliche Zeugnisse über einen Bediensteten — in Betracht kommen hauptsächlich solche des Amtsarztes oder Personalarztes — die aufgrund konkreter dienstlicher Veranlassung erstellt werden, betreffen das Dienstverhältnis als solches. Sie gehören somit *materiell zur Personalakte*. Die materielle Personalakte umfaßt auch die Unterlagen, die der Personalarzt führt. Da die angesprochenen Zeugnisse in der Regel Entscheidungsgrundlage oder -hilfe für konkrete dienstliche Maßnahmen sind (Änderung der dienstlichen Verwendung, vorzeitige Zurruhesetzung), gehören sie auch in die *formelle* Personalakte. Nicht in die formelle Personalakte gehören hingegen andere ärztliche Unterlagen wie etwa Befundbögen und medizinische Gutachten, auf denen das ärztliche Zeugnis basiert.

Die Frage, ob ein Bediensteter für eine bestimmte Verwendung geeignet ist, hat danach das Zeugnis nur in den Kategorien „geeignet", „eingeschränkt", „nicht geeignet" oder in ähnlicher Weise zu beantworten. Für Ermessensentscheidungen des Dienstherrn wird eine *ausführlichere Auskunft* (im Zeugnis) für zulässig erachtet, ohne daß der Umfang näher bestimmt wird (2. TB, S. 23). Dazu halte ich folgende Verdeutlichung für geboten:

— Einstellung

Ist ein Bewerber gesundheitlich *uneingeschränkt* für ein Dienstverhältnis geeignet, reicht die Angabe der Eignung aus. Diagnosedaten über „Randbefunde", die letztlich nicht zu einer Einschränkung der Eignung führen, müssen der Personalstelle nicht bekannt sein.

Stellt der Arzt eine *eingeschränkte* Eignung fest, hat er diese Einschränkung im Zeugnis darzustellen. Dazu kann es unter Umständen erforderlich sein, den medizinischen Hintergrund seiner Bewertung zu skizzieren.

Stellt der Arzt fest, daß der Bewerber aus gesundheitlichen Gründen für eine Einstellung *nicht* in Betracht kommt, teilt der Arzt nach

pflichtgemäßem Ermessen im Zeugnis die für die Begründung der Ablehnung erforderlichen Daten mit.

Legt ein Bewerber von sich aus ein umfangreiches ärztliches Gutachten vor, so sollte die Personalstelle dieses dem personalärztlichen Dienst verschlossen zuleiten, der daraus ein Zeugnis anfertigt, das den vorstehenden Kriterien genügt. Die Tatsache, daß das ärztliche Gutachten freiwillig der Personalstelle offenbart wurde, rechtfertigt eine Einsichtnahme durch die Personalstelle allenfalls um zu prüfen, ob die Einschaltung des personalärztlichen Dienstes überhaupt noch sinnvoll ist; sie rechtfertigt aber nicht den dauernden Verbleib des Gutachtens in der Personalstelle.

— Maßnahmen während der Dienstzeit

Sieht sich die Personalstelle vor Entscheidungen gestellt, die in ein bestehendes Dienstverhältnis eingreifen, so ist sie darauf angewiesen, daß ihr der Arzt jeweils die tragenden medizinisch-diagnostischen Gründe mitteilt, die sie einerseits als Entscheidungsgrundlage benötigt und die sie andererseits in die Lage versetzen, ihre Entscheidung ausreichend — das heißt mit Angabe der wesentlichen tatsächlichen und rechtlichen Entscheidungselemente — zu begründen (§ 39 Abs. 1 VwVfG).

Dies ist insbesondere der Fall bei

— gesundheitsbedingter Zuweisung einer anderen Tätigkeit

— vorzeitiger Zurruhesetzung, sei es auf Antrag des Bediensteten oder auf Initiative der Personalstelle.

Dabei hat die Personalstelle die Fragestellung an den Arzt möglichst so zu konkretisieren, daß dieser die dienstliche Veranlassung erkennen und konkret antworten kann. Unter Berücksichtigung der Fragestellung ist es Aufgabe des Arztes, nach pflichtgemäßem Ermessen zu entscheiden, welche Angaben er in dem Zeugnis machen muß, damit die Dienststelle in der Lage ist, ihre Entscheidung zu begründen.

— Einsichtnahme durch Personalsachbearbeiter

Die zuständigen Bearbeiter haben ein Recht auf Einsichtnahme in die in der Personalakte aufbewahrten ärztlichen Zeugnisse. Um jedoch eine aus dienstlicher Sicht überflüssige Lektüre zu verhindern, müssen diese im verschlossenen Umschlag mit Aufschrift „Vertrauliche Arztsache" in der Personalakte aufbewahrt werden. Auf dem Umschlag ist im Falle einer Öffnung das Datum, der Öffnende und der Anlaß der Öffnung zu vermerken.

Im Zusammenhang mit Beihilfefällen und Dienstunfällen ist es teilweise zu Schwierigkeiten bei der Frage gekommen, welche Angaben ein Arzt bzw. der Ärztliche und Soziale Dienst der Beihilfestelle gegenüber machen darf bzw. muß. In Übereinstimmung mit dem Leitenden Arzt des Ärztlichen und Sozialen Dienstes der obersten Bundesbehörden vertrete ich dazu folgende Auffassung:

Die Regelung über den Inhalt ärztlicher Zeugnisse anläßlich der Übernahme von Bewerbern in das Beamtenverhältnis oder der Beurteilung der Verwendungsfähigkeit für bestimmte Dienstposten ist auf Beihilfeangelegenheiten nur begrenzt übertragbar. In diesen Fällen werden in der Regel weitergehende diagnostische Auskünfte erforderlich sein. Unter der Voraussetzung, daß die Beihilfesachen und ähnliche Vorgänge bearbeitende Stelle organisatorisch und personell von der übrigen Personalverwaltung abgeschottet ist, hängt die Ausführlichkeit der Auskünfte davon ab, in welchem Umfag die Kenntnis medizinischer Angaben für die Aufgabenerfüllung dieser Stelle unverzichtbar ist.

Dabei ist zu berücksichtigen, daß im Beihilfeverfahren die Festsetzungsstelle verpfichtet ist, die Angemessenheit der ärztlichen Leistungen zu prüfen. Dies kann sie nur, wenn sie vom Arzt erfährt, welcher medizinische Sachverhalt den Leistungen zugrundeliegt. Lediglich die Angabe der Spezifikation nach GOÄ reicht dazu nicht aus, weil sich daraus nur entnehmen läßt, daß der Arzt eine bestimmte Maßnahme durchgeführt hat, nicht aber, ob diese Maßnahme auch erforderlich war.

Der Beihilfestelle müssen daher die tragenden medizinischen Feststellungen mitgeteilt werden, damit sie ihre Aufgaben verantwortlich wahrnehmen kann. Letztlich hat aber der Arzt nach pflichtgemäßem Ermessen zu entscheiden, wie umfangreich seine Angaben sein dürfen bzw. müssen, um das Ergebnis seiner Untersuchung für den Empfänger nachvollziehbar zu machen.

5.1.3 Einzelfälle

Der Bundesminister für das Post- und Fernmeldewesen verwahrt alte ärztliche Atteste mit Diagnoseangaben offen in Personalakten und notierte sie in Personalkarteien. Er hat sich bereit erklärt, auf Wunsch der Bediensteten die Daten in den Karteien zu löschen und in den Akten in einen verschlossenen Umschlag zu nehmen. Ich fordere nicht, daß eine solche Bereinigung von Amts wegen erfolgt, bedauere aber, daß wegen des zu erwartenden Verwaltungsaufwandes meiner Anregung nicht gefolgt wurde, die Bediensteten über die individuelle Bereinigungsmöglichkeit zu informieren.

Eine weitere Angelegenheit halte ich für klärungs- und regelungsbedürftig: Vorgänge, die im Zusammenhang mit dem organisatorischen Betriebsablauf in einer Behörde stehen, enthalten oft personenbezogene Daten über Bedienstete, wenn es etwa um Fragen der Stellenbesetzung geht. Dabei werden z. B. Aussagen zur Qualifikation oder zur gesundheitlichen Belastbarkeit verschiedener Bewerber schriftlich festgehalten und einander gegenübergestellt. Diese Vorgänge werden, da sie aufgrund einer organisatorischen Maßnahme entstanden sind, als Sachakten geführt. Sie unterliegen daher weder dem besonderen Schutz der Personalakten noch besteht ein Einsichtsrecht. Ich halte diesen Zustand für änderungsbedürftig.

Einige Behörden verlangen von ihren Bediensteten nach einer Ehescheidung wegen der besoldungs-

und tarifrechtlichen Auswirkungen eine Ablichtung des Scheidungsurteils für die Personalakte. Ich meine, die Vorlage des Urteilstenors und gegebenenfalls der besoldungserheblichen Teile des Urteils sollte ausreichen. In den konkreten Fällen stimmten die betroffenen Behörden darin mit mir überein.

Bedienstete haben sich darüber beschwert, daß auf Urlaubsanträgen die Urlaubsanschrift angegeben werden muß. Diese Beschwerden sind auch von einem Mitglied des Deutschen Bundestages aufgegriffen worden. Da nach meiner Ansicht die notwendige Erreichbarkeit des Bediensteten auch dadurch sichergestellt werden kann, daß er nur seinem direkten Vorgesetzten eine Erreichbarkeitsadresse mitteilt, habe ich den Bundesminister des Innern um eine Änderung des Verfahrens gebeten. Er hat bisher darüber noch nicht entschieden.

5.2. Automatisierte Personaldatenverarbeitung

5.2.1 Personalinformationssysteme

Im Bereich der Bundesverwaltung werden inzwischen zahlreiche sogenannte *Personalinformationssysteme* betrieben oder befinden sich im konkreten Planungsstadium.

Die *Deutsche Bundespost* plant ein Personalinformationssystem für die Beamten des höheren Dienstes. Dieses System soll beim Bundesminister für das Post- und Fernmeldewesen geführt werden. Zugriff werden nur die zuständigen Mitarbeiter der Personalverwaltung haben. Das System enthält zwar auch wertende Angaben, wie das Ergebnis der dienstlichen Beurteilung, sowie die Verwendungswünsche und Verwendungsvorschläge. Das Verfahren wird jedoch dadurch weitgehend unproblematisch, daß lediglich eine Einzelanzeige auf dem Bildschirm für jeweils einen Mitarbeiter, gewissermaßen eine Reproduktion des Personalbogens, vorgesehen ist. Eine vergleichende Auswertung der Daten mehrerer Mitarbeiter wird es nicht geben. Bei dieser Ausgestaltung wäre das geplante System unter datenschutzrechtlichen Gesichtspunkten akzeptabel.

Die Planungen der *Deutschen Bundesbahn* für die automatisierte Personaldatenverarbeitung lassen sich noch nicht abschließend bewerten. Danach ist ein dezentrales Personalinformationssystem vorgesehen, das sich über drei Ebenen erstrecken soll:

— Bei den Dienststellen der Bundesbahn ist der Einsatz von Mehrplatzcomputern geplant, mit denen je eine Mitarbeiter- und eine Dienstpostendatei geführt werden soll. Aufgabe dieses Systems ist in erster Linie die Personalbuchführung (ÖPDV-Örtliche Personaldatenverarbeitung).

— Bei den Bundesbahndirektionen und den zentralen Stellen (insgesamt 40) werden sowohl eine Mitarbeiter- als auch eine Dienstpostendatei geführt. Aufgaben dieses Systems sind Personalverwaltung und Personalwirtschaft (PSV-Personalstammdatenverwaltung).

— Zur Information der Unternehmensleitung sollen schließlich bisher schon bestehende Verfahren durch ein zentrales Verfahren abgelöst werden. Nähere Einzelheiten liegen noch nicht fest. Ob und inwieweit dabei personenbezogene Daten verarbeitet werden sollen, läßt sich gegenwärtig noch nicht absehen (zentrale PDV).

Aus der Sicht des Datenschutzes ist positiv zu bemerken, daß ein Einsatz freier Abfragesprachen bei allen drei Systemen ausdrücklich ausgeschlossen wird. Beurteilungen sind in der Mitarbeiterdatei des Systems PSV enthalten; sie sollen jedoch weder zu einer maschinellen Reihung verwandt noch mit anderen Daten verknüpft, sondern lediglich angezeigt werden.

Neben diesen zentral gesteuerten Systemen plant die Deutsche Bundesbahn auch ein dezentralisiertes Personaldatenverarbeitungssystem mit Kleinrechnern, das aus der Sicht des Datenschutzes besonders kritisch zu überprüfen ist; ich werde darauf im Zusammenhang mit dezentralen Systemen näher eingehen (vgl. unten zu 5.2.3).

Ob und inwieweit in der übrigen Bundesverwaltung wertende Angaben zu maschinellen Reihungen und Abgleichen im Rahmen von Personalinformationssystemen benutzt werden oder geplant sind, ist mir nicht bekannt. Die erforderlichen Infrastrukturen hierfür stehen jedenfalls zur Verfügung. Es ist zu befürchten, daß diese auch so genutzt werden, zumal moderne DV-Systeme in der Regel freie Abfragesprachen anbieten. Auch wenn eine Entscheidung durch technische Systeme nicht unmittelbar getroffen, sondern nur vorbereitet wird, sind derartige Systeme unter datenschutzrechtlichen Gesichtspunkten problematisch. Eines ihrer Probleme ist der Kontextverlust. Schon bei der Darstellung der Fähigkeiten eines Mitarbeiters in der Personalakte gehen wesentliche Umstände und Einzelheiten verloren. Dies ist um so mehr der Fall, wenn der Inhalt der Personalakte auszugsweise und verkürzt in ein Personalinformationssystem übernommen wird. Wird dann die Personalakte für eine Entscheidung erst gar nicht herangezogen, besteht die Gefahr, daß Fehlentscheidungen von weittragender Bedeutung getroffen werden, etwa bei Beförderungen, Versetzungen usw. In diesem Zusammenhang verweise ich auch auf meine Empfehlung im Zweiten Tätigkeitsbericht (S. 21 f.), von der automatisierten Verarbeitung der Beurteilungsnoten abzusehen — sofern diese sich nicht nur auf eine Speicherung zur Einzelanzeige am Bildschirm beschränkt.

5.2.2 Leistungs- und Verhaltenskontrolle

Die automatisierte Datenverarbeitung dringt immer weiter zu den Arbeitsplätzen vor. Art und Zahl der Aufgaben, die mit ihrer Hilfe erledigt werden, nehmen sprunghaft zu. Dazu werden zunehmend Sachbearbeiter-Dialogsysteme eingesetzt.

Bei solchen Systemen werden auch Daten über das Arbeitsverhalten der Mitarbeiter aufgezeichnet, die

mit dem jeweiligen System arbeiten. Die Aufzeichnungen sind aus technischen und aus Gründen des Datenschutzes erforderlich.

Die Verwendung solcher Daten (z. B. aus Log-Dateien, ADV-Auslastungsstatistiken, Aufzeichnungen zu Kontrollzwecken gemäß Anlage zu § 6 BDSG) zu einer individuellen Leistungs- oder Verhaltenskontrolle habe ich bereits früher als datenschutzrechtlich problematisch beurteilt (vgl. 3. TB S. 25 f., 5. TB S. 26 f. und 6. TB S. 17). Personaldaten, die im Rahmen der Durchführung der Kontrollmaßnahmen nach der Anlage zu § 6 BDSG gespeichert werden, unterliegen dem strikten Zweckbindungsprinzip; sie entziehen sich daher mangels entsprechender ausdrücklicher Einwilligung und mangels gesetzlicher Grundlage einer Nutzung zu anderen Zwecken als der Überwachung der Einhaltung der Maßnahmen zu § 6 BDSG.

5.2.3 Dezentralisierung der automatisierten Personaldatenverarbeitung

Das Vordringen von Personal Computern (PC) versetzt immer mehr Arbeitgeber in die Lage, die Durchführung der Arbeit maschinell zu überwachen. Auch hier besteht eine Gefährdung der Persönlichkeitsrechte durch maschinelle Kontrolle. Hinzu kommen typische Gefahren, die in den besonderen Eigenschaften kleiner Systeme und der dezentralisierten Datenverarbeitung als solcher liegen (vgl. dazu unten Nr. 16.3).

Einen Überblick konnte ich mir im Berichtsjahr bei der Deutschen Bundesbahn verschaffen, nachdem ich durch Eingaben auf die Verwendung von PC zur Personaldatenverarbeitung in drei Dienststellen einer Bundesbahndirektion hingewiesen worden war. Im einzelnen ergab sich dabei folgendes Bild:

Bei einer Fernmeldewerkstätte wurden auf einer Klein-Rechenanlage Personaldaten für Lohn- und Gehaltsempfänger und Auszubildende verarbeitet. Sie enthielten teilweise neben den Stammdaten u. a. auch Angaben über die Schulbildung, Schulnoten, Religion und den Grad der Schwerbehinderung. Die Existenz dieser Dateien stand im Widerspruch zu einer schriftlichen Mitteilung der DB vom Juli 1984, wonach Anwendungen mit personenbezogenen Daten auf PC nicht implementiert und bis zur Festlegung der erforderlichen Datensicherungsmaßnahmen auch nicht beabsichtigt seien. Bis auf die Datei für Auszubildende wurden alle Dateien inzwischen gelöscht. Eine Antwort auf meine Bitte, den Zweck dieser Datei und der vorgesehenen Datenübermittlung näher zu erläutern, steht noch aus.

Bei einer Signalmeisterei wird ein Pilotprojekt „Vorläufige Auftragsabrechnung in signal- und fernmeldetechnischen Dienststellen" durchgeführt. Für diesen Zweck wird ein PC mit einem Datenbanksystem eingesetzt. Zweck des Projektes ist in erster Linie die Ermittlung des tatsächlichen Personalbedarfs für die Aufgabenbereiche Instandhaltung und Montage. Die Erledigung dieser Aufgaben erfordert nach Auffassung der DB eigentlich keinen Personenbezug. Da das System aber gleichzeitig dazu genutzt wird, um Fehlzeiten plausibel nachweisen zu können, werden alle Daten erfaßt, mit deren Hilfe beantwortet werden kann, wer wo wie lange was gearbeitet hat. Die Datenerfassung erfolgt auf einem Stundennachweis-Formblatt.

Bei einem Bahnbetriebswerk wird das Pilotprojekt „Arbeitsvorbereitung in elektrotechnischen Dienststellen" durchgeführt. Das Pilotprojekt läuft unter dem Namen DIVA („DV-gestütztes Instandhaltungsverfahren für Anlagen"). Nach Abschluß der Einführung des Verfahrens sollen 54 Kleinrechner eingesetzt werden. Anlagebezogener Zweck des Verfahrens ist die Terminüberwachung bei der Arbeitsvorplanung für mehrere Jahre und die Ermittlung des Zeitaufwands für Instandhaltung nach Anlagegruppen. Personenbezogen geht es um die Erstellung des Tagewerkbuches je Mitarbeiter; hierfür werden jeweils die manuell erstellten Arbeitsnachweise und Fehlzeiten pro Mitarbeiter erfaßt.

Er entsteht jeweils ein vollständiger Überblick über die geleistete Arbeit und die Fehlzeiten jedes Bediensteten. Anhand dieser Aufstellung erfolgt die Lohnberechnung einschließlich der Zulagen.

Weil es sich bei diesen Verfahren um Anwendungen von Personal-Computern handelt, sind besondere Maßnahmen geboten, um den unter Nr. 16.3 im einzelnen beschriebenen Mißbrauchsrisiken dieser Technik zu begegnen. Der für diese technischen und organisatiorischen Maßnahmen erforderliche Aufwand richtet sich im Rahmen des Verhältnismäßigkeitsprinzips nach dem jeweiligen Schutzbedarf. Dieser wiederum hängt von den im Einzelfall gegebenen Umständen ab. Bei Personaldaten ist von einem besonders hohen Schutzbedarf auszugehen: Zum einen geht es um die Verarbeitung besonders sensibler Daten, die u. a. zur Verhaltens- und Leistungskontrolle sowie zu beliebigen weiteren Datenverknüpfungen und Abgleichen über Mitarbeiter verwendet werden könnten. Zum anderen handelt es sich nicht nur um lokal begrenzte Vorhaben, sondern um ein für die gesamte DB geplantes System der Personaldatenverarbeitung mit PC. Der qualitative Aspekt der Gefährdung der Persönlichkeitsrechte wird damit im Hinblick auf die große Zahl der betroffenen Mitarbeiter um ein quantitatives Element wesentlich erweitert.

Unter den bei der DB bislang gegebenen bzw. geplanten Einsatzbedingungen von PC in der Personaldatenverarbeitung halte ich u. a. folgende organisatorische und technische Maßnahmen für unverzichtbar:

- Eine lückenlose Menüsteuerung, d. h. eine Zwangsführung des Benutzers, die ihm nur die Auswahl unter den planmäßigen — zulässigen — Verarbeitungen ermöglicht.
- Kryptographische Verschlüsselung der personenbezogenen Daten, damit sich Zugriffsmöglichkeiten über andere Software ausschließen lassen.

— Die Benutzerberechtigung muß an die Fachzuständigkeit gebunden sein und im übrigen so restriktiv wie möglich vergeben werden.

— Ein zentrales Melde- und Freigabe- bzw. Genehmigungsverfahren für Anlagen, personenbezogene Dateien und Verarbeitungssysteme, das auch die Beteiligung der Personalvertretung vorsehen sollte. Gemeldet werden müssen auch PC, die nicht zur personenbezogenen Datenverarbeitung vorgesehen, aber dafür geeignet sind. Wegen der bei der DB zutage getretenen Probleme der örtlichen Dienststellen mit der Qualifizierung personenbezogener Dateien müssen sämtliche Dateien der Hauptverwaltung gemeldet und dort bewertet werden (§ 15 BDSG).

— Eine Freigabe für die Beschaffung und Implementierung von Anlagen und Verarbeitungssystemen sollte erst erteilt werden, wenn feststeht, daß ein unter datenschutzrechtlichen Gesichtspunkten angemessenes und praktikables Kontrollsystem zur Verfügung steht. Nur so kann auch die Vorbeugungsfunktion von Kontrollerwartungen genutzt werden. Es reicht nicht aus, hier auf die externe Kontrolle durch den BfD zu vertrauen, da diese schon wegen der großen Zahl von Anlagen nur bedingt wirksam sein kann.

Falls und soweit diese Sicherungsmaßnahmen bzw. Verarbeitungsregeln durchgeführt werden, wäre die Einhaltung der §§ 15 Abs. 1, 6 BDSG und damit faktisch ein Verfahren der Personaldatenverarbeitung sichergestellt, das dem Einsatz zentraler Datenverarbeitungsanlagen vergleichbar wäre. Das sogenannte „personal computing", das heißt, die beliebige individuelle Nutzung der spezifischen PC-Möglichkeiten wäre weitgehend ausgeschlossen.

Angesichts der oben beschriebenen Vorbereitungen der DB für ein zentral gesteuertes, mit Mehrplatzcomputern betriebenes Personalinformationssystem (ÖPDV/PSV) wird die DB entscheiden müssen, ob und gegebenenfalls in welchem Umfang daneben noch die Verarbeitung personenbezogener Daten auf PC unter Berücksichtigung der verbleibenden spezifischen Restrisiken angemessen ist.

Die vorstehenden Probleme habe ich mit der DB erörtert. Sie hat zugesagt, bis April 1986 ein umfassendes Datenschutzkonzept zu erstellen. Ich habe darum gebeten, mir dieses Konzept zuzuleiten und alle Beschaffungs- und Freigabeentscheidungen für PC-Anlagen, Dateien und Vorbereitungssysteme erst zu treffen, wenn feststeht, daß das geplante Steuerungs- und Überwachungssystem den datenschutzrechtlichen Anforderungen voll entspricht.

5.2.4 Mitbestimmung und bereichsspezifische gesetzliche Regelung des Arbeitnehmerdatenschutzes

Die besondere Gefährdung der Persönlichkeitsrechte beim Einsatz der automatisierten Datenverarbeitung in der Personalverwaltung kann durch das Mitbestimmungsrecht der Personalvertretungen weitgehend ausgeglichen werden. Im Hinblick auf die weittragenden datenschutzrechtlichen und gesellschaftspolitischen Risiken und die große Zahl der im Einzelfall Betroffenen halte ich dessen Ergänzung und darüber hinaus bereichsspezifische gesetzliche Regelungen zum Arbeitnehmerdatenschutz für dringlich. In früheren Tätigkeitsberichten habe ich bereits mehrfach auf einen solchen Regelungsbedarf hingewiesen (vgl. 5. TB S. 27, 115; 7. TB S. 92).

Die Bundesregierung hat in Ausführung des Beschlusses des Deutschen Bundestages zu meinem fünften Tätigkeitsbericht vom 20. September 1984 (vgl. Drucksache 10/1719, Nr. I/13) in einem ausführlichen Bericht die Notwendigkeit bereichsspezifischer Regelungen zum Schutz der Arbeitnehmerrechte insbesondere bei der automatisierten Datenverarbeitung bejaht und zugesagt, die erforderlichen gesetzgeberischen Schritte einzuleiten.

Der Bundestagsausschuß für Arbeit- und Sozialordnung hat diesen Bericht erörtert und die Bundesregierung aufgefordert, die „vom Ausschuß für drängend gehaltenen Fragen verstärkt aufzugreifen und den Entwurf einer bereichsspezifischen Regelung des Arbeitnehmerdatenschutzes zu Beginn der nächsten Legislaturperiode dem Deutschen Bundestag vorzulegen".

Für dieses Gesetzgebungsvorhaben gebe ich folgende Empfehlungen:

— Die Speicherung, Auswertung, Veränderung und Übermittlung von Arbeitnehmerdaten muß auf die Fälle gesetzlicher Verarbeitungspflichten und den Zweck der Durchführung des Arbeitsverhältnisses beschränkt werden; „berechtigte Interessen" des Arbeitgebers reichen hierfür nicht aus.

— Auswertungen und Verknüpfungen, die zur Herstellung eines „Persönlichkeitsabbildes" der Arbeitnehmer führen können, müssen unzulässig sein.

— Daten der Beschäftigten, die im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen nach § 6 BDSG und dessen Anlage gespeichert werden, dürfen grundsätzlich nicht zu Zwecken der Verhaltens- und Leistungskontrolle ausgewertet werden.

— Dienst- und arbeitsrechtliche Beurteilungsnoten des Beschäftigten dürfen nur unter eingeschränkten Voraussetzungen automatisiert verarbeitet werden.

— Medizinische und psychologische Befunde oder Daten, aus denen diese abgeleitet werden können, dürfen allenfalls in selbständigen und streng abgeschotteten Systemen des personalärztlichen Dienstes automatisiert verarbeitet werden.

— Der Auskunftsanspruch des Arbeitnehmers muß erweitert werden. Insbesondere soll er einen Auskunftsanspruch über alle Empfänger seiner Daten sowie über alle regelmäßigen Verwendungen erhalten.

— Ein Mitbestimmungsanspruch der Personalvertretung bei Planung und Einführung automatisierter Personaldatenverarbeitung muß eindeutig festgelegt werden.

6. Deutsche Bundespost

6.1 Zusammenarbeit mit dem Bundesminister für das Post- und Fernmeldewesen

Angesichts der vielfältigen datenschutzrechtlich relevanten Aktivitäten der Deutschen Bundespost — insbesondere im Rahmen der Einführung moderner Kommunikationstechniken — habe ich Kontakte zu vielen Stellen der Deutschen Bundespost (DBP). Diese ergeben sich nicht nur im Zusammenhang mit der Durchführung von Beratungen und datenschutzrechtlichen Kontrollen. Auch zahlreiche an mich gerichtete Eingaben von Bürgern betreffen den Bereich der DBP und erfordern eine Stellungnahme des Bundesministers für das Post- und Fernmeldewesen (BMP). Die Arbeitskontakte können im allgemeinen als offen und konstruktiv bezeichnet werden. Die Effektivität der Zusammenarbeit wird jedoch durch Probleme der folgenden Art beeinträchtigt:

— Wiederholt habe ich erst aus der Presse von neuen oder durch Rechnereinsatz neu gestalteten Dienstleistungen der DBP erfahren, deren Ausgestaltung zahlreiche Fragen aus der Sicht des Datenschutzes aufwirft. Beispiele hierfür sind die Einführung eines neuen Autotelefon-Systems und des Elektronischen Telefonbuches (siehe unten Nr. 6.4.2). Die präventive Zielrichtung der mir durch das BDSG zugewiesenen Beratungsaufgabe bedeutet jedoch, daß die Beratung möglichst früh einsetzen muß. Sie bezieht sich nicht etwa nur auf Rechts- und Verwaltungsvorschriften, sondern auch auf die technische Ausgestaltung neuer Dienstleistungen. Probleme, die bereits im Vorbereitungsstadium einer neuen Dienstleistung erkannt werden, lassen sich in der Regel leichter beheben bzw. vermeiden. Ich würde es daher begrüßen, wenn ich künftig frühzeitig über geplante Dienste bzw. Techniken informiert würde, in denen personenbezogene Daten verarbeitet werden.

— Wiederholt hat mir der BMP in seinen Stellungnahmen entgegengehalten, die betreffenden Daten würden nicht in Dateien gespeichert; sie unterlägen somit auch nicht dem Schutz des BDSG (siehe unten Nr. 6.8). Da dies im allgemeinen im Zusammenhang mit der Bearbeitung von Eingaben geschah, ist ein solches Vorgehen besonders bedauerlich. Wenn ein Bürger mir bestimmte Tatsachen mitteilt, die eine Beeinträchtigung seiner schutzwürdigen Belange durch Datenverarbeitung vermuten lassen, erscheinen mir die von ihm gewünschte Aufklärung des Sachverhaltes und das Finden möglicher Lösungen vordringlich, auch wenn das BDSG unmittelbar nicht anwendbar ist. Ich beabsichtige in solchen Fällen keineswegs, mir nicht zustehende Kompetenzen zu beanspruchen, also etwa Beanstandungen auszusprechen, sondern ich möchte dem Bürger, der nach meinen Erfahrungen in der Regel für eine formale Abweisung seines Anliegens kein Verständnis hat, im Wege von Empfehlungen oder Ratschlägen weiterhelfen.

  Zuweilen wurde vom BMP die Auffassung vertreten, eine Beratung durch Empfehlungen zur Verbesserung des Datenschutzes (§ 19 Abs. 1 Satz 2 BDSG) setze das Vorhandensein einer Datei voraus, oder Empfehlungen im Bezug auf eine interne Datei dürften nur technisch-organisatorische Maßnahmen i. S. des § 6 BDSG zum Inhalt haben, oder gar eine Beratung könne nur dann in Betracht kommen, wenn darum gebeten werde. Ich kann diese Auffassung nicht akzeptieren; sie widerspricht meinem Amtsverständnis und den Erwartungen der betroffenen Bürger und findet meines Erachtens keine Stütze im Gesetz.

— Die Bearbeitungsdauer von Vorgängen, die ich dem BMP mit der Bitte um Stellungnahme übersandt habe, ist gelegentlich unverhältnismäßig lang. Dies führt nicht nur (durch Wiedervorlagen und Nachfragen) zu einer vermeidbaren Belastung meiner Dienststelle, sondern auch oft zu Verärgerungen der betroffenen Bürger. Selbst bei komplexen Fragestellungen sollte sich dieses Problem — z. B. durch Teilbescheide — mildern lassen.

6.2 Bildschirmtext

6.2.1 Stand der Entwicklung

Noch im Oktober 1984 ging die DBP für die Entwicklung von Bildschirmtext (Btx) von Planungen aus, die ca. 180 000 Teilnehmer und 2,5 Millionen abrufbare Seiten für Ende 1985 erwarten ließen. Tatsächlich waren es am 31. Dezember 1985 ca. 38 000 Teilnehmer und rund 763 000 (zum Teil entgeltpflichtige) Btx-Seiten. Als kommerziell bedeutsamer Schwerpunkt der Btx-Nutzung hat sich — neben Warenbestellungen — die elektronische Girokontoführung, das sogenannte „Homebanking" herausgestellt. Bereits Mitte des Jahres wurde die Anzahl dieser sogenannten Telekonten auf 28 000 geschätzt. Zweitgrößter Anbieter mit über 7 500 Telekonten im Postgirodienst ist hier die DBP selbst.

6.2.2 Kontrollkompetenz; Regelungsdefizite

Die datenschutzrechtliche Kontrollkompetenz für Btx ist geteilt: Soweit es sich um die Deutsche Bundespost als Betreiber des Dienstes oder um sie und andere öffentliche Stellen des Bundes als Anbieter handelt, liegt die Kontrollzuständigkeit beim BfD. Im Staatsvertrag der Länder über Bildschirmtext bzw. den Zustimmungsgesetzen der Länder ist die Kontrollkompetenz für den übrigen Nutzungsbereich geregelt.

Bereits seit Aufnahme der Btx-Feldversuche dauert die Diskussion über den Datenschutz bei Btx an. Im Mittelpunkt besonderen Interesses stehen dabei Fragen nach der Sicherheit des Systems gegenüber

unbefugtem Systemzugang, der Verfälschung von Übermittlungen und Seiteninhalten sowie der Manipulation bei Telekonten. Spektakuläre Fälle, in denen es sogenannten „Hackern" gelungen war, Sicherheitsschranken zu überwinden, haben dazu beigetragen, daß die DBP einige meiner Anregungen zur Erhöhung der Sicherheit aufgegriffen hat. Besondere Aufmerksamkeit erregte in der Öffentlichkeit der Fall eines Computer-Clubs, der im Bildschirmtext entgeltpflichtige Seiten anbietet. Mitglieder des Clubs hatten unter der vorgegebenen Identität einer Sparkasse ihre eigenen Btx-Seiten in einer solchen Anzahl abgerufen, daß der Sparkasse vom System eine Vergütungsschuld von ca. DM 135 000 zugunsten des Clubs in Rechnung gestellt wurde. Dabei hatten sich die Clubmitglieder der Anschlußkennung und des „persönlichen Kennwortes" der Sparkasse bedient. Nach ihren Angaben hatten sie diese unter Ausnutzung eines (inzwischen beseitigten) Programmfehlers des Btx-Systems von diesem selbst erhalten. Ob diese Darstellung zutrifft, oder aber die der DBP, nach der die genannten Angaben anläßlich einer Btx-Demonstration „ausgespäht" wurden, konnte nachträglich nicht zweifelsfrei geklärt werden.

Unbefriedigend ist aus meiner Sicht nach wie vor die mangelnde Normenklarheit bei Btx: Die Rechtsvorschriften, die den Dienst selbst regeln sowie die Rechte und Pflichten von Teilnehmern und Anbietern aus dem Teilnehmerverhältnis — auch bezüglich des Datenschutzes — bestimmen, sind selbst für den Rechtskundigen nur schwer zu überblicken. Ich habe den BMP schon im Jahre 1984, zuletzt in einem Schreiben vom 26. Juni 1985 darauf hingewiesen, daß eine zusammengefaßte und übersichtliche Darstellung dieser Vorschriften unerläßlich ist, und eingehende Empfehlungen für die notwendigen Regelungsinhalte gegeben. Außer einer Absichtserklärung, in dieser Richtung etwas zu tun, lag mir bis vor kurzem leider keine Äußerung des BMP in dieser Angelegenheit vor. Ich bin lediglich auf den Entwurf einer „Telekommunikationsordnung (TKO)" hingewiesen worden, die auch Btx regeln soll. Dieser Entwurf ist mir erst im Dezember 1985 zugegangen und konnte daher bis Redaktionsschluß noch nicht ausgewertet werden.

Beim Erlaß einer Benutzungsordnung wie der TKO stützt sich der BMP auf das Postverwaltungsgesetz (PostVwG), das ihn ermächtigt, „die Rechtsverordnungen über die Bedingungen ... für die Benutzung der Einrichtungen des Post- und Fernmeldewesens zu erlassen" (§ 14 PostVwG). Nach der Wesentlichkeitstheorie des Bundesverfassungsgerichtes hat jedoch der *„Gesetzgeber ...* in grundlegenden normativen Bereichen, zumal im Bereich der Grundrechtsausübung, ... alle wesentlichen Entscheidungen selbst zu treffen" (BVerfGE 49, S. 126). Neue Kommunikationsdienste wie Btx und TEMEX schaffen eine Infrastruktur, die zumindest geeignet ist, Persönlichkeitsrechte zu beeinträchtigen.

Ich halte daher eine Prüfung für erforderlich, ob § 14 PostVwG als ausreichende Rechtsgrundlage für die Einführung und Regelung solcher neuer technischer Kommunikationsdienste anzusehen ist.

6.2.3 Datenschutzkontrollen

Bereits im Jahre 1984 kontrollierte ich die Btx-Leitzentrale, die das gesamte Netz steuert (vgl. 7. TB S. 25). Ich begrüße es, daß die meisten meiner Anregungen und Vorschläge als Ergebnis der Prüfung inzwischen umgesetzt worden sind bzw. noch werden. Dies betrifft z. B. meine Empfehlungen bezüglich der datenschutzgerechten Gestaltung der Organisationsabläufe und die Benennung eines „Sicherheitsbeauftragten". Auch die fehlende EDV-Programmdokumentation liegt inzwischen der DBP vor. Die Überarbeitung des Verfahrens zur Speicherung und Verarbeitung von Btx-Abrechnungsdaten wurde aufgenommen und sollte bald abgeschlossen sein. Auch bezüglich der im Btx-System automatisiert geführten Dateien personenbezogener Daten ist die DBP inzwischen ihrer gesetzlichen Meldepflicht nachgekommen. Hingegen fehlen noch immer wirksame Verfahren zur Erkennung und Verfolgung von Versuchen, durch „Probieren" das Kennwort eines anderen zu ermitteln. Insbesondere wird der dadurch gefährdete Teilnehmer nicht gewarnt.

Die lokalen Knoten des Btx-Netzes bilden die Btx-Vermittlungsstellen. Die Datenschutzkontrolle einer Btx-Vermittlungsstelle ergab keine gravierenden Datenschutzmängel. Über mögliche Verbesserungen im technischen und organisatorischen Bereich bin ich mit dem BMP im Gespräch.

6.3 Telefon-Fernwirksystem TEMEX

6.3.1 Projektstand

Zum Ende dieses Jahres sollen in den Versuchsgebieten München und Ludwigshafen durch Anschaltung der ersten Haushalte die TEMEX-Systemversuche aufgenommen werden (vgl. 7. TB, S. 26). Als typische Anwendungen bieten dabei private Wachdienste und Hilfseinrichtungen die Bearbeitung von Notfallmeldungen an. Dabei kann z. B. ein Kranker oder Behinderter — mittels Knopfdruck oder automatisch arbeitender Einrichtungen — der ständig besetzten Alarmzentrale ein Hilfesignal übermitteln. In der umgekehrten Übermittlungsrichtung kann ein Wach- und Schließdienst z. B. in Abwesenheit des Hausbesitzers die Markisen herablassen oder vor dessen Rückkehr die Heizung in Betrieb setzen.

Bei solchen Anwendungen speichert die DBP lediglich kurzfristig und vorübergehend Informationen, wie z. B. daß in der betreffenden Wohnung ein Schalter betätigt wurde. Sie weiß in der Regel nicht einmal, daß hierdurch z. B. ein Notruf signalisiert werden soll. Angesichts solcher Speicherungen sind im Rahmen der *Systemversuche* nach meiner Beurteilung für die genannten oder weiteren TEMEX-Anwendungen im Bereich der Deutschen Bundespost keine Beeinträchtigungen schutzwürdiger Belange im Sinne des BDSG zu erwarten.

6.3.2 Datenschutzbegleitgremium

Die DBP hat meine Anregungen aufgegriffen und — zunächst für den Bereich München — ein Be-

gleitgremium für die Systemversuche konstituiert, das Datenschutzprobleme bei TEMEX definieren und Lösungsvorschläge erarbeiten soll. Mitglieder des Gremiums sind neben dem Bayerischen Landesbeauftragten und mir auch TEMEX-Anbieterfirmen.

6.3.3 Regelungsbedarf

Für die Systemversuche werden die Rechtsverhältnisse zwischen DBP, TEMEX-Anbietern und -Nutzern durch Einzelverträge geregelt, bei deren Gestaltung ich mitgewirkt habe. Wichtig ist dabei aus meiner Sicht einmal die *Transparenz:* Der Nutzer muß nicht nur seine Rechte und Pflichten aus der Vereinbarung klar erkennen können, vielmehr müssen ihm auch die wichtigsten Aspekte der Wirkungsweise von TEMEX erläutert werden. Erst durch die Transparenz wird die weitere wichtige Voraussetzung ermöglicht, die *Freiwilligkeit* der Teilnahme, die auch eine nutzerfreundliche Kündigungsmöglichkeit verlangt.

Im Anschluß an die Systemversuche sind sogenannte *Betriebsversuche* vorgesehen, in denen auch weitergehende Anwendungen, wie z. B. Zählerablesungen erprobt werden sollen. Ich gehe davon aus, daß von der DBP bis dahin die in ihrem Bereich noch offenen Datenschutzprobleme gelöst werden und in entsprechende Regelungen Eingang finden. Im Hinblick auf den Schutz des Persönlichkeitsrechts sollte hierbei auch die Erforderlichkeit einer *gesetzlichen* Regelung geprüft werden. Ob § 14 Postverwaltungsgesetz noch als ausreichende Ermächtigung zur Regelung der sich aus den neuen Fernmeldediensten ergebenden datenschutzrechtlichen Probleme angesehen werden kann (siehe auch Nr. 6.2), bedarf einer eingehenden Prüfung. Der zusätzlich im Anbieter-Nutzer-Verhältnis, also außerhalb des Fernmelderechts, bei TEMEX bestehende Regelungsbedarf ist Gegenstand von Ressortbesprechungen, an denen ich beteiligt bin.

6.4 Eintrag der Teilnehmer ins Telefonbuch

6.4.1 „Zwangseintragung"

Durch Zugeständnisse der DBP bei der Gestaltung der Einträge ins Telefonbuch und auch bei der Genehmigung von Nichteintragungen kommt es nach meinen Beobachtungen für viele der Betroffenen zu befriedigenden Regelungen. Es gibt jedoch Telefonteilnehmer, die eine Beeinträchtigung ihrer schutzwürdigen Belange schon darin erblicken, daß gegen ihren erklärten Willen *überhaupt* eine Eintragung vorgenommen wird. Sie sehen auch in der Verpflichtung zur Darlegung von Gründen („Gefährdung oder erhebliche Belästigung"), die auf Antrag eine Nichteintragung ermöglichen, einen Eingriff in ihre Privatsphäre.

Nach geltendem Recht ermöglicht § 39 Abs. 2 Satz 1 Fernmeldeordnung eine Eintragung auch gegen den Willen des Teilnehmers. Die Vereinbarkeit dieser „Zwangseintragung" mit den vom Bundesverfassungsgericht im Volkszählungsurteil aufgestellten Grundsätzen für die Voraussetzungen einer Einschränkung der informationellen Selbstbestimmung bedarf der Überprüfung. Insbesondere muß die Zulässigkeit der genannten Vorschriften daraufhin geprüft werden, ob die durch sie bestimmte Einschränkung des Rechtes auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse liegt.

6.4.2 Elektronisches Telefonbuch

Btx-Teilnehmer können derzeit bezüglich der Telefon-Ortsnetze von Hamburg, Berlin und München das sogenannte Elektronische Telefonbuch (ETB) benutzen. In Analogie zum gedruckten Telefonbuch muß der Btx-Teilnehmer auch hierbei grundsätzlich den Wohnort des gesuchten Teilnehmers eingeben, um dann über den Nachnamen und — soweit nötig — weitere Zusätze wie Vorname, Straße, usw. die Telefonnummer des Gesuchten angezeigt zu bekommen.

Gegenüber dem gedruckten Telefonbuch weist das ETB einige bedeutsame qualitative Unterschiede auf:

a) Größerer Suchbereich

   Durch die sogenannte Nahbereichssuche des ETB kann ein Teilnehmer nicht nur im Telefonbuchbezirk, sondern auch im Telefon-Nahbereich gefunden werden (in Bonn z. B. in 19 anstatt in 12 Orten).

b) Wesentlich höhere „Trefferquote"

   Das ETB gestattet die sog. „phonetische Namenssuche". Dadurch werden — z. B. bei Eingabe des Namens „Meier" — alle Teilnehmer gleicher und ähnlicher Schreibweise angezeigt. Es werden auch nicht nur — wie bei der Fernsprechauskunft — maximal fünf gleichlautende Namen, sondern *30* angezeigt. Dadurch kann oftmals auch bei unpräzisen Suchangaben der Gesuchte gefunden werden.

c) Suchgeschwindigkeit

   Insbesondere bei der Nahbereichssuche wird die Suchgeschwindigkeit gegenüber konventionellen Verfahren um ein Mehrfaches erhöht.

d) Aktualität

   Während das amtliche Telefonbuch durch den Erscheinungszyklus lediglich jahresaktuell ist — bei einer jährlichen Änderungsquote von über 30 % — ist das ETB wochenaktuell.

e) Auskunftsbreite

   Die Auskunft beschränkt sich nicht auf die Teilnehmer mit dem eingegebenen Namen, sondern berücksichtigt auch mögliche Ergänzungen. So würden z. B. bei der Eingabe des Namens „Krumm" nicht nur alle Eintragungen zu diesem Namen sondern auch die zu Krummacher, Krumme, Krummeich, Krummel usw. angezeigt.

Diese Unterschiede begründen die Besorgnis, mit Hilfe des ETB könnte — mit relativ geringem Aufwand — der Aufenthaltsort eines Fernsprechteil-

nehmers bundesweit ermittelt werden. Insbesondere unter Verwendung intelligenter Btx-Terminals kann der Inhalt des ETB bedeutend leichter ausgewertet und kopiert werden. Angesichts der hohen Telefondichte der Bundesrepublik käme das einem Bundesadreßregister nahe.

Andere Besorgnisse stellen auf die leichtere Auswertbarkeit der im ETB enthaltenen Adressen zu Werbezwecken ab.

Angesichts dieser Unterschiede zum gewöhnlichen Telefonbuch, die noch einer gründlichen datenschutzrechtlichen Untersuchung bedürfen, stellt sich auch hier mit besonderer Eindringlichkeit die Frage sowohl nach der Tragfähigkeit der Verordnungsermächtigung des § 14 PostVerwG (siehe oben Nr. 6.2 und Nr. 6.3) wie auch nach der Gewährleistung des Rechts auf informationelle Selbstbestimmung bei der Eintragung ins Telefonbuch.

6.5 Fernsprechauskunft

Immer wieder erreichen mich Eingaben von Bürgern, die sich darüber beschweren, daß die Fernsprechauskunft der DBP ihnen unter Hinweis auf Datenschutzgründe die Angabe der Wohnanschrift des gesuchten Teilnehmers verweigert.

Die DBP hat hierzu ausgeführt, daß die Fernsprechauskunft im wesentlichen nur über die Angaben verfügt, die auch in die Fernsprechbücher eingetragen sind. Diese stehen jedoch jedermann öffentlich zur Verfügung. Ich habe daher dem BMP meine Auffassung mitgeteilt, nach der Datenschutzgründe einer Bekanntgabe solcher Angaben durch die Fernsprechauskunft nicht entgegenstehen, die auch im Telefonbuch eingetragen sind.

Dagegen kommt es nach meiner Auffassung darauf an, ob im Rahmen informationeller Selbstbestimmung der Teilnehmer selbst darüber entscheiden kann, ob seine Anschrift ins Telefonbuch eingetragen wird und damit der Auskunft wie der öffentlichen Einsichtnahme zur Verfügung steht. Ich verweise insoweit auf meine Ausführungen unter Nr. 6.4.1.

6.6 Registrierung der Verbindungsdaten von Telefongesprächen bei belästigenden Anrufen

In den Fällen, in denen ein Bürger sich durch Telefonanrufe bedroht, beleidigt oder in erheblichem Umfange belästigt fühlt, kann er bei der DBP die sog. „Beobachtung eines Teilnehmeranschlusses" beantragen. Dabei genügt das Vorbringen allein nicht, der Antragsteller muß vielmehr die Antragsgründe glaubhaft machen. Entspricht die DBP diesem Antrag, kann sie — je nach technischen Gegebenheiten — verschiedene Maßnahmen treffen. Im Regelfall wird die sog. Fangschaltung eingerichtet, mit der derjenige Anschluß ermittelt wird, von dem der vom Antragsteller als belästigend bezeichnete Anruf ausging. In bestimmten Fällen wird jedoch auch eine Aufzeichnung mit Hilfe einer sogenannten Zählvergleichseinrichtung an demjenigen Anschluß vorgenommen, den der Antragsteller als Quelle der belästigenden Anrufe angegeben hat.

Mit der DBP besteht Einvernehmen, daß in diesen Fällen ein betrieblicher Anlaß für die Aufzeichnung besteht, der diese rechtfertigt. Indem die DBP den Angerufenen in die Lage versetzt, gegen den Anrufer vorzugehen, unterstützt sie dessen Rechtsschutzbedürfnis und dient seinem wie ihrem Anliegen, einem Mißbrauch von Telefoneinrichtungen entgegenzuwirken.

Aber auch der beobachtete Anrufer sollte nach Abschluß der Beobachtung über die Aufzeichnung der von ihm ausgegangenen Gespräche informiert werden. Ich halte es für geboten, ihm auch den konkreten betrieblichen Anlaß für die Aufzeichnung, d. h. den Mißbrauchsvorwurf des Angerufenen, zu nennen. Ich sehe mithin die DBP für verpflichtet, nicht nur das Rechtschutzbedürfnis des Angerufenen zu unterstützen, gegen Beleidigungen bzw. Belästigungen vorzugehen, sondern auch das des Anrufers, sich gegen etwaige falsche Anschuldigungen zu wehren. Den Antragsteller sollte die Post über dieses Verfahren bei der Antragstellung unterrichten. Eine Änderung der derzeitigen Praxis halte ich für dringend erforderlich.

6.7 Weitergabe von Telefonkundenanschriften zu Werbezwecken

Die DBP übermittelt die Anschriften der Fernsprechteilnehmer zur werblichen Nutzung an die Deutsche Postreklame in Frankfurt am Main, es sei denn, der Kunde hat dagegen Widerspruch eingelegt. Im Rahmen einer datenschutzrechtlichen Kontrolle bei verschiedenen Fernmeldeämtern einer Oberpostdirektion habe ich stichprobenweise geprüft, ob und wie dem Widerspruch durch die DBP nachgekommen wird. Es hat sich gezeigt, daß in einem Massenverfahren vorliegender Art Fehler — wie im folgenden beschrieben — wohl nie ganz auszuschließen sein werden, daß aber weitere Beobachtungen und Bemühungen zur Reduzierung des Fehleranteils geboten sind. Dazu habe ich angeregt, bei allen Oberpostdirektionen in regelmäßigen Abständen den Inhalt der Fernsprechteilnehmerakten mit den daraus gewonnenen und automatisiert gespeicherten Daten zu vergleichen. Der BMP hat mir inzwischen mitgeteilt, er habe die Oberpostdirektion gebeten, die Datenschutzbeauftragten bei den Fernmeldeämtern mit entsprechenden Prüfungen zu beauftragen.

Meine Nachforschungen in diesem Bereich haben ferner gezeigt, daß eine durch den Fernsprechteilnehmer nachträglich verfügte Sperre der Weitergabe seiner Anschrift zur werblichen Nutzung nach sehr unterschiedlichen Zeiten, oft erst nach mehreren Monaten, wirksam wird. Dies ist davon abhängig, ob der Widerspruch beim zuständigen Fernmeldeamt oder aber bei der Deutschen Postreklame in Frankfurt am Main eingelegt wird. Ich habe die DBP schon im Frühjahr 1984 aufgefordert, die Zeiten bis zum Wirksamwerden der gewünschten

Sperre durch geeignete Verfahren einheitlich zu gestalten und dabei zu prüfen, ob sie verkürzt werden können. Eine Antwort liegt mir bisher nicht vor.

Ein weiterers datenschutzrechtliches Problem ergibt sich in den Fällen, in denen trotz eines Widerspruchs oder bei einem Nichteintrag im Telefonbuch die Anschrift durch die DBP der Deutschen Postreklame zu Werbezwecken zur Verfügung gestellt worden ist. Ich habe den BMP hierzu um Stellungnahme gebeten. Insbesondere interessieren mich in diesem Zusammenhang die Maßnahmen der DBP zur Schadensminderung und -begrenzung sowie zum Regreßanspruch des Fernmeldekunden. Die Mitteilung allein, daß nunmehr künftig der Widerspruch beachtet werde, reicht m. E. nicht aus.

Wie ich schon bei früherer Gelegenheit gegenüber dem BMP zum Ausdruck brachte, habe ich auch Zweifel, ob die jetzige Form der Adressenweitergabe an die Deutsche Postreklame den Grundsätzen des Urteils des Bundesverfassungsgerichts zum Volkszählungsgesetz entspricht; wenn — wie hier — eine Rechtsgrundlage fehlt, gilt die Selbstbestimmung des Bürgers. Neben der ausdrücklichen schriftlichen Zustimmung des Kunden unterstellt die DBP aber auch dann sein Einverständnis zur Übermittlung seiner Anschrift an die Deutsche Postreklame, wenn er nicht ausdrücklich Widerspruch einlegt. Kreuzt er nämlich weder das Kästchen für sein Einverständnis noch das Kästchen für den Widerspruch an, so wertet die DBP dies als Zustimmung, weist hierauf allerdings im sog. „Kleingedruckten" hin. Ich trete hier für mehr Klarheit ein und habe empfohlen, nur dann eine Adressenweitergabe vorzunehmen, wenn der Fernsprechteilnehmer dieser Übermittlung ausdrücklich zugestimmt hat.

6.8 Ermittlung von Anschriften Neugeborener durch Postzusteller

In einer Eingabe bin ich darauf aufmerksam gemacht worden, daß die DBP die Brief- und Paketzusteller dazu anhält, ihr aufgrund des Kontaktes zur Bevölkerung Anschriften von Neugeborenen mitzuteilen. Die Eltern des Kindes sollen sodann zur Einrichtung eines Postsparkassenbuches für das Kind gezielt geworben werden. Die DBP führt in dem entsprechenden schriftlichen Aufruf dazu aus: „Die besten Anschriftenbeschaffer erhalten im Rahmen einer Verlosung Geld- bzw. Sachpreise."

Nach meiner Meinung ist nicht auszuschließen, daß die Aufforderung der DBP an ihre Zusteller — zumindestens im Einzelfall — einen Anreiz zur Durchbrechung des Postgeheimnisses und des Amtsgeheimnisses darstellt. Die Verschwiegenheitspflicht des Zustellers umfaßt auch solche Erkenntnisse, die er unmittelbar oder durch Rückschlüsse aus seiner amtlichen Tätigkeit gewinnt, z. B. aus dem Umstand, daß eine Familie Werbesendungen von Kindernahrungsproduzenten erhält. Deshalb erscheint mir eine Weitergabe in Bereiche bedenklich, die mit den Betriebsvorgängen der Zustellung nichts zu tun haben, nämlich der des Postsparwesens und des Marketingbereichs der DBP.

Der BMP sieht in diesem Verfahren keine Verletzung des Post- oder Amtsgeheimnisses. Er führt vielmehr aus: „Der Zustand einer werdenden Mutter bleibt in der Regel einem Brief- oder Paketzusteller, der häufig Kontakt mit den Bewohnern seines Zustellbezirks hat, nicht verborgen." Nach meiner Auffassung ist jedoch zu unterscheiden, ob ein Zusteller solches wahrnimmt oder ob es ihm zu einer dienstlichen Aufgabe gemacht wird, dies für Werbezwecke weiterzugeben.

7. Verkehrswesen

Meine Tätigkeit auf dem Gebiet des Verkehrswesens bestand hauptsächlich in der Beratung der im Deutschen Bundestag vertretenen Parteien, des Bundesministers für Verkehr, des Kraftfahrt-Bundesamtes, der Deutschen Bundesbahn sowie in der Behandlung von Bürgereingaben.

Stellvertretend für viele Problemstellungen seien erwähnt:

— Änderung des Straßenverkehrsgesetzes (Fahrzeugregistergesetz)

— Änderung des Straßenverkehrsgesetzes (Führerschein auf Probe)

— Auswirkungen einer Geschwindigkeitsbegrenzung auf das Abgasverhalten von Pkw (Versuch Tempo 100)

— Einführung des „Zentralen Verkehrsinformationssystems (ZEVIS)" beim Kraftfahrt-Bundesamt (Anhörung der SPD-Fraktion im Dezember 1984)

— Verkehrszentralregister (Datenübermittlung für Forschungszwecke)

— Schwarzfahrer-Datei bei der Deutschen Bundesbahn

— Forderung von Nachweisen bei Fahrpreiserstattungen durch die Deutsche Bundesbahn.

Diese vielfältigen Beratungstätigkeiten führten dazu, daß von den für 1985 im Arbeitsbereich Verkehrswesen vorgesehenen Datenschutzprüfungen nur eine durchgeführt werden konnte.

7.1 Fahrzeugregistergesetz (ZEVIS)

Zu dem Gesetzentwurf des Bundesministers für Verkehr zur Änderung des Straßenverkehrsgesetzes, der Regelungen über die Fahrzeugregister bei den örtlichen Kfz-Zulassungsstellen sowie beim Kraftfahrt-Bundesamt (KBA) in Flensburg vorsieht, habe ich meine grundsätzlichen Positionen bereits dargelegt (7. TB S. 27 ff.) und beschränke mich daher auf die wesentlichen Punkte, die in bisherigen Verhandlungen geklärt werden konnten, und auf die aus meiner Sicht noch unzureichenden Regelungen. Der Deutsche Bundestag hatte die Bundesregierung mit dem Beschluß zu meinem Fünften Tätigkeitsbericht vom 20. September 1984 um Vorlage eines Gesetzentwurfs zur Regelung des ZEVIS ersucht (BT-Drucksache 10/1719, Nr. I.11).

7.1.1 Datenerhebung

Grundsätzlich bestehen aus meiner Sicht keine Bedenken gegen den Umfang der Daten, die vom Bürger im Rahmen der Kfz-Zulassung erhoben werden. Außerdem halte ich es für zweckgerecht, daß die Halterdaten in Form eines Katalogs im Gesetz abschließend festgelegt werden, während der Umfang der Fahrzeugdaten im Gesetz nur inhaltlich umschrieben und die Festlegung der Daten im einzelnen einer Rechtsverordnung vorbehalten werden soll.

Meine Bedenken gegen die Erhebung der Berufs- und Gewerbeangaben für Maßnahmen nach dem Bundesleistungsgesetz und dem Verkehrssicherstellungsgesetz wurden allerdings bisher nicht ausgeräumt. Zwar ist es eine Verbesserung, wenn im zentralen Fahrzeugregister nur noch die Berufsangaben der Selbständigen registriert werden; die Notwendigkeit der Speicherung von Berufs- und Gewerbeangaben aller Kfz.-Halter (auch der Nichtselbständigen) im örtlichen Fahrzeugregister vermag ich aber nicht zu erkennen. Meiner Meinung nach würde es durchaus genügen, nach bestimmten Berufs- und Gewerbeangaben nur zu fragen, wenn in diesen Fällen Fahrzeuge für Zwecke der zivilen Verteidigung nicht in Anspruch genommen werden sollen. Ich werde die Angelegenheit erneut mit dem Bundesminister für Verkehr erörtern.

7.1.2 Datennutzung

Grundsätzlich dürfen die Daten, die vom Bürger faktisch unter Zwang erhoben werden (ohne Daten keine Zulassung), nur zu dem Zweck genutzt werden, zu dem sie erhoben wurden (Grundsatz der Zweckbindung). Hiervon kann eine gesetzliche Regelung abweichen, wenn eine anderweitige Nutzung im überwiegenden Allgemeininteresse erforderlich ist. Um jedoch die jeweiligen Verwendungszwecke auf ihre Vereinbarkeit mit dem ursprünglichen Erhebungszweck prüfen zu können, muß dieser präzise definiert werden. Diese Definition muß auf der inhaltlichen Ebene ansetzen, d. h. den Verwendungszweck inhaltlich benennen und begrenzen. Für bedenklich hielte ich es, die Erteilung von Auskünften zu inhaltlich nicht näher bestimmten Zwecken bereits zum Speicherungszweck zu erklären und dadurch die Prüfung der Vereinbarkeit der Zwecke zu unterlaufen.

Hierzu habe ich im einzelnen Vorschläge unterbreitet.

7.1.3 Kontrolle der Datennutzung

Die Rechtmäßigkeit der Übermittlung von personenbezogenen Daten muß im Rahmen der Datenschutzkontrolle überprüfbar sein. Das heißt, daß im nachhinein feststellbar sein muß, welche Angaben an wen übermittelt wurden und welches die rechtfertigenden Gründe hierfür waren. Dies gilt unabhängig vom Verfahren der Übermittlung.

Soweit zu diesem Zweck besondere Aufzeichnungen gefertigt werden müssen, ist zu beachten, daß dadurch zusätzliche Informationssammlungen mit personenbezogenen Daten entstehen, die ihrerseits unter dem Gesichtspunkt des Datenschutzes bedenklich sein können.

Eine Lösung muß beiden Aspekten Rechnung tragen und versuchen, das Gesamtrisiko zu minimieren z. B. dadurch, daß die Aufzeichnungen nicht allen interessierten Stellen zur Verfügung stehen. Weiterhin kann eine relativ kurz bemessene Löschungsfrist festgelegt werden. Schließlich kann an die Stelle der Aufzeichnung aller Übermittlungsvorgänge eine flexibel zu handhabende Auswahlprotokollierung treten.

Diesen Überlegungen wird der Gesetzentwurf noch nicht voll gerecht. Auch hierzu habe ich Vorschläge unterbreitet.

In diesem Zusammenhang ist darauf hinzuweisen, daß auch die praktischen Voraussetzungen für eine wirksame externe Kontrolle geschaffen werden müssen. Bisher waren Kontrollmaßnahmen in diesem Bereich wegen der unzureichenden Personalausstattung des BfD nicht möglich. Die Kontrollkapazität muß dem technischen Ausbau angepaßt werden. Dies wurde jahrelang versäumt. Das Gleichgewicht von Datenverarbeitung und Datenschutz muß wiederhergestellt werden.

7.1.4 Abruf im automatisierten Verfahren

Grundsätzlich ist zu unterscheiden zwischen der materiell-rechtlichen Zulässigkeit der Übermittlung (was wann an wen?) und der Wahl der Übermittlungs*verfahren* (wie?). Dieser Unterschied sollte in der Gesetzesfassung deutlicher hervortreten. Die Zulässigkeit der Übermittlung hat sich an den Grundsätzen der Erforderlichkeit und der Vereinbarkeit der Zwecke, die Wahl des Übermittlungsverfahrens dagegen an der Angemessenheit auszurichten.

Bei der Frage, in welchen Fällen die Online-Nutzung eines Registers zugelassen wird, hat der Gesetzgeber daher einen gewissen Entscheidungsspielraum. Einer unkontrollierten Ausdehnung läßt sich allerdings nur entgegentreten, indem man die Voraussetzungen der Online-Nutzung klar abgrenzt und für eine effektive Kontrolle sorgt.

Ich werte es als einen Erfolg meiner Beratungstätigkeit, daß — entgegen früheren Vorstellungen — beispielsweise

- Erhebungszwecke und Übermittlungszwecke klar voneinander getrennt sind,
- die Speicherung von Suchvermerken und Steckbriefnachrichten ausgeschlossen ist und
- ein umfangreicher Datenabgleich nicht mehr stattfinden soll.

Bei der weiteren Beratung des Gesetzentwurfs sollte erhöhte Aufmerksamkeit auch auf die Lesbarkeit und die Verständlichkeit der Vorschriften gerichtet werden.

Bei einem Kontrollbesuch beim KBA habe ich mich über den Ausbaustand von ZEVIS unterrichtet. Die interne Erweiterung von ZEVIS ist inzwischen abgeschlossen. Damit steht für interne Zwecke des KBA der Gesamtbestand der Fahrzeug- und Halterdaten zur Verfügung. Durch ein Filterprogramm wird sichergestellt, daß externe ZEVIS-Anfragen nur in dem bisherigen Umfang möglich sind.

7.2 Führerschein auf Probe

Mit dem von der Bundesregierung eingebrachten Gesetzentwurf zur Änderung des Straßenverkehrsgesetzes und des Fahrlehrergesetzes soll u. a. der „Führerschein auf Probe" eingeführt werden. Als Probezeit sollen die ersten zwei Jahre nach Erwerb der Fahrerlaubnis gelten; die Dauer der Probezeit wird auf dem Führerschein vermerkt.

Durch die Einführung des Führerscheins auf Probe soll der Unfallhäufigkeit von Fahranfängern begegnet werden.

Die Fahranfänger, die Straftaten im Zusammenhang mit der Teilnahme am Straßenverkehr oder Verkehrsordnungswidrigkeiten begangen haben, die zur Eintragung in das Verkehrszentralregister (VZR) in Flensburg führen, sollen nach einem festgelegten Verfahren

— an Nachschulungskursen teilnehmen,

— sich einer medizinisch-psychologischen Untersuchung unterziehen bzw.

— die Fahrprüfung erneut ablegen.

Zur Feststellung, ob eine Fahrerlaubnis auf Probe vorliegt, sollen sämtliche Fahranfänger mit ihren identifizierenden Daten und ihren Führerscheindaten in einer zentralen Datei beim KBA gespeichert werden, und zwar während des Laufs der Probezeit und für ein weiteres Jahr als Überliegefrist (durchschnittliche Verfahrensdauer bei Einlegung von Rechtsmitteln). Der Umfang der Datei wird auf ca. 3 Mio. Fahranfänger geschätzt. Eine weitergehende Nutzung dieser Daten ist nur für wissenschaftliche Zwecke, für Statistiken und zur Vorbereitung von Rechts- und allgemeinen Verwaltungsvorschriften, und zwar grundsätzlich nur in anonymisierter Form zulässig. Ausnahmen von diesem Anonymisierungsgebot sind unter Beachtung von Datenschutz-Sicherungen möglich.

Die Meldung über begangene Straftaten und Verkehrsordnungswidrigkeiten laufen von sämtlichen Gerichten und Ordnungswidrigkeitsbehörden beim Kraftfahrt-Bundesamt zum VZR zusammen. Der Einstellung dieser Mitteilungen in das VZR soll nach dem vorliegenden Gesetzentwurf zunächst die Prüfung vorausgehen, ob der Betreffende die gemeldete Straftat oder Ordnungswidrigkeit während der Probezeit begangen hat. Bejahendenfalls führt dies zu einer Mitteilung an die zuständige Fahrerlaubnisbehörde, die wiederum die entsprechenden Maßnahmen nach dem genannten Gesetz einzuleiten hat.

In Verhandlungen mit dem Bundesminister für Verkehr habe ich mich u. a. dafür eingesetzt, daß der Führerschein auf Probe befristet eingeführt wird, damit zunächst Erkenntnisse über die Eignung des Gesetzes zur Erreichung des verfolgten Ziels gewonnen werden können (wissenschaftliche Begleituntersuchung). Erst danach kann der Gesetzgeber m. E. endgültig beurteilen, ob die Errichtung einer zentralen Datei aller Fahranfänger verhältnismäßig und erforderlich ist. Diesem Vorschlag ist die Bundesregierung gefolgt.

Alternativen zu der vorgesehenen Regelung wie

— Erfassung nur derjenigen Fahranfänger in einer gesonderten Datei, die Straftaten oder Verkehrsordnungswidrigkeiten begangen haben,

— Einführung dezentraler Dateien,

— Einführung eines zeitlich befristeten vorläufigen Führerscheins,

sind erörtert worden. Ich habe mich davon überzeugt, daß diese Maßnahmen die Gesamtheit der Führerscheininhaber stärker belasten würde und aus der Sicht des Datenschutzes ungünstiger als das vorgesehene Verfahren zu beurteilen wären.

7.3 Video-Überwachung von Einrichtungen der Deutschen Bundesbahn (DB)

In mehreren Eingaben wurde die Befürchtung geäußert, daß die Video-Überwachung auf Bahnhöfen der Beobachtung bestimmter Personengruppen diene und in diesem Zusammenhang auch Aufzeichnungen erfolgten.

Ich messe der Problematik der Video-Überwachung in bezug auf das Grundrecht auf freie Entfaltung der Persönlichkeit große Bedeutung bei, insbesondere wenn die Aufnahmen heimlich, d. h. ohne Wissen der Betroffenen, gemacht oder dauerhaft aufgezeichnet werden.

Bei meinen Überprüfungen solcher Vorgänge auf einigen Bahnhöfen haben sich diese Befürchtungen jedoch nicht bestätigt. Es haben sich keine Anhaltspunkte für eine unsachgemäße oder datenschutzrechtlich bedenkliche Datenverarbeitung ergeben. Ich habe mir allerdings noch kein vollständiges Bild über den Umfang der Video-Nutzung machen können.

Die Video-Überwachung durch die Deutsche Bundesbahn dient nach den bisherigen Erkenntnissen

— der Eigensicherung der Bahnpolizei (Zugangsbereich zum Bereitschaftsraum),

— der Bekämpfung von Diebstahl und Sachbeschädigung von Einrichtungen der DB (u. a. Schließfächer, Aufzüge, Abstellplätze für Stückgut),

— der Sicherung von Schalterräumen der Deutschen Verkehrs-Kredit-Bank (DVKB), die zum Service-Bereich der Deutschen Bundesbank gehört,

— der Verhinderung von Belästigungen und Überfällen auf die Kunden der DB, vor allem in schwer einsehbaren Bereichen der Empfangsgebäude sowie

— der zentralen Zugabfertigung im Bereich der Hamburger S-Bahn.

Abgesehen von der zentralen Zugabfertigung erfolgt die Videoüberwachung durch feststehende oder schwenkbare Kameras, deren Bilder auf Monitore in die Räume der Bahnpolizeiwache übertragen und dort beobachtet werden; sie ersetzt bzw. ergänzt insoweit die Streifentätigkeit der Bahnpolizei. Da keine Aufzeichnungen erfolgen, sind auch keine späteren Auswertungen möglich.

Pressemitteilungen über die Fahndung der schleswig-holsteinischen Polizei mit Hilfe von Video-Aufnahmen aus dem Bereich der Hamburger S-Bahn veranlaßten mich, eine Prüfung des Verfahrens bei der Bundesbahndirektion Hamburg durchzuführen. Dabei habe ich folgendes festgestellt:

— Video-Aufnahmen mit Aufzeichnung werden von der Deutschen Bundesbahn ausschließlich im Bereich der Hamburger S-Bahn vorgenommen. Sie erfolgen dort im Rahmen der zentralen Zugabfertigung und dienen der Beweissicherung. Deren Notwendigkeit ergibt sich daraus, daß der für die ordnungsgemäße Abfertigung und gefahrlose Abfahrt des Zuges verantwortliche Aufsichtsbeamte sich nicht auf dem Bahnsteig befindet, sondern bei einer zentralen Kontrollstelle, der sog. zentralen Zugabfertigung, von wo aus er das Geschehen über Video-Kameras beobachtet.

— Die Kameras sind für die Fahrgäste sichtbar installiert, nicht beweglich und machen keine Nah-Aufnahmen. Die Aufnahmepraxis wird nicht geheimgehalten.

— Aufzeichnungen der aufgenommenen Bilder erfolgen nicht permanent, sondern jeweils automatisch gesteuert von der Abfahrt des Zuges bis zur Ausfahrt aus dem Bahnhof für etwa zehn Sekunden. Der Aufsichtsbeamte kann außerdem eine Aufzeichnung individuell auslösen, um Zwischenfälle oder besondere Ereignisse festzuhalten.

— Dieses Verfahren zeigt, daß sich die Bahn nicht für das Verhalten der Fahrgäste, sondern für die einwandfreie Zugabfertigung und die Sicherheit auf den Bahnsteigen interessiert. Nur wenige Fahrgäste kommen so ins Bild, daß sie identifiziert werden können.

— Die Aufnahmen stehen unter Verschluß und werden nur für wenige Tage aufbewahrt. Sie dienen in Absprache mit dem Personalrat ausschließlich zur Aufklärung von Unregelmäßigkeiten bei der Abfertigung eines Zuges oder von Zwischenfällen auf den Bahnsteigen.

— Bei Schadensersatzansprüchen oder Beschwerden von Fahrgästen, z. B. wegen zu frühen Abfahrens oder sonstiger Fehler bei der Zugabfertigung, haben sich die Video-Aufzeichnungen als Beweismittel bewährt. Während früher oft Aussage gegen Aussage stand, werden heute die meisten Fälle in gutem Einvernehmen mit den Fahrgästen abgewickelt.

— Der zuständige Personalrat legt großen Wert auf die Beibehaltung des Video-Verfahrens, weil sich die Mitarbeiter nur dadurch gegen ungerechtfertigte Beschuldigungen verteidigen können. Daß mitunter auch Fehler von Mitarbeitern durch das Videoband nachgewiesen werden, wird in Kauf genommen.

— An Strafverfolgungsorgane werden Bänder nur ausgegeben, wenn dies nach der Strafprozeßordnung geboten ist. Dies kommt nur in seltenen Fällen in Betracht.

Zusammenfassend ist festzustellen, daß das System der Sicherheit des Bahnbetriebs und der leichteren Beilegung von Konflikten zwischen Fahrgast, Bahn und Mitarbeitern dient. Belästigungen und Risiken für die Fahrgäste sind praktisch ausgeschlossen. Von einer unzumutbaren Überwachung der Fahrgäste kann nicht gesprochen werden.

Ich weise allerdings darauf hin, daß das deutsche Datenschutzrecht noch keine Regelungen darüber enthält, unter welchen Voraussetzungen und für welche Zwecke staatliche und private Stellen Video-Aufnahmen machen dürfen, auf denen einzelne Personen erkennbar sind. Fortschritte in der Technik der automatischen Bildverarbeitung und der Mustererkennung können u. a. dazu führen, daß solche Aufnahmen durch Computer — ähnlich wie gespeicherte personenbezogene Daten — ausgewertet werden können. Ich bin daher der Auffassung, daß der gesetzliche Datenschutz künftig auch auf stehende und bewegliche Bilder ausgedehnt werden muß, um der Gefahr einer übermäßigen Video-Überwachung entgegentreten zu können.

8. Bundesarchivgesetz

In einer öffentlichen Anhörung vor dem Innenausschuß des Deutschen Bundestages wurde vor allem die Frage erörtert, ob das Gesetz in besonderen Fällen vorschreiben soll, daß bestimmte Unterlagen vor der Übergabe an das Bundesarchiv anonymisiert werden müssen. Von Historikern wurde unter anderem der Vorwurf erhoben, Anonymisierung in diesem Zusammenhang bedeute Urkundenfälschung. Bei diesen Vorwürfen wird meines Erachtens verkannt, daß das Anonymisierungsgebot nur solche Unterlagen betreffen soll, die das Archiv nach geltendem Recht nicht erhält und die auch in anderen Ländern regelmäßig nicht in die Archive gelangen. Betroffen sind nur solche Unterlagen, die die Ursprungsbehörde nach anderen Rechtsvorschriften vernichten kann oder muß, oder die sie auch dem Archiv gegenüber geheimzuhalten hat. Solche Geheimhaltungspflichten dienen vor allem der Erhaltung wichtiger Vertrauensverhältnisse; so kann z. B. der Arzt seinen Patienten nur dann helfen, wenn diese sich ihm dank der ärztlichen Schweigepflicht rückhaltslos anvertrauen können

und nicht befürchten müssen, daß ihre Angaben Dritten zur Kenntnis gelangen. Die Übergabe von Unterlagen mit solchen besonders geschützten Daten ist deshalb nicht möglich. Allerdings können gerade auch derartige Daten für die historische Forschung von großer Bedeutung sein. Die Anonymisierung ist der Ausweg, der die Daten zugänglich macht. Richtig besehen handelt es sich also nicht um eine Restriktion für die Forschung, sondern im Gegenteil um eine Erweiterung ihrer bisherigen Möglichkeiten.

9. Statistik

9.1. Volkszählungsgesetz und Mikrozensusgesetz

Beide Gesetze sind im Berichtsjahr verabschiedet worden und in Kraft getreten. Sie erfüllen die Anforderungen, die das Bundesverfassungsgericht in seinem Volkszählungsurteil an statistische Erhebungen gestellt hat.

Der Mikrozensus wurde im Sommer dieses Jahres durchgeführt. Besorgnisse betroffener Bürger sind in diesem Zusammenhang kaum an mich herangetragen worden. Ich sehe darin einen ersten Erfolg der intensiven Bemühungen des Deutschen Bundestages, der Bundesregierung und meiner Behörde um einen überzeugenden Datenschutz im Bereich der amtlichen Statistik.

Nachdem die von der Bundesregierung vorgelegten Gesetzentwürfe für ein Mikrozensusgesetz und ein Volkszählungsgesetz bereits weitgehend datenschutzgerechte Regelungen enthielten, hat der Innenausschuß des Deutschen Bundestages beide Entwürfe in öffentlichen Anhörungen erörtert und weitere Verbesserungen vorgenommen. Beim Mikrozensus hatte der Innenausschuß vor allem die Frage zu prüfen, ob eine gesetzliche Verpflichtung der Betroffenen zur Auskunft wirklich unentbehrlich ist. Dagegen spricht, daß Antwortausfälle bei einer Repräsentativstatistik das Ergebnis nicht notwendigerweise beeinträchtigen; bei freiwilligen Angaben sind überdies weniger unzutreffende Angaben zu erwarten. Die Befragung der Sachverständigen hat jedoch ergeben, daß nach heutigem Erfahrungsstand im Falle freigestellter Antworten eine wesentliche Ergebnisverzerrung nicht auszuschließen sei, insbesondere weil mehr Verweigerer zu erwarten seien und diese sich nicht gleichmäßig auf die gesellschaftlichen Gruppen verteilen würden. Die Aussagen der Sachverständigen waren im einzelnen allerdings weder einheitlich noch sonderlich präzise. Der Gesetzgeber hat deshalb die Bundesregierung verpflichtet, Alternativen zum Auskunftszwang empirisch zu erproben. Auf meine Empfehlung wurde ein wissenschaftlicher Beirat vorgesehen, der die Untersuchungen der Statistischen Ämter begleitet.

Für die Volkszählung 1987 hat das neue Volkszählungsgesetz das Erhebungsverfahren wesentlich verbessert. Es stellt z. B. strenge Anforderungen an die Zählerauswahl und schreibt zwingend die räumliche, organisatorische und personelle Trennung der kommunalen Erhebungsstellen von anderen Verwaltungsstellen vor. Der Gesetzgeber hat ferner sowohl im Volkszählungsgesetz wie auch im Mikrozensusgesetz Vorsorge für den Schutz des Betroffenen bei der Nutzung der statistischen Angaben getroffen. Das bedeutet allerdings nicht, daß die Statistischen Ämter nur anonymisierte Daten erhalten dürfen. Bei offenkundig widersprüchlichen Angaben muß der Personenbezug vielmehr herstellbar sein, um klärende Rückfragen zu ermöglichen. Bei der Volkszählung wird der Personenbezug außerdem für den Fall benötigt, daß die auf der Grundlage dieser Erhebung festgestellte amtliche Bevölkerungszahl in ihrer Richtigkeit bestritten wird. Zum Schutz des Betroffenen schreiben Mikrozensusgesetz und Volkszählungsgesetz aber die frühzeitige Trennung der Hilfsangaben von den Erhebungsmerkmalen und anschließend die baldige Löschung der Hilfsmerkmale vor. Auf diese Weise wird eine unbefugte Kenntnisnahme der personenbezogenen Angaben erschwert. Die beiden Gesetze enthalten außerdem eindeutige Geheimhaltungspflichten und Zweckentfremdungsverbote für alle Beteiligten und stellen die unbefugte Herstellung des Personenbezuges für nicht vollständig anonymisierte Daten unter Strafe.

Im Volkszählungsgesetz hat es der Gesetzgeber nach eingehender Prüfung zugelassen, daß die Angaben der Betroffenen zwar ohne Hilfsmerkmale, aber in nicht vollständig anonymisierter Form auch den statistischen Ämtern von Gemeinden für eigene Statistiken zugänglich gemacht werden, allerdings nur unter zusätzlichen Bedingungen und Auflagen, die einen gleichwertigen Schutz der Belange der Betroffenen sicherstellen.

9.2 Handels- und Gaststättenzählung

Die meisten statistischen Rechtsvorschriften wurden noch nicht an die Anforderungen des vor über zwei Jahren verkündeten Volkszählungsurteils angepaßt. Das gilt auch für das Handelsstatistikgesetz, auf dessen Grundlage im Frühjahr 1985 die Handels- und Gaststättenzählung durchgeführt wurde.

Die Statistischen Ämter haben die Anforderungen des Urteils auch im Verwaltungswege nicht vollständig erfüllt. Das Volkszählungsurteil verlangt vom Gesetzgeber, durch detaillierte Vorschriften dafür zu sorgen, daß die Hilfsmerkmale, die der Identifizierung des Betroffenen dienen, möglichst frühzeitig gelöscht werden. Eine solche Regelung gibt es für die im Rahmen der Handels- und Gaststättenzählung von den Finanzbehörden nach § 6 Abs. 2 Handelsstatistikgesetz gelieferten Merkmale „Name, Anschrift und Gewerbekennziffer" (Kennzeichnung des Wirtschaftszweiges) nicht. Diese Merkmale werden nach einer Vereinbarung der Statistischen Ämter vom Dezember 1984 auch nicht kurzfristig gelöscht, sondern in eine Adreßdatei eingestellt, damit sie später für andere Statistiken genutzt werden können.

Für die langfristige Speicherung und umfassende Verwendung der Hilfsmerkmale könnte sprechen, daß die Statistischen Ämter dadurch in den Stand gesetzt werden, die Auskunftspflichtigen für Repräsentativstatistiken aus einer größeren Grundgesamtheit auszuwählen und die Auskunftspflichtigen häufiger auszutauschen. Auf diese Weise würde dem Gleichbehandlungsgrundsatz besser Rechnung getragen. Die langfristige Speicherung von Hilfsmerkmalen und ihre Verwendung für eine Vielzahl von Statistiken steht andererseits aber im Widerspruch zu dem Gebot ihrer kurzfristigen Löschung. Die Datenschutzbeauftragten des Bundes und der Länder haben darauf hingewiesen, daß die für die Handels- und Gaststättenzählung geführte Adreßdatei einer gesetzlichen Regelung bedarf und daß die Daten bis dahin jedenfalls nicht für andere statistische Erhebungen genutzt werden dürfen. Der Entwurf des Bundesstatistikgesetzes sieht jetzt eine allgemeine Vorschrift über Adreßdateien vor (vgl. dazu unten Nr. 9.4).

Zur Zeit prüfe ich, ob Finanzbehörden im Zusammenhang mit der Handels- und Gaststättenzählung gegen das Steuergeheimnis oder andere Geheimhaltungsvorschriften verstoßen haben und ob der Bundesminister der Finanzen oder andere Stellen des Bundes daran beteiligt waren. Den Finanzbehörden ist nämlich in der Presse vorgeworfen worden, sie hätten zusätzlich zu den in § 6 Abs. 2 Handelsstatistikgesetz vorgesehenen Angaben auch die Steuernummer der betroffenen Unternehmen an die Statistischen Landesämter übermittelt und damit Geheimhaltungsvorschriften verletzt.

9.3 Hochschulstatistikgesetz

Nach wie vor ist umstritten, ob die Studentenstatistik bei einer Neufassung des Hochschulstatistikgesetzes als Verlaufsstatistik geführt und mit der Prüfungskandidatenstatistik verknüpft werden soll. In meinem Siebenten Tätigkeitsbericht (S. 39) habe ich dargestellt, daß eine Verlaufsstatistik stärker in die Rechte der Betroffenen eingreift als eine periodische Bestandsstatistik, weil bei einer Verlaufsstatistik die zeitliche Entwicklung jedes betroffenen Individuums aufgezeichnet wird und deshalb die sonst übliche frühzeitige Anonymisierung der Daten nicht stattfindet. Ich habe daraus den Schluß gezogen, daß die Durchführung als Verlaufsstatistik besonders begründet werden muß, etwa mit der besonderen Qualität und Bedeutung ihrer Ergebnisse für politische Entscheidungen.

Der Bundesminister für Bildung und Wissenschaft hat sich vor diesem Hintergrund dazu entschlossen, einen Entwurf für eine Neufassung des Hochschulstatistikgesetzes vorzulegen, welcher darauf verzichtet, die Studentenstatistik als Verlaufsstatistik durchzuführen und sie mit der Prüfungskandidatenstatistik zu verknüpfen. Ich sehe darin eine Bestätigung meiner Zweifel, ob eine Verlaufsstatistik, so wie sie ursprünglich geplant war (es sollten alle Studenten an allen Hochschulen für die gesamte Dauer ihres Studiums in ihrer Entwicklung erfaßt werden), erforderlich ist und ob sie zeitnah wertvolle Ergebnisse liefern könnte.

9.4 Bundesstatistikgesetz

Zu dem Entwurf des Bundesministers des Innern für die Neufassung des Bundesstatistikgesetzes konnte ich trotz der Kürze der eingeräumten Frist eine erste Stellungnahme abgeben. Auf folgende von mir aufgezeigte Mängel, die auch in der überarbeiteten Fassung der Kabinettvorlage vom 19. Dezember 1985 noch enthalten sind, möchte ich besonders hinweisen:

- Die Ermächtigung zum Erlaß von Verordnungen mit Auskunftspflicht ist m. E. nicht hinreichend bestimmt. So darf der Gesetzgeber dem Verordnungsgeber z. B. nicht die Entscheidung überlassen, ob ein Auskunftszwang für beliebige Wirtschaftsstatistiken sachgerecht ist, wenn nur Unternehmen befragt werden und ein bestimmter Kostenrahmen nicht überschritten wird.
- Der Gesetzentwurf sieht vor, daß bei Statistiken, die bereits in Einzelstatistikgesetzen geregelt sind, die Verpflichtung bestehen soll, die *von den Ämtern* festgelegten Hilfsmerkmale anzugeben, und zwar unabhängig davon, ob sie in den Einzelstatistikgesetzen vorgesehen sind. Hilfsmerkmale, die vom Bürger erhoben werden, sind aber im einzelnen vom Gesetzgeber festzulegen.
- Die Funktionsbegrenzung für Hilfsmerkmale bleibt unklar; der Gesetzgeber sollte abschließend festlegen, wofür Hilfsmerkmale genutzt werden dürfen und wofür nicht.
- Das Statistikgeheimnis darf nicht auf Einzelangaben begrenzt werden, es muß sich vielmehr auch auf zusammengefaßte Angaben erstrecken, soweit diese noch auf einzelne Personen beziehbar sind.
- Der Gesetzentwurf entspricht an einigen Stellen nicht dem Gebot der Normenklarheit.

Außerdem müssen noch offene Fragen im Zusammenhang mit den in § 13 des Gesetzentwurfs vorgesehenen Adressdateien geklärt werden. Die Vorschrift erlaubt es, Hilfsmerkmale zusammen mit einigen Erhebungsmerkmalen langfristig zu speichern. Das bedeutet, daß die Hilfsmerkmale nicht, wie vom Bundesverfassungsgericht bei der Volkszählung gefordert, von den Erhebungsmerkmalen getrennt und dann kurzfristig gelöscht werden. Vielmehr bleibt der unmittelbare Personenbezug für die in den Adressdateien gespeicherten Angaben erhalten. Darin liegt eine stärkere Einschränkung des Rechts auf informationelle Selbstbestimmung. Sie ist nur zulässig, wenn die Adressdateien in dem vorgesehenen Umfang im überwiegenden Allgemeininteresse notwendig sind. Daß dies der Fall ist, müßte noch im einzelnen dargelegt werden. Außerdem sollte der Gefahr einer Deanonymisierung der sonstigen Erhebungsmerkmale durch entsprechende gesetzliche Schutzvorkehrungen entgegengewirkt werden.

In § 16 des Gesetzentwurfes, der das Statistikgeheimnis und seine Ausnahmen regelt, muß klargestellt werden, daß alle bisherigen Vorschriften der

Einzelstatistikgesetze, die die Übermittlung von Einzelangaben an oberste Bundes- oder Landesbehörden gestatten, obsolet sind. Das Statistische Bundesamt hat den Vollzug dieser Vorschriften zu Recht ausgesetzt, weil die strikte Trennung von Statistik und Verwaltungsvollzug, die das Bundesverfassungsgericht fordert, zumindest ohne ergänzende Schutzvorschriften nicht gewährleistet erscheint.

10. Sozialwesen

10.1 Bundeserziehungsgeldgesetz

Im Februar des Berichtsjahres hat mir der Bundesminister für Jugend, Familie und Gesundheit den Referentenentwurf eines Bundeserziehungsgeldgesetzes zugeleitet. Ich habe die vorgesehenen Vorschriften unter Datenschutzgesichtspunkten geprüft und noch im gleichen Monat einige klarstellende bzw. ergänzende Regelungen vorgeschlagen und um weitere Unterrichtung gebeten.

Leider ist dieser Bitte nicht entsprochen worden, so daß ich erst dem Plenarprotokoll des Deutschen Bundestages die Einbringung des Gesetzentwurfes entnehmen und mir anschließend den Entwurf (BT-Drucksache 10/3792) beschaffen konnte.

In einem Punkt wurde meiner Anregung gefolgt und § 12 um einen Absatz 3 ergänzt, wonach die nach dem Bundeskindergeldgesetz erhobenen (Einkommens)Daten auch für die Berechnung des einkommensabhängigen Erziehungsgeldes verwendet werden dürfen. Diese Regelung war nach meiner Auffassung im Hinblick auf die vom Bundesverfassungsgericht geforderte strikte Zweckbindung der Daten erforderlich, um die zu erwartende Verwaltungspraxis rechtlich abzusichern. Ich hatte allerdings vorgeschlagen, die *gegenseitige* Verwendung der erhobenen Daten ausdrücklich zu erlauben. Im Gegensatz zu der in der Begründung der Bundesregierung zu § 12 Abs. 3 getroffenen Feststellung ist dies jedoch nach meiner Auffassung durch die vorliegende Fassung nicht abgedeckt, so daß auch künftig für die Zwecke des Erziehungsgeldes erhobenen Einkommensdaten nicht ohne weiteres für Zwecke der Kindergeldgewährung verwendet werden dürfen; insofern ist jeweils eine Einwilligung des Betroffenen erforderlich.

Einer weiteren, nach den Erfahrungen beim Kindergeld (vgl. 6. TB S. 31, 7. TB S. 43) mir wichtig erscheinende Anregung wurde leider nicht gefolgt: Es sollte klargestellt werden, inwieweit der Antragsteller und sein Ehegatte beim Nachweis der nach § 6 Abs. 1 maßgeblichen Summe der positiven Einkünfte auch Angaben über die einzelnen Einkunftsarten zu machen haben.

10.2 Hinterbliebenenrenten- und Erziehungszeiten-Gesetz (HEZG)

An der Konzeption des Gesetzes war ich bereits in der Vorbereitungsphase beteiligt worden, soweit datenschutzrechtliche Bezüge erkennbar waren (Einkommensermittlung, Auskunftspflichten, Geburtsmeldungen). Nach zwischenzeitlichen Beteiligungsdefiziten wurden im Laufe des Gesetzgebungsverfahrens die mir wichtig erscheinenden Klarstellungen und Ergänzungen im Gesetz berücksichtigt. Einzelheiten zu Geburtsmeldungen durch die Meldebehörden sowie zu Inhalt, Form und Frist der Auskunftspflichten der Versicherten und über die Feststellung der Kindererziehungszeiten einschließlich der Speicherung, Verarbeitung und Löschung der Daten sollen durch Rechtsverordnungen geregelt werden, an deren Erarbeitung ich beteiligt bin bzw. werde.

In der 2. Meldedaten-Übermittlungs-Verordnung des Bundes (2. BMeldDÜV) wird nunmehr bestimmt, daß die Meldebehörden zur Durchführung der Versicherung nach dem HEZG unverzüglich nach Bekanntwerden der Geburt eines Kindes der Datenstelle des Verbandes der Rentenversicherungsträger Daten der Mutter zu übermitteln haben. Diese sogenannte Geburtsmitteilung umfaßt den jetzigen und früheren Namen, die Vornamen, den Geburtstag und -ort und die Anschrift der Mutter und lediglich den Monat und das Jahr der Geburt des Kindes. Diese gesetzlich vorgeschriebene Datenübermittlung ist notwendig, da nach dem HEZG mit der Geburt eines Kindes von der Mutter grundsätzlich ein Anspruch auf Rente erworben wird. Sie kann in Einzelfällen (minderjährige Mutter, ledige Mutter, Freigabe des Kindes innerhalb des ersten Lebensjahres zur Adoption) zu Problemen führen, wenn die Frauen in späteren Lebenssituationen ihre Mutterschaft nicht offenbart wissen wollen. Hier müssen mit den Versicherungsträgern Lösungen angestrebt werden, die den schutzwürdigen Belangen der Mütter gerecht werden.

Auch zu den Auskunftspflichten der wegen Kindererziehung Versicherten soll in einer Rechtsverordnung Näheres über das Verfahren der Speicherung, Verarbeitung und Löschung der Daten der Versicherten geregelt werden. Hierzu liegt mir jedoch noch kein Entwurf vor.

Der BMA hat zugesagt, mich an der Vorbereitung dieser Vorschriften und an den Vereinbarungen mit den Versicherungsträgern zu beteiligen.

10.3 Sozialversicherungsnummer

In meinem Siebenten Tätigkeitsbericht (S. 40) habe ich — unter Bezugnahme auf den Bericht des Innenausschusses zu meinem Fünften Tätigkeitsbericht (BT-Drucksache 10/1719, S. 16, zu II 14) ausgeführt, daß über die Konzeption des Bundesministers für Arbeit und Sozialordnung zur Einführung einer allgemeinen Versichertennummer (Sozialversicherungsnummer) ein erstes Gespräch stattgefunden hat. In diesem Jahr wurden die Erörterungen fortgesetzt. Der BMA hat in einem „Vorentwurf eines Gesetzes zur Beschränkung der Verwendung von Versicherungsnummern" seine Vorstellungen präzisiert und die beabsichtigten Regelungen for-

muliert. Nach diesem Entwurf soll die Verwendung der Rentenversicherungsnummer als einheitliche Versicherungsnummer im Bereich der Sozialversicherung einschließlich der Arbeitslosenversicherung prinzipiell zulässig sein, wenn dies zur personenbezogenen Zuordnung der Daten im Rahmen der Erfüllung einer gesetzlichen Aufgabe erforderlich ist. Die Verwendung durch andere Sozialleistungsträger und darüber hinaus durch sonstige Personen und Stellen soll abgestuften Zulässigkeitsvoraussetzungen unterliegen, die insbesondere auf die Erforderlichkeit für die Erfüllung bestimmter Aufgaben abstellen. Ich habe dazu noch einige Änderungen zur Klarstellung und Verdeutlichung vorgeschlagen. So ist es z.B. nach meiner Auffassung erforderlich, für den Bereich außerhalb der Sozialversicherung ausdrücklich auszuschließen, daß mit der Rentenversicherungsnummer Dateien erschlossen werden. In diesem Bereich darf die Rentenversicherungsnummer lediglich verwendet werden, um im Kontakt mit den Sozialversicherungsträgern bei zulässigen Datenübermittlungen den Betroffenen eindeutig zu bestimmen und ihm in dem notwendigen Umfang die Daten zuzuordnen.

Ich gehe davon aus, daß bei der weiteren Vorbereitung des Gesetzentwurfs meine Überlegungen berücksichtigt werden und letztlich eine sachgerechte Regelung zur Verwendung der Rentenversicherungsnummer zustandekommt.

10.4 Arbeitsverwaltung

Wiederholt habe ich auf Schwierigkeiten hingewiesen, die im Arbeitslosenhilfeverfahren dadurch entstehen, daß Einkommensnachweise von Unterhaltspflichtigen an das Arbeitsamt über den Arbeitslosen vorgelegt werden müssen und der Arbeitslosenhilfebescheid nicht nur den Unterhaltsanrechnungsbetrag, sondern die gesamte Berechnung einschließlich des Einkommens des Unterhaltspflichtigen und seiner Sonderausgaben enthält. (5. TB S. 58, 6. TB S. 31, 7. TB S. 42 f). Meinen Vorstellungen hält die Bundesanstalt für Arbeit nach wie vor Praktikabilitäts- und Rechtsgründe entgegen, wobei sie sich hinsichtlich der Vorlage der Einkommensnachweise bereiterklärt hat, im Rahmen eines Modellversuches in fünf Arbeitsämtern die unmittelbare Vorlage durch den Unterhaltspflichtigen zuzulassen. Abgesehen von der Tatsache, daß eine solche — an sich von mir gewünschte — Verfahrensänderung dann ins Leere geht, wenn der Arbeitslosenhilfebescheid anschließend die Einkommensverhältnisse offenlegt, habe ich als Nebenerkenntnis aus zahlreichen Einzeleingaben den Eindruck gewonnen, daß das von mir vorgeschlagene Verfahren inzwischen bei einer großen Zahl von Arbeitsämtern bereits üblich ist. Ich neige daher zu der Ansicht, daß es des Modellversuches gar nicht mehr bedarf, da er von der Praxis überholt worden ist, z.Z. also nur noch um Prinzipien gestritten wird. Die Reaktion der Bundesanstalt auf meine diesbezüglichen Hinweise halte ich allerdings für unbefriedigend. So wurde meine Mitteilung, im Bereich des Landesarbeitsamtes Berlin werde so verfahren, wie ich es für wünschenswert halte, nicht zum Anlaß genommen, die geltenden Regelungen nochmals zu überdenken. Vielmehr hat die Bundesanstalt das Landesarbeitsamt umgehend angewiesen, das Verfahren in ihrem Sinne zu ändern.

Weicht im vorgenannten Fall die Praxis zugunsten der Betroffenen teilweise von den geltenden Weisungen ab, so geschieht dies in einem anderen Bereich zu deren Nachteil, nämlich bei der Arbeitsvermittlung. Es besteht dort die Weisung, jeden geplanten Vermittlungsvorschlag zunächst mit den Arbeitsuchenden zu besprechen. Damit ist ausgeschlossen, daß die Bewerbungsunterlagen ohne Wissen des Betroffenen an potentielle Arbeitgeber verschickt werden. Mehrere Eingaben haben aber gezeigt, daß sich nicht alle Arbeitsämter daran halten. In einigen Fällen wurde Petenten sogar ausdrücklich erklärt, die Unterlagen würden auch ohne Wissen und Zustimmung des Arbeitsuchenden versandt. Die Bundesanstalt beabsichtigt, alle Arbeitsämter auf die Rechtslage hinzuweisen. Bis Redaktionsschluß für diesen Bericht war noch nicht entschieden, ob ein solcher Hinweis in das Merkblatt für den Arbeitsuchenden aufgenommen oder Inhalt eines Runderlasses werden soll. Neben dem Erlaß eines Rundschreibens würde ich aus Transparenzgründen eine Ergänzung des Merkblattes begrüßen.

Zu Unzuträglichkeiten hat auch die Durchführung des von mir in meinem Siebenten Tätigkeitsbericht (S. 43) kurz dargestellten Verfahrens des automatisierten Datenabgleichs mit den Finanzbehörden für die Kindergeldberechnung geführt. Obwohl Einigkeit darüber erzielt werden konnte, daß die Kindergeldberechtigten nur mit ihrer ausdrücklichen Einwilligung an diesem Verfahren teilnehmen, habe ich aufgrund einer großen Zahl von Eingaben festgestellt, daß viele Betroffene sogar gegen ihren erklärten Willen in den Datenabgleich einbezogen worden sind. Eine umfangreiche Untersuchung durch die Bundesanstalt für Arbeit hat meine Erkenntnisse im wesentlichen bestätigt.

Die Bundesanstalt führte die fehlerhafte Bearbeitung vor allem auf Arbeitsüberlastung des Personals bei Einführung des Verfahrens zurück. Nach meiner Auffassung lag der Grund jedoch überwiegend in einem organisatorischen Mangel. Der von den Bearbeitern auszufüllende Erfassungsbogen enthielt nämlich keinen Hinweis auf den Zustimmungsvorbehalt. Es bestand nur die Weisung, die Steuernummer dann nicht einzutragen, wenn die Zustimmung zum Datenabgleichverfahren fehlte, da ohne Steuernummer die Einbeziehung in das Verfahren nicht möglich ist.

Obwohl die Bundesanstalt einen Organisationsmangel bestritt und zunächst einen besonderen Hinweis auf die Zustimmungserklärung im Erhebungsbogen für überflüssig hielt, hat sie sich inzwischen bereiterklärt, den Bogen um ein Datenfeld, in dem nach der Zustimmung gefragt wird, zu erweitern. Desweiteren hat sie die Arbeitsämter angewiesen, alle bereits in den Datenabgleich einbezogenen Fälle darauf zu überprüfen, ob die Zustimmung der

Betroffenen vorliegt. Aus diesem Grunde habe ich von einer förmlichen Beanstandung abgesehen.

Im Berichtszeitraum hat die Bundesanstalt für Arbeit weitere Regelungen zur Erstellung und Behandlung ärztlicher und psychologischer Gutachten erlassen.

Ich würde es begrüßen, wenn diese Materie in einem zusammenfassenden Runderlaß dargestellt werden könnte. Zur Zeit gelten meines Wissens dazu sechs Runderlasse aus den Jahren 1981 bis 1985 sowie die Aktenordnung, in denen jeweils Teilbereiche der Thematik behandelt werden. Dies führt nach meiner Einschätzung zu großer Unübersichtlichkeit und erhöht damit das Fehlerrisiko. Inhaltlich begrüße ich die Tendenz der neuen Regelungen, halte aber in mehreren Punkten eine Ergänzung bzw. Präzisierung für erforderlich. Darüber bin ich mit der Bundesanstalt weiter im Gespräch.

10.5 Krankenversicherung

In der gesetzlichen Krankenversicherung bereiten die Vorschriften über den Anspruch auf Familienkrankenhilfe nach wie vor in der Praxis erhebliche datenschutzrechtliche Probleme (vgl. 6. TB S. 30/31).

Nach § 205 RVO erhalten der Ehegatte und die Kinder eines Versicherten Leistungen aus dessen Krankenversicherung, wenn bestimmte Voraussetzungen vorliegen. Zur Feststellung, ob die Versicherten Angehörige haben, die entweder der Krankenkasse bisher nicht bekannt sind oder bei denen sich die tatsächlichen Verhältnisse bezüglich der Anspruchsvoraussetzungen geändert haben, verschicken die Krankenkassen im großen Umfang Fragebogen an ihre Mitglieder. In diese Fragebogen sollen alle Angehörigen eingetragen und Angaben zu deren persönlichen und sachlichen Verhältnissen gemacht werden, die sich auf die gesetzlichen Anspruchsvoraussetzungen beziehen.

Die Kritik vieler Betroffener richtet sich dagegen, daß mit dem Fragebogen häufig Angaben erhoben und gespeichert würden, die zur Prüfung und Feststellung der Anspruchsberechtigung von Angehörigen nicht erforderlich seien. Diese Kritik ist berechtigt.

Die Fragebogen sind in der Regel so gestaltet, daß alle Fragen zu beantworten sind; auf die Notwendigkeit der vollständigen Beantwortung aller Fragen wird besonders hingewiesen. Diese Notwendigkeit ist jedoch keineswegs in allen Fällen gegeben. Die einzelnen Voraussetzungen müssen nämlich kumulativ vorliegen, so daß beim Fehlen nur einer Voraussetzung kein Anspruch auf Familienkrankenhilfe besteht. Die weiteren Voraussetzungen sind dann nicht zu prüfen; weitere Angaben des Betroffenen sind folglich nicht erforderlich. Angaben, die zur rechtmäßigen Erfüllung der Aufgaben nicht erforderlich sind, dürfen aber nicht gespeichert (9 Abs. 1 BDSG) und deshalb auch nicht erhoben werden.

Durch die auf dem Fragebogen als Rechtsgrundlage der Datenerhebung angegebene Vorschrift des § 60 SGB I wird dem Betroffenen die Angabe von Tatsachen auch nur insoweit auferlegt, als sie für die beantragte oder gewährte Leistung erheblich sind. Der Betroffene kann jedoch mangels der notwendigen Fachkenntnisse nicht beurteilen und entscheiden, welche Angaben im Einzelfall erheblich sind, zumal er besonders angewiesen wird, alle Fragen zu beantworten.

Eine Krankenkasse hat eingeräumt, daß nicht alle Fragen in jedem Fall zur Feststellung der Anspruchsberechtigung notwendig seien. Es sei jedoch zu bedenken, daß es äußerst schwierig sei, in einem Fragebogen, der sich an eine Vielzahl von Personen richte, alle denkbaren Möglichkeiten einzubeziehen, ohne u. U. auch im Einzelfall nicht notwendige Fragen aufzunehmen. Ebenso schwierig sei es, die Erläuterungen, ohne sie gänzlich unverständlich zu machen, so ausführlich zu gestalten, daß jeder Laie bei der Vielgestaltung der Fallmöglichkeiten in jedem Fall erkennen könne, welche Frage im Einzelfall nicht relevant sei. Einfacher sei es für die Betroffenen sicher, im Zweifelsfall eine Frage mehr zu beantworten.

Diese Auffassung kann ich nicht akzeptieren. Es ist nicht Aufgabe des Betroffenen, die Erforderlichkeit der verlangten Angaben zu beurteilen, sondern Aufgabe der fragenden Krankenkasse. Verwaltungsmäßige Schwierigkeiten der Darstellung können nicht Grundlage für eine Erhebung nicht erforderlicher Daten sein, zumal diese Schwierigkeiten nach meiner Überzeugung nicht unüberwindbar sind. Bei einer sachgerechten Gestaltung des Vordrucks und einer sinnvollen Reihenfolge der Fragen, die in aller Regel mit Ja/Nein beantwortet werden können, kann nach jeder Frage aus der entsprechenden Antwort die Entscheidung vorgegeben werden, ob die Beantwortung der nächsten Frage erforderlich ist oder nicht.

Im übrigen zwingt das geltende Recht dazu, zunächst für erforderlich gehaltene oder in Unkenntnis der Rechtslage gemachte aber nicht erforderliche Angaben nicht zu speichern bzw. bereits gespeicherte Angaben zu löschen (§ 84 SGB X). Dies gilt nicht nur für einzelne Angaben über Angehörige, sondern für die Speicherung von Daten des Angehörigen überhaupt. Hat die Prüfung ergeben, daß ein Angehöriger keinen Anspruch auf Familienkrankenhilfe hat, dann dürfen Daten dieses Angehörigen nicht gespeichert werden.

Ein weiteres Problem der Familienkrankenhilfe ist auch in diesem Jahr wiederholt aufgetreten, nämlich daß Kassenmitglieder von ihrer Krankenkasse über Krankheiten und Therapiemaßnahmen eines Angehörigen unterrichtet wurden. So haben sich volljährige, studierende „Kinder", die längst einen selbständigen Haushalt führten, mit Recht dagegen gewandt, daß die von ihnen im Rahmen der Familienkrankenhilfe der jeweiligen Krankenkasse zur Genehmigung vorgelegten Anträge auf psychotherapeutische Behandlung mit der ärztlichen Verordnung und Begründung dem Vater als Kassenmitglied „zur Unterschrift" vorgelegt wurden. Die Ge-

nehmigung und Kostenübernahmeerklärung wurde anschließend ebenfalls dem Vater übersandt.

Nach § 35 SGB I hat jeder Anspruch darauf, daß Einzelangaben über seine persönlichen und sachlichen Verhältnisse von den Leistungsträgern als Sozialgeheimnis gewahrt und nicht unbefugt offenbart werden. Das gilt selbstverständlich auch in dem Verhältnis von Angehörigen untereinander. In den genannten Fällen war die Offenbarung der Krankheit und der Behandlungsbedürftigkeit des Angehörigen an den Vater nicht notwendig und daher auch nicht zulässig.

Diese rechtliche Beurteilung wird zwar vom Bundesminister für Arbeit und Sozialordnung und, soweit ersichtlich, von den Spitzenverbänden der Träger der gesetzlichen Krankenversicherung geteilt. Eine Rechtsänderung ist nach Mitteilung des Bundesministers für Arbeit und Sozialordnung gleichwohl nicht erforderlich, weil sich solche Kollisionen mit dem Datenschutz aus dem geltenden Recht heraus lösen ließen (vgl. auch Stellungnahme der Bundesregierung zum 6. TB zu 10.3). Demgegenüber zeigen jedoch die von Betroffenen immer wieder vorgetragenen Fallbeispiele, daß jedenfalls in der Praxis solche Kollisionen nicht selten auftreten. Ganz ohne Zweifel liegt dies in dem gegenwärtigen System der Familienkrankenhilfe begründet. Eine generelle Lösung kann m. E. nur dadurch erfolgen, daß dem Angehörigen ein eigenständiger Anspruch auf Krankenhilfe zugestanden wird, wie ich dies bereits in meinem 6. TB angeregt habe. Der Bundesminister für Arbeit und Sozialordnung hat mir dazu mitgeteilt, daß bei der für die nächste Legislaturperiode in Aussicht genommenen Kodifizierung des Rechts der gesetzlichen Krankenversicherung geprüft werde, ob und unter welchen Voraussetzungen dem Familienangehörigen ein eigenes Antragsrecht eingeräumt werden soll. Ich halte derartige Regelungen aus datenschutzrechtlichen Gründen für dringend geboten.

10.6 Gesundheitswesen

10.6.1 Ärztliche Entlassungsberichte

Nach dem Abschluß von medizinischen Rehabilitationsmaßnahmen (Kuren) durch die Träger der Rentenversicherung bzw. in deren Auftrag wird von dem behandelnden Arzt der Kureinrichtung ein detaillierter sog. Kurentlassungsbericht gefertigt. Durchschriften dieses umfangreichen Entlassungsberichts werden meist routinemäßig an den Rentenversicherungsträger und/oder an dessen ärztlichen Untersuchungsdienst bzw. Sozialmedizinischen Dienst, an den behandelnden Hausarzt sowie an die Krankenkasse des Patienten übersandt. Die Problematik dieser „Streuung" ärztlicher Entlassungsberichte war mehrfach Gegenstand von Eingaben, Anfragen und Stellungnahmen wie auch einer örtlichen Kontrolle bei einer Kurklinik. Die datenschutzrechtliche Beurteilung führt allgemein und bezogen auf die einzelnen Empfänger der Berichte zu folgenden Ergebnissen:

Der Entlassungsbericht unterliegt in seiner Gesamtheit der ärztlichen Schweigepflicht. Gegenüber dem Rentenversicherungträger hat der Patient darüber hinaus einen Anspruch darauf, daß Angaben über seine persönlichen und sachlichen Verhältnisse als Sozialgeheimnis gewahrt und nicht unbefugt offenbart werden (§ 35 SGB I). Dieser Anspruch besteht gegen den Rentenversicherungsträger in seiner Gesamtheit, also auch gegen Kureinrichtungen, die der Versicherungsträger als eigene Einrichtung selbst unterhält. Gegen Fremdeinrichtungen, die vom Versicherungsträger mit der Durchführung von Kurmaßnahmen beauftragt werden (sog. Belegkliniken), besteht dieser Anspruch nach dem Wortlaut des Gesetzes nicht. Das würde bedeuten, daß der Patient in einer Belegklinik bei im übrigen gleicher Situation einen minderen Datenschutz genießen würde, und daß es für die Anwendung des Sozialdatenschutzrechts darauf ankäme, ob die Belegklinik von ihr selbst erhobene oder ihr vom Versicherungsträger übermittelte Daten weitergibt (§ 78 SGB X) und ob die Belegklinik Daten direkt oder über den Versicherungsträger an Dritte übermittelt.

Eine derartige Differenzierung wäre nicht sachgerecht und dogmatisch auch nicht zwingend. Die Beziehungen zwischen dem Rentenversicherungsträger und den Belegkliniken sind als Auftragsverhältnis nach § 97 SGB X i. V. m. § 1236 RVO, § 13 AVG, § 35 RKG zu definieren. Den Belegkliniken und den dort tätigen Ärzten kommt keine selbständige Funktion innerhalb eines Sozialleistungsverhältnisses zu. Sie werden vielmehr quasi als Erfüllungsgehilfen für den Rentenversicherungsträger tätig. Die Übersendung von Entlassungsberichten an Dritte ist in die Auftragstätigkeit mit einzubeziehen. Diese Auffassung vertritt auch das Bundesversicherungsamt. Daraus folgt, daß der Patient in Belegkliniken den gleichen sozialrechtlichen Datenschutz genießt wie in eigenen Kureinrichtungen des Versicherungsträgers. In diese Richtung weist auch § 97 SGB X. Danach muß bei einer Aufgabenwahrnehmung durch Dritte sichergestellt sein, daß der Dritte die Gewähr für eine die Rechte und Interessen des Betroffenen wahrende Erfüllung der Aufgaben bietet.

Die Zulässigkeit der Übersendung von Kurentlassungsberichten ist deshalb stets nach dem Recht des Sozialdatenschutzes zu beurteilen und aufgrund des § 76 Abs. 1 SGB X auch nach den Regeln der ärztlichen Schweigepflicht. Nur in bestimmten Fällen ist dieses „Zwei-Schranken-Prinzip" kraft ausdrücklicher gesetzlicher Regelung aufgehoben. Nach § 76 Abs. 2 SGB X ist ungeachtet der ärztlichen Schweigepflicht die Offenbarung solcher Daten zulässig, die von einem Arzt im Zusammenhang mit einer Begutachtung wegen der (künftigen) Erbringung von Sozialleistungen oder wegen der Ausstellung einer Bescheinigung zugänglich gemacht worden sind, soweit dies zur Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch erforderlich ist; der Betroffene kann der Offenbarung jedoch widersprechen.

Die Zulässigkeit der Übersendung des Kurentlassungsberichts an die verschiedenen genannten Stellen ist danach wie folgt zu beurteilen:

— *Rentenversicherungsträger*

Der Kurarzt wird bei der Behandlung des Kurpatienten im Rahmen medizinischer Rehabilitationsmaßnahmen im Auftrag des Rentenversicherungsträgers tätig. Im Rahmen dieses Auftrags ist er zur Offenbarung von Patientengeheimnissen gegenüber dem Auftraggeber befugt, wenn dem Patienten bekannt oder bewußt ist, daß die von dem Arzt getroffenen Feststellungen zur Mitteilung an den Träger der Maßnahme bestimmt sind. Davon kann bei der Bewilligung einer Kur auf Veranlassung und Kosten des Rentenversicherungsträgers grundsätzlich ausgegangen werden.

Materielle Grundlage des Behandlungsauftrages sind die Vorschriften des § 1236 RVO/§ 13 AVG/§ 35 RKG. Nach Abs. 1 Satz 5 dieser Vorschriften bestimmt der Rentenversicherungsträger im Einzelfall Art, Umfang und Durchführung der Leistungen zur Rehabilitation sowie die Rehabilitationseinrichtung unter Beachtung der Grundsätze der Wirtschaftlichkeit und Sparsamkeit nach pflichtgemäßem Ermessen. Dazu gehören auch eine Erfolgskontrolle und auf der Grundlage des Behandlungsverlaufs und des Behandlungsergebnisses zu treffende Entscheidungen über etwa notwendige Folgemaßnahmen. Zu diesem Zweck ist die Übersendung des Entlassungsberichts an den Rentenversicherungsträger als Auftraggeber zulässig. Zweifelhaft erscheint allenfalls die Notwendigkeit bestimmter, üblicherweise in dem Bericht enthaltener Angaben z. B. über Laborbefunde, Vorerkrankungen, Familienanamnese. Der ärztliche Entlassungsbericht sollte daher insgesamt auf den notwendigen Umfang hin überprüft und gegebenenfalls reduziert werden.

— *Ärztlicher Untersuchungsdienst/Sozialmedizinischer Dienst*

Soweit diese Dienste in die Organisation des Rentenversicherungsträgers eingebunden und ihnen die vorgenannten Aufgaben des Rentenversicherungsträgers zugewiesen sind, ist gegen die Übersendung des Entlassungsberichts an sie — statt an eine andere Organisationseinheit des Rentenversicherungsträgers — nichts einzuwenden. Soweit jedoch eine parallele Übersendung einer weiteren Durchschrift des Berichts an diese Dienste erfolgt, obwohl sie mit diesen Aufgaben nicht betraut sind, steht dem die ärztliche Schweigepflicht entgegen. Denn Ärzte (oder ärztliche Dienststellen) sind auch untereinander von der Schweigepflicht nur befreit, wenn sie gleichzeitig oder nacheinander denselben Patienten untersuchen oder behandeln und soweit das Einverständnis des Patienten anzunehmen ist. Die Übersendung setzt also voraus, daß der Ärztliche Untersuchungsdienst/Sozialmedizinische Dienst des Rentenversicherungsträgers den Patienten nach Abschluß der Kur tatsächlich untersucht oder behandelt. Eine routinemäßige Übersendung aller Entlassungsberichte ist somit nicht zulässig. Es kommt allenfalls eine spätere Übersendung durch den Rentenversicherungsträger nach Prüfung der Erforderlichkeit im Einzelfall in Betracht, wenn eine Untersuchung des Patienten tatsächlich vorgenommen werden soll.

— *Behandelnder Hausarzt*

Unter dem Gesichtspunkt der ärztlichen Schweigepflicht gilt hier das gleiche wie für den Ärztlichen Untersuchungsdienst/Sozialmedizinischen Dienst als untersuchende oder behandelnde Stelle. Die Erforderlichkeit der Offenbarung von Sozialdaten an den Hausarzt für die Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch ist jedoch in keinem Fall anzunehmen. Dies ergibt sich auch aus § 101 SGB X. Danach haben die Leistungsträger (nur) *auf Verlangen* eines behandelnden Arztes Untersuchungsbefunde, die für die Behandlung von Bedeutung sein können, mitzuteilen, sofern der Betroffene im Einzelfall in die Übermittlung eingewilligt hat. Die Übersendung des Kurentlassungsberichts an den (behandelnden) Hausarzt setzt deshalb stets das Einverständnis des Patienten im Einzelfall voraus. Dabei ist jedoch zu beachten, daß eine rechtswirksame Einwilligung die Kenntnis dessen voraussetzt, was offenbart werden soll. Eine von vornherein — bei Kurantritt — regelmäßig abverlangte Einwilligung ohne Kenntnis vom Inhalt des Entlassungsberichts kann dem nicht genügen.

— *Krankenkasse*

Die Zulässigkeit der Übersendung der (vollständigen) Kurentlassungsberichte an die jeweilige Krankenkasse des Patienten steht nicht nur unter dem Vorbehalt der Erforderlichkeit für die Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch (§ 69 Abs. 1 Nr. 1 SGB X), sondern auch unter dem Vorbehalt der befugten Offenbarung von Patientengeheimnissen (§ 76 Abs. 1 SGB X).

Die Aufgaben nach dem Sozialgesetzbuch in diesem Bereich können offenbar nicht ausreichend konkret definiert werden. Nach allen Erfahrungen bestehen hier sehr große Meinungsunterschiede. Ungeachtet dessen ist aber jedenfalls eine allgemeine Befugnis zur Offenbarung von Patientengeheimnissen unter Durchbrechung der ärztlichen Schweigepflicht nicht gegeben. Die Übersendung der vollständigen Kurentlassungsberichte an die Krankenkasse bedarf deshalb in jedem Einzelfall der Einwilligung des Patienten. Hinsichtlich des routinemäßigen Verlangens der Einwilligung gilt dasselbe wie beim Hausarzt (siehe oben).

Wegen der insoweit ungeklärten Aufgaben, die die Krankenkassen in diesem Zusammenhang geltend machen, kann die für notwendig gehaltene Unterrichtung der Krankenkassen auch weiterhin dadurch aufrecht erhalten werden, daß die regelmäßige Übersendung von Entlassungsberichten auf die Teile beschränkt wird, deren Inhalt die Krankenkassen für ihre etwaige Entscheidung über gegebenenfalls sich anschließende weitere Leistungen tatsächlich benötigen, mit Ausnahme also der besonders sensitiven Angaben, die der Patient während der

Rehabilitationsmaßnahme dem Arzt im Vertrauen auf dessen Schweigepflicht gemacht hat. Die Zulässigkeit dieser eingeschränkten Offenbarung könnte nach § 69 Abs. 1 Nr. 1 i. V. m. § 76 Abs. 2 SGB X beurteilt werden; insoweit steht dem die ärztliche Schweigepflicht nicht entgegen.

Auf dieser Grundlage hat die Bundesversicherungsanstalt für Angestellte mit dem Verband der Angestelltenkrankenkassen vereinbart, daß künftig nur noch das erste Blatt des Kurentlassungsberichts nach ausdrücklichem Hinweis des Patienten auf sein Widerspruchsrecht an die Krankenkasse übersandt wird. Dies ist auch nach meiner Auffassung ein geeigneter Weg, sowohl dem Informationsbedürfnis der Krankenkasse als auch den schutzwürdigen Interessen des Patienten Rechnung zu tragen.

10.6.2 Perinatologische Erhebungen

In mehreren Bundesländern führen die Ärztekammern in Verbindung mit den kassenärztlichen Vereinigungen perinatologische Erhebungen bei zahlreichen Krankenhäusern durch. In meinem Zuständigkeitsbereich sind daran acht Knappschaftskrankenhäuser in Nordrhein-Westfalen, Bayern und im Saarland beteiligt.

Im Rahmen dieser Erhebungen wird vom Krankenhaus für jeden Geburtsfall ein sog. Basis-Erhebungsbogen ausgefüllt. Dieser Basiserhebungsbogen enthält ca. 100 Einzelangaben über den sozialen Status der Mutter, vorausgegangene Schwangerschaften, Geburten, Aborte und Abbrüche, den Verlauf der Schwangerschaft und der Entbindung sowie über die Umstände der Geburt und den Gesundheitszustand des Kindes. Das Vorhaben dient der perinatologischen Forschung mit dem Ziel der Qualitätssicherung der gesundheitlichen Versorgung von Mutter und Kind und, soweit nötig und möglich, der Entwicklung gezielter Verbesserungsmaßnahmen.

Die Eintragung der Daten auf dem Erhebungsbogen erfolgt personenbezogen, d. h. mit Namen und Anschrift des Patienten. Eine Durchschrift des Erhebungsbogens — jedoch ohne Name und Anschrift — erhält die zuständige Ärztekammer, die die Angaben in einem automatisierten Verfahren erfaßt und auswertet. Eine ausreichende Anonymisierung ist dadurch nicht gegeben, da der übermittelte Erfassungsbogen weitere Identifizierungsdaten enthält, aus denen die Person der Betroffenen bestimmbar bleibt.

Die Erhebung, Weiterleitung, Erfassung und (statistische) Auswertung erfolgt in der Regel ohne Kenntnis und Einwilligung der Betroffenen. Die naheliegende Forderung, das Vorhaben nur mit Einwilligung der Betroffenen durchzuführen, wirft jedoch nach Meinung der Forscher Probleme auf (unzureichende Response-Quote und damit Beeinträchtigung der wissenschaftlichen Aussagen, Inhalt und Umfang der Einwilligung, besondere Notsituation der Patientin), auf die hier nicht näher eingegangen werden soll. Es ist vielmehr eine Lösung zu finden, die dem wissenschaftlichen Interesse und den schutzwürdigen Belangen der Betroffenen gleichermaßen gerecht wird. Dazu hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einem gemeinsamen Beschluß vom 10. Mai 1985 ein entsprechendes Verfahren empfohlen. Der Beschluß ist als Anlage 1 abgedruckt.

Mit diesem Beschluß hat sich am 8./9. Oktober 1985 die Konferenz der für das Gesundheitswesen zuständigen Minister und Senatoren der Länder befaßt. Sie hat in einer Entschließung das Ergebnis der Abstimmung mit den Datenschutzbeauftragten über die Modalitäten der Datenerhebung begrüßt und festgestellt, daß dies einen vertretbaren Kompromiß zwischen den Erfordernissen des Persönlichkeitsschutzes der Betroffenen und den Anforderungen einer fundierten wissenschaftlichen Untersuchung darstellt. Unterschiedliche Auffassungen bestehen allerdings hinsichtlich der Erhebung einzelner Daten. Darüber werden gegebenenfalls weitere Erörterungen stattfinden müssen.

10.6.3 Dialyse-Patienten-Fragebogen

Mitte des Jahres ist mir bekanntgeworden, daß zahlreiche Krankenhäuser in der Bundesrepublik (rd. 80, sowie weitere ca. 1 500 Krankenhäuser in 30 überwiegend europäischen Ländern) detaillierte Erhebungen über Diagnose, Krankheitsursache, Behandlungsmethode und Behandlungsverlauf bei Dialyse-Patienten sowie über vorgenommene Nierentransplantationen durchführen. Die standardisierten Angaben werden in einen einheitlichen Erhebungsbogen eingetragen, der mit Namen und Geburtsdatum des Patienten an die European Dialysis and Transplant Association (EDTA) in London zur wissenschaftlichen Auswertung übermittelt wird. Die Erfassung und Übermittlung dieser hochsensiblen Daten erfolgt — soweit bekannt — ohne Kenntnis und Einwilligung der betroffenen Patienten. Dafür ist weder eine gesetzliche Grundlage vorhanden, noch besteht eine Offenbarungsbefugnis, die eine Durchbrechung der ärztlichen Schweigepflicht rechtfertigt. Nach § 2 Abs. 7 der ärztlichen Berufsordnung dürfen der Schweigepflicht unterliegende Tatsachen und Befunde zum Zwecke der wissenschaftlichen Forschung nur dann an Dritte mitgeteilt werden, wenn dabei die Anonymität des Patienten gesichert ist oder dieser der Mitteilung ausdrücklich zustimmt. Eine danach unbefugte Offenbarung kann nach Maßgabe des § 203 StGB einen Straftatbestand darstellen. Daneben liegt gegebenenfalls eine Verletzung des Sozialgeheimnisses (§ 35 SGB I) vor.

Dieser Zusammenhang wurde anscheinend von den beteiligten Krankenhausärzten nicht gesehen. Die Initiativen der Datenschutzbeauftragten des Bundes und der Länder, die — jeweils in ihrem Bereich — die Beteiligten auf die Problematik hingewiesen haben, führten bereits zu entsprechenden Reaktionen. Von einer Klinik wurde mitgeteilt, daß die Übermittlung der Daten an die EDTA bis zur endgültigen Klärung eingestellt worden sei. Außerdem sollte die Angelegenheit als ein Hauptthema auf der Jahrestagung der Gesellschaft für klinische Ne-

phrologie im September 1985 behandelt werden; Ergebnisse liegen mir noch nicht vor. Darüber hinaus wurde der Vorschlag gemacht, gemeinsam mit den Datenschutzbeauftragten, mit den Vertretern der Patientenverbände und den Vertretern der Ärzteschaft eine für die weitere Erhebung der notwendigen Daten erforderliche, einvernehmliche Lösung zu erarbeiten, nach der dann jedes einzelne Dialysezentrum verfahren muß und dann auch sicher sein kann, daß alle geforderten gesetzlichen Bestimmungen berücksichtigt werden.

Ich begrüße diesen Vorschlag und werde mich gegebenenfalls an der Erarbeitung von Lösungen beteiligen.

11. Öffentliche Sicherheit-Allgemeines

11.1 Kontrollen und Ergebnisse

Neben der Bearbeitung der zunehmenden Zahl der Einzeleingaben fanden im Jahre 1985 verschiedene, z. T. sehr umfangreiche Querschnittskontrollen im Sicherheitsbereich statt. Ziel dieser Kontrollen war u. a.

- die Überprüfung der Einhaltung früherer Zusagen für Verbesserungsmaßnahmen;
- die Prüfung weiterer Maßnahmen der Datenverarbeitung (DV) bei diesen Behörden und/oder
- die Befassung mit neuen Strukturen der Datenverarbeitung, die eingeführt wurden oder werden sollen.

Als wichtigste Kontrollen sind folgende stichpunktartig hervorzuheben (zu Einzelfragen siehe unten Nr. 12 ff.).

11.1.1 Bundeskriminalamt (BKA)

Als Ergebnis meiner *Kontrolle der Datenverarbeitung im Zusammenhang mit der Bekämpfung der Rauschgiftkriminalität* habe ich vor allem Vorschläge zur Behebung von Strukturmängeln der Datenverarbeitung unterbreitet, die nicht nur den Rauschgiftbereich allein betreffen, sondern Strukturmängel genereller Art sind und zu einer Gefährdung schutzwürdiger Belange des Betroffenen führen. Hierbei handelt es sich u. a. darum, daß

- die Berücksichtigung justizieller Entscheidungen, die für die Zulässigkeit der Aufrechterhaltung von Speicherungen von Bedeutung sind, nicht gesichert ist,
- die Speicherung von Daten ohne ausreichende Belege für die Überprüfung ihrer Richtigkeit erfolgt (insbesondere bei personengebundenen Hinweisen);
- die automatische Vergabe von Löschungsfristen auf den Zeitpunkt der Eingabe in das DV-System anstatt auf das Ereignis abstellt, ohne daß eine in vielen Fällen erforderliche Korrektur durch den Sachbearbeiter erfolgt;
- bei nahezu allen kriminalpolizeilichen Hinweisen, die das BKA im Rahmen der Zusammenarbeit mit den Landespolizeibehörden erhält, auch eine schematische Speicherung von Unterlagen im Aktennachweis des BKA vorgenommen wird; dies hat zur Folge, daß hier ein umfangreicher zentraler Datenbestand entsteht entgegen der Beschränkung des Kriminalaktennachweises im INPOL-System auf Unterlagen von überregionaler Relevanz; darüber hinaus sind die Akten in der Regel unvollständig (näher hierzu unten zu Nr. 12.2);
- bei der Einstufung von Personen als „andere Personen" Fehler unterlaufen mit der Folge, daß dadurch die nach den Richtlinien vorgeschriebene kurze Überprüfungsfrist von einem Jahr nicht beachtet wird und gegebenenfalls die danach vorgesehene Benachrichtigung entfällt.

Der Bundesminister des Innern hat in seiner Stellungnahme zu verschiedenen Punkten Verbesserungsmaßnahmen, u. a. auch einen verstärkten Dienstkundeunterricht für das Personal zugesagt. Wichtige Probleme bleiben jedoch ungelöst, so das Verhältnis des Aktennachweises des BKA zu anderen Dateien des INPOL-Systems, die Problematik der Speicherung personengebundener Hinweise oder die Frage, ob und wie sichergestellt ist, daß die Regelungen der §§ 100 a und 100 b StPO nach Abschluß von Telefonüberwachungsmaßnahmen eingehalten werden. Ich habe den Bundesminister des Innern um eine ergänzende Stellungnahme gebeten. Im übrigen wird auf die Darstellung von Einzelfragen verwiesen (vgl. unten zu Nr. 12).

Die *Kontrolle des Interpolverkehrs* des BKA bezog sich vor allem auf die Auswirkungen der neuen Richtlinie von 1984, mit deren Hilfe mehr Datenschutz in diesem Bereich erreicht werden soll (vgl. 7. TB S. 71). Dies gilt insbesondere für

- die Pflicht zur Relevanzprüfung vor Übermittlung der Daten;
- die stärkere Beachtung des Grundsatzes der Verhältnismäßigkeit bei der Übermittlung;
- die Pflicht zum Nachbericht wichtiger Änderungen zu einer Information nach deren Übermittlung an den ausländischen Datenempfänger.

Die Prüfung ergab, daß bei diesen für den internationalen polizeilichen Informationsaustausch zentralen Fragen noch ein erheblicher Verbesserungsbedarf besteht.

Kritisiert habe ich darüber hinaus

- die automatische Vergabe von im konkreten Fall zu langen Löschungsfristen;
- die Aufrechterhaltung der zentralen Speicherung von Daten über Personen, die als vermißt zur Fahndung ausgeschrieben sind, auch noch nach Erledigung der Fahndung;
- das Fehlen geeigneter Vorkehrungen, durch die verhindert wird, daß Daten nach Tilgung im BZR entgegen dem Verbot des § 51 BZRG im Ausland noch verwertet werden.

Die Antwort des Bundesministers des Innern ging erst unmittelbar vor Drucklegung dieses Tätigkeitsberichts ein und konnte daher nicht mehr berücksichtigt werden.

11.1.2 Bundesgrenzschutz

Hier wurde die Datenverarbeitung der Fahndungsleitstelle der Grenzschutzdirektion im Zusammenhang mit dem im Aufbau befindlichen neuen Grenzaktennachweis (GAN) des Grenzschutzeinzeldienstes überprüft. Als Ergebnis wurden einige Verbesserungen festgestellt, die im Anschluß an frühere Kontrollen bereits zugesagt worden waren (vgl. 6. TB S. 48, 7. TB S. 71 f.). Die Prüfung hat aber wiederum bedenkliche Maßnahmen der Datenverarbeitung offengelegt. Dies gilt insbesondere

- für zahlreiche Verstöße gegen die Fristenregelung nach der Errichtungsanordnung für den GAN,
- für die Speicherung personenbezogener Daten in bestimmten Fällen ohne grenzpolizeilich relevanten Bezug, sei es daß dieser von Anfang an fehlte, sei es daß er (z. B. aufgrund von Nachberichterstattung) zwischenzeitlich entfallen war;
- für die durchweg fehlende Erkundigung über den weiteren Verlauf von Erkenntnissen, die Grundlage für Speicherungen bei der GSD waren;
- für die Behandlung von erledigten Fahndungsersuchen der Nachrichtendienste. Das gegenwärtige Verfahren, die Daten der von den Ersuchen betroffenen Personen noch ein Jahr nach Erledigung im GAN zu speichern, habe ich beanstandet, weil hierzu nicht nur der grenzpolizeiliche Bezug, sondern auch die erforderliche gesetzliche Aufgabenzuweisung fehlt. Für die Speicherung der Hinweise trotz Erledigung des Ersuchens ist im übrigen keine Notwendigkeit erkennbar.

Meinen Bedenken wurde in verschiedenen, darunter auch den drei ersten angesprochenen Punkten, entsprochen und weitere Verbesserungen zugesagt. Außerdem wurde eine Überarbeitung der Richtlinien und der Errichtungsanordnung für den GAN angekündigt.

Bei der Speicherung von Amtshilfeersuchen (4. Anstrich) sowie in mehreren anderen Fragen (so insbesondere zur Online-Zugriffsbefugnis der Grenzschutzstellen, vgl. hierzu schon 7. TB S. 72) bleibt der Bundesminister des Innern dagegen bei seiner bisherigen Auffassung. Seine Auseinandersetzung mit meinen Bedenken halte ich noch nicht für ausreichend und habe ihn deshalb um ergänzende Stellungnahme gebeten.

11.1.3 Bundesamt für Verfassungsschutz (BfV)

Hier wurde eine erneute *Kontrolle der Datenübermittlungen an ausländische Dienste* durchgeführt. Insgesamt konnte die anläßlich meiner Kontrolle von 1984 (vgl. 7. TB S. 76 f.) vorgenommene positive datenschutzrechtliche Bewertung des Auslandsauskunftsverkehrs aufrecht erhalten werden. Die jetzige Prüfung zeigte auch, daß das BfV begonnen hat, meine Anregungen in die Praxis umzusetzen, wie z. B.

- die Bitte um Konkretisierung des Anfragegrundes vor Auskunftserteilung;
- den Nachbericht bei späteren wesentlichen Änderungen der Bewertung der übermittelten Daten und
- die Verweisung an die für die Beantwortung einer Anfrage zuständige Stelle in der Bundesrepublik, anstatt selbst eine inhaltliche Auskunft zu erteilen.

Andererseits hat diese Prüfung auch gezeigt, daß die Datenverarbeitung gerade in diesem sensiblen Bereich noch der Verbesserung bedarf. Das betrifft u. a. die

- Nichtbeachtung vorrangiger gesetzlicher Zuständigkeiten für die Übermittlung an ausländische Dienststellen bei Auskünften aus staatsanwaltlichen oder polizeilichen Erkenntnissen (vgl. § 73 IRG, §§ 1 Abs. 2, 10 BKAG, § 57 BZRG),
- fehlende Präzisierung des Anfragegrundes, wenn das BfV bei inländischen Behörden um Auskunft zur Beantwortung von Anfragen ausländischer Dienste bittet.

Der Bundesminister des Innern hat zugesagt, meine Anregungen aufzugreifen und auch die notwendige Schulung der Mitarbeiter zu verstärken.

Im Dezember 1985 wurde mit einer Kontrolle der Datenverarbeitung der Abteilung V (Geheimschutz) des BfV begonnen. Im Zentrum der Prüfung stehen hier die Fragen der Erhebung und weiteren Verarbeitung von Daten für die Sicherheitsüberprüfung. Zu wichtigen Teilaspekten, zwischenzeitlich getroffenen Vereinbarungen und der aus meiner Sicht gebotenen Pflicht zur Transparenz des Verfahrens und Zweckbindung der Daten habe ich mehrfach meine Auffassung dargelegt (vgl. zuletzt 7. TB, S. 64 f. und 82 sowie unten Nr. 13.1.3).

Die Ergebnisse der Kontrolle werde ich im nächsten Tätigkeitsbericht behandeln.

11.1.4 Militärischer Abschirmdienst (MAD)

Verschiedene Aspekte der Datenverarbeitung wurden sowohl bei der Zentrale als auch bei Außenstellen des MAD geprüft. Als Schwerpunkt meiner Vorschläge sind die Empfehlungen zu nennen, die zum Ziel haben, daß sich der MAD bei seiner Tätigkeit auf die Belange der unmittelbaren militärischen Sicherheit beschränkt. Sowohl die vorgesehene Aufgabenumschreibung für den MAD im MAD-Gesetzentwurf als auch die beabsichtigte Änderung der Datenverarbeitung im Zusammenhang mit der personellen Vorbeugung belegen, daß der Bundesminister der Verteidigung bemüht ist, meinen seit Jahren vorgetragenen Anregungen Rechnung zu tragen (vgl. zuletzt 7. TB S. 81 und näher hierzu unten Nr. 13.2.1)

11.1.5 Bundesnachrichtendienst (BND)

Hier fanden zwei größere Kontrollen in der Zentrale statt; außerdem habe ich eine Außenstelle des BND kontrolliert. Im Ergebnis wurden vor allem Restriktionen für die Speicherung und Übermittlung personenbezogener Daten erreicht sowie die Löschung einer größeren Anzahl von Einzelfällen.

In folgenden Punkten konnte noch keine datenschutzrechtlich befriedigende Lösung erzielt werden:

— Bei der Speicherung von Daten über bestimmte Personen zu Zwecken der eigenen Sicherheit des BND. Zwar sind hier erhebliche Verbesserungen gegenüber der früheren Praxis zu verzeichnen (vgl. hierzu 7. TB S. 78). Doch ist der Kreis der betroffenen Personen m. E. noch unverhältnismäßig groß und zu sehr von formalistischen Erwägungen bestimmt.

— Bei der Speicherung von Daten über Personen, die der BND zur Mitarbeit anwerben möchte. Hier sind m. E. sowohl bei dem Kreis der betroffenen Personen als auch insbesondere bei der Dauer der Speicherung Änderungen notwendig.

Um bei diesen und anderen Fragen Klarheit zu gewinnen, wäre — neben gesetzlichen Regelungen für den BND — die von mir seit längerem geforderte detaillierte Aufstellung des von der Datenverarbeitung des BND erfaßten Personenkreises eine wichtige Hilfe für die Entscheidung über die Speicherung und über differenzierte Löschungs- und Übermittlungsregelungen (vgl. hierzu 7. TB S. 78).

Die Kontrolle der Einhaltung der Richtlinien über die Amtshilfe des BGS für den BND zur Gewinnung von Sachinformationen hat ergeben, daß die in den Richtlinien vorgeschriebene ausschließlich sachbezogene Auswertung der vom BGS übermittelten Erkenntnisse eingehalten wird (vgl. auch 5. TB. S. 97).

11.1.6 Zusammenfassende Würdigung

Es ist anzuerkennen, daß sich alle Sicherheitsbehörden des Bundes im Dialog mit meiner Behörde bemühen, die datenschutzrechtlichen Aspekte verstärkt zu berücksichtigen. Dabei sind als besonders erfreulich der stetige Abbau älterer Speicherungen und das erkennbare Bestreben zu erwähnen, bei der Neueinspeicherung personenbezogener Daten restriktiver als bisher zu verfahren. Als Beispiele hierfür sind zu nennen die Reduzierung der Speicherungen bei der Spezialdatei PIOS-Terrorismus des BKA um mehr als 50 % und im Bereich der Datenverarbeitung für die Staatsschutzkriminalität um fast 70 % des bisherigen Bestandes seit den von mir dort durchgeführten Kontrollen.

Auf der anderen Seite schreitet der Ausbau der Datenverarbeitung stetig voran. Die DV wird vielgestaltiger, komfortabler und umfassender; dementsprechend werden auch die Probleme des Datenschutzes schwieriger. Als Problembereiche seien beispielhaft angeführt.

— zunehmende Freitextverarbeitung,

— steigende Menge der zu einer einzelnen Person gespeicherten Daten wie z. B. personengebundener Hinweise,

— zunehmender Übergang von Aktenhinweissystemen zu umfangreichen Recherchiersystemen und

— die stetig fortschreitende Automatisierung der Bearbeitung administrativer und sicherheitsbehördlicher Vorgänge.

Diese technische Entwicklung hat sich schrittweise vom geltenden Recht entfernt (vgl. näher 7. TB S. 65 ff.). Die Datenschutzbeauftragten des Bundes und der Länder haben hierauf seit Jahren hingewiesen und eine kritische Bestandsaufnahme der Praxis der DV gefordert, um daraus Erkenntnisse für gesetzgeberische Maßnahmen zu gewinnen. Das Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983 hat diese Notwendigkeit verstärkt.

Die Probleme sollen nunmehr durch eine Reihe gesetzgeberischer Vorhaben gelöst werden. Aus datenschutzrechtlicher Sicht ist jedoch Skepsis angebracht, ob dies mit den mir bekannt gewordenen, nachstehend erörterten Entwürfen in vollem Umfang möglich ist.

11.2 Gesetzgebungsvorhaben und deren datenschutzrechtliche Bewertung

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat im Jahr 1985 unter meiner maßgeblichen Mitwirkung zwei grundsätzliche Beschlüsse gefaßt zu den Anforderungen an Datenschutzregelungen im Polizeirecht (Beschluß vom 24. Januar 1985, Anlage 2) und für den Verfassungsschutz (Beschluß vom 16. September 1985, Anlage 3).

Ohne schon hier auf Einzelheiten einzugehen, scheint mir vor allem folgendes wichtig zu sein:

In beiden Beschlüssen hat die Datenschutzkonferenz betont, daß es bei der Neuregelung des Polizei- und Verfassungsschutzrechts (ähnliches gilt für erforderliche Regelungen für den MAD und den BND) nicht darum gehen kann, nur die derzeitige Praxis gesetzlich festzuschreiben. Vielmehr muß der Umfang zulässiger Informationsverarbeitung der Sicherheitsbehörden auf der Grundlage des Volkszählungsgesetzurteils des Bundesverfassungsgerichts wie auch der von mir seit Jahren gemachten Vorschläge von Grund auf überprüft und durch spezielle Aufgaben- und Befugnisnormen konkretisiert und begrenzt werden.

Folgende Gesetzentwürfe der Bundesregierung, des Arbeitskreises II der Innneministerkonferenz bzw. der Koalitionsfraktionen, mit denen die Gesetzgebung für die Sicherheitsbehörden neu geordnet werden soll, wurden mir zur Stellungnahme zugeleitet:

— Änderung des Musterentwurfs eines einheitlichen Polizeigesetzes,

— Neufassung des Bundesverfassungsschutzgesetzes, dem gleichsam Pilotfunktion für die Neuregelung der Landesverfassungsschutzgesetze zukommen soll,

— MAD-Gesetz,

— Gesetz über die informationelle Zusammenarbeit der Sicherheits- und Strafverfolgungsbehörden des Bundes und der Länder in Angelegenheiten des Staats- und Verfassungsschutzes (ZAG).

Mit diesen Gesetzen soll u. a. den Bedenken entsprochen werden, die vor allem von den Datenschutzbeauftragten gegen die Entwürfe für die Neufassung des Personalausweis- und Paßgesetzes mit dem Ziel der Einführung eines maschinenlesbaren Personalausweises bzw. Passes geltend gemacht wurden (vgl. hierzu 6. TB S. 6 ff. und 7. TB S. 7 ff.).

Bei aller Anerkennung des Bemühens um bereichsspezifische präzise Regelungen, wie sie besonders für die Tätigkeit der Sicherheitsbehörden erforderlich sind, ist es m. E. mit den gegenwärtigen Entwürfen noch nicht gelungen, dem Gebot der Normenklarheit hinreichend Geltung zu verschaffen.

Außerdem ist generell zu kritisieren, daß die Gesetzentwürfe im Ergebnis darauf hinauslaufen, die gegenwärtige Praxis festzuschreiben und zum Teil sogar erheblich zu erweitern. Ich habe daher eine Reihe von Bedenken gegen die Entwürfe geltend gemacht.

Sie lassen sich zu den Entwürfen für die Polizeibehörden und Nachrichtendienste wie folgt zusammenfassen:

— Die *Aufgabenumschreibung* ist zu ungenau. Zu bemängeln ist etwa beim Musterentwurf für ein Polizeigesetz die beabsichtigte Ausdehnung auf den Bereich der bisher nicht definierten „Gefahrenvorsorge" und das Fehlen einer Definition des Begriffes der vorbeugenden Straftatbekämpfung. Beim Entwurf für die Novellierung des Bundesverfassungsschutzgesetzes fehlt es für die seit Jahren diskutierte Frage, ab wann und unter welchen Voraussetzungen personenbezogene Datenverarbeitung im Zusammenhang mit der Beobachtung extremistischer Bestrebungen stattfinden darf, an einer befriedigenden Regelung. Dieses Grundsatzproblem zieht sich gleichsam wie ein roter Faden auch durch die Entwürfe für ein MAD-Gesetz sowie für das Zusammenarbeitsgesetz und führt damit zu einer Vervielfältigung der offenen Fragen.

— Die *Befugnisse* sind zu generalklauselhaft formuliert. Sie heben überwiegend ausschließlich auf die „Erforderlichkeit" ab. Notwendige Differenzierungen nach Art und Umfang der Datenerhebung, den dabei zugunsten des Betroffenen zu beachtenden Rechtsvorschriften sowie nach Art und Inhalt der Datenverarbeitung fehlen fast vollständig. Wo sie vorhanden sind, handelt es sich um Befugnisse, die über geltendes Recht und die gegenwärtige Praxis hinausgehen, so die vorgesehene Übermittlung von Erkenntnissen aus Wohnungsdurchsuchungen und Telefonkontrollen gemäß § 100 a StPO (vgl. hierzu 5. TB S. 94 und 6. TB S. 49).

— Die *Übermittlungsregelungen* entsprechen noch nicht dem im Volkszählungsurteil formulierten Zweckbindungsprinzip; sie werden außerdem dadurch ausgehöhlt, daß die Behörden des Verfassungsschutzes und der MAD zu gegenseitiger umfassender Unterrichtung verpflichtet sind, ohne daß am Zweckbindungsprinzip orientierte Beschränkungen vorgesehen sind. Bei den Befugnissen für die informationelle Zusammenarbeit der verschiedenen Behörden verstärken sich die Probleme dadurch, daß bisher nicht berücksichtigt wird, wie die unterschiedlichen Fristen oder speziellen Verwertungsbestimmungen der verschiedenen übermittelnden Stellen eingehalten werden können, wenn die gleichen Daten mehrfach hintereinander übermittelt werden, ohne daß irgendwelche Auflagen oder Bedingungen vorgesehen sind.

— Beim ZAG kommt zu diesen Einwänden noch hinzu, daß der Entwurf der Forderung nach *Normenklarheit* nicht nur nicht gerecht wird, sondern zugleich zusätzliche Unklarheiten schafft, da der Bürger nicht mehr davon ausgehen kann, daß die in den Spezialgesetzen enthaltenen Übermittlungsregelungen abschließend sind. Sie werden vielmehr jeweils erweitert durch die generalklauselhaften Regelungen im ZAG.

Für den *Zollbereich* habe ich seit Jahren auf die restlichen Lücken bei der Tätigkeit des Zollkriminalinstituts (ZKI) als einer Zentralstelle für die Zollfahndung hingewiesen. Um diesen Bedenken sowie den Anforderungen des Volkszählungsurteils Rechnung zu tragen, hat mir der Bundesminister der Finanzen im Frühjahr d. J. einen Entwurf für ein Steuerbereinigungsgesetz 1986 zugeleitet, der inzwischen vom Deutschen Bundestag beschlossen wurde. Im Rahmen dieses Gesetzes ist auch das Finanzverwaltungsgesetz geändert und eine gesetzliche Grundlage für die Tätigkeit des ZKI geschaffen worden.

Zu dieser Regelung für die Datenverarbeitung des ZKI ist folgendes zu bemerken:

Die von mir empfohlene umfassende Lösung der Probleme in einem besonderen ZKI-Gesetz wurde vom Bundesminister der Finanzen abgelehnt. Zwar wurde meine Anregung aufgegriffen, neben der in einem neuen Absatz des § 12 Finanzverwaltungsgesetz enthaltenen „Regelung" für die Datenverarbeitung des ZKI zumindest eine detaillierte Rechtsverordnungsermächtigung aufzunehmen, die inhaltliche Regelung über Voraussetzungen, rechtliche Grundlagen, Art und Umfang der Datenverarbeitung des ZKI ermöglicht. Da Entwürfe für solche Rechtsverordnungen aber bisher nicht vorliegen, kann auch hier keine Aussage zur Vereinbarkeit mit den Forderungen des Bundesverfassungsgerichts getroffen werden. Dies wiegt um so schwerer, als gerade im Bereich der Zollverwaltung meine Kontrollkompetenz nach wie vor bestritten und Kontrollen (von Einzelangaben abgesehen) dadurch

verhindert werden (vgl. 7. TB S. 73). In meiner Stellungnahme gegenüber dem Bundesminister der Finanzen habe ich daher auch darauf hingewiesen, daß ich gerade angesichts dieser „kleinen Lösung" davon ausgehe, daß meine umfassende datenschutzrechtliche Kontrolle als Ausgleich hierfür gesichert sein muß. Leider entspricht dem die bisherige Praxis nicht. Zu welch sinnwidrigen und für den Bürger nachteiligen Folgen dies insbesondere bei der Zusammenarbeit von Zoll- und Polizeibehörden führt, ist unten zu Nr. 11.5 näher dargestellt.

11.3 Datenschutz bei der Sicherheitsüberprüfung

11.3.1 Die jüngsten Ereignisse und das Verlangen nach mehr Sicherheit

Die spektakulären Spionagefälle des vergangenen Jahres haben den Ruf nach verschärften Sicherheitsüberprüfungen und dem Abbau vermeintlicher datenschutzrechtlicher Hemmnisse laut werden lassen, obwohl nur einer der erwähnten Spionagefälle auf Fehler oder Schwachstellen der Sicherheitsrichtlinien zurückzuführen sein soll.

Es steht außer Streit, daß die Chance, Spione bei der Sicherheitsüberprüfung zu entlarven oder von einer sicherheitsempfindlichen Position fernzuhalten, durch die Überprüfung aller Personen, die mit Verschlußsachen oder in sicherheitsempfindlichen Bereichen arbeiten, genutzt werden muß. Bestrebungen, hierbei nach dem Grad der Geheimhaltungsbedürftigkeit der Materie, mit der der Betreffende betraut werden soll, zu differenzieren, finden auch aus der Sicht des Datenschutzes Zustimmung. Schematisches „Über-einen-Kamm-Scheren" ist jedoch Datenschutz *und* Sicherheit abträglich.

11.3.2 Forderungen des Datenschutzes

Das datenschutzrechtliche Interesse hat sich deshalb von Anfang an auf zwei Schwerpunkte konzentriert, nämlich auf *Transparenz* und *Zweckbindung* (vgl. auch schon 6. TB S. 41 f. und 7. TB S. 64 f. und S. 82):

— Gerade weil die Sicherheitsüberprüfung notwendigerweise viele Personen betrifft, muß sie nicht nur effektiv, sondern vor allem rechtsstaatlich und fair sein. Dies bedeutet, daß dem Betroffenen gegenüber soviel an Transparenz hergestellt werden muß, wie es mit den Sicherheitsbelangen vereinbar ist. Nach Abschluß der Überprüfung sind etwaige Bedenken grundsätzlich mit dem Betroffenen zu erörtern und es ist ihm Auskunft über die Datenspeicherung zu erteilen. Auch im Verhältnis zu den Personen, deren Daten allein aus Anlaß der Sicherheitsüberprüfung eines *anderen* gespeichert werden können (z. B. Ehegatten, Verlobte oder Personen, die mit dem Betroffenen in eheähnlicher Lebensgemeinschaft leben), gilt der Grundsatz der Transparenz.

— Die für eine erfolgreiche Sicherheitsüberprüfung notwendigerweise erhobenen umfangreichen und u. U. intime Details enthaltenden Daten dürfen grundsätzlich nicht für andere Zwecke verwendet werden. Ausnahmen halte ich lediglich für die Spionageabwehr und für mit § 7 Abs. 3 G 10 vergleichbare Fallgruppen für zulässig. Sowohl über den Betroffenen als auch über die anderen Beteiligten werden die Daten ausdrücklich zum Zweck der Sicherheitsüberprüfung erhoben und von diesen auch nur für diesen Zweck gegeben. Daher kann es nicht angehen, daß die Sicherheitsbehörden diese Daten nach Abschluß der Sicherheitsüberprüfung zur freien Verfügung für ihre sonstigen Aufgaben haben. Bisher ist die gebotene Zweckbindung aber nicht gewährleistet (näher unten 13.2.2 am Beispiel des MAD).

Die Beachtung und Kontrolle dieser beiden aus meiner Sicht wichtigsten Grundsätze muß ergänzt und festgeschrieben werden durch eine einwandfreie gesetzliche Grundlage für die Sicherheitsüberprüfung (vgl. auch Anforderungen an Datenschutzregelungen für den Verfassungsschutz Ziff. V in Anlage 3 zu diesem Bericht). Auch dies ist nach meiner Auffassung ein verfassungsrechtliches Gebot, das durch das Volkszählungsurteil besonders herausgestellt wurde. Die Effektivität der Sicherheitsüberprüfung oder sonstige Sicherheitsinteressen werden dadurch nicht gefährdet. Dies gilt auch nach den Spionagefällen des vergangenen Jahres. Zur Speicherung von personenbezogenen Daten im Rahmen der Sicherheitsüberprüfung beim BfV siehe unten Nr. 13.1.2.

11.4 Internationale Zusammenarbeit der Sicherheitsbehörden und internationaler Datenschutz bei den Sicherheitsbehörden

11.4.1 Verstärkung der internationalen Zusammenarbeit

Die Notwendigkeit verbesserter internationaler Zusammenarbeit der Sicherheitsbehörden insbesondere auch beim personenbezogenen Informationsaustausch kann nicht bestritten werden. Zur Begründung genügt der Hinweis auf die allgemeine Internationalisierung der Kriminalität und die zunehmende Durchlässigkeit der Staatsgrenzen als Folge stetig wachsender internationaler Verflechtungen. Speziell für den Bereich der Europäischen Gemeinschaft ist in diesem Zusammenhang der angestrebte Abbau der Grenzkontrollen als weitere Voraussetzung für den gemeinsamen europäischen Binnenmarkt zu nennen. Entsprechende Abkommen, die ein stufenweises Vorgehen bis zum vollständigen Abbau vorsehen, bestehen inzwischen mit mehreren EG-Staaten sowie mit Österreich. Es ist verständlich, daß bei dieser Situation die Polizeibehörden (ähnliches gilt auch für die Nachrichtendienste) nach Ausgleichsmaßnahmen suchen. Inzwischen gibt es Vorschläge zur Errichtung einer europäischen Fahndungsunion sowie eines verstärkten allgemeinen Informationsaustausches mit automatisierten Verfahren zwischen den nationalen zentralen Sicherheitsbehörden. Darüber hinaus ist die Angleichung verschiedener Rechtsmaterien geplant (so im Betäubungsmittel-, Waffen-, Sprengstoff- und Melderecht), um dem Anreiz für einen

Grenzübertritt entgegenzuwirken, wenn damit die Absicht verfolgt wird, sich Maßnahmen zur Gefahrenabwehr oder Strafverfolgung zu entziehen.

Was bisher jedoch in den Planungen fehlt, ist die unerläßliche Angleichung auch des Datenschutzrechts in Verbindung mit den Befugnissen zur Informationsverarbeitung. Eine Intensivierung des internationalen Informationsaustausches kann nur akzeptiert werden, wenn gleichzeitig die bestehenden Unterschiede beim informationellen Befugnisrecht und beim Datenschutzstandard der Sicherheitsbehörden beseitigt werden. Es darf weder ein Befugnis- noch ein Datenschutzgefälle geben. Um ein solches so weit wie möglich zu vermeiden, habe ich dem Bundesminister des Innern eine Reihe von Maßnahmen vorgeschlagen, von denen ich die folgenden für vordringlich halte:

— Es ist sicherzustellen, daß die weitere Verwertung übermittelter Daten über den konkreten Anfragegrund hinaus nur mit Zustimmung der übermittelnden Stelle möglich ist.

— Für die Aufbewahrung personenbezogener Daten sollten für alle Stellen einheitliche Löschungs- und Überprüfungsfristen angestrebt werden.

— Die gegenwärtigen erheblichen Diskrepanzen beim Auskunftsrecht des Betroffenen gegenüber Polizeibehörden sollten beseitigt und

— das informationelle Befugnisrecht der Sicherheitsbehörden sollte soweit wie möglich harmonisiert werden.

Da dies auf absehbare Zeit wohl nicht zu erreichen sein wird, können die Lücken gegenwärtig nur im Wege bilateraler oder multilateraler Absprachen und Auflagen im Einzelfall geschlossen werden, um eine Gefährdung der schutzwürdigen Belange der Betroffenen soweit wie möglich zu verhindern. Hierauf hat auch die Datenschutzkonferenz in ihren Beschlüssen über Anforderungen an Datenschutzregelungen im Polizei- und im Verfassungsschutzrecht unter dem Aspekt des grenzüberschreitenden Datenaustausches hingewiesen (vgl. Anlagen 2 und 3). Der Bundesminister des Innern hat zugesagt, daß er meine Vorschläge in die Beratungen mit den zuständigen Gremien einbringen und mich weiterhin beteiligen wird.

11.4.2 Verstärkung des internationalen Datenschutzes

Erfreulicherweise ist man sich in verschiedenen internationalen Gremien der vorstehend beschriebenen Notwendigkeiten bewußt. So hat die internationale Konferenz der Datenschutzkontrollinstitutionen auf ihrer diesjährigen Tagung vom 23. bis 26. September 1985 in Luxemburg einen Beschluß gefaßt, der Mindestregelungen für die Datenverarbeitung durch Polizeibehörden enthält. Wenn diese Vorschläge von den zuständigen nationalen Behörden beachtet und hierfür gemeinsame Konkretisierungen getroffen werden, dann sind wesentliche Voraussetzungen für einen internationalen bereichsspezifischen Datenschutz bei den Polizeibehörden geschaffen (im einzelnen vgl. Anlage 4).

Ein wichtiger Schritt in diese Richtung könnten auch die beim Europarat laufenden Arbeiten über Grundsätze der Datenverarbeitung durch Polizeibehörden sein. Eine Arbeitsgruppe beim Europarat hat nach mehreren Sitzungen in diesem Jahr unter meiner Beteiligung im November einen Entwurf erstellt, der den Grundsätzen der internationalen Datenschutzkonferenz Rechnung trägt. Ich hoffe, daß diese Vorschläge vom Europarat auch beschlossen werden.

Ein Abbau des bisher im internationalen Vergleich bestehenden Datenschutz- und Datenschutzrechtsgefälles könnte auch durch den Erlaß von ergänzenden Vorschriften zu den Interpol-Datenschutzregelungen von 1982/1984 betreffend die Löschungsvorschriften beim Generalsekretariat von Interpol und den Informationsaustausch zwischen den Nationalen Zentralbüros erfolgen. Die Notwendigkeit hierzu habe ich mehrfach betont (vgl. 5. TB S. 92, 6. TB S. 45). Auf meine Anregung hin hat die internationale Konferenz der Datenschutzkontrollinstitutionen in ihren Grundsätzen zur polizeilichen Datenverarbeitung ebenfalls hierauf hingewiesen und empfohlen, daß diese Grundsätze von den zuständigen Gremien von Interpol beim Erlaß der vorgenannten Ausführungsvorschriften berücksichtigt werden.

Ich werde mich weiterhin bemühen, zur Lösung dieser Probleme beizutragen. Hierzu gehört in erster Linie auch die Kontrolle der Einhaltung schon beschlossener Regelungen. Wie wichtig dies ist, haben meine Kontrollen des internationalen Datenaustausches beim BKA und beim BfV in diesem Jahr erneut gezeigt. Mit der Verabschiedung von Regelungen allein ist es aber nicht getan; erst durch ihre Umsetzung in die Praxis, durch ständige Kontrollen und auch durch Gespräche mit den Verantwortlichen kann der Datenschutz gewährleistet werden.

11.5 Offene Fragen aus meiner Kontrolltätigkeit

Ich habe im Jahre 1984 dem Bundesminister der Finanzen einen pragmatischen Vorschlag hinsichtlich der Ausübung meiner — von ihm bestrittenen — Kontrollkompetenz im Bereich der Zoll- und Steuerfahndung unterbreitet (vgl. 7. TB S. 73). Vor wenigen Wochen ist seine Antwort auf meine Initiative eingegangen; meine Vorschläge wurden abgelehnt. Das Steuergeheimnis, so hat er ausgeführt, stehe auch im Bereich der Zoll- und Steuerfahndung einer datenschutzrechtlichen Kontrolle entgegen. Dies entspricht nach meiner Auffassung nicht der Gesetzeslage. Das Bundesdatenschutzgesetz hat auch die Behörden der Finanzverwaltung ohne Ausnahme der Datenschutzkontrolle unterstellt (vgl. u. a. § 19 Abs. 3 Satz 1 in Verbindung mit § 12 Abs. 2 Nr. 1 BDSG).

Die Haltung des Bundesministers der Finanzen ist aber auch von der Sache her nicht überzeugend: Im vergangenen Jahr habe ich die Falldatei Rauschgift (FDR) datenschutzrechtlich überprüfen lassen. In der FDR sind auch Rauschgiftfälle der Zollfahn-

dung erfaßt. Sie werden von den Zollbehörden an das jeweilige Landeskriminalamt gemeldet und dann von diesem in der FDR gespeichert. Eine datenschutzrechtliche Überprüfung dieser Fälle ist nur bei den Zollbehörden selbst möglich, da nur sie im Besitz der vollständigen Unterlagen sind. Ein Versuch, die von mir in der FDR vorgefundenen Fälle aus dem Zollbereich dort nachzuprüfen, scheiterte an der ablehnenden Haltung des Bundesministers der Finanzen. Er verweigerte eine Einsichtnahme in die entsprechenden Unterlagen unter Berufung auf das Steuergeheimnis. Keine Bedenken hinsichtlich einer möglichen Verletzung des Steuergeheimnisses hat der Bundesminister der Finanzen offenbar, soweit es um die Übermittlung dieser Daten an die Polizei geht. Dort haben nämlich nicht nur die mit der Bekämpfung der Rauschgiftkriminalität befaßten Dienststellen Zugriff auf Daten der FDR. Auch in der weiteren Nutzung und insbesondere in der konventionellen Weiterübermittlung dieser Daten sind die Polizeibehörden nicht auf den Zweck der Bekämpfung der Rauschgiftkriminalität beschränkt.

Ich hoffe, daß der Deutsche Bundestag den derzeitigen Zustand ändert, da es m. E. nicht hingenommen werden kann, daß ein so großer Datenverarbeitungsbereich wie die Zoll- und Steuerverwaltung entgegen dem Wortlaut des BDSG von der datenschutzrechtlichen Kontrolle ausgenommen ist.

Aus den vorgenannten Gründen habe ich die erneute Verweigerung der Einsichtnahme in die für meine Prüfung erforderlichen Akten beanstandet. Der Bundesminister der Finanzen hat die Beanstandung zurückgewiesen, da die Regelung des Steuergeheimnisses (§ 30 AO) keine für meine Kompetenz erforderliche Ausnahmeregelung zugunsten der Datenschutzkontrolle enthalte. Dies ist eine Begründung, die nicht zuletzt wegen des klaren Wortlauts von § 19 BDSG, der keinen Vorbehalt für das Steuergeheimnis kennt, nicht stichhaltig ist.

12. Bundeskriminalamt (BKA)

12.1 Probleme aus der Datenverarbeitungsstruktur beim BKA

In meinem Siebenten Tätigkeitsbericht (S. 60 ff. und 67 ff.) habe ich die Entwicklung der Datenverarbeitung beim Bundeskriminalamt dargestellt und die Sorge geäußert, daß die zunehmende Dateienvielfalt in Zukunft die Durchsetzung datenschutzrechtlicher Regelungen erschweren könnte. Diese Bedenken wurden bestätigt durch die im Rahmen der datenschutzrechtlichen Kontrolle bei der Abteilung (EO) des BKA gewonnenen Erkenntnisse, die für originäre Ermittlungen zuständig ist. Die unter der Bezeichnung INPOL-Bund betriebenen Anwendungen des BKA sind datenverarbeitungstechnisch eng miteinander verbunden. Rechtlich handelt es sich zwar um unterschiedliche und selbständige Dateien, wie z. B. die Haftdatei, die Fahndungsdatei, den Aktennachweis. Für sie gelten auch jeweils unterschiedliche Errichtungsanordnungen. Technisch ist die Verarbeitung dieser Daten aber so organisiert, daß die unterschiedlichen Dateien lediglich Abschnitte einer großen zentralen Datenbank sind, in der die Personalien (sog. P-Datensatz) nur einmal geführt werden, unabhängig davon, in wieviel unterschiedlichen Dateien Daten zu der jeweiligen Person gespeichert sind. An diesen P-Datensatz werden dann die für die jeweilige Datei spezifischen Informationen (sog. Datengruppen) „angehängt". Dies mag unter dem Gesichtspunkt der Datenverarbeitungstechnik ein rationelles Verfahren sein. Datenschutzrechtlich ergeben sich daraus aber neue Gefahren.

Da der P-Datensatz zu jeder Person nur einmal gespeichert wird, werden bei Aufnahme einer Person in eine weitere Datei dort lediglich die dateispezifischen Informationen erfaßt. Zum Inhalt des P-Datensatzes gehören aber nicht nur die Angaben, die zur Identifikation einer Person erforderlich sind, sondern auch personengebundene Hinweise (PHW), die eine knappe erste Einschätzung der Person ermöglichen sollen (wie z. B. gewalttätig, bewaffnet oder Ausbrecher, Näheres hierzu Nr. 12.3). Dies bedeutet, daß die in den einzelnen Errichtungsanordnungen enthaltenen Vorschriften für den Umfang des P-Datensatzes möglichst einheitlich sein müssen, damit dieser für möglichst viele Anwendungen mehr oder weniger unverändert verwendet werden kann. So ist es z. B. zu erklären, wenn in einer ganzen Reihe von Errichtungsanordnungen vorgesehen ist, daß personengebundene Hinweise im P-Datensatz gespeichert werden dürfen.

Die Notwendigkeit, personengebundene Hinweise in Dateien zu erfassen, ist aber aus der Zweckbestimmung einer Reihe von Dateien nicht nachvollziehbar. Beispielsweise könnten die Informationen, die mit Hilfe von personengebundenen Hinweisen gespeichert werden, auch in der Falldatei Rauschgift selbst erfaßt werden. Die Speicherung eines Datensatzes in der Falldatei Rauschgift erfordert jedoch bisher die Anlegung eines P-Datensatzes im Datenbereich Personen oder die Verknüpfung des Falldatensatzes mit einem bereits bestehenden Personendatensatz. Dies bedeutet, daß jeder, der Zugriff auf die Falldatei Rauschgift hat, auch den kompletten Personendatensatz einschließlich der personengebundenen Hinweise erhält, und zwar auch dann, wenn die PHW gar nicht im Zusammenhang mit der Speicherung dieses Falldatensatzes erfaßt worden sind. Sofern aber PHW im Zusammenhang mit einem Falldatensatz gespeichert wurden, haben hierauf auch alle diejenigen Stellen Zugriff, die zwar nicht auf diesen Falldatensatz, wohl aber — im Zusammenhang mit anderen INPOL-Anwendungen — auf den P-Datensatz zugreifen können. Nur aus der Struktur der Datenverarbeitung heraus ist es erklärlich, weshalb in der Errichtungsanordnung für die Falldatei Rauschgift generell vorgesehen ist, daß personengebundene Hinweise gespeichert werden dürfen. Ähnlich verhält es sich mit anderen Anwendungen. Zur Frage, ob und in welchem Umfang PHW überhaupt erforderlich sind, wird nachstehend unter Nr. 12.3 noch gesondert Stellung genommen.

In der Sache bedeutet diese Struktur der Datenverarbeitung, daß im Grunde ein zentraler Personenindex betrieben wird, der aus den Personalien all derer gebildet ist, die in irgendeiner INPOL-Datei gespeichert sind. Die Speicherung in der jeweiligen Spezialdatei stellt sich dann als eine Zusatzinformation zum Personendatensatz dar. Eine derartige Struktur ermöglicht dateiübergreifende Recherchen und sonstige Nutzungen der Daten, die über den jeweils konkreten Zweck der einzelnen Datei hinausgehen. Die Grundsätze der Zweckbindung, die für jede Datei in der betreffenden Errichtungsanordnung spezifisch festgelegt sind, sind bei einer solchen Datenverarbeitungsstruktur nur dann einzuhalten, wenn man die Zwecke der polizeilichen Datenverarbeitung von vornherein entsprechend weit definiert, so daß jede dateiübergreifende Nutzung noch vom Zweck der Datenspeicherung gedeckt ist. Dies wäre dann letztlich die Angleichung des Datenverarbeitungsrechts an die vorgegebene technische Struktur.

Ein weiteres daraus resultierendes Problem kann sich aus den unterschiedlichen Fristen in den verschiedenen Dateien ergeben. So hatte sich in einem Fall eine Petentin an mich gewandt und mit meiner Hilfe die Zusage der Löschung ihrer Daten im BKA-Aktennachweis (AN) erreicht. Als ich dies nachprüfte, stellte ich fest, daß diese Zusage nicht erfüllt worden war. Dies habe ich gegenüber dem Bundesminister des Innern beanstandet. Das BKA hat in seiner Stellungnahme zu dem Fall wie folgt argumentiert: da die Daten der Petentin zugleich von der Polizeidienststelle eines Landes mit einem späteren Aussonderungsdatum in einer anderen Datei gespeichert waren, sei es nicht notwendig, die BKA-Speicherung fristgerecht zu löschen, da der Personendatensatz ohnehin gespeichert bleibe. Die Löschung werde nach Ablauf der Speicherfrist des betreffenden Landes erfolgen. In diesem Fall konnte jedoch im weiteren Verlauf erreicht werden, daß auch das Land seinen Aktennachweis löschte, so daß der Personendatensatz der Petentin inzwischen vollständig gelöscht ist.

Unabhängig von der konkreten Lösung dieses Falles stellt sich aber die Frage, ob es hinnehmbar ist, daß das BKA sich auf den Standpunkt stellt, die Löschungsfrist in einer Datei sei nicht zu beachten, wenn die betreffende Person auch noch in einer anderen Datei mit einer längeren Frist erfaßt ist. Das ganze Gefüge der unterschiedlichen und auf den spezifischen Zweck der Dateien zugeschnittenen Speicherfristen würde aufgehoben, wenn die jeweils längste Speicherung die nach den Errichtungsanordnungen der anderen Dateien kürzeren Fristen verdrängen könnte.

Eng mit dem Vorstehenden hängt auch die Frage des Zugriffs auf die im Rahmen von INPOL-Bund gespeicherten Daten zusammen. Alle Polizeidienststellen, die auf INPOL-Bund Zugriff haben, erhalten bei Benutzung des entsprechenden Operationscodes in jedem Fall die Information, ob über die angefragte Person Daten in einer anderen Datei gespeichert sind. Auch dies ist, ebenso wie die vorstehend geschilderte Fristenproblematik, nur erklärbar auf der Grundlage einer Datenverarbeitungsorganisation, die von einem einheitlichen, zentralen Personenindex aller in den INPOL-Bund-Anwendungen gespeicherten Personen ausgeht. Die bisherige Konzeption des Datenschutzrechts im Sicherheitsbereich ging aber von einzelnen Dateien aus, die selbständig zu betrachten sind und für die jeweils eigene Zweckbindungs- und Verwertungsregelungen gelten. Künftig wird daher das Datenschutzrecht verstärkt den Aspekt der Datenverarbeitungsstruktur einbeziehen müssen, wenn nicht Datenschutzregelungen im Ergebnis leerlaufen sollen.

Ein weiteres Problem der Datenverarbeitungsstruktur beim BKA besteht in der Art und Weise, wie dort eingehende Meldungen verarbeitet werden und innerhalb welcher Organisationseinheit die Entscheidung über die Anlegung einer Kriminalakte und den Aufbau und die Speicherung eines Personendatensatzes getroffen wird. Derzeit ist es so, daß eine zentrale Serviceeinheit — noch ehe die zuständige Fachabteilung sich damit beschäftigt hat — die gesamten Eingänge bearbeitet, die pro Tag mehrere tausend Vorgänge umfassen können. Dort wird unter großem Zeitdruck und mit relativ geringer Personalausstattung eine Kriminalakte angelegt und der Personendatensatz gespeichert, wenn die betreffende Person bislang noch nicht erfaßt war. Danach geht die neu angelegte Akte in die Fachabteilung. Dort besteht zwar die Möglichkeit und auch die Pflicht, die vorgenommene Speicherung zu korrigieren, wenn dies nach der Sachlage geboten ist. Dies geschieht aber äußerst selten, so daß man davon ausgehen kann, daß die Entscheidung über die Anlegung einer Kriminalakte und damit auch über die Speicherung von Personendaten sowie über die Speicherfrist bei diesem zentralen Servicereferat für die anderen Fachabteilungen getroffen wird.

Wie meine Kontrollen in diesem Jahr erneut gezeigt haben, ist es aufgrund der geschilderten Umstände unvermeidlich, daß bei der Entscheidung über die Speicherung schematisch verfahren wird, da anders die täglich eingehenden Datenmengen nicht zu bewältigen wären. Ein Charakteristikum dieser Verfahrensweise ist es beispielsweise, daß das Unterlagen-Aussonderungsdatum, d. h. die Löschungsfrist (sei es bei Erstspeicherung, sei es bei Fristverlängerung), maschinell vergeben wird und zwar orientiert nach dem Tag der Bearbeitung, wenn nichts Abweichendes verfügt wird. Das maschinell vergebene Aussonderungsdatum ist aber fast immer insofern falsch, als der Tag der Bearbeitung beim BKA in aller Regel erheblich später liegt als das Ereignis selbst, das der Grund für die Speicherung ist. Deshalb müßte der Bearbeiter das Aussonderungsdatum manuell korrigieren, was jedoch bisher überwiegend nicht geschieht. Dadurch können Verzögerungen von mehreren Monaten eintreten. Entsprechend länger bleiben dann die jeweiligen Personendatensätze gespeichert. Ich habe mich gegenüber dem Bundesminister des Innern auf den Standpunkt gestellt, daß Fristen nur nach dem Ereignis berechnet werden dürfen und nicht nach dem Tag der Bearbeitung der Information im BKA. Im Ergebnis bedeutet dies, daß das Regel/Ausnah-

meverhältnis umgekehrt werden muß, so daß grundsätzlich das Aussonderungsprüfdatum manuell und orientiert am Sachverhalt des Einzelfalles vergeben wird.

Die bisherige Verfahrensweise hat sich zum Teil besonders deutlich bei der Behandlung von Gerichtsurteilen ausgewirkt, die an das BKA übersandt worden sind. Der Bereich der Bekämpfung der Rauschgiftkriminalität ist einer der wenigen Kriminalitätsbereiche, in dem die Rückmeldung von der Justiz an die Polizei offenbar lückenlos funktioniert. Im Ergebnis erreichen das BKA jährlich Zehntausende von gerichtlichen oder staatsanwaltschaftlichen Entscheidungen. Nach meinem Eindruck wurden diese bislang bei der Entscheidung über die weitere Aufrechterhaltung von Speicherungen nur in sehr unbefriedigender Weise ausgewertet. Statt vorhandene Speicherungen daraufhin zu überprüfen, ob sie im selben Umfang und mit derselben Frist noch weiter aufrechterhalten werden können, wurde nicht selten die Übersendung einer Gerichtsentscheidung zum Anlaß genommen, die Aussonderungsfrist entweder nach dem Tag des Urteils oder nach dem Tag der Bearbeitung im BKA zu verlängern. In einem Fall führte die Mitteilung eines Freispruchs aus tatsächlichen Gründen dazu, vom Tag der Bearbeitung dieses Urteils an eine neue Speicherfrist von zehn Jahren festzusetzen. Der Bundesminister des Innern hat in einer ersten Stellungnahme meiner Ansicht zugestimmt, daß Anknüpfungspunkt für eine Speicherung nur das Ereignis selbst sein darf und nicht die spätere justizielle Behandlung. Desgleichen hat er eingeräumt, daß der Tag der Bearbeitung im BKA kein Ausgangspunkt für den Lauf von Speicherfristen sein darf, und angekündigt, in Zukunft werde vermehrt dafür gesorgt, daß Aussonderungsprüfdaten justiziellen Entscheidungen angepaßt werden.

Die Entscheidung über die Anlegung einer Kriminalakte und die damit verbundene Speicherung der Personendaten ist eine Angelegenheit, die in den Fachbereichen entschieden werden muß. Die Möglichkeit der Fachbereiche, Entscheidungen der zentralen Serviceeinheit zu korrigieren, hat bisher ganz offensichtlich nicht die erwartete Wirkung gehabt. Ich halte es deshalb für notwendig, durch geeignete Verfahrensänderungen sicherzustellen, daß über die Anlage von Kriminalakten und die Speicherung von Personendaten nicht schematisch, zentral und unter Zeitdruck entschieden wird.

12.2 Kriminalaktennachweis — Theorie und Praxis

Das Konzept für einen bundeseinheitlichen Kriminalaktennachweis (KAN) der deutschen Polizei enthält aus verfassungs- und datenschutzrechtlicher Sicht einen wichtigen Grundsatz: Den Verzicht auf die zentrale und ausnahmslose Erfassung jeder bei irgendeiner Polizeibehörde angelegten Kriminalakte. Demzufolge sollen im KAN, auf den alle Polizeibehörden mit kriminalpolizeilichen Aufgaben Zugriff haben, nur Kriminalakten gespeichert werden, die schwere oder überregional bedeutsame Straftaten betreffen. Bei der Definition dessen, was überregional bedeutsam ist, und insbesondere bei der Erarbeitung konkreter Straftatenverzeichnisse, die für die Praxis von der Polizei angelegt worden sind, wurde indes ein großzügiger Maßstab angelegt, der mit den Vorstellungen der Datenschutzbeauftragten nicht immer im Einklang stand (vgl. 5. TB S. 87 f.).

Die grundsätzliche Beschränkung des KAN auf schwere Fälle oder solche mit überregionaler Bedeutung war innerhalb der Polizei von Anfang an heftig umstritten. Bei meinen Kontrollen stoße ich immer wieder auf Sachverhalte und Verfahrensweisen, die geeignet sind, das Grundkonzept des KAN in Frage zu stellen. Ein Beispiel hierfür ist die zentrale Speicherung von erkennungsdienstlichen (ed) Unterlagen beim BKA. Sie führt auch dann zur Speicherung von Personalien beim BKA, wenn die vorgeworfene Straftat keine überregionale Bedeutung hat. Dies ist bei ed-Behandlungen häufig der Fall (vgl. 5. TB S. 88 f.). Fragt in solchen Fällen eine auf den KAN zugriffsberechtigte Polizeidienststelle im Online-Verkehr zu einer Person an, die wegen einer nicht unter die KAN-Kriterien fallenden Straftat ed behandelt wurde, so erhält sie zwar keinen KAN-Bestand. Dennoch bekommt sie aber die Personendaten, weil über die angefragte Person ed-Unterlagen vorliegen. Im Ergebnis erhält sie damit sogar in der Regel mehr an Daten, als sie bei Speicherung der Person im KAN erhalten würde, da der Umfang der Speicherung in den betreffenden Dateien, in denen ed-Unterlagen registriert werden (sog. E- und D-Gruppe), größer ist als im KAN.

Eine andere Variante hat sich im Bereich der Rauschgiftkriminalität ergeben. Dort wird — wie schon erwähnt — eine eigene Falldatei Rauschgift (FDR) betrieben. In dieser Datei werden alle in der Bundesrepublik oder im Ausland mit Bezug zur Bundesrepublik begangenen Rauschgiftstraftaten erfaßt. Dies gilt auch bei Erwerb einer kleinen Menge Rauschgift für den Eigenverbrauch. Für Zwecke der Bekämpfung der Rauschgifkriminalität ist es sicher notwendig, alle Straftaten zu erfassen, da der Endverbraucher nur das letzte Glied einer Kette ist, die bis hin zum Hersteller des Rauschgifts führt. Die Speicherung der Daten einer Person in der FDR setzt aber voraus, daß eine zentrale Speicherung des P-Datensatzes und des Aktenzeichens in INPOL-Bund vorgenommen wird. Zugriff auf diese Daten haben nicht nur die mit der Bekämpfung der Rauschgiftkriminalität befaßten Polizeidienststellen, sondern alle, die auch Zugriff auf den KAN haben. Diese erhalten bei einer Anfrage im Online-Verkehr zwar KAN-Bestand nur bei schweren Straftaten mit überregionaler Bedeutung. Daneben erhalten sie aber auch bei allen Rauschgiftstraftaten dieselben Informationen, als ob die Person im KAN gespeichert wäre, nämlich die Personendaten und das Aktenzeichen.

Im Bereich der Rauschgiftkriminalität läuft die KAN-Konzeption damit praktisch leer. Da in den kommenden Jahren weitere Falldateien aufgebaut werden sollen, ist abzusehen, daß dies auch in anderen wichtigen Kriminalitätsbereichen der Fall sein wird. Ich habe den Bundesminister des Innern in

meinem Prüfbericht aufgefordert dafür Sorge zu tragen, daß auf Informationen, die nur deswegen zentral gespeichert werden, weil die besonderen — von mir nicht bestrittenen — Bedingungen der Bekämpfung der Rauschgiftkriminalität dies notwendig machen, nur solche Polizeidienststellen zugreifen können, die auch tatsächlich mit der Bekämpfung dieses Deliktsbereiches befaßt sind. Dies hat der Bundesminister des Innern abgelehnt.

Eine weitere Fallgruppe, die mit der KAN-Konzeption nicht vereinbar ist, beruht darauf, daß das BKA selbst umfangreiche Aktensammlungen mit einem eigenen Aktennachweis (sog. BKA-AN) anlegt, die es von den Länderpolizeien und deren Speicherungen „unabhängig" machen. Im Rahmen meiner Prüfung im Bereich der Abteilung EO habe ich festgestellt, daß beim BKA in großzügigem Umfang „Kriminalakten" angelegt und die Personalien der Verdächtigen gespeichert werden. Im Grunde führen auch solche Informationen, die nur im weitesten Sinne kriminalpolizeilich relevant sind, im BKA zur Anlegung einer Kriminalakte und zur Speicherung der Personendaten, und zwar unabhängig davon, ob das BKA im betreffenden Fall zuständig ist oder auch nur eine ins Gewicht fallende Aktivität entwickelt hat.

So können Anfragen anderer Polizeibehörden, die im Betreff der Anfrage den Verdacht einer Straftat erkennen lassen, zur Anlegung einer eigenen Kriminalakte des BKA führen. Dies geschieht auch bei Meldungen über die Einleitung von Ermittlungsverfahren im Rahmen der Sondermeldedienste. Im Rahmen meiner Kontrolle habe ich eine Reihe von Fällen beispielhaft aufgegriffen, in denen zum Teil nur vage Verdachtsmomente auf dem Rauschgiftsektor, die noch nicht einmal in den Spezialdateien Falldatei Rauschgift und Arbeitsdatei PIOS-Rauschgift erfaßt wurden, zur Anlegung einer deliktsneutralen Kriminalakte führten. Der Bundesminister des Innern hat mir inzwischen mitgeteilt, daß diese Fälle überwiegend gelöscht bzw. mit einer erheblich kürzeren Speicherfrist versehen wurden.

Auch unabhängig von diesen beispielhaft herausgegriffenen Fällen begegnet die dargestellte Verfahrensweise datenschutzrechtlichen Bedenken. Beim BKA entstehen auf diese Weise „Kriminalakten", die nicht selten aus nur einem oder wenigen Blättern bestehen. Häufig enthalten diese Blätter nicht mehr als einen Anfangsverdacht, über dessen Bestätigung oder Ausräumung das BKA nicht immer etwas erfährt. Gleichwohl bleiben diese Akten in der Regel zehn Jahre gespeichert.

Ein weiteres Problem liegt darin, daß sich das BKA auf diesem Wege bis zu einem gewissen Grade unabhängig vom KAN machen kann. Wenn es selbst Hinweise der vorstehend beschriebenen Art, und seien sie auch lückenhaft, über Personen speichert, so wird damit die Beschränkung, daß die Länder nach den KAN-Kriterien nur schwere oder überregional bedeutsame Straftaten im KAN und damit im Direktzugriff des BKA speichern dürfen, faktisch aufgehoben. Aufgrund der eigenen gespeicherten Daten kann das BKA gezielt konventionell bei der Polizeibehörde anfragen, von der es die Information ursprünglich erhalten hat. Wenn ferner dritte Polizeibehörden beim BKA anfragen, kann es Hinweise auch auf solche Unterlagen anderer Polizeibehörden geben, die im KAN nicht erfaßt sind. Anläßlich meiner Kontrolle bei der Abteilung EO habe ich festgestellt, daß ca. 800 Personendatensätze als KAN-relevant vom BKA selbst eingestuft und entsprechend gespeichert waren. Insgesamt waren aber in der Personendatei des BKA ca. 2,7 Millionen Personendatensätze erfaßt, von denen der größte Teil auf den BKA-AN, also den Nachweis der nicht KAN-fähigen Kriminalakten des BKA, entfallen dürfte. Im BKA-AN sind demnach nicht nur Kriminalakten über vom BKA bearbeitete Fälle gespeichert, sondern zum großen Teil solche der Länderpolizeien, in denen das BKA, wie oben beschrieben, lediglich Teilinformationen besitzt.

Inzwischen ist mir auch eine Errichtungsanordnung für die Datei BKA-AN zugegangen, die im wesentlichen die bisherige Praxis und damit meine Befürchtungen bestätigt. Unter anderem ist dort geregelt, daß auch Kriminalakten im Zusammenhang mit „sonstigem polizeilich relevanten Schriftverkehr" angelegt und die Personendaten im BKA-AN gespeichert werden dürfen.

Ich habe meine Bedenken hierzu und zu anderen Punkten der Errichtungsanordnung dem Bundesminister des Innern mitgeteilt. Seine Stellungnahme lag bei Fertigstellung des Berichts noch nicht vor.

12.3 Personengebundene Hinweise und Gefahr der sozialen Abstempelung

Die Datenschutzbeauftragten des Bundes und der Länder haben zu den personengebundenen Hinweisen (PHW) einen Beschluß gefaßt, der als Anlage zu diesem Bericht abgedruckt ist (Anlage 5). PHW sind Kurzhinweise im INPOL-Personendatensatz zur Charakterisierung einer Person, die deren erste Einschätzung möglich machen sollen. Es handelt sich dabei im Rahmen von INPOL-Bund (außer bei PIOS- und SPUDOK-Anwendungen) um folgende PHW, die in den Anwendungen Fahndungs- und Falldateien vollständig und in den übrigen Dateien in reduziertem Umfang verwendet werden:

BEWA = bewaffnet
GEWA = gewalttätig
AUSB = Ausbrecher
ANST = Ansteckungsgefahr
GEKR = geisteskrank
GESW = geistesschwach
ENTM = entmündigt
BTMK = Betäubungsmittelkonsument
FREI = Freitodgefahr
PROS = Prostituierte
INTR = Internationaler Rechtsbrecher
LAST = Land-/Stadtstreicher
HWAO = häufig wechselnder Aufenthaltsort

Derartige Merkmale bergen stets die Gefahr einer negativen sozialen Abstempelung. Diese Bedenken müssen allerdings dann zurückstehen, wenn es um die Abwehr von Gefahren für Polizeibeamte wie

auch u. U. für den Betroffenen selbst geht. Deshalb kann die Verwendung von PHW bei der Fahndungsdatei im Grundsatz hingenommen werden, nicht aber ohne weiteres auch darüber hinaus. Wie oben beschrieben, wird für alle in INPOL verwalteten Dateien stets ein und derselbe Personendatensatz verwendet. Somit werden auch immer die PHW zur Verfügung gestellt, und zwar auch dann, wenn auf Dateien zugegriffen wird, in denen Daten gespeichert sind, die nicht für ein unmittelbares polizeiliches Handeln gegen den Betroffenen bestimmt sind. Typisch hierfür ist der Kriminal*aktennachweis* (KAN); wenn auf ihn zugegriffen wird, sind die PHW nicht erforderlich (vgl. auch 7. TB S. 61). Sie stellen darüber hinaus eine erhebliche Fehlerquelle dar.

Die zuletzt beim BKA durchgeführten Kontrollen haben diesen Eindruck noch verstärkt. Bei dem Versuch, aus den Akten festzustellen, warum eine Person als „gewalttätig", „Ausbrecher" usw. eingestuft war, stellte sich folgendes heraus:

— Informationen, die zur Speicherung eines PHW geführt haben, stehen nicht an einer bestimmten Stelle, sondern können irgendwo in zum Teil umfangreichen Kriminalakten vermerkt sein. Die konkrete Nachprüfung und Korrektur von PHW wird dadurch wesentlich erschwert.

— Zum Teil konnten in den Akten keine Anhaltspunkte gefunden werden, warum zu einer Person ein PHW gespeichert worden ist.

— Zum Teil befanden sich in den Akten nur die Bitten anderer Polizeibehörden ohne nähere Begründung, zu einer Person ein PHW zu speichern. Dies hängt — wie oben geschildert — damit zusammen, daß im Rahmen von INPOL-Bund für jede Person die Personalien nur einmal gespeichert und die speziellen Informationen aus anderen Dateien nur „angehängt" werden. „Besitzer" dieses Personendatensatzes ist in der Regel derjenige, der ihn ursprünglich aufgebaut hat. Nur der Besitzer ist zur Änderung des Personendatensatzes, beispielsweise durch Anfügung eines PHW, befugt. „Mitbesitzer" müssen deshalb den „Erstbesitzer" um Speicherung eines PHW ersuchen. Außer dieser Bitte hat der Besitzer des Datensatzes dann meist keinen weiteren Beleg über die Richtigkeit des PHW.

— Zum Teil befanden sich Informationen in den Akten, auf die die Speicherung von PHW einmal gestützt worden war, die aber längst veraltet waren. Wer einmal ausgebrochen ist, auch wenn er beispielsweise aus einem Fürsorgeheim entwichen ist, behält regelmäßig den PHW „Ausbrecher" solange, bis sein gesamter Personendatensatz gelöscht ist, also im Normalfall zehn Jahre. Eine systematische, kurzfristige Überprüfung speziell der PHW findet jedenfalls nach meinen Feststellungen und den mir vorliegenden Errichtungsanordnungen nicht statt.

Zusammenfassend bin ich der Auffassung, daß PHW lediglich für die Fahndungsdatei notwendig und vertretbar sind, aber auch hier nicht in dem zur Zeit praktizierten Umfang. Die Konferenz der Datenschutzbeauftragten hat daher in ihrem Beschluß vom 15. November 1985 eine entsprechende Änderung der gegenwärtigen Praxis gefordert (vgl. Anlage 5).

Sofern die Polizei auf der Speicherung der PHW auch im Zusammenhang mit anderen Dateien des INPOL-Systems bestehen sollte, müßte zumindest durch geeignete Verfahrensregeln sichergestellt werden, daß

— die Richtigkeit der PHW jederzeit einwandfrei nachgewiesen werden kann;

— die PHW (unabhängig vom zugehörigen Personendatensatz) nach einer kurzen Frist (ca. ein Jahr) überprüft und gelöscht werden, wenn nicht besondere Gründe entgegenstehen.

Erfreulicherweise hat der Bundesminister des Innern seine Auffassung für den Grenzaktennachweis des BGS (GAN) geändert und die bisherige Praxis, auch dort PHW zu speichern, beendet. Die Errichtungsanordnung wurde entsprechend geändert. Das BKA sollte sich zu einer solchen Verfahrensweise — außerhalb des Bereichs der Fahndungsdateien — ebenfalls entschließen.

12.4 Das fortdauernde Problem der Speicherung „anderer Personen"

In früheren Tätigkeitsberichten (6. TB S. 43 f. und 7. TB S. 65 ff.) habe ich die Entwicklung der Datenverarbeitung beim Bundeskriminalamt dargestellt. Ein wesentlicher Aspekt dieser Entwicklung ist die immer stärkere Tendenz, neben Beschuldigten und Verdächtigen auch „andere Personen" zu erfassen. Die ständige Zunahme von PIOS- und SPUDOK-Anwendungen macht dies zu einem Dauerproblem. Diese Entwicklung geht teilweise am bestehenden Recht vorbei. Als „Ausgleich" hierfür ist in Ziffer 4.5 der Dateienrichtlinien vorgesehen, daß „andere Personen" über die Tatsache der Speicherung zu unterrichten sind, wenn die Dauer der Speicherung ein Jahr überschritten hat. Mir ist indes kein Fall bekannt, in dem eine derartige Unterrichtung vorgenommen worden ist. Seitens der Polizei wurde vielmehr die Ziffer 4.5 der Dateienrichtlinien von Anfang an kritisiert. Bereits bei meiner Kontrolle der Datei PIOS-Terrorismus (PIOS-TE) im BKA im Jahre 1981 habe ich festgestellt, daß keine der in nicht unbedeutender Zahl dort gespeicherten „anderen Personen" nach Ziffer 4.5 der Dateienrichtlinien unterrichtet worden war. Ein Einzelfall, der mir im vergangenen Jahr durch eine Eingabe bekannt geworden ist, läßt Zweifel aufkommen, ob sich daran etwas geändert hat. Die Ausweispapiere des Petenten waren im Jahre 1978 abhanden gekommen. Aufgrund verschiedener Indizien konnte man annehmen, daß die Papiere in die Hände von Terroristen gelangt waren und dort für Falschidentitäten genutzt wurden. Die personenbezogenen Daten des Petenten wurden deswegen in PIOS-TE gespeichert. Er selbst war weder Beschuldigter noch Verdächtiger. Gleichwohl hat eine Unterrichtung nach Ziffer 4.5 der Dateienrichtlinien nicht stattgefunden. Auf meine Beanstandung hat sich der Bun-

desminister des Innern auf den Standpunkt gestellt, die Daten des Petenten seien gar nicht „direkt gespeichert" gewesen, sondern nur als mögliche Aliaspersonalien erfaßt worden.

Die Arbeitsgemeinschaft der Kriminalpolizeibehörden und der Arbeitskreis II der Innenministerkonferenz haben sich in den vergangenen Jahren mehrfach mit dem Fragenkomplex der „anderen Personen" befaßt (Vgl. 6. TB S. 43 f.). Der ursprüngliche Plan, die Frist, innerhalb der „andere Personen" zu unterrichten sind, auf drei Jahre zu verlängern, wurde nicht realisiert. Statt dessen wurde die Ausnahmeregelung der Ziffer 4.5.2 der Dateienrichtlinien neu interpretiert. Dort ist bestimmt, daß die Unterrichtung zurückgestellt werden kann, solange durch sie der mit der Speicherung verfolgte Zweck gefährdet würde. Für den Bereich PIOS-TE wurde festgelegt, daß diese Ausnahmeregelung stets anzuwenden ist. Im Ergebnis bedeutet dies die Verlängerung der Jahresfrist für die Unterrichtung nach Ziffer 4.5 der Dateienrichtlinien, ohne daß der Richtlinien-Text selbst geändert wurde.

Der Bundesminister des Innern hat mir mitgeteilt, daß auch das BKA im Terrorismusbereich unter Berufung auf Ziffer 4.5.2 der Dateienrichtlinien die Benachrichtigung „anderer Personen" grundsätzlich zurückstellt. Damit ist ein wichtiges Korrektiv für die weitgehend ohne gesetzliche Grundlage erfolgende Speicherung „anderer Personen" auf dem Weg über eine Neuinterpretation der Dateienrichtlinien beseitigt worden. Der Zwang, nach Ablauf eines Jahres „andere Personen" entweder zu benachrichtigen oder ihre Daten zu löschen, ist weggefallen. Damit ist zu befürchten, daß „andere Personen" nunmehr in diesem Bereich länger gespeichert bleiben als bisher.

Eine andere Variante dieser Problematik habe ich bei meiner Kontrolle im Bereich der Bekämpfung der Rauschgiftkriminalität kennengelernt. Von der Abteilung EO des BKA wird eine PIOS-Datei mit der Bezeichnung Arbeitsdatei PIOS-Rauschgift (APR) betrieben. Auch in diesem Bereich ist nach den mir erteilten Auskünften noch keine „andere Person" nach Ablauf eines Jahres über die Speicherung unterrichtet worden. Statt dessen werden die entsprechenden Datensätze in Übereinstimmung mit der genannten Regelung nach einem Jahr gelöscht. Dies ist für die Abteilung EO allerdings deshalb kein allzu großes Problem, weil in der APR nur sehr wenige „andere Personen" gespeichert sind. Insgesamt waren zum Zeitpunkt meiner Prüfung ca. 67 000 Personen in der APR gespeichert. Die meisten sind nach Auffassung des BKA Verdächtige, nur ca. 500 sind als „andere Personen" eingestuft. Diese Zahlen machen deutlich, daß es in starkem Maße auch eine Interpretationsfrage ist, wer als Verdächtiger und wer als „andere Person" gespeichert wird. So bleibt beispielsweise unklar, ob eine Person, die im Notizbuch eines Verdächtigen verzeichnet ist, nun ihrerseits bereits verdächtigt ist oder ob es sich lediglich um eine „andere Person" handelt, deren Daten bis zur Klärung des Verdachts gegen den Notizbuchinhaber gespeichert werden müssen.

Von dieser Interpretation, über die man im Einzelfall streiten kann, hängt das weitere Verfahren ab. Handelt es sich um eine „andere Person", so erfolgt nach einem Jahr die Löschung der Daten oder die Person muß unterrichtet werden. Handelt es sich dagegen um einen „Verdächtigten", so können seine Daten nach der jetzigen Errichtungsanordnung genau so lange gespeichert werden wie die eines konkret Beschuldigten.

Weil hier die Grenzen der Interpretation fließend, andererseits die Konsequenzen für die Speicherung gravierend sind, habe ich dem Bundesminister des Innern vorgeschlagen, bei der Speicherfrist zwischen Verdächtigen und Beschuldigten zu differenzieren. Daten über Verdächtige, gegen die der Verdacht nicht zur Einleitung eines Ermittlungsverfahrens reicht (sonst wären sie Beschuldigte), sollten nach meiner Auffassung grundsätzlich nur für maximal drei Jahre gespeichert werden. In dieser Zeit müßte sich in der Regel der Verdacht erhärtet oder entkräftet haben. Unter- und Überschreitungen dieser Frist müßten im Einzelfall möglich sein. Bei einer derartigen Differenzierung würde jedoch die extensive Ausnutzung eines möglichen Interpretationsspielraums zwischen Verdächtigen und „anderen Personen" nicht so sehr ins Gewicht fallen.

In seiner Stellungnahme zu meinem Prüfbericht ist der Bundesminister des Innern bislang auf diesen Vorschlag noch nicht konkret eingegangen.

Abschließend ist zu betonen, daß die stets steigende Zahl der PIOS- und SPUDOK-Anwendungen die „anderen Personen" zu einem immer drängenderen Problem macht (vgl. 7. TB S. 67). Gerade für diesen Problemkreis muß der Gesetzgeber klare und eingrenzende Regelungen treffen, die den zunehmenden Einsatz technischer Mittel besser beherrschbar machen. Die Instrumente der Dateienrichtlinien und Errichtungsanordnungen reichen hierfür nicht aus, wie sich in der Praxis gezeigt hat.

12.5 Ungelöste Probleme bei der Abteilung Staatsschutz

Bei meiner datenschutzrechtlichen Kontrolle der Abteilung Staatsschutz des BKA im Jahre 1983 habe ich festgestellt, daß dort sehr viele Vorgänge existieren, in denen eine Landespolizeibehörde dem BKA die Einleitung eines Ermittlungsverfahrens gemeldet hat, über dessen weiteren Verlauf aber dort nichts bekannt wird. In meinem 6. Tätigkeitsbericht (S. 46) habe ich dargelegt, daß das BKA nach meiner Auffassung nicht darauf warten darf, bis die Länder Informationen über den Stand von Ermittlungsverfahren schicken, sondern als speichernde Stelle selbst eine aktive Erkundigungspflicht hat. Ich habe vorgeschlagen, daß das BKA spätestens nach drei Jahren von sich aus bei derjenigen Polizeibehörde nachfragt, die das Ermittlungsverfahren eingeleitet hat. Dies halte ich für einen vernünftigen Weg, der die Arbeitsbelastung für das BKA in erträglichen Grenzen hält. Dort werden nämlich Fälle geringerer Bedeutung ohnehin nur mit einer Frist von drei Jahren gespeichert. Bei meinem Lösungsvorschlag würde deswegen nur in

denjenigen Fällen nachgefragt werden müssen, in denen eine längere Speicherung beabsichtigt ist.

Ich habe mich beim Bundesminister des Innern mehrfach um eine Übernahme dieses Vorschlages bemüht. Er hat mir nunmehr mitgeteilt, daß bei kriminaltaktischen Anfragen, also bei der Meldung von Straftaten durch Länderpolizeien und gleichzeitiger Bitte um Auskunftserteilung, das BKA mit der Erteilung der Auskunft seinerseits die Bitte verbindet, über den Ausgang des Verfahrens informiert zu werden. Außerdem soll, wenn später in derartigen Verfahren von dritten Behörden um Auskunft nachgesucht wird, diese erteilt und zugleich die ursprünglich meldende Polizeibehörde gebeten werden, den Ausgang des Verfahrens sowohl dem BKA als auch der dritten Behörde mitzuteilen.

Ich halte diese Vorschläge nicht für ausreichend. Zu dem Zeitpunkt, zu dem eine Polizeibehörde beim BKA eine Straftat im Bereich des Staatsschutzes im Wege der kriminaltaktischen Anfrage meldet, kennt sie selbst den Ausgang des Verfahren nicht. Wenn also das BKA bei der Rückantwort um Mitteilung über den Ausgang des Verfahrens bittet, so kann in aller Regel die Polizeibehörde zu diesem Zeitpunkt dieser Bitte noch nicht entsprechen. Statt dessen kommt es nach meiner Erfahrung darauf an, daß später noch einmal aktiv nachgefragt wird. Auch die Lösung hinsichtlich der Auskunftserteilung an dritte Behörden ist datenschutzrechtlich nicht befriedigend. Sie bedeutet, daß zunächst einmal möglicherweise unvollständige und damit eventuell unrichtige Daten weiterübermittelt werden. Ferner wird es in die Verantwortung derjenigen Polizeibehörde gelegt, die ursprünglich den Fall an das BKA gemeldet hat, ob sie die Informationen ergänzt oder nicht. Das BKA selbst kann dies nicht durchsetzen.

Ich bedauere, daß meinen Vorschlägen bislang nicht nähergetreten wurde. Gerade im Bereich des polizeilichen Staatsschutzes werden nach meinen Erfahrungen häufig Straftaten gemeldet, ohne daß es später zu einer Verurteilung kommt. Da unter polizeilichem Staatsschutz die Bekämpfung jeder Straftat verstanden wird, die aus politischen Motiven begangen sein könnte, führt dies zur Meldung und Erfassung einer großen Zahl von kleineren Delikten, wie z. B. Sachbeschädigung durch „wildes Plakatieren", Beleidigung etc. Häufig werden in letzter Zeit auch sogenannte Blockade-Straftaten, d. h. Straftaten im Zusammenhang mit der Blokkade von militärischen Einrichtungen gemeldet. Kommt es in derartigen Fällen zu Freisprüchen oder zu Verfahrenseinstellungen, so wird dies dem BKA in der Regel nicht bekannt. Es verfügt dann nur über die Information, daß über eine bestimmte Person ein Ermittlungsverfahren eingeleitet worden ist.

Ich halte es in diesem Bereich für besonders wichtig, daß die weitere justizielle Behandlung der gemeldeten Ermittlungsverfahren in der polizeilichen Datenverarbeitung berücksichtigt wird. Bei der bisherigen Verfahrensweise ist dies nicht sichergestellt. Deshalb halte ich nach wie vor an meinem Vorschlag fest, daß das BKA selbst insoweit seine Verantwortung als speichernde Stelle wahrnimmt und sich aktiv um die Ergänzung und ggfs. Richtigstellung bzw. Löschung der bei ihm gespeicherten Daten bemüht, sei es regelmäßig oder zumindest jeweils *vor* der Übermittlung von Informationen an dritte Stellen. Der Einwand der „Arbeitsmehrbelastung" ist demgegenüber nicht überzeugend, da der von mir gemachte Vorschlag so gestaltet ist, daß sich der Mehraufwand in akzeptablen Grenzen hält. Er dürfte sogar zum Teil dadurch aufgewogen werden, daß die Datenbestände im Ergebnis schneller bereinigt werden können und so vermieden wird, polizeiliches Handeln auf unrichtige bzw. unvollständige Daten zu stützen. Ich hoffe, den Bundesminister des Innern und das BKA noch zu einer Änderung ihrer Haltung bewegen zu können.

13. Nachrichtendienste

13.1 Bundesamt für Verfassungsschutz (BfV)

13.1.1 Konsequenzen aus der datenschutzrechtlichen Kontrolle bei der Abteilung III

In früheren Tätigkeitsberichten (6. TB S. 47 f. und 7. TB S. 73 ff.) habe ich über meine datenschutzrechtliche Kontrolle bei der Abteilung III des BfV berichtet. In den Beratungen über diese beiden Berichte im Innenausschuß des Deutschen Bundestages wurden die Einzelheiten meiner Beanstandungen und Empfehlungen detailliert erörtert.

Inzwischen hat mir der Bundesminister des Innern eine Reihe von Maßnahmen mitgeteilt, die aufgrund meines Prüfberichts im BfV veranlaßt worden sind. Im wesentlichen handelt es sich dabei um verschiedene Neuregelungen, die zum Teil auch in den anderen Abteilungen des BfV angewandt werden. Aus Gründen des Geheimschutzes kann hier nur folgendes wiedergegeben werden:

— Verlängerungen der Speicherfristen über die NADIS-Löschungsrichtlinien hinaus werden unter Angabe der maßgeblichen Gründe aktenkundig gemacht.

— Das für die Berechnung von Speicherfristen maßgebliche Datum wird nunmehr vom Bearbeiter — orientiert am veranlassenden Ereignis — eingegeben und nicht mehr durch Programme automatisch bei jeder Veränderung des Datensatzes vergeben.

— Sind Organisationen zu Unrecht in die Liste der Beobachtungsobjekte aufgenommen worden, so werden in Zukunft alle Speicherungen personenbezogener Daten gelöscht, die allein im Zusammenhang mit der Beobachtung dieser Organisation erfolgten. Wird eine extremistisch beeinflußte Organisation aus der Liste der Beobachtungsobjekte gestrichen, so wird eine generelle Überprüfung auf Löschungsfähigkeit vorgenommen. Bei den sogenannten Kern- oder Nebenorganisationen erfolgt dagegen keine besondere Relevanzprüfung.

— Unterlagen über demokratische Organisationen, die im Zusammenhang mit der Beobachtung ex-

tremistischer Beeinflussungsversuche gesammelt worden sind, werden nunmehr gesondert als Hintergrundmaterial geführt.

— Vor der Weitergabe von löschungsreifen Informationen wird künftig eine besondere Relevanzprüfung durchgeführt. Dies gilt vor allem für die Übermittlung an Behörden außerhalb des Verfassungsschutzbereiches.

Diese Maßnahmen werden von mir ausdrücklich begrüßt. Zum Teil sind sie aber noch nicht ausreichend, um meine datenschutzrechtlichen Bedenken in vollem Umfang auszuräumen. Dies gilt insbesondere für die Übermittlung von Daten, die eigentlich bereits gelöscht sein müßten. Ich stehe nach wie vor auf dem Standpunkt, daß eine Anfrage, die sich auf löschungsreife Daten bezieht, grundsätzlich negativ beschieden werden muß. Etwas anderes kann nur in besonderen Ausnahmefällen gelten. Das jetzt vorgesehene Verfahren bleibt hinter diesen Vorstellungen deutlich zurück. Auch hinsichtlich der Unterlagen über demokratische Organisationen, die im Zusammenhang mit der Beobachtung extremistischer Beeinflussungsversuche gesammelt worden sind, sind nach meiner Auffassung weitergehende Maßnahmen notwendig. In diesen Hintergrundakten sollten — von engen Ausnahmen abgesehen — prinzipiell keine personenbezogenen Informationen über Mitglieder demokratischer Organisationen enthalten sein. Sofern dies nicht zu vermeiden ist, sollten solche Unterlagen nur strikt zweckgebunden verwendet werden. Dies bedeutet, daß sie ausschließlich für die Beurteilung extremistischer Beeinflussungsversuche herangezogen werden dürfen. Jede weitere Nutzung ist mit dem Grundsatz der Zweckbindung nicht zu vereinbaren.

Die 15jährige Regelspeicherfrist sollte nicht generell für alle Abteilungen des BfV gelten. Zumindest im Extremismusbereich halte ich eine kürzere Speicherfrist von maximal 10 Jahren für angemessen.

In den Beratungen meiner Tätigkeitsberichte und der ihnen zugrundeliegenden Prüfberichte hat der Innenausschuß des Deutschen Bundestages den Bundesminister des Innern aufgefordert, seine Konzeption für die Neuregelung des Verkartungsplanes der Abteilung III sowie für die bereits in meinem 6. Tätigkeitsbericht (S. 50) und im 7. Tätigkeitsbericht (S. 76) erwähnten speziellen Dateien, die in erster Linie der Identifizierung dienen, vorzulegen. Dies ist kurz vor der Fertigstellung dieses Berichts geschehen.

Eine erste Wertung des Entwurfs der Neufassung des Verkartungsplanes hat ergeben, daß zwar wesentliche Verbesserungen vorgesehen sind, meinen Bedenken indes nur zum Teil Rechnung getragen wird. Zu begrüßen ist vor allem, daß man in Zukunft verstärkt von dem Instrument der Zeitspeicherung Gebrauch machen will. Dies bedeutet, daß insbesondere in Verdachtsfällen nicht von vornherein eine 15jährige Speicherfrist, sondern zunächst eine kürzere Frist eingegeben wird, innerhalb der sich dann klären soll, ob der Verdacht zu Recht besteht. Positiv sind auch einige Begriffserklärungen zu bewerten, die dazu beitragen können, daß in Zukunft nicht mehr unter Berufung auf weitgefaßte Formulierungen (wie z. B. „linksextremistischer Hintergrund") bedenkliche Datenspeicherungen vorgenommen werden.

Dagegen ist der Entwurf in folgenden Punkten zu kritisieren:

— Auch in der vorgesehenen Neufassung des Verkartungsplans wird nicht hinreichend genau zwischen extremistischen Kern- und Nebenorganisationen einerseits sowie beeinflußten Organisationen andererseits unterschieden. Bei letzteren handelt es sich um solche, in denen, teils sogar überwiegend, auch Demokraten mitarbeiten. Das wird vom Bundesminister des Innern ausdrücklich anerkannt. Sind derartige Organisationen einem bestimmenden extremistischen Einfluß ausgesetzt, so besteht kein Zweifel an der Zuständigkeit des BfV, einen derartigen Einfluß im Auge zu behalten. Jedoch sollte in den Regelungen über die Voraussetzungen, unter denen personenbezogene Daten gespeichert werden dürfen, zwischen Kern- und Nebenorganisationen einerseits und beeinflußten Organisationen andererseits unterschieden werden. Denn es bestehen Grenzen zwischen extremistischer Betätigung und bloßer kritischer Meinungsäußerung im Rahmen des demokratischen Willensbildungsprozesses, die vom BfV zu beachten sind. Dies ist auch in der beabsichtigten Neufassung nicht ausreichend berücksichtigt.

— Problematisch erscheinen mir auch einige im neuen Verkartungsplan enthaltenen Begriffe, die hier im einzelnen wegen des vertraulichen Charakters des Verkartungsplanes nicht dargestellt werden können. Sie führen meines Erachtens im Ergebnis dazu, daß unter Berufung auf sie erneut Speicherungen vorgenommen werden können, die einer kritischen Überprüfung nicht standhalten. Ich habe vorgeschlagen, an den entsprechenden Stellen weitere Präzisierungen vorzunehmen.

Meine grundsätzliche Auffassung zur Befugnis des BfV, personenbezogene Daten zu erheben und zu verarbeiten, habe ich in meinem 7. Tätigkeitsbericht auf S. 43 f. im einzelnen dargestellt. Dem Bundesminister des Innern und dem Innenausschuß des Deutschen Bundestages habe ich auch zur Neufassung des Verkartungsplanes eine Reihe von Verbesserungsvorschlägen unterbreitet.

Hinsichtlich der besonderen Dateien, die vor allem der Identifizierung unbekannter Personen dienen sollen, sind inzwischen einige der von mir gerügten Mängel abgestellt worden. Die von mir beanstandete Speicherung besonders intimer Daten wurde eingestellt. Der Katalog von Merkmalen, mit deren Hilfe insbesondere höchst private Eigenschaften von Personen beschrieben werden können, wurde um mehr als die Hälfte verringert. Gleichwohl bleiben Zweifel, ob sich das BfV zur Beobachtung extremistischer Bestrebungen eines Instruments von der Art dieser besonderen Dateien bedienen darf. Die

damit möglichen Erfolge bei der Beobachtung des Extremismus stehen nach meiner Auffassung in keinem Verhältnis zur Tiefe des in diesen Fällen besonders gravierenden Eingriffes in Grundrechtspositionen. Auch wenn die Zahl der Merkmale stark reduziert worden ist, so ändert dies nichts daran, daß hier eine Person anhand der genauen Darstellung ihrer persönlichen und privaten Eigenschaften so beschrieben wird, daß dadurch automatisiert Persönlichkeitsbilder erstellt werden können. Dadurch kann die Person auch dann identifiziert werden, wenn ihr Name nicht bekannt ist. Ich habe deshalb gegenüber dem Innenausschuß des Deutschen Bundestages und dem Bundesminister des Innern zum Ausdruck gebracht, daß es die beste Lösung wäre, auf die Erfassung von Merkmalen aus der Privatsphäre zum Zwecke der Identifizierung von Personen im Rahmen der Extremismusbeobachtung gänzlich zu verzichten.

13.1.2 Die Weiterentwicklung der Datenverarbeitung beim BfV

Das BfV ist derzeit dabei, seine Datenverarbeitung weiter auszubauen. Bereits in meinem 6. Tätigkeitsbericht (S. 50) habe ich über Pläne berichtet, beim BfV in Form sog. „Personenarbeitsdateien" (PAD) mehr Daten mit Hilfe komfortablerer Verfahren zu verarbeiten. Der Bundesminister des Innern hat nunmehr im Rahmen der Diskussion über meine Prüfung der Abteilung III über die der Identifizierung dienende Datei mitgeteilt, daß in ca. 2—3 Jahren das Konzept der PAD realisiert sein wird. Sie sollen auch die Funktionen der Identifizierungsdatei mit übernehmen.

Einzelheiten des neuen Verfahrens sind mir bislang noch nicht bekannt. Es ist aber davon auszugehen, daß mit seiner Hilfe mehr Daten als bisher personenbezogen verarbeitet werden sollen. Der Bundesminister des Innern hat zugesagt, mich an der Erstellung der Errichtungsanordnungen für diese neue Dateien zu beteiligen. Ich werde dabei darauf achten, daß die bei den bisherigen Indentifizierungsdateien festgestellten Mängel nicht in anderer Form in den neuen Dateien wieder auftreten.

Mit der Konzeption und Realisierung dieser Dateiform wird ein wichtiger Schritt auf dem Weg in die weitere Automatisierung der Datenverarbeitung vollzogen. Schon heute werden beim BfV neben der NADIS-Personenzentraldatei (PZD) auch andere Dateien automatisiert betrieben. Die PZD ist zwar aus datenschutzrechtlicher Sicht besonders bedeutsam, weil sie die wichtigste Grundlage der Verwendung personenbezogener Daten ist. Die daneben schon heute eingesetzten Dateien, die in ihren Einzelheiten hier nicht dargestellt werden können, haben alle mehr oder weniger die Aufgabe, die in Aktenform vorhandenen Informationen gezielt wiederauffinden zu können. Dabei geht es allerdings überwiegend noch um andere als personenbezogene Daten.

Der jetzt schon erreichte Stand der automatisierten Datenverarbeitung beim BfV und die geplanten Ausweitungen zwingen dazu, die manuelle und automatisierte Datenverarbeitung mehr als bisher als Einheit zu verstehen. Die Beschränkung des Datenschutzes auf die Datenverarbeitung in Dateien erweist sich dabei aus der Sicht des Betroffenen als verfehlt. Die in Dateien gespeicherten Daten beziehen sich unmittelbar auf in Akten enthaltene Daten. Bei Löschung der Daten einer Person, über die eine Personenakte angelegt ist, wird zwar grundsätzlich auch die P-Akte vernichtet. Die weit überwiegende Anzahl personenbezogener Speicherungen erfolgt aber auf der Grundlage von Sachakten (Akten über verfassungsschutzrechtlich relevante Ereignisse oder Organisationen). Werden in diesen Fällen nur die Daten in der Datei gelöscht, so ist für den Betroffenen unter Umständen wenig erreicht, wenn die zugrundeliegenden Aktenteile weiter aufbewahrt werden. Der Zugriff auf solche Akten und das gezielte Auffinden von Fundstellen zu Personen ist ohne Datenspeicherung der Personendaten zwar schwieriger. Doch auch die neben der NADIS-PZD noch betriebenen weiteren automatisierten Dateien, die keinen Personenbezug haben müssen, ermöglichen mit Hilfe anderer Suchkriterien als dem Namen durchaus ein gezieltes Wiederauffinden von Informationen in Aktensammlungen. Es erscheint mir deshalb in immer stärkerem Maße notwendig, bei Löschung von Personendaten in der PZD auch die zugehörigen Akten oder Aktenteile zu vernichten. Dies ist zumindest immer dann möglich und geboten, wenn der Sinnzusammenhang des verbleibenden Rests der Akte nicht zerstört wird. Bislang wurde eine entsprechende Verfahrensweise im BfV noch nicht zugesagt.

13.1.3 Sonderdatei im Rahmen der Sicherheitsüberprüfung

Speziell für die Sicherheitsüberprüfung ist im BfV in den vergangenen Jahren eine Sonderdatei eingerichtet worden. Ihre Einzelheiten können aus Geheimhaltungsgründen hier nicht dargestellt werden. Vorbehaltlich einer detaillierten Nachprüfung habe ich Bedenken gegen die Erforderlichkeit und Zulässigkeit einiger der hierfür vorgesehenen Datenfelder geäußert. Ich befürchte, daß durch die vorgesehenen Speicherungen das Persönlichkeitsrecht der Betroffenen verletzt werden kann. Immerhin handelt es sich jährlich um Tausende von Beamten und öffentlich Bediensteten sowie Angestellten in der Privatwirtschaft, die sich einer Sicherheitsüberprüfung unterziehen müssen. Daß dabei auch intime Informationen erhoben und bewertet werden müssen, ist hinnehmbar, wenn dies durch eine bereichsspezifische, präzise gesetzliche Grundlage gerechtfertigt ist.

Eine andere Frage ist es aber, wie die so erhobenen Daten nach Abschluß der Sicherheitsüberprüfung gespeichert und weiter verarbeitet werden. Ich habe mich auf den Standpunkt gestellt, daß es nicht erforderlich, aber darüber hinaus auch im Hinblick auf das Recht auf informationelle Selbstbestimmung der betroffenen Beamten und Angestellten höchst bedenklich ist, Speicherungen so vorzunehmen, daß durch entsprechende Auswertungen Daten jeweils derjenigen sicherheitsüberprüften Beamten und Angestellten systematisch zusammen-

gestellt werden können, die ein bestimmtes Merkmal haben. Die Betroffenen wären damit negativ in einer bestimmten Richtung abgestempelt — trotz des erteilten Sicherheitsbescheides. Zu einem derartigen fortdauernden Eingriff in die Privatsphäre besteht nach dem oben Dargelegten keine Notwendigkeit.

Die Gespräche mit dem BfV über diese Datei sind noch nicht abgeschlossen. Ihr bisheriger Verlauf bestätigt aber die Schwierigkeit, ein einmal eingeführtes Verfahren nachträglich unter datenschutzrechtlichen Gesichtspunkten noch zu korrigieren.

13.2 Militärischer Abschirmdienst

13.2.1 Personelle Vorbeugung

Der Bundesminister der Verteidigung hat mir mitgeteilt, daß das Verfahren der personellen Vorbeugung beim MAD neu geregelt wird. Bisher wurden im Rahmen der personellen Vorbeugung beim MAD sicherheitsrelevante Daten über Personen gespeichert, die von ihrem Alter her möglicherweise einmal auf die Bundeswehr zukommen könnten. Dies bedeutet, daß Daten über zumeist Jugendliche oder Heranwachsende, die allenfalls bei der Polizei oder bei den Verfassungsschutzbehörden gespeichert sein dürften, parallel dazu auch beim MAD gespeichert werden. Hieran habe ich wiederholt Kritik geübt (vgl. zuletzt 7. TB 81 f.).

Das nunmehr beabsichtigte Verfahren trägt dieser Kritik Rechnung. Erkenntnisse, die bislang zur Speicherung im Rahmen der personellen Vorbeugung geführt haben, sollen nunmehr wie folgt verarbeitet werden: Durch geeignete Maßnahmen bei den Wehrersatzbehörden wird sichergestellt, daß im Falle der Einberufung der betreffenden Person zuvor der MAD benachrichtigt wird. Dieser fragt dann bei den Verfassungsschutzbehörden nach, ob über diese Person Erkenntnisse vorhanden sind. Ist dies der Fall, so wird geprüft, ob und gegebenenfalls welche Absicherungsmaßnahmen notwendig sind. Erst in diesem Stadium, wenn sich die Notwendigkeit zu solchen Maßnahmen zeigt, erfolgt eine Speicherung beim MAD. Ich habe in meinem Siebenten Tätigkeitsbericht (S. 81 f.) dargelegt, daß grundsätzlich zu prüfen ist, ob die personelle Vorbeugung überhaupt notwendig ist. Nachdem der Bundesminister der Verteidigung dies bejaht, sehe ich in der nunmehr vorgeschlagenen Lösung aus datenschutzrechtlicher Sicht einen Kompromiß, der u. a. sicherstellt, daß polizeiliche und Verfassungsschutzerkenntnisse beim MAD nicht parallel zu Polizei und Verfassungsschutz gespeichert werden, nur weil die betreffende Person einmal zur Bundeswehr einberufen werden könnte. In der Praxis dürfte dies eine beträchtliche Reduzierung der Neueinspeicherungen zur Folge haben. Hinzu kommt die den Wehrersatzbehörden obliegende Pflicht, das Unterrichtungsersuchen des MAD der betreffenden Person gegenüber in keiner Weise nachteilig zu verwenden. Außerdem können Maßnahmen der Absicherung somit auf aktuelle, beim Verfassungsschutz auch zu Recht gespeicherte Informationen gestützt werden. Besonders bedeutsam erscheint mir, daß die jahrgangsweise Überprüfung aller Wehrpflichtigen vermieden wird. Die weiteren Einzelheiten des Verfahrens, insbesondere die notwendigen Durchführungserlasse, sind mit dem Bundesminister der Verteidigung noch zu erörtern.

13.2.2 Zweckbindung der Daten aus der Sicherheitsüberprüfung

Weder beim MAD noch bei den Verfassungsschutzbehörden ist die Zweckbindung der im Rahmen einer Sicherheitsüberprüfung erhobenen Daten gewährleistet. Beide Stellen gehen vielmehr davon aus, daß diese Informationen auch für die gesamte sonstige Aufgabenerfüllung zur Verfügung stehen. Dies halte ich vor allem im Hinblick auf die dem Betroffenen gegebenen Zusicherung, wonach seine Daten „streng vertraulich" behandelt werden, für nicht zulässig. Ausnahmen können allenfalls wegen der gleichen Zweckrichtung bei der Spionageabwehr sowie in Analogie zu § 7 Abs. 3 Gesetz zu Artikel 10 GG in Betracht kommen.

Bislang konnte in dieser Frage mit dem MAD keine Einigkeit erzielt werden. Dies ist auch deshalb bedauerlich, weil derzeit ohnehin das gesamte Verfahren der Sicherheitsüberprüfung beim MAD neu organisiert wird. Dies wäre eine gute Gelegenheit, auch den datenschutzrechtlichen Belangen besser Rechnung zu tragen. Bei mir häufen sich in letzter Zeit die Eingaben Wehrpflichtiger, die die Notwendigkeit aller im Erklärungsbogen zur Sicherheitsüberprüfung erhobenen Daten bezweifeln und Sorge haben, daß diese Daten auch anderweitig verwendet werden. Bislang bin ich gehalten, diesen Petenten mitzuteilen, daß die von ihnen gemachten Angaben nicht nur für die Sicherheitsüberprüfung, sondern gegebenenfalls für die Erfüllung aller Aufgaben des MAD herangezogen werden. Es ist auch nicht auszuschließen, daß diese Daten im Wege der Amtshilfe an andere Sicherheitsbehörden übermittelt werden.

14. Verteidigung

14.1 Wehrersatzwesen

Auch in diesem Jahr bezogen sich viele Eingaben und Anfragen auf den Umgang mit personenbezogenen Daten im Wehrersatzwesen und in anderen Bereichen der Bundeswehr. Die Betroffenen wollen erfahren, warum Daten von ihnen verlangt werden, was mit den Daten geschieht und wie sie verarbeitet werden. Hierzu wurden von den Stellen, mit denen der Betroffene Kontakt hatte, gelegentlich nur unzureichende Antworten gegeben, was nach meinem Eindruck dann erst bewirkte, daß man sich an mich wandte. Die Mitarbeiter in diesen Ämtern kennen die Datenflüsse nicht in allen Einzelheiten und wissen nicht selten zu wenig über den Datenschutz. Auch verstehen sie die Neugierde der Bürger nicht, „denn bisher hatte ja fast nie jemand gefragt".

Die Eingaben betreffen oft nur örtlich auftretende Probleme, so zum Beispiel einen im Bereich eines Bataillions entwickelten Fragebogen, der dann auf mein Betreiben zurückgenommen wurde. Aber auch auf generelle Probleme wurde aufmerksam gemacht. So habe ich aufgrund von Anfragen Betroffener erreichen können, daß der Bundesminister der Verteidigung die Regelung über die Anforderung und die Weitergabe von Scheidungsurteilen z. B. zum Zwecke der Ermittlung des Versorgungsausgleichs (vgl. auch oben Nr. 5.1.3) präzisierte.

14.1.1 Umgang mit KDV-Unterlagen

Immer wieder wurde ich zum Umgang mit Unterlagen von anerkannten und abgelehnten Kriegsdienstverweigerern (KDV) befragt. Durch eine solche Anfrage wurde mir erst im Berichtsjahr bekannt, daß durch das Wehrersatzwesen-Informationssystem (WEWIS) seit etwa zwei Jahren für jedes Kreiswehrersatzamt eine Liste der aus der Wehrüberwachung ausgeschiedenen Wehrpflichtigen erstellt wird, die auch die Gründe des Ausscheidens (z. B. ausgemustert oder anerkannter Kriegsdienstverweigerer) enthält. Die Daten der Betroffenen sind dann zwar nicht mehr in WEWIS gespeichert, und auch die dazugehörigen Akten sind an andere Stellen, wie z. B. das Bundesamt für den Zivildienst, abgegeben oder bereits vernichtet. Aber die Liste existiert dann noch. Da für diese Liste keine Frist zur Vernichtung bestimmt ist, wird sie in einigen Kreiswehrersatzämtern seit ihrer Einführung aufbewahrt. Sie ist für die Mitarbeiter dort ein Hilfsmittel, wenn sich aus der Wehrüberwachung Ausgeschiedene auch noch nach längerer Zeit mit Fragen an das zuletzt für sie zuständige Kreiswehrersatzamt wenden. Im Zusammenhang mit einer Kontrolle in einem Kreiswehrersatzamt habe ich dem Bundesminister der Verteidigung wegen der Festlegung des Inhalts der Liste und einer Aufbewahrungsfrist Vorschläge gemacht. Der Bundesminister der Verteidigung hat meine Anregungen aufgegriffen und will sie in die Praxis umsetzen.

Für den Umgang mit Akten aus dem Anerkennungsverfahren als Kriegsdienstverweigerer waren aus zwei Gründen Änderungen zu erwarten. Zum einen hatte das Kriegsdienstverweigerungs-Neuordnungsgesetz (KDVNG) von 1983 Änderungen im Verfahren zur Folge, die sich auf den Inhalt und die Behandlung der Unterlagen auswirkten. Zum anderen ist ein Verwaltungsstreitverfahren eines anerkannten Kriegsdienstverweigerers über den Verbleib seiner Unterlagen beim Bundesverwaltungsgericht anhängig. Nach meinen Informationen wird der Bundesminister der Verteidigung im Benehmen mit dem Bundesminister für Familie, Jugend und Gesundheit die Revision jedoch zurückziehen, so daß das Verfahren ohne eine Grundsatzentscheidung beendet wird.

Da inzwischen auch das KDVNG so weit umgesetzt ist, daß weitere, noch unbekannte Anpassungsprobleme in der Praxis der betroffenen Ämter nicht mehr auftreten werden, halte ich es für geboten, den Umgang mit den im Anerkennungsverfahren angelegten Unterlagen endgültig zu regeln. Soweit der Bundesminister der Verteidigung daran beteiligt ist, ist dies insbesondere für die Unterlagen der nicht als Kriegsdienstverweigerer anerkannten Antragsteller (3. Abschnitt KDVNG) notwendig. Auch hierzu hat die Kontrolle in einem Kreiswehrersatzamt gezeigt, daß zur Sicherung eines datenschutzgerechten Umgangs mit diesen Unterlagen, die Bestandteile der Personalunterlagen der Betroffenen sind, bestehende Regelungen des Bundesministers der Verteidigung geändert werden müssen. Ich habe dem Bundesminister der Verteidigung u. a. empfohlen, die Ablage der Unterlagen aus dem Anerkennungsverfahren als Kriegsdienstverweigerer sowie die Einsichtnahme und Löschungsfristen für diese Unterlagen ausdrücklich zu regeln. Eine Stellungnahme des Bundesministers der Verteidigung lag zum Zeitpunkt der Fertigstellung dieses Berichtes noch nicht vor.

14.1.2 Vorschriften zur Wehrerfassung

Nach § 15 Abs. 3 Wehrpflichtgesetz ist die Erfassung der Wehrpflichtigen eine Aufgabe der Länder; sie wird von den Meldebehörden wahrgenommen. Der Bundesminister des Innern hat zur Regelung der Durchführung der Erfassung Verwaltungsvorschriften erlassen. Im Zusammenhang mit Überlegungen zur Vereinfachung der Erfassung und aufgrund des Urteils des Bundesverfassungsgerichtes zum Volkszählungsgesetz 1983 soll die Wehrerfassung künftig durch Rechtsverordnung geregelt und dafür eine Ermächtigung im Wehrpflichtgesetz geschaffen werden. Um feststellen zu können, welche Arbeitsschritte zur Aufgabe „Erfassung" gehören und wie sie zur Zeit in der Praxis ablaufen, habe ich mit Vertretern des Bundesministers der Verteidigung, des Bayerischen Staatsministeriums des Innern, des Bayerischen Landesbeauftragten für den Datenschutz, einer Wehrbereichsverwaltung, eines Kreiswehrersatzamtes und der Verwaltung der Landeshauptstadt München Informationsgespräche geführt. Diese haben gezeigt, daß über die *tatsächlichen* Abläufe und die Verarbeitung der Daten von Wehrpflichtigen bei allen Beteiligten unterschiedliche Vorstellungen und Erwartungen bestehen. Ich habe dem Bundesminister der Verteidigung, der vom Bundesminister des Innern um Vorschläge zur Neuregelung der Erfassung gebeten wurde, meine weitere Beratung hierzu angeboten. Ich halte es für wichtig, daß die Neuregelung gerade auch unter dem Aspekt der Wehrgerechtigkeit, die eine vollständige Erfassung aller zum Wehrdienst heranstehenden Personen verlangt, in enger Abstimmung mit denen erarbeitet wird, die für den Vollzug verantwortlich sind.

14.2 Verband der Reservisten

Die Übermittlung personenbezogener Daten von Reservisten an den Verband der Reservisten der Deutschen Bundeswehr e. V. (VdRBw) hat seit Bestehen meiner Behörde immer wieder Anfragen von Reservisten ausgelöst. Hier werden — auch im Hinblick auf die privatrechtliche Rechtsform des

Verbandes — unzulässige Datenübermittlung vermutet, und die enge Zusammenarbeit zwischen dem Bundesminister der Verteidigung und dem VdRBw ist meist nicht bekannt. Ich habe bereits in meinem Zweiten Tätigkeitsbericht (S. 53) dazu Stellung genommen. Die rechtliche Bewertung ist unverändert.

Der VdRBw nimmt Aufgaben der Reservistenarbeit wahr, die im Interesse und in der Zuständigkeit der Bundeswehr liegen. Es handelt sich dabei insbesondere um Maßnahmen der Betreuung und Fortbildung aus der Bundeswehr ausgeschiedener Soldaten. Soweit diese Aufgaben außerhalb der Bundeswehr durchgeführt werden können, bedient sich der Bundesminister der Verteidigung zu ihrer Erfüllung des VdRBw. Der Verband ist insoweit besonders beauftragter Träger der Reservistenarbeit, er erhält hierfür Zuwendungen aus dem Bundeshaushalt und ist bei der Durchführung seiner Aufgaben an die Vorgaben des Bundesministers der Verteidigung gebunden. Dies ist in der Reservistenkonzeption der Bundeswehr vom 29. Mai 1980 festgelegt. Diese Konzeption wurde dem Deutschen Bundestag zur Kenntnis gegeben und von ihm gebilligt. Der Auftrag des VdRBw ist auch in seiner Satzung festgehalten.

Nach der Reservistenkonzeption unterrichtet der Bundesminister der Verteidigung alle zur Entlassung heranstehenden Soldaten sowie Angehörige von Mobilmachungseinheiten über die Pflichten der Reservisten, die Reservistenarbeit und den VdRBw. Der Bundesminister der Verteidigung teilt dem VdRBw die Anschriften der aus dem aktiven Wehrdienst ausgeschiedenen Soldaten mit, um ihm die Möglichkeit zu geben, Mitglieder zu werben. Die Anschriften werden als Aufklebe-Etiketten zur Verfügung gestellt. Diese Übermittlung von personenbezogenen Daten ist nach § 7 Abs. 3 in Verbindung mit § 24 Abs. 1 BDSG zulässig.

Der VdRBw verwendet die Aufklebe-Etiketten zum Versand von Informationsmaterial an die Reservisten und behält danach keinerlei Daten zurück. Erklärt ein Reservist seinen Beitritt zum Verband, so werden seine Daten erst aus der Beitritts-Erklärung vom VdRBw gespeichert. Die Datenverarbeitung erfolgt im Auftrag des VdRBw im Rechenzentrum der Bundeswehr in Bonn. Laut Weisung des Generalsekretariats des VdRBw sollen diese dem Verband durch die Kreiswehrersatzämter überlassenen Anschriftenlisten innerhalb von 3 Monaten nach Empfang zweckentsprechend aufgearbeitet werden. Abschriften oder sonstige Formen der Zwischenspeicherung sind nicht erlaubt.

Diese Weisung scheint jedoch nicht immer befolgt zu werden, wie ich aus an mich gerichteten Eingaben schließen kann. Ich habe daher den VdRBw, der als privatrechtlich organisierte Stelle nicht meiner Kontrollkompetenz unterliegt, in einem auf Vermittlung des Bundesministers der Verteidigung zustandegekommenen Gespräch empfohlen,

- die Mitarbeiter im VdRBw darauf hinzuweisen, daß sie keine Zwischenspeicherungen aus den Anschriftenlisten vornehmen dürfen, sich also an die Weisungen des Generalsekretariats zu halten haben,
- deutlicher auf die Quelle der Daten hinzuweisen und über die datenschutzrechtliche Zulässigkeit dieser Übermittlung von der Bundeswehr an den VdRBw zu informieren und
- in dem verbandseigenen Informationsblatt ggf. regelmäßig für entsprechende Informationen zu sorgen.

Der VdRBw hat zugesagt, meinen Empfehlungen zu folgen; er wird mich darüber unterrichten.

15. Nicht-öffentlicher Bereich

15.1 SCHUFA-Klausel

Von großer Bedeutung für den Datenschutz im privaten Bereich war die am 19. September 1985 verkündete Entscheidung des Bundesgerichtshofs zur sogenannten „SCHUFA-Klausel". Das Gericht hatte zu entscheiden, ob die in den Allgemeinen Geschäftsbedingungen bei der Vergabe von Konsumentenkrediten von der Kreditwirtschaft üblicherweise verwendete Klausel

> „Die Bank ist berechtigt, der Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA) ... Daten des Kreditnehmers und etwaiger Mitschuldner über die Aufnahme (Kreditbetrag, Laufzeit, Ratenhöhe) und Abwicklung dieses Kredits zur Speicherung zu übermitteln"

den gesetzlichen Anforderungen entsprach. In seinem Urteil hat das Gericht diese Frage verneint, weil die Klausel, indem sie den Kreditgeber pauschal ermächtigt, alle Daten des Kreditnehmers an Dritte weiterzugeben, mit wesentlichen Grundgedanken des Bundesdatenschutzgesetzes nicht vereinbar ist und deshalb zu einer unangemessenen Benachteiligung des betroffenen Kreditnehmers im Sinne des Gesetzes zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen (AGB-Gesetz) führt.

Nach den Urteilen des Bundesgerichtshofs vom 15. Dezember 1983 (Abwägungspflicht der SCHUFA bei der Speicherung) und vom 6. November 1984 (keine SCHUFA-Auskunft an Kreditvermittler) bestätigt diese Entscheidung erneut meine datenschutzrechtiche Beurteilung der Klausel und des Verfahrens. Schon bei der Einführung der Klausel hatte ich darauf hingewiesen, daß sie den Anforderungen des § 3 BDSG wegen der mangelnden Konkretisierung des Datenumfangs nicht genügt (1. TB S. 42) und deshalb Konflikte heraufbeschwört (2. TB S. 36).

Als einen wesentlichen Grundgedanken des BDSG hat der Bundesgerichtshof das Gebot der Abwägung zwischen den Belangen des Betroffenen und den Interessen der übermittelnden Stelle oder eines Dritten hervorgehoben, wie es in den §§ 24 und 32 BDSG zum Ausdruck kommt. Das Gericht hat damit zugleich Leitlinien für die Neufassung der Klausel aufgestellt. So hat die übermittelnde Stelle

in jedem Einzelfall vor der Übermittlung die beteiligten Interessen sorgfältig abzuwägen und dabei die Aussagekraft und Auswirkung einer Mitteilung zu prüfen. Die undifferenzierte Weitergabe von Negativmerkmalen (Einmeldung) aufgrund einseitiger Maßnahmen, wie „Mahnbescheid" oder „Kreditkündigung", ist damit unzulässig.

Erneut hat der Bundesgerichtshof auch darauf hingewiesen, daß das Informationssystem der SCHUFA ein Kreditinformationssystem ist, das nur dann und so lange im Interesse der Allgemeinheit liegt, wie die gespeicherten Daten ein möglichst vollständiges, zutreffendes und aktuelles Bild der Kreditwürdigkeit bieten und die Weitergabe dieser Daten nur an solche Anschlußnehmer erfolgt, die ein berechtigtes Interesse an Auskünften über die Kreditwürdigkeit eines Betroffenen haben. Dieser Grundsatz ist für die Gestaltung des SCHUFA-Systems im ganzen von entscheidender Bedeutung. Er fordert eine datenschutzgerechte Organisation des Systems und erklärt diese zugleich zur Voraussetzung für dessen rechtmäßigen Betrieb. Datenschutzgerechte Organisation bedeutet dabei Sicherung der Verwirklichung des auch im privaten Bereich grundsätzlich geltenden Rechts auf informationelle Selbstbestimmung. Der einzelne muß auch im Privatrechtsverkehr über die Preisgabe und Verwendung seiner persönlichen Daten selbst entscheiden und wissen können, wer was wann bei welcher Gelegenheit über ihn weiß. Dieser Zusammenhang ist bisher noch nicht von allen Beteiligten so klar gesehen worden. Die jetzt veranlaßte Neuordnung des SCHUFA-Systems muß genutzt werden, alle Möglichkeiten zu überprüfen, mit denen sich eine datenschutzgerechte Organisation erreichen läßt.

Im Rahmen der Gespräche zwischen den Spitzenverbänden der Kreditwirtschaft, den Verbänden des Handels und den obersten Aufsichtsbehörden für den Datenschutz über die Neufassung der Klausel und des Verfahrens habe ich mit dieser Zielrichtung vorgeschlagen, das Verfahren künftig so zu regeln, daß der Betroffene, wenn er dies wünscht, die Möglichkeit hat, von Übermittlungsvorgängen nicht nur der Bank an die SCHUFA, sondern auch der SCHUFA an Dritte inhaltlich Kenntnis zu nehmen.

Damit werden zwei Datenschutzziele verfolgt. Zum einen erhält der Betroffene erstmals eine praktikable Möglichkeit, von sich aus die Richtigkeit, Aktualität und Vollständigkeit der gespeicherten Daten zeitnah zu überprüfen und Korrekturen zu veranlassen, noch ehe ein Schaden eingetreten ist. Bisher bleibt dem Betroffenen nichts anderes übrig, als entweder täglich eine (kostenpflichtige) Auskunft anzufordern oder fehlerhafte Auskünfte hinzunehmen.

Zum anderen dient die Information des Betroffenen dazu, die Rechtmäßigkeit der Datenübermittlungen zu sichern. Sie ist insofern eine nach § 6 BDSG gebotene organisatorische Vorkehrung der Gesetzesdurchführung. Bislang wird eine wirksame Zulässigkeitskontrolle bei Übermittlungen von der SCHUFA nicht durchgeführt. § 32 Abs. 2 BDSG läßt eine Übermittlung personenbezogener Daten nur zu, wenn der Empfänger ein „berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat". In der Praxis begnügt man sich aber damit, daß der Empfänger sein berechtigtes Interesse angibt, etwa indem er in einer Liste von Anfragegründen einen bestimmten Grund (z. B. „Ratenkauf") ankreuzt. Auf das eigentliche Glaubhaftmachen, etwa durch Übersendung von Unterlagen (Bestellung, Kreditantrag) oder eidesstattliche Versicherung verzichtet man. Zwar werden auf Verlangen der Aufsichtsbehörden den Empfängern nach einem Stichprobenverfahren Kontrollmitteilungen über erfolgte Datenanforderungen zugesandt. Diese erlauben aber allenfalls dem Empfänger, seine Mitarbeiter zu kontrollieren, dienen aber nicht der Kontrolle des Empfängers selbst. Da an das SCHUFA-System nicht nur Banken und Großfirmen, sondern auch zahlreiche kleine und kleinste Unternehmen angeschlossen sind, hat dieser Unterschied auch große praktische Bedeutung. Gegen mißbräuchliche Abfragen durch Anschlußnehmer bestehen bislang keine auch nur annähernd wirksamen Schutzvorkehrungen. Die Unterrichtung der Betroffenen von Datenübermittlungen könnte hier Abhilfe schaffen. Sie würde nicht nur den Betroffenen und der SCHUFA die Wahrnehmung ihrer Rechte ermöglichen (Schadensersatz, Unterlassungsanspruch, Anschluß-Kündigung), sondern hätte auch einen ganz wesentlichen präventiven Effekt auf das Verhalten der Anschlußnehmer.

Die Vertreter der Bundes-SCHUFA e.V. haben zugesagt, zu prüfen, in welcher Weise und mit welchem Aufwand eine stärkere Einbeziehung des Betroffenen in das Verfahren erfolgen könnte.

Über eine informativere und präzisere Formulierung des Textes der SCHUFA-Klausel wurde in den bisherigen Gesprächen bereits weitgehende Einigkeit erzielt. Nur das Kleingedruckte zu korrigieren, reicht jedoch nicht aus. Eine tragfähige Lösung setzt voraus, daß das Verfahren im ganzen unter dem Vorzeichen des Datenschutzes neu geordnet wird.

15.2 Versicherungen

Ähnlich wie die Kreditwirtschaft bei der Einräumung von Krediten kommt auch die Versicherungswirtschaft beim Abschluß von Versicherungsverträgen nicht ohne Klauseln aus, die die Speicherung und Übermittlung personenbezogener Daten aus der engsten Privatsphäre des Vertragspartners betreffen. Über die sog. Datenschutzklausel, auf deren Grundlage die Versicherer Daten der Versicherten z. B. an Rückversicherer und Versicherungsverbände übermitteln, habe ich bereits in meinem Ersten (S. 41) und Zweiten (S. 55) Tätigkeitsbericht berichtet.

Alle Versicherungsunternehmen verlangen beim Abschluß von Lebens-, Kranken- und Unfallversicherungen auf dem Antragsformular außerdem die Abgabe einer Erklärung über die Entbindung von der Schweigepflicht (Schweigepflichtentbindungsklausel), die etwa bei einer Krankenversicherung folgenden Wortlaut hat:

„Ich ermächtige den Versicherer, auch zugleich für die mitzuversichernden Personen, soweit und

solange sie von mir gesetzlich vertreten werden, jederzeit Auskünfte über frühere, bestehende und bis zum Ende des Vertrages eintretende Krankheiten, Unfallfolgen und Gebrechen sowie über beantragte, bestehende oder beendete Personenversicherungen einzuholen. Dazu darf er Ärzte, Zahnärzte, Heilpraktiker, Krankenanstalten aller Art, Versicherungsträger, Gesundheits- und Versorgungsämter befragen. Diese befreie ich von ihrer Schweigepflicht und ermächtige sie, dem Versicherer alle erforderlichen Auskünfte zu erteilen."

Sinn dieser Bestimmung ist es, dem Versicherer eine zutreffende Beurteilung des Risikos und der Leistungspflicht zu ermöglichen.

Den Erfordernissen des Datenschutzes genügt diese Klausel jedoch nicht. Die Aufsichtsbehörden der Länder, deren Aufsicht die Mehrzahl der Versicherungsunternehmen unterliegt, sind sich mit mir darin einig, daß sie die Anforderungen, die an eine datenschutzrechtlich wirksame Einwilligung zu stellen sind, nicht erfüllt. Die Klausel leidet im wesentlichen an denselben Schwächen wie die vom Bundesgerichtshof beanstandete SCHUFA-Klausel der Kreditwirtschaft. Hier wie dort wird dem Vertragspartner eine pauschale Einwilligung in die Übermittlung und Speicherung personenbezogener Daten formularmäßig abverlangt. Ein Unterschied besteht lediglich darin, daß nicht die Versicherer Adressat dieser Erklärung sind, sondern die betreffenden „Ärzte, Zahnärzte, Heilpraktiker, Krankenanstalten . . " etc.

Eine formularmäßig abverlangte Erklärung, mit der sich der Betroffene für einen wesentlichen Teil der Individualsphäre pauschal seines Rechts auf informationelle Selbstbestimmung entäußert, ist mit den Grundsätzen des BDSG nicht vereinbar.

Bei einer pauschalen Freistellung von der Schweigepflicht müßte als Regulativ zumindest vorgesehen sein, daß Datenübermittlungen nur nach sorgfältiger Abwägung der Interessen aller Beteiligten erfolgen. Schon der Versicherer muß im Einzelfall abwägen, ob sein Interesse an der Auskunft durch einen Arzt oder ein Krankenhaus das Interesse des Versicherten an grundsätzlicher Geheimhaltung seiner Gesundheitsdaten überwiegt. Der Arzt hat zu prüfen, ob mit der Offenbarung der gesundheitlichen Verhältnisse schutzwürdige Belange des Patienten verletzt werden können. Schließlich darf sich der Datenaustausch zwischen Arzt und Versicherer nicht im Verborgenen abspielen. Der Versicherer muß dem Betroffenen mitteilen, bei wem er von der Entbindung von der Verschwiegenheitspflicht Gebrauch machen will. Anderenfalls kann der Versicherungsnehmer nicht mehr wissen, welche Daten der Versicherer wann bei welcher Gelegenheit und von wem über ihn erhalten hat. Das auch im privaten Bereich grundsätzlich gewährleistete Recht des einzelnen, über die Preisgabe und Verwendung seiner Daten selbst zu entscheiden, setzt Transparenz der Datenflüsse und Kenntnis möglicher Übermittlungen voraus.

Die zur Zeit verwendete Klausel verbindet zwei Zwecke: Risikobeurteilung durch den Versicherer bei Vertragsabschluß und Beurteilung seiner Leistungspflicht bei Geltendmachung eines Anspruchs. Die Klausel ist dadurch so kompliziert geraten, daß sich ihre Tragweite dem Leser nur schwer erschließt. Besser wäre deshalb eine Fassung, die die beiden Zwecke klar voneinander trennt. Der Versicherte könnte leichter erkennen, warum überhaupt von ihm eine Erklärung über die Entbindung von der Schweigepflicht erwartet wird.

Zur Risikobeurteilung vor Vertragsabschluß scheint es mir notwendig, den Kreis der Stellen, die von der Verschwiegenheitspflicht befreit werden sollen, möglichst präzise abzugrenzen. Zur Beurteilung der Leistungspflicht während des laufenden Versicherungsverhältnisses dürfte es für die Versicherer ausreichend und zumutbar sein, jeweils im Einzelfall eine Schweigepflichtentbindungserklärung beim Versicherten einzuholen. Auch hierbei würde es sich zwar um eine formularmäßige Erklärung handeln, doch brauchte von ihr im Unterschied zur gegenwärtigen Praxis der Vertragsabschluß nicht abhängig gemacht zu werden. Dem Betroffenen bliebe die Entscheidung im Einzelfall überlassen, ob er beispielsweise einen bestimmten Arzt oder ein bestimmtes Krankenhaus von der Schweigepflicht seiner Krankenversicherung gegenüber befreien will oder nicht (was freilich negative Auswirkungen auf die Leistungspflicht haben könnte).

Angesichts der steigenden Zahl von Eingaben, die mich zu den Schweigepflichtentbindungsklauseln in Versicherungsverträgen von Betroffenen und Ärzten erreichen, halte ich es für geboten, die zwischen den beteiligten Behörden und Wirtschaftsverbänden laufenden Gespräche rasch zu einem Abschluß zu bringen.

15.3 Fehlende Datenschutzkontrolle bei mittelbarer Datenverarbeitung

Zu den Aufgaben verschiedener Bundesbehörden, die im Bereich der Wirtschaftsaufsicht tätig sind, gehört es, die Verarbeitung personenbezogener Daten durch Unternehmen verbindlich zu regeln. So unterliegen etwa AGB-Klauseln der Versicherungsunternehmen, welche die Speicherung oder Übermittlung von Daten des Versicherungsnehmers betreffen, der Genehmigung durch das Bundesaufsichtsamt für das Versicherungswesen. Auch kann das Bundesaufsichtsamt die Unternehmen zu bestimmten Datenübermittlungen und Speicherungen anweisen, etwa indem es den Unternehmen aufgibt, vor jeder Einstellung eines Außendienstmitarbeiters eine Auskunft über diesen bei der Auskunftsstelle für den Versicherungsaußendienst e.V. (AVAD) einzuholen und bei jedem Ausscheiden bestimmte Daten des Mitarbeiters dorthin zu übermitteln.

In allen diesen Fällen trifft die Behörde durch die Ausübung ihrer Aufsichts- und Genehmigungsbefugnisse wesentliche Entscheidungen über die Verarbeitung personenbezogener Daten, ohne dabei einer datenschutzrechtlichen Kontrolle zu unterliegen. Meine Kontrollbefugnis nach § 19 Abs. 1 und 3

BDSG betrifft nur die eigene Datenverarbeitung der Bundesbehörden, d. h. soweit sie selbst speichernde Stellen sind. Die Kompetenz der (Landes-)Aufsichtsbehörde für den Datenschutz im privaten Bereich erfaßt zwar das datenverarbeitende Unternehmen, nicht aber dessen Fach-Aufsichtsbehörden.

Damit besteht die Gefahr, daß Fachaufsichtsbehörde und Datenschutzaufsichtsbehörde unterschiedliche Anforderungen an ein Unternehmen stellen, was nicht zuletzt die Glaubwürdigkeit des Datenschutzes gefährden könnte. Um dies zu vermeiden, scheint es mir notwendig, daß die betreffenden Bundesbehörden mich beteiligen, damit ich sie beraten und die notwendige Koordination mit den Datenschutzaufsichtsbehörden der Länder einleiten kann. Im Rahmen der Novellierung sollte daher auch die mittelbare Datenverarbeitung in die Kontrolle nach § 19 BDSG in geeigneter Weise einbezogen werden.

16. Datensicherung

16.1 Beratung in Sicherheitsfragen

Wegen des raschen Fortschritts in der Informationstechnik und auch wegen des zunehmenden Bedarfs an Informationsverarbeitung zur Erfüllung politischer, gesellschaftlicher und administrativer Anforderungen wachsen die Anwendungen der automatisierten Datenverarbeitung in den öffentlichen Stellen des Bundes ständig. Dieses Wachstum ist gekennzeichnet durch leistungsfähigere zentrale DV-Anlagen, die durch Zunahme der Datenübertragung oder zumindest von entsprechenden Planungen und durch die beginnende Verwendung von Personal-Computern oder ähnlichen Einrichtungen zur individuellen Datenverarbeitung durch Sachbearbeiter.

In welchen Formen der Einsatz von moderner Informationstechnik auch erfolgt, stets ist die Organisationskraft der zuständigen Stelle besonders gefordert. Da diese Anforderungen kurzfristig wachsen und oft nur für die Zeit der Umstellung besonders hoch sind, kann man ihnen häufig am besten mit Hilfe externer Beratung gerecht werden. Dabei besteht besonderer Beratungsbedarf hinsichtlich der fachneutralen aber jeweils anwendungsspezifisch zu lösenden Fragen der Datensicherung, die oft mit allgemeinen Organisationsproblemen verbunden sind. Im Rahmen meiner Möglichkeiten biete ich entsprechende Beratungen an. Es hat sich aber gerade auch im abgelaufenen Berichtsjahr gezeigt, daß selbst wichtige Beratungstermine wegen anderer Verpflichtungen manchmal nur sehr schwer und mit entsprechenden Verzögerungen wahrgenommen werden konnten. Für den Beratungsbedarf aller Behörden und sonstigen öffentlichen Stellen des Bundes ist meine Dienststelle aber nicht nur wegen der geringen Kapazität wenig geeignet, sondern auch weil es eine im Grunde unberechtigte, aber durchaus verständliche Zurückhaltung der Behörden gibt, ausgerechnet die Kontrollinstanz um Beratung zu bitten und dabei vielleicht auch alte Schwächen und Versäumnisse offenbaren zu müssen.

Eine andere Beratungsstelle für Datensicherung ist aber nicht bekannt, und die Stellen, die über die nötigen Kenntnisse verfügen, haben ebenfalls nicht die voraussichtlich erforderliche Kapazität, so daß sie diese Leistung nicht erbringen könnten, selbst wenn eine solche Beratung zu ihrer Aufgabe gehörte oder gemacht würde. Nach meinen Erfahrungen aus Kontrollen und Beratungen ist es aber wichtig, daß eine Beratung für allgemeine Fragen der Datensicherung — was sowohl technische und organisatorische Maßnahmen zum Datenschutz wie auch Vorkehrungen gegen Sabotage und mutwillige Zerstörung einschließt — nicht nur möglich ist, sondern auch offensiv angeboten wird, damit gerade organisationsschwache Stellen davon auch im erforderlichen Umfang Gebrauch machen.

16.2 Der Beitrag von Kontrollen zur Datensicherung

Zur Sicherung eines Datenverarbeitungsverfahrens gehören — wie zur Sicherung anderer Objekte auch — zum einen die Einrichtung von Schranken gegen unerwünschte Einwirkungen und zum anderen planmäßige Kontrollen zum Überprüfen der Wirksamkeit dieser Schranken und zur Beobachtung des Systems. So genügt es z. B. nicht, die unbefugte Benutzung eines DV-Systems über Terminals allein durch die Vergabe von Paßwörtern an die Berechtigten und die Prüfung der Paßwörter vor der Benutzung zu verhindern. Es ist vielmehr auch erforderlich, sich ein Bild über die erfolglosen Zugriffsversuche mit falschen Paßwörtern zu verschaffen, denn sonst könnten unbemerkt Paßwörter ausprobiert werden, was auf die Dauer sehr wohl zum (unerwünschten) Erfolg führen kann. Auch die Zugriffe mit gültigem Paßwort sollten und können leicht kontrolliert werden (vgl. 6. TB S. 55 f.).

Eine entsprechende Beobachtung der Systembenutzung ist zwar nicht sehr schwierig, sie erfordert aber dennoch stets einen gewissen Aufwand. Im Vertrauen auf die automatische Wirksamkeit der getroffenen Maßnahmen unterbleibt deshalb oft die ergänzende Überwachung, auch weil man sich keine besonderen Erkenntnisse davon verspricht. Aber selbst wenn solche Kontrollen nichts anderes lieferten als die Gewißheit, daß die getroffenen Maßnahmen den gewünschten Erfolg auch wirklich haben, so wären sie doch nicht nutzlos. Denn gerade für die öffentliche Verwaltung ist es nicht nur wichtig, Sicherheit zu gewährleisten, sondern es kommt auch darauf an, darlegen zu können, daß vermutete Mängel bei der Sicherung nicht existieren.

Ähnliches gilt auch für die Datenträgerverwaltung, die bei der Verhinderung mißbräuchlicher Datennutzung erhebliche Bedeutung hat. Selbst wenn die Verwaltung der Datenträger gut organisiert ist und mit tagesaktuellen Nachweisen arbeitet, sollten gelegentliche Stichproben bestätigen, daß die Datenträger sich tatsächlich dort befinden, wo sie planmäßig und dem Nachweis entsprechend sein soll-

ten. Solche Kontrollen werden zwar kaum zur Aufdeckung unzulässiger Handlungen führen. Sie sind aber geeignet und nach meinen Erfahrungen auch erforderlich, um Lücken im System aufzuzeigen, die unzulässige Handlungen erheblich erleichtern können. Solche Lücken entstehen z. B. dann, wenn der Lauf der Datenträger aus vernünftigen Gründen stillschweigend geändert wird, ohne das Nachweissystem entsprechend anzupassen, oder wenn die Aufgaben, für die der Datenträger laut Nachweis benötigt wird, so umfangreich, langandauernd und differenziert geworden sind, daß der genaue Verbleib des Datenträgers aus dem Nachweis schließlich nicht mehr feststellbar ist. Solche Entwicklungen, die zum Entstehen von Schwachstellen in einem sonst gut organisierten System führen, fallen in der täglichen Arbeit kaum auf, sie werden vielmehr oft erst durch Kontrollen aufgedeckt. Und es reicht zur Datensicherung nicht aus, wenn ich im Rahmen meiner Kontrollen gelegentlich solche Mängel feststelle.

Je nach der Bedeutung eines Datenverarbeitungsverfahrens kann es zur Gewährleistung der ordnungsgemäßen Verarbeitung auch geboten sein, nicht nur alle Programme, die freigegeben und zur Ausführung bestimmt gespeichert sind, gegen Veränderungen besonders zu schützen (Schreibschutz), sondern auch in gewissen Abständen die auszuführenden Programme mit einer „genehmigten Urfassung" zu vergleichen. Damit können auf die Dauer riskante Nachlässigkeiten bei schnellen Änderungen erkannt und das Sicherungssystem ständig den praktischen Erfordernissen angeglichen werden, ohne daß sich die Benutzung hilfreicher — aber auch gefährlicher — direkter Wege einbürgert. Darüber hinaus könnten damit auch böswillig oder nur spielerisch vorgenommene Änderungen und Ergänzungen (z. B. durch sogenannte Virusprogramme) erkannt werden, deren Entdeckung sonst erst im Rahmen der Fehleranalyse möglich ist, also erst nach dem Schadensereignis.

Ich verkenne nicht, daß Kontrollen dieser Art stets gegen jemanden gerichtet sind, also zumindest einen abstrakten Verdacht voraussetzen, und ich weiß, daß der öffentlichen Verwaltung Mißtrauen insbesondere gegen die eigenen Mitarbeiter weitgehend fremd ist. Es ist auch im Regelfall völlig unbegründet. Die Sicherungsmaßnahmen müssen sich aber nicht am Regelfall des zuverlässigen Mitarbeiters orientieren, sondern gerade auch Sicherungen gegen Fehlverhalten einzelner Mitarbeiter bieten. Mit Kontrollen so lange zu warten, bis ein konkreter Verdacht z. B. auf den gezielten Mißbrauch personenbezogener Daten entstanden ist, bedeutet den Verzicht auf ihre vorbeugende Wirkung. Dabei finden Kontrollen dort ihre Grenzen, wo durch sie die Privatsphäre der Mitarbeiter unangemessen beeinträchtigt und ihre Datenschutzrechte verletzt werden. Im konkreten Fall dürften hier aber stets vernünftige Lösungen möglich sein. Deshalb sollte diese Mühe nicht gescheut werden, weil in dem Maße, in dem die öffentliche Verwaltung moderne Systeme der automatisierten Datenverarbeitung einsetzt und damit vom zuverlässigen Funktionieren dieser Systeme abhängig wird, auch die Sicherungsmaßnahmen einschließlich der dazugehörigen Kontrollen alle denkbaren Möglichkeiten berücksichtigen müssen. Denn ein durch unzulässige Eingriffe bewirkter Schaden kann — bedingt durch die Größe der Systeme und ihre weite Verbreitung — sehr groß sein, und besonders der Vertrauensverlust bei den betroffenen Bürgern wäre nur schwer wieder zu beseitigen.

16.3 Personal Computer

Viele erprobte Prinzipien zur Gewährleistung des Datenschutzes sind an der Vorstellung orientiert, daß die Datenverarbeitung im Zusammenwirken einer Fachabteilung mit einem arbeitsteilig organisierten Rechenzentrum erfolgt. Wesentliche Elemente der Sicherung sind hier das Vier-Augen-Prinzip, Funktionentrennung, kontrollierte Auftragsverfahren, Programmfreigabe durch die Fachabteilung und Beteiligung des Datenschutzbeauftragten an der Verfahrensentwicklung und -freigabe.

Die technische Entwicklung hat zum einen dazu geführt, daß die Rechenzentren leistungsfähiger wurden, was an dieser Struktur wenig geändert hat. Sie hat aber auch dazu geführt, daß leistungsfähige Anlagen zur automatisierten Datenverarbeitung unter Bedingungen einsetzbar sind, die ihre dezentrale Verwendung erlauben. Damit kann es wirtschaftlich vernünftig sein, einem Mitarbeiter eine DV-Anlage zur persönlichen Nutzung im Rahmen seiner Aufgaben zur Verfügung zu stellen. Dies gilt in erster Linie für das breite Angebot an Personal Computern (PC) und sogenannten Home Computern, aber auch für Microcomputer, selbständige Anlagen zur programmgesteuerten Datenerfassung und komfortable Textverarbeitungssysteme, die eine Dateiverwaltung ermöglichen. Ähnliche Probleme verursacht auch die Möglichkeit, über ein Terminal eine zentrale DV-Anlage *individuell* zu nutzen, etwa im time-sharing-Betrieb, worauf hier nicht näher eingegangen wird.

Bei der unkontrollierten Nutzung der Möglichkeiten solcher Anlagen ist der Anwender in einer ganz anderen Situation als bei der Übergabe eines Auftrages an ein Rechenzentrum. Er allein

— verfügt über die Anlage und alle Datenträger, ist also allein verantwortlich für die Sicherung der Daten,

— ist Auftraggeber und Auftragnehmer in einer Person,

— aktiviert die Anlage mit einem Betriebssystem, das er möglicherweise selbst auswählen und modifizieren kann,

— setzt aus einem vorhandenen Angebot ausgewählte Programme ein oder entwickelt die Programme je nach Bedarf auch selbst,

— verarbeitet selbst eingegebene oder von anderen Stellen eingelesene Daten und

— verfügt zunächst allein über die Ergebnisse der Verarbeitung.

Diese Umstände gefährden die Persönlichkeitsrechte der Betroffenen erheblich, wenn die Verarbeitung personenbezogener Daten nicht durch besondere Maßnahmen zur Gewährleistung des Datenschutzes gesichert wird. Neben § 6 BDSG und der Anlage dazu schreibt hierfür auch § 15 BDSG die Zielrichtung der Maßnahmen vor. Er verpflichtet dazu, sich eine Übersicht über die Verarbeitung personenbezogener Daten zu verschaffen und die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme zu überwachen. Beides ist gerade beim Einsatz von PC schwierig, aber auch in besonderem Maße geboten.

16.3.1 Datenschutzmaßnahmen für Anlagen, die nicht zur Verarbeitung personenbezogener Daten eingesetzt werden sollen

Die Vorschriften des Bundesdatenschutzgesetzes beziehen sich auf die Verarbeitung personenbezogener Daten und enthalten deshalb keine Regelungen über Anlagen zur automatisierten Datenverarbeitung, mit denen keine personenbezogene Daten verarbeitet werden. Gerade beim Einsatz von kleineren DV-Systemen zur arbeitsplatzspezifischen Nutzung kommt es aber erfahrungsgemäß häufig vor, daß Systeme, die *planmäßig* für die Verarbeitung nicht personenbezogener Daten eingesetzt werden, außerdem auch personenbezogene Daten verarbeiten. Einfache Anwendungen enthalten z. B. nur Geburtstage, Anschriften und Telefonnummern; aber es ist leicht möglich und aus der Sicht des Benutzers oft hilfreich, je nach Bedarf auch andere Daten zu führen und auszuwerten.

Um die Ausführung des BDSG sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen (§ 15 BDSG) ist es deshalb erforderlich, auch die Benutzer von DV-Systemen, die planmäßig ausschließlich nicht personenbezogene Daten verarbeiten sollen, entsprechend zu belehren und durch gelegentlich wiederholte Informationen und Kontrollen zu gewährleisten, daß auch jede tatsächliche Verwendung dieser Geräte mit den Datenschutzvorschriften vereinbar ist.

Dazu ist unerläßlich, daß dem für den Datenschutz Verantwortlichen ein Gerätenachweis zur Verfügung steht, in dem die Art, der Standort und die planmäßige Nutzung jeder DV-Anlage aufgeführt sind, und daß er Gelegenheit hat, sich von den realen Einsatzbedingungen der Anlage zu überzeugen. Nur so wird er in der Lage sein, das Erforderliche zur Gewährleistung des Datenschutzes zu veranlassen.

16.3.2 Sicherung gegen unbefugte Datenverarbeitung mit PC

Wegen der oben beschriebenen Bedingungen bedarf die Sicherung gegen unbefugte personenbezogene Datenverarbeitung beim Einsatz von PC besonderer Maßnahmen. Dies gilt zum einen für die Sicherung der leicht und unauffällig transportablen und in der Regel nicht von einem hauptamtlichen Archivar besonders überwachten Datenträger, z. B. gegen unbefugte Mitnahme. Zum anderen ist auch die Anlage selbst gegen die Benutzung durch Unbefugte zu sichern. Dabei ist zu beachten, daß gerade der Betrieb von PC oft sehr einfach und benutzerfreundlich und oft auch durch das System selbst erläutert ist. Zudem haben sich Standards herausgebildet, so daß es nicht unwahrscheinlich ist, daß sogar völlig sachfremde und lediglich neugierige „Besucher" als unbefugte Benutzer in Frage kommen. Deshalb muß der PC durch Bewachung, Schlüsselschalter, Abschließen des Raumes o. ä. gegen unbefugte Benutzer gesichert sein.

Die Sicherung gegen Dritte muß beim Einsatz von PC ergänzt werden um Sicherungsmaßnahmen dagegen, daß der befugte Benutzer die Anlage, die Programme oder die Daten unbefugt nutzt. Gerade wegen der großen Freiheit bei der Benutzung eines PC sind besondere Maßnahmen geboten, um die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, kontrollieren zu können und auch zu kontrollieren. Die Verantwortlichen werden also zunächst für jede Anwendung genau prüfen müssen, welche Daten für welchen Zweck mit welchen Verfahren verarbeitet werden sollen. Ergibt diese Prüfung, daß von den Daten, ihrer vorgesehenen und der möglichen Verarbeitung keine Gefährdung für die Betroffenen zu erwarten ist, kann ohne weiteres auch eine Verarbeitung auf PC erfolgen. So bestehen z. B. keine datenschutzrechtlichen Bedenken, wenn auf einem PC unabhängig von seiner sonstigen Nutzung nebenbei ein internes Telefonverzeichnis geführt wird.

Handelt es sich dagegen um personenbezogene Daten von größerer Aussagefähigkeit, sind angemessene Beschränkungen geboten. Ihre Art muß sich an der Qualität der Daten, dem Verwendungszusammenhang und den daraus resultierenden Gefährdungen ausrichten. So reicht es z. B. für Systeme, mit denen (sensible) personenbezogene Daten verarbeitet werden, für die praktisch jede mögliche interne Verarbeitung und Auswertung zulässig ist, von denen aber keine auf einzelne Betroffene bezogenen Ergebnisse außerhalb des Systems verwertet oder bekannt werden dürfen, sicher aus, wenn die Bindung des Systems an den berechtigten Benutzer gewährleistet ist. Typisch für solche Umstände ist der Einsatz von PC im Forschungsbereich: Die Auswertung (auch sehr sensibler Daten) ist spontan und vielfältig. Der Benutzer muß die Freiheit haben, nach seinen Vorstellungen Auswertungen zu entwickeln und durchzuführen. Die Ergebnisse veröffentlicht er jedoch in nicht personenbezogener Form. Hier reicht es aus datenschutzrechtlicher Sicht aus, wenn der Forschende PC und Datenträger nach Arbeitsende sicher verschließt.

Häufig wird aber bei personenbezogener Datenverarbeitung mit PC eine Abgrenzung zwischen zulässigen und unzulässigen Verarbeitungen ebenso möglich und geboten sein wie die zwischen zulässigen und unzulässigen Verwertungen der Daten. Dies gilt insbesondere für die Verarbeitung von Da-

ten über die Beschäftigung der jeweiligen Stelle. Solche Verarbeitungen können zulässig und zweckmäßig sein, z. B. im Rahmen der Personaleinsatzplanung oder des Soll-Ist-Vergleichs für eine Organisationseinheit, bezogen auf abgeschlossene Planungsperioden, während aber bestimmte, auf die Einzelperson bezogene Auswertungen unzulässig sein können — auch wenn gelegentlich daran Interesse besteht.

Hier kommt es darauf an, Sicherheit auch gegen den möglicherweise nur unbedachten Fehlgebrauch durch den befugten Benutzer zu erreichen. Wirksame Maßnahmen zur Gewährleistung des Datenschutzes sind

— eine strikte und lückenlose Menü-Steuerung aller planmäßigen (zulässigen) Verarbeitungen, die auch den richtigen Einsatz von Hilfsprogrammen (Kopieren, Ausdrucken, Sortieren u. ä.) garantiert,

— die kryptographische Verschlüsselung aller Daten auf externen Speichern, die nur im Rahmen der planmäßigen (menü-gesteuerten) Verarbeitung aufgehoben werden kann, und

— die maschinelle Protokollierung (logging) der Systemaktivitäten.

Damit ist es praktisch ausgeschlossen, daß auf Dateien, die zu einem DV-Verfahren gehören, andere als die zugelassenen Programme angewandt werden. So wird auch gewährleistet, zugelassene aber kritische Verarbeitungen durch Protokolle nachweisbar und kontrollierbar zu machen.

Werden für personenbezogene Anwendungen andere, insbesondere weniger strikt wirkende Maßnahmen getroffen, so ist durch ergänzende organisatorische Regelungen und Kontrollen sicherzustellen, daß Datenschutzvorschriften nicht verletzt werden. Bleiben die getroffenen Maßnahmen hinter den nach §§ 6, 15 BDSG erforderlichen zurück, so ist dieser Rechtsverstoß zu beanstanden.

Ergänzend sollte jeder PC-Einsatz begleitet werden durch

— Schulung in allgemeinen Datenschutzfragen, zumindest im Rahmen der Einweisung in die PC-Benutzung,

— Unterrichtung über generell durchzuführende Sicherungsmaßnahmen,

— Hinweise auf die verfahrensabhängigen, besonderen Datenschutzprobleme und Datensicherungsmaßnahmen auch für den Einsatz von Standardsoftware,

— Benennung eines leicht erreichbaren Ansprechpartners für alle beim Betrieb auftretenden Fragen des Datenschutzes und der Datensicherung,

— Kontrollen, die je nach Art der Anwendung mehr oder minder häufig sicherstellen, daß die Vorgaben in der Praxis auch eingehalten werden.

16.3.3 Datenschutzrechtliche Überlegungen vor der Anschaffung und dem Einsatz von PC

Ein besonderes Charakteristikum von PC ist es, daß trotz der möglichen Sicherung erhöhte datenschutzrechtliche Risiken bestehen bleiben. Dazu gehören z. B. die erhöhte Verfügbarkeit, die schnellere Auswertbarkeit und die prinzipiell uneingeschränkte Verknüpfbarkeit aller gespeicherten Daten, und zwar unter Bedingungen, die immer weniger spezielles Wissen über Datenverarbeitung voraussetzen. Deshalb sollten diese Risiken, die grundsätzlich für jeden Einsatz von PC gelten, gegen die zu erwartenden Vorteile abgewogen werden, und zwar bevor über die Anschaffung und den Einsatz von PC entschieden wird.

Das Bundesdatenschutzgesetz fordert in den §§ 6 und 15 organisatorische und technische Maßnahmen, die sich am Schutzbedarf der Daten je nach Anwendung orientieren und unter Berücksichtigung von Aufwand, Wirtschaftlichkeit und Vorteilen für die speichernde Stelle angemessene Sicherheit gewährleisten. Diese im BDSG für Datensicherungsmaßnahmen vorgeschriebene Abwägung, die dem Verhältnismäßigkeitsprinzip entspricht, sollte bereits die Entscheidung über die zur Erfüllung einer Aufgabe einzusetzende Technik bestimmen. Schon in der konzeptionellen Phase, also vor Installation eines PC, sollten deshalb neben den üblichen Wirtschaftlichkeitsüberlegungen auch die verbleibenden datenschutzrechtlichen Risiken in die Entscheidungsfindung mit einbezogen werden. Ich halte es für erwägenswert, eine spezielle Regelung zu schaffen, nach der vor Einführung neuer Datenverarbeitungstechniken und Organisationsformen, insbesondere vor dem Einsatz von PC, zu prüfen und zu dokumentieren ist, inwieweit deren Einführung nicht nur wirtschaftlich, sondern in diesem Sinne auch datenschutzrechtlich sinnvoll und vertretbar ist. Nur bei Beachtung dieser an sich üblichen Organisationsgrundsätze kann bei Wahrung des Verhältnismäßigkeitsprinzips vermieden werden, daß ein PC angeschafft wird, dessen Einsatz unangemessen wäre. Der Druck vollendeter Tatsachen, mit dem gerade im technisch-organisatorischen Bereich gern argumentiert wird, ließe sich damit vermeiden. Die Gründe für eine Entscheidung zum Einsatz eines PC sollten nach den oben genannten Prinzipien auch deshalb dokumentiert werden, damit eine spätere Prüfung möglich ist.

Im Hinblick auf die erheblichen Schwierigkeiten, akzeptable Einsatzbedingungen für PC bei der Verarbeitung sensibler Daten zu verwirklichen, habe ich die Mitteilung einer großen Berufsgenossenschaft und eines Krankenkassenverbandes mit Verständnis zur Kenntnis genommen, wonach diese auf den Einsatz von PC zur Verarbeitung von Sozialdaten wegen der besonderen Risiken vorerst verzichten wollen.

17. Novellierung des Bundesdatenschutzgesetzes und Gesetzgebung im Bereich der öffentlichen Sicherheit

Das von mir in fast allen zurückliegenden Tätigkeitsberichten behandelte und seit Verkündung des Volkszählungsurteils des Bundesverfassungsgerichts mit neuer Aktualität diskutierte Thema der Novellierung des BDSG beschäftigte mich intensiv auch in diesem Berichtsjahr. Am 24. Juni 1985 veranstaltete der Innenausschuß des Deutschen Bundestages zu dem von der SPD-Fraktion schon am 27. März 1984 eingebrachten Gesetzentwurf zur Änderung des BDSG (Drucksache 10/1180) eine öffentliche Anhörung, zu der ich als Sachverständiger eingeladen war. Die mir und den anderen Sachverständigen gestellten zahlreichen Fragen gingen über den Regelungsinhalt des SPD-Gesetzentwurfs weit hinaus und betrafen allgemein Umfang und Möglichkeiten der Umsetzung der verfassungsrechtlichen Grundsätze des Volkszählungsurteils in das BDSG. Ich habe im wesentlichen die Positionen vertreten, die ich bereits in meinem Siebenten Tätigkeitsbericht S. 87 ff. dargestellt habe.

Im Laufe des Berichtsjahres hat eine aus Mitgliedern der Fraktionen der CDU/CSU und der FDP zusammengesetzte Arbeitsgruppe einen eigenen Gesetzentwurf zur Änderung des BDSG und des Verwaltungsverfahrensgesetzes erarbeitet. Ich hatte Gelegenheit, mich in einer bestimmten Arbeitsphase zu den Vorstellungen und Teilergebnissen dieses Gremiums kritisch, aber auch mit Gegenvorschlägen zu äußern. Der schließlich als Ergebnis dieser Arbeiten zustandegekommene Gesetzentwurf ist der Öffentlichkeit bei Abfassung dieses Berichts noch nicht vorgelegt worden. Bei diesem Sachstand halte ich es für angemessen, hier auf eine umfassende Stellungnahme zu dem noch internen Entwurf zu verzichten. Auf einige wenige allgemeine Aspekte, die auch schon Gegenstand von Pressemeldungen waren, kann ich jedoch eingehen, ohne die Vertraulichkeit des Entwurfs zu verletzen.

Positiv bewerte ich u. a., daß Regelungen auch für die Datenverwendung vorgesehen sind und dabei die vom Bundesverfassungsgericht geforderte Zweckbindung personenbezogener Daten ausdrücklich festgelegt wird. Die Voraussetzungen für zweckfremde Verwendungen sollen eng begrenzt und im einzelnen definiert werden.

Vorgesehen sind ferner ein verschuldensunabhängiger Schadensersatzanspruch bei rechtswidriger automatischer Datenverarbeitung, Regelungen über die Einrichtung automatisierter Abrufverfahren (online), ferner die Unentgeltlichkeit der Auskunft an den Betroffenen sowie ihre Ausdehnung auf Herkunft und Empfänger der Daten und den Zweck der Speicherung. Beabsichtigt ist auch eine Änderung der Löschungsvorschriften in dem Sinne, daß die Löschung der für die Aufgabenerfüllung bzw. den Speicherungszweck nicht mehr erforderlichen Daten zum Regelfall, die Sperrung zur Ausnahme wird. Dies sind Gesetzesänderungen, die ich seit langem fordere.

Zu kritisieren ist indessen vor allem, daß der Entwurf zur Änderung des BDSG stärker als das geltende Recht nur noch die Datenverarbeitung in Dateien umfaßt, was auch in der Bezeichnung und in der Zieldefinition des Gesetzes zum Ausdruck kommt. Zwar werden durch Änderungen des Verwaltungsverfahrensgesetzes auch Datenschutzvorschriften für die Informationsverarbeitung außerhalb von Dateien geschaffen. Abgesehen von diesem m. E. rechtssystematisch verfehlten Ansatz, sind diese Vorschriften jedoch unzureichend, erfassen große Verwaltungsbereiche — wie die Finanzverwaltung, die Benutzung der Einrichtungen des Post- und Fernmeldewesens, die Strafverfolgung sowie die Verfolgung und Ahndung von Ordnungswidrigkeiten sowie Teilbereiche der Sozialverwaltung — nicht und entziehen sich, obwohl sie Sondervorschriften über den Datenschutz sind, der Datenschutzkontrolle, soweit die Bestimmungen des BDSG nichts Gegenteiliges vorsehen.

Die Datenerhebung beim Betroffenen als der erste und die weitere Datenverarbeitung einleitende und bedingende Schritt, der den wichtigsten Eingriff in die Rechtsposition des Betroffenen darstellt und an den das Bundesverfassungsgericht im Volkszählungsurteil deshalb wesentliche rechtliche Konsequenzen geknüpft hat, soll im BDSG überhaupt nicht mehr geregelt werden, sondern (abgesehen von bereichsspezifischen Vorschriften) in allgemeiner Form nur noch im Verwaltungsverfahrensgesetz mit seinem — wie erwähnt — begrenzten Geltungsbereich.

Unbefriedigend ist auch die Beibehaltung des generellen Auskunftsverweigerungsrechts der Nachrichtendienste ohne eine Abwägungspflicht zwischen schutzwürdigen Belangen des Betroffenen und Geheimhaltungsinteressen, wie sie für Staatsanwaltschaft und Polizei gelten soll. Zwar ist nunmehr vorgesehen, daß im Falle der Verweigerung der Auskunft diese auf Verlangen des Betroffenen dem Bundesbeauftragten für den Datenschutz zu erteilen ist, doch bedeutet dies keine wirkliche Verbesserung der Position des Betroffenen, weil in der gegenwärtigen Praxis bereits so verfahren wird.

In dieser ersten Stellungnahme möchte ich auch nicht verschweigen, daß mich die Neuregelung der Kontrollbefugnisse des Bundesbeauftragten nicht befriedigen kann. Ich begrüße zwar die von mir seit langem geforderte Klarstellung, daß Geheimhaltungsvorschriften meinem Auskunfts- und Einsichtsrecht nicht entgegenstehen. Unbefriedigend ist jedoch, daß eine systematische Kontrolle von Datenschutzvorschriften ausgeschlossen werden soll, soweit diese die Datenverarbeitung außerhalb von Dateien regeln — als Beispiel nenne ich die Offenbarungsbefugnisse und -verbote im SGB X. Daß in diesen Fällen eine Einzelfallkontrolle ermöglicht wird, wenn hinreichende Anhaltspunkte für eine Rechtsverletzung bestehen oder vom Betroffenen dargetan werden, kann zwar für den einzelnen Betroffenen hilfreich sein; eine solche Regelung kann sich jedoch auch als hinderlich erweisen,

generelle Verbesserungen des Datenschutzes bei einer Behörde durchzusetzen. Auch fürchte ich, daß Konflikte über den Umfang einer Einzelfallkontrolle oder über die häufig unscharfen Grenzen zwischen Datenverarbeitung in und außerhalb von Dateien nicht ausbleiben werden.

Ich hoffe, daß der Gesetzentwurf zur Änderung des BDSG von den Fraktionen der CDU/CSU und der FDP in Kürze im Parlament eingebracht und mir damit eine eingehende Prüfung des Gesetzgebungsvorhabens ermöglicht wird. Ich gehe davon aus, daß ich im Laufe des Gesetzgebungsverfahrens Gelegenheit haben werde, ausführlich dazu Stellung zu nehmen. Gleiches gilt für die von den Koalitionsfraktionen angekündigten Gesetzentwürfe zur Neuregelung der Aufgaben und Tätigkeiten der Sicherheitsbehörden (siehe dazu oben Nr. 11.2) und zur Änderung des Straßenverkehrsgesetzes (siehe dazu oben Nr. 7.1).

18. Ausland und Internationales

18.1 Europarat

Das Ministerkomitee des Europarats hat zwei vom Expertenkomitee für Datenschutz ausgearbeitete Empfehlungen beschlossen: Die Empfehlung über den Datenschutz im Bereich der sozialen Sicherheit und die Empfehlung über den Datenschutz beim Direktmarketing (siehe dazu Anlage 6).

18.2 Zusammenarbeit der Datenschutz-Kontrollinstanzen

Die internationale Konferenz der Datenschutz-Kontrollinstanzen widmete ihre Tagung im September 1985 in Luxemburg verschiedenen Themen, die Schwerpunkte in der Kontroll-Praxis bilden, so etwa dem Gesundheitswesen, der wissenschaftlichen Forschung und der Speicherung und Erschließung personenbezogener Angaben bei der Dokumentation von Gerichtsentscheidungen (Datenschutz im Verhältnis zu den Grundsätzen der Öffentlichkeit des Gerichtsverfahrens und der Pressefreiheit).

Zur Frage, wie der Datenschutz auf die sich verändernde Datenverarbeitungstechnik reagieren muß, trug die deutsche Delegation ein Referat über Personal-Computer bei. Zur polizeilichen Datenverarbeitung, die die Konferenz schon seit längerem beschäftigt, wurde eine Entschließung gefaßt (siehe dazu Anlage 4).

19. Bilanz

In meinem Siebenten Tätigkeitsbericht konnte ich sowohl über eine Reihe von erfolgversprechenden Entwicklungen berichten wie auch darüber, daß sich für andere Probleme noch keine Lösungen abzeichneten. Die nachfolgende Aufstellung zeigt, daß die Bemühungen, gemeinsam mit den datenverarbeitenden Stellen und den zuständigen obersten Bundesbehörden tragbare Ergebnisse zu erarbeiten, überwiegend erfolgreich waren. In einigen Bereichen stehen endgültige Lösungen auch noch aus, aber nur in wenigen Bereichen stehen sich unverändert gegensätzliche Rechtsansichten gegenüber.

1. Die notwendigen Änderungen im Personalausweisgesetz habe ich erläutert (7. TB S. 8). In den Diskussionen darüber wurden Verbesserungen in einzelnen Bereichen erreicht; in einer Reihe von Punkten ist eine abschließende Antwort auf meine Empfehlungen aber noch nicht erfolgt, siehe dazu auch Nr. 2.1 in diesem Bericht.

2. Über die erreichte Verbesserung der Dienstanweisung für die Standesbeamten und ihre Aufsichtsbehörden (DA) hinaus habe ich an die Neuordnung der rechtlichen Grundlagen für die Mitteilungen im Personenstandswesen erinnert (7. TB S. 11). Interne Überlegungen auch im zuständigen Arbeitskreis des Bundes und der Länder haben noch nicht zu einer Entwurfsvorlage geführt.

3. Auf die Notwendigkeit, Datenerhebung und Datenschutz auch im Waffengesetz ausdrücklich zu regeln, habe ich hingewiesen (7. TB S. 11 f.). Der Bundesminister des Innern hat den Entwurf eines Dritten Gesetzes zur Änderung des Waffengesetzes um eine entsprechende Vorschrift ergänzt, deren endgültige Fassung noch zu diskutieren ist.

4. Über einige Problempunkte bei der Datenverarbeitung des Bundeszentralregisters habe ich berichtet (7. TB S. 12 f.). Die angekündigte Nachprüfung hat zu positiven Ergebnissen geführt, siehe dazu Nr. 3.1 in diesem Bericht.

   Meine Vorschläge zur Novellierung des Bundeszentralregistergesetzes, zu der auch der Deutsche Bundestag unter Nr. II.2 seines Beschlusses zu meinem Fünften Tätigkeitsbericht Stellung genommen hat, konnte ich im Rahmen der im Bundesjustizministerium anlaufenden Vorarbeiten zum Dritten BZRG-Änderungsgesetz erläutern und aktualisieren.

5. Im Hinblick auf die notwendige Neufassung der Anordnung über Mitteilungen in Strafsachen habe ich auf eine Reihe von Problemen hingewiesen (7. TB S. 14). Entsprechend dem Ersuchen des Deutschen Bundestages unter Nr. II.3 seines Beschlusses zu meinem Fünften Tätigkeitsbericht hat der Bundesminister der Justiz in Aussicht gestellt, in der ersten Hälfte des Jahres 1986 einen Referentenentwurf zu versenden. Dieser Entwurf soll auch eine Regelung der Mitteilungen in Zivilsachen enthalten, siehe dazu Nr. 3.2 in diesem Bericht.

6. Die für das Schuldnerverzeichnis gebotenen Verbesserungen, insbesondere bei den Übermittlungsregelungen und der Information der Betroffenen, habe ich angemahnt (7. TB S. 15 f.). Zu dem inzwischen vorliegenden Referentenentwurf habe ich empfohlen, den Datenschutz noch mehr zu berücksichtigen, siehe dazu Nr. 3.3 in diesem Bericht.

7. Über das Steuerbereinigungsgesetz und die darin enthaltenen Ansätze zur Verbesserung des Datenschutzes habe ich berichtet (7. TB S. 16). Im Berichtsjahr wurden auch die zunächst zurückgestellten Teile im Steuerbereinigungsgesetz 1986 beschlossen, womit auch den Vorstellungen des Deutschen Bundestages unter Nr. II.6 seines Beschlusses zu meinem Fünften Tätigkeitsbericht entsprochen wurde.

8. Auf die Notwendigkeit, den Datenschutz in der Verwaltung des Deutschen Bundestages zu verbessern, habe ich hingewiesen (7. TB S. 17). In einigen wesentlichen Punkten wurden Verbesserungen erreicht oder sie sind eingeleitet; die beabsichtigte Fortsetzung der Prüfung mußte aus Kapazitätsgründen verschoben werden.

9. Auf die Notwendigkeit, den Datenschutz für Arbeitnehmer besonders zu regeln, habe ich hingewiesen (7. TB S. 17 f.). Entsprechend dem Ersuchen des Deutschen Bundestages unter Nr. II.13 seines Beschlusses zu meinem Fünften Tätigkeitsbericht hat die Bundesregierung erklärt, daß sie eine gesetzliche Regelung für erforderlich hält und die Arbeit daran aufgenommen hat, siehe dazu Nr. 5.2.4 in diesem Bericht.

10. Zu Verbesserungen bei der Verarbeitung von Daten über dienstliche und private Ferngespräche der Beschäftigten habe ich Vorschläge gemacht (7. TB S. 19 f.), die sich an der auch vom Deutschen Bundestag in seinem Beschluß zu meinem Fünften Tätigkeitsbericht unter Nr. II.8 besonders herausgestellten Erforderlichkeit orientieren. Der Bundesminister der Finanzen hat den Entwurf neuer Dienstanschlußvorschriften vorgelegt, der zur Zeit diskutiert wird.

11. Unter Nr. II.7 seines Beschlusses zu meinem Fünften Tätigkeitsbericht hat der Deutsche Bundestag die Bundesregierung ersucht, zu prüfen, ob eine umfassende Regelung des Personalaktenrechts notwendig ist, und welche Informationen in Personalakten unbedingt aufzunehmen sind. Über meine Beteiligung an einer interministeriellen Arbeitsgruppe zur Neuregelung des Personalaktenrechts habe ich berichtet (7. TB S. 20). Im Berichtsjahr hat keine Sitzung dieser Arbeitsgruppe stattgefunden.

12. Über meine Empfehlungen zur Registrierung und Bekanntgabe von Telefonverbindungsdaten, die auch der Ausschuß für das Post- und Fernmeldewesen des Deutschen Bundestages zustimmend zur Kenntnis genommen hat, habe ich berichtet (7. TB S. 23). Die DBP hat einige dieser Grundsätze bisher noch nicht angewandt und dabei darauf hingewiesen, daß ein Votum des Innenausschusses noch aussteht, siehe auch Nr. 6.6 in diesem Bericht.

13. Unter Nr. II.9 seines Beschlusses zu meinem Fünften Tätigkeitsbericht hat der Deutsche Bundestag die Bundesregierung ersucht, „auf eine Änderung des Antragsformulars auf Fernmeldehauptanschlüsse dahingehend hinzuwirken, daß jeder Antragsteller sich eindeutig dazu erklären muß, ob er mit einer Weitergabe seiner Anschrift und Berufsangabe zu Werbezwecken an die Deutsche Postreklame einverstanden ist oder nicht und nicht mehr wie bisher von einem Einverständnis dann ausgegangen wird, wenn keine Angabe erfolgt."

    Der BMP hat mit mir inzwischen den Entwurf eines neuen Formulars erörtert. Es enthält zwar Verbesserungen, trägt jedoch bislang der zitierten Empfehlung des Bundestages, die meinen Vorschlägen entspricht, nicht Rechnung, siehe dazu auch Nr. 6.7 in diesem Bericht.

14. Auf offene Probleme des Datenschutzes beim Bildschirmtext-Dienst der DBP habe ich hingewiesen (7. TB S. 24 f.). In einigen Fragen zeichnen sich Verbesserungen ab, für andere Bereiche ist eine datenschutzgerechte Lösung noch nicht gefunden, siehe dazu Nr. 6.2 in diesem Bericht.

15. Hinsichtlich der Datenschutzprobleme beim Funkfernsprechdienst (Autotelefon) habe ich die Erwartung ausgesprochen, daß bei der Konzipierung künftiger Netze der Datenschutz stärker berücksichtigt wird (7. TB S. 25 f.). Nach meinen bisherigen Informationen hat die DBP aber meinen Bedenken auch bei der Gestaltung des neuen Funkfernsprechnetzes C nicht Rechnung getragen.

16. Über Datenschutzfragen beim Telefon-Fernwirkdienst TEMEX habe ich berichtet (7. TB S. 26). Der Dialog mit dem BMP ist auf diesem Gebiet gut, siehe dazu Nr. 6.3 in diesem Bericht.

17. Gegen die Übermittlung von Daten der Kraftfahrzeug-Halter vom Kraftfahrt-Bundesamt (KBA) an den Funkkontrollmeßdienst der Deutschen Bundespost habe ich Bedenken angemeldet (7. TB S. 30 f.). Die beteiligten Stellen haben auf die Übermittlung verzichtet.

18. Die vom KBA praktizierte Speicherung und Auskunftserteilung, z. B. über die Erteilung von Fahrerlaubnissen nach vorangegangener Versagung oder Entziehung, habe ich beanstandet, weil dafür die gesetzliche Grundlage fehlt (7. TB S. 31 f.). Der Bundesminister für Verkehr (BMV) hält an der beanstandeten Praxis fest und hat für die angekündigte Neuregelung noch keinen Entwurf vorgelegt. Entsprechendes gilt für meine Empfehlung, die Eintragung in das Verkehrszentralregister wegen Versagung der Fahrerlaubnis einzuschränken (7. TB S. 31).

19. Von den Erörterungen der Behandlung der Meldungen über die Entziehung von Sonderfahrerlaubnissen habe ich berichtet (7. TB S. 32). Der BMV hat im Berichtsjahr eine Änderungsverordnung zur StVZO erlassen, die meinen Bedenken Rechnung trägt.

20. Auf die Notwendigkeit, den Entwurf eines neuen Verkehrszentralregistergesetzes bald vorzulegen, habe ich hingewiesen (7. TB S. 33). Damit hätte auch dem Ersuchen des Deutschen Bundestages unter Nr. II.10 seines Beschlusses zu meinem Fünften Tätigkeitsbericht Rechnung

getragen werden können, die Eintragung, die Auskunftserteilung und die Fristen für die Tilgung am zwingend erforderlichen Rahmen zu orientieren. Die Vorlage des angekündigten Entwurfs ist jedoch noch nicht erfolgt.

21. Gegen die Speicherung von Angaben über Beruf und Gewerbe der Halter von Kraftfahrzeugen habe ich erneut Bedenken geltend gemacht, weil diese Speicherung zur Erreichung des angegebenen Zweckes besonders bei Nichtselbständigen ungeeignet ist (7. TB S. 34). Der BMV hat inzwischen das KBA angewiesen, bis zu einer gesetzlichen Regelung diese Angaben nur noch für Selbständige zu speichern. Über die Modalitäten der Löschung der noch bestehenden Speicherungen über Nichtselbständige ist noch nicht entschieden.

22. Auf das Fehlen von Rechtsgrundlagen für die Datenverarbeitung des Luftfahrt-Bundesamtes habe ich hingewiesen (7. TB S. 36). Der BMV hat anerkannt, daß Rechtsgrundlagen geschaffen werden müssen; Entwürfe dazu sind mir noch nicht bekannt.

23. Auf die Notwendigkeit, das neue Volkszählungsgesetz möglichst datenschutzgerecht zu gestalten, habe ich hingewiesen (7. TB S. 38 f.). Das vom Deutschen Bundestag verabschiedete Gesetz berücksichtigt den Datenschutz in allen wesentlichen Punkten, siehe dazu Nr. 9.1 in diesem Bericht.

24. Im Zusammenhang mit der Beanstandung organisatorischer Mängel beim Versand von Datenträgern durch das Statistische Bundesamt habe ich die Überarbeitung des Sicherheitskonzepts dieser Behörde angemahnt (7. TB S. 40). Die Mängel beim Datenträgerversand wurden vollständig behoben, die erforderliche Gesamtlösung steht aber noch aus.

25. Unter Nr. II.14 seines Beschlusses zu meinem Fünften Tätigkeitsbericht hat der Deutsche Bundestag die Bundesregierung ersucht, einen Gesetzentwurf über die Verwendung der Rentenversicherungsnummer vorzulegen. Über die Notwendigkeit, diese Verwendung nur eng begrenzt zuzulassen, habe ich berichtet (7. TB S. 40). Nach Besprechungen mit dem Bundesminister für Arbeit und Sozialordnung über eine gesetzliche Regelung liegt mir seit kurzem eine Entwurfsfassung vor, siehe dazu Nr. 10.3 in diesem Bericht.

26. Die überlange Aufbewahrungszeit für ärztliche Gutachten in der Arbeitsverwaltung hatte ich beanstandet (7. TB S. 41 f.). Die angekündigte generelle Regelung ist durch die Bundesanstalt für Arbeit inzwischen getroffen worden, siehe dazu Nr. 10.4 in diesem Bericht.

27. Über die Notwendigkeit der Bereinigung von Altfällen in allen Dateien der Sicherheitsbehörden, die auch der Deutsche Bundestag in seinem Beschluß zu meinem Fünften Tätigkeitsbericht unter Nr. II.19.1 als dringend herausgestellt hat, habe ich berichtet (7. TB S. 62). Die Löschung der Altfälle bei den Sicherheitsbehörden hat weitere Fortschritte gemacht, ist aber noch nicht abgeschlossen.

28. Auf die Datenschutzprobleme bei der internationalen Zusammenarbeit der Sicherheitsbehörden und meine Mitarbeit an ihrer Lösung habe ich hingewiesen (7. TB S. 63 f.). Im Berichtsjahr habe ich u. a. zu den Plänen, auch durch internationale Fahndungsmaßnahmen einen Ausgleich für den Wegfall von Grenzkontrollen zu schaffen, Stellung genommen, siehe dazu Nr. 11.4.1 in diesem Bericht.

29. Auf die Notwendigkeit, bei der Sicherheitsüberprüfung die Datenschutzrechte der Betroffenen zu wahren, habe ich hingewiesen (7. TB S. 64 f.). Die angekündigte Kontrolle hat im Berichtsjahr begonnen, sie wird 1986 fortgesetzt. Möglicherweise ergeben sich aus ihr weitere Erkenntnisse für die Neugestaltung der Richtlinien.

30. Gegen die ausgedehnte Speicherung von personenbezogenen Daten im „Forensischen Informationssystem Handschriften (FISH)" habe ich Bedenken geäußert (7. TB S. 68). Die Speicherung von Daten über Geschädigte erfolgt nun nicht mehr; in anderen wichtigen Punkten, wie z. B. der Berücksichtigung von Vorschriften über erkennungsdienstliche Unterlagen, ist ein datenschutzgerechtes Ergebnis bisher nicht erzielt worden.

31. Über bessere Regelungen für die Übermittlungen des Bundeskriminalamtes an Interpol habe ich berichtet (7. TB S. 71). Die angekündigte Prüfung der Praxis hat gezeigt, daß hier weiterer Verbesserungsbedarf besteht, siehe dazu Nr. 11.1.1 in diesem Bericht.

32. Datenschutzrechtliche Bedenken zu einigen Punkten beim Grenzaktennachweis, insbesondere zur Speicherung personengebundener Hinweise, habe ich erläutert (7. TB S. 71 f.). Im Rahmen einer Prüfung des Grenzaktennachweises hat der Bundesminister des Innern mitgeteilt, daß in Zukunft hier keine personengebundenen Hinweise mehr gespeichert werden; zu weiteren Ergebnissen siehe Nr. 11.1.2 in diesem Bericht.

33. Über die bevorstehende Beendigung des unzulässigen Online-Zugriffs der Polizei auf Daten der zollrechtlichen Überwachung habe ich berichtet (7. TB S. 72 f.). Diese Frage hatte der Deutsche Bundestag unter Nr. II.19.5 seines Beschlusses zu meinem Fünften Tätigkeitsbericht aufgegriffen. Die Zugriffsmöglichkeit ist inzwischen aufgehoben; meine Kontrollkompetenz in diesem Bereich wird jedoch nach wie vor bestritten, siehe dazu Nr. 11.2 in diesem Bericht.

34. Auf die Notwendigkeit, beim Bundesamt für Verfassungsschutz die Speicherung bestimmter Daten, die nicht erforderlich sind und die Intimsphäre der Betroffenen berühren, einzustellen, habe ich hingewiesen (7. TB S. 76). Meine Bemühungen haben erste Verbesserungen gebracht, sind aber noch nicht abgeschlossen, siehe dazu Nr. 13.1.1 in diesem Bericht.

35. Über Verbesserungsvorschläge für die Datenübermittlung vom Bundesamt für den Verfassungsschutz an ausländische Dienststellen habe ich berichtet (7. TB S. 77). In den Diskussionen mit den zuständigen Stellen konnten Regelungen erreicht werden, die dem Datenschutz stärker Rechnung tragen, siehe dazu Nr. 11.1.3 in diesem Bericht.

36. Die Notwendigkeit, die weitere Verarbeitung der im Rahmen der Post- und Fernmeldekontrolle durch den Bundesnachrichtendienst gewonnenen personenbezogenen Daten zu kontrollieren, habe ich erläutert (7. TB S. 79 f.). Eine Prüfung konnte ich in diesem Berichtsjahr noch nicht durchführen.

37. Die Abgrenzungs- und Verfahrensprobleme bei der personellen Vorbeugung durch den Militärischen Abschirmdienst (MAD) habe ich erläutert (7. TB S. 81 f.). Im Berichtsjahr konnte eine zufriedenstellende Regelung erreicht werden, siehe dazu Nr. 13.2.1 in diesem Bericht.

38. Unter Nr. II.18 seines Beschlusses zu meinem Fünften Tätigkeitsbericht hat der Deutsche Bundestag meine Bemühungen um eine datenschutzgerechte Lösung für die Erteilung von Bankauskünften unterstützt. Über die neue Regelung habe ich berichtet (7. TB S. 83). Sie hat sich im Berichtsjahr voll bewährt. Zum verwandten Problem der SCHUFA-Klausel siehe Nr. 15.1 in diesem Bericht.

39. Unter Nr. II.20 seines Beschlusses zu meinem Fünften Tätigkeitsbericht hat der Deutsche Bundestag die Bundesregierung ersucht, zur Praxis von Vermietern, Mietinteressenten die Beantwortung von Fragebögen über ihre persönlichen und wirtschaftlichen Verhältnisse abzuverlangen, eine gesetzliche Regelung herbeizuführen, die den datenschutzrechtlichen Bedenken Rechnung trägt. Über voraussichtlich wenig wirksame Anregungen und Empfehlungen, bestimmte Fragen nicht mehr zu stellen, habe ich berichtet (7. TB S. 84 f.). Ein Gesetzentwurf ist bisher nicht vorgelegt worden.

40. Über die bevorstehende Ratifikation der Datenschutz-Konvention des Europarates, habe ich berichtet (7. TB S. 94). Nachdem im Berichtsjahr das Ratifikationsgesetz verabschiedet wurde, trat die Konvention am 1. Oktober 1985 in Kraft.

Anlage 1 (Zu Nr. 10.6.2)

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 10. Mai 1985 zum Datenschutz bei der Perinataldokumentation

Die Konferenz der Datenschutzbeauftragten hält folgendes Verfahren für notwendig, um den Datenschutz bei der bundesweit durchgeführten Perinatalstudie zu gewährleisten:

1. Die Verarbeitung von Patientendaten für die Perinatalstudie erfolgt bei der Kassenärztlichen Vereinigung/Ärztekammer (je nach Land unterschiedlich) im Auftrag der beteiligten Klinik.

   Sie geschieht nach Weisung der auftraggebenden Klinik. Die Daten dürfen nur im Rahmen der Zweckbestimmung der Perinatalstudie verwendet und verarbeitet werden. Eine Verknüpfung mit anderen Datenbeständen der auftragnehmenden Kassenärztlichen Vereinigung/Ärztekammer ist (vertraglich) auszuschließen.

   Die Auftragnehmerin hat in einem Datensicherungskonzept darzulegen, auf welche Weise die perinatologischen Daten von den übrigen Datenbeständen in technischer und organisatorischer Hinsicht getrennt gespeichert und verarbeitet werden.
2. Grundsätzlich dürfen an andere als die jeweils auftraggebende Klinik nur aggregierte Daten bzw. anonymisierte Mikrodatensätze weitergegeben werden. Die Regelauswertung ist die klinikspezifische Statistik und die Übersichtsstatistik ohne personenbezogene Einzelangaben von Patienten bzw. Kindern.
3. Im Hinblick auf die Gestaltung bzw. Ausfüllung des Erhebungsbogens wird empfohlen:
   3.1 die Geburtsnummer (Zeile 1 des Erhebungsbogens) nach Abschluß der maschinellen Plausibilitätsprüfung zu löschen,
   3.2 nur die beiden ersten Stellen der Postleitzahl (Zeile 3) zu erheben,
   3.3 für die Nationalität (Zeile 4) und für die Schulbildung (Zeile 5) Zusammenfassungen in größeren Gruppen vorzunehmen,
   3.4 auf die spezifizierte Benennung des Berufs des Ernährers (Zeile 8) zu verzichten und statt dessen eine Gruppenklassifikation vorzunehmen,
   3.5 die Entbindungseinrichtungen/Kliniken darauf hinzuweisen, daß Freitextangaben in den letzten Zeilen des Vordrucks nicht an die auftragnehmenden Stellen KV/ÄK übermittelt werden dürfen.
4. Es bestehen grundsätzlich keine Bedenken gegen eine Weiterverwendung der bereits gedruckten Formulare, wenn die Ausfüllanleitung entsprechend der Punkte zu Ziffer 3. verändert wird. Die Konferenz der Datenschutzbeauftragten behält sich vor, die Empfehlung nach konkreten Prüfungserfahrungen entsprechend zu modifizieren.

Anlage 2 (zu Nrn. 11.2 und 11.4.1)

Anforderungen an Datenschutzregelungen im Polizeirecht

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. Januar 1985

I. Notwendigkeit bereichsspezifischer Regelungen

1. Die Datenschutzbeauftragten des Bundes und der Länder haben seit Jahren auf die Notwendigkeit präziser gesetzlicher Regelungen für die Datenverarbeitung durch die Vollzugspolizei hingewiesen. Einzelne Maßnahmen wie z. B. die polizeiliche Beobachtung oder die Verarbeitung von Daten Unbeteiligter stehen weitgehend im Widerspruch zum geltenden Polizei- und Strafverfahrensrecht. Gesetzlich nicht hinreichend abgedeckt sind insbesondere die Erhebung und Nutzung personenbezogener Daten zu Zwecken der vorbeugenden Bekämpfung von Straftaten.

   Spätestens seit dem Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz ist eine bereichsspezifische Regelung der polizeilichen Informationsverarbeitung unerläßlich. Dabei kann es nicht darum gehen, die derzeitige, durch eine Ausweitung der Datenverarbeitung gekennzeichnete Praxis der Datenverarbeitung festzuschreiben, sie muß vielmehr überprüft und der Umfang zulässiger Informationsverarbeitung durch spezielle Befugnisnormen konkret bestimmt und begrenzt werden.

2. Eine solche Regelung muß zumindest die nachfolgenden Grundsätze beachten. Diese Grundsätze sollten — evtl. differenziert je nach spezifischer Aufgabenzuweisung — sowohl in den Polizeigesetzen des Bundes und der Länder als auch in der Strafprozeßordnung, soweit es um gleichartige Maßnahmen geht, berücksichtigt werden.

II. Grundsätze polizeilicher Informationsverarbeitung

1. Allgemeine Prinzipien

1.1

Die gesetzlichen Regelungen über die Informationsverarbeitung müssen die polizeilichen Befugnisse klar und rechtsstaatlich umschreiben. Dies bedeutet

- dem Gebot der Normenklarheit entsprechende Spezialregelung und damit die Zurückdrängung von Generalklauseln,
- Beachtung des Grundsatzes der Verhältnismäßigkeit,
- prinzipielle Beschränkung auf die Aufgaben Gefahrenabwehr und Strafverfolgung,
- Beachtung des Grundsatzes der Zweckbindung der Daten.

1.2

In Übereinstimmung mit dem vom Bundesverfassungsgericht anerkannten Recht auf informationelle Selbstbestimmung müssen die Regelungen jede Art und Form der Verarbeitung personenbezogener Daten durch die Polizei erfassen.

Sowohl die Erhebung als auch jede Nutzung von Daten sind in die Regelung mit einzubeziehen.

Die Form der Verarbeitung ist bei der Intensität der einzelnen Regelung zu berücksichtigen.

Die Speicherung personenbezogener Merkmale wie Krankheit oder besonderer Verhaltensweisen, insbesondere mit Hilfe automatischer Verfahren, ist nur zulässig, wenn die möglichen Verwendungen in einem angemessenen Verhältnis zu den Gefahren für die schutzwürdigen Belange der Betroffenen stehen. Durch die Automatisierung darf keine Verzerrung oder unangemessene Verkürzung des Sachverhalts entstehen.

2. Für die Datenverarbeitung sollten folgende Grundsätze Beachtung finden

2.1 Zum Erheben und Speichern personenbezogener Daten

2.1.1 Grundsätze

Die Verarbeitung von Daten muß grundsätzlich der Abwehr einer im einzelnen Fall bestehenden (konkreten) Gefahr oder der Aufklärung einer konkreten Straftat dienen.

- Eine darüber hinausgehende Verarbeitung kann nur in eng begrenzten Fällen zugelassen werden. Insbesondere bedürfen Befugnisse zur vorbeugenden Bekämpfung von Straftaten einer klaren abschließenden Umschreibung im Gesetz.
- Für die Erfüllung spezialgesetzlich zugewiesener Aufgaben stehen der Polizei nur die jeweiligen spezialgesetzlichen Befugnisse zu.
- Der Bürger muß — wie zuletzt auch das Bundesverfassungsgericht im Volkszählungs-Urteil festgestellt hat — grundsätzlich unbeobachtet von staatlichen Stellen an Versammlungen teilnehmen können. Bei Befugnissen zur Informationserhebung in Versammlungen ist stärker als in der bisherigen Praxis dem Grundrecht der Versammlungsfreiheit Rechnung zu tragen.

Werden personenbezogene Informationen in Dateien gespeichert, müssen die Herkunft und die Richtigkeit der Informationen in Akten oder anderen Unterlagen nachweisbar sein. Werden Bewertungen gespeichert, muß erkennbar sein, wer die Bewertung vorgenommen hat und wo die Erkenntnisse gespeichert sind, die ihnen zugrunde liegen.

2.1.2 Datenerhebung und -speicherung

— Die Gewinnung von Informationen muß grundsätzlich offen geschehen; heimliche Informationserhebung ist nur dann zulässig, wenn dies zur Aufgabenerfüllung im Einzelfall unerläßlich ist.

— Die Erhebung durch selbsttätige Lese- und Aufzeichnungsgeräte ist gesetzlich zu regeln.

— Bei Erhebung von Daten unter Mitwirkung des Betroffenen ist dieser in der Regel auf seine Aussage- oder Mitwirkungspflicht oder auf die Freiwilligkeit hinzuweisen.

— Werden heimlich erhobene Daten gespeichert, ist der Betroffene grundsätzlich nach Wegfall der Zweckgefährdung zu informieren.

— Die Anfertigung und Aufbewahrung erkennungsdienstlicher Unterlagen muß präziser und restriktiver geregelt werden. Vorschriften über die Anfertigung und Verarbeitung von erkennungsdienstlichen Unterlagen dürfen nicht durch neue technische Möglichkeiten umgangen werden (z. B. Überwachung bestimmter Orte durch Videogeräte, automatische Stimmerkennung).

— Die Übernahme der in Strafermittlungsverfahren erhobenen Informationen in Unterlagen für Zwecke der Gefahrenabwehr und vorbeugenden Bekämpfung von Straftaten ist an strenge Voraussetzungen zu knüpfen.

— Der Abgleich von oder mit Fremddatenbeständen darf künftig nur zur Abwehr erheblicher gegenwärtiger Gefahren sowie zur Aufklärung abschließend festgelegter schwerer Straftaten zugelassen werden. Die hierbei gewonnenen Daten müssen einer strengen Zweckbindung unterliegen. Voraussetzungen, Art und Umfang des Abgleichs, Verwertung und Dauer der Aufbewahrung sind im Gesetz abschließend zu regeln.

— Der Einsatz besonderer Verfahren, die über ein Aktenhinweissystem hinausgehen (z. B. Spurendokumentationsverfahren), bedarf einer gesetzlichen Regelung.

— Personenbezogene Daten dürfen grundsätzlich nur bei der sachbearbeitenden Dienststelle in kriminalpolizeilichen Sammlungen oder entsprechenden Dateien gespeichert werden. Die Speicherung dieser personenbezogenen Daten bei polizeilichen Zentralstellen ist nur aufgrund ausdrücklicher gesetzlicher Regelung zulässig.

— Erkenntnisfragen oder Bitten um Amtshilfe dürfen bei den angefragten Stellen grundsätzlich nicht zur Anlage kriminalpolizeilicher Personenakten oder -dateien führen. Gleiches muß für bloße Unterrichtungen gelten.

2.2 Übermittlung von Daten

2.2.1

Die zu polizeilichen Zwecken gewonnenen Daten sind grundsätzlich zweckgebunden zu verwerten.

2.2.2

Bei der Übermittlung an Polizeibehörden ist hinsichtlich Art und Inhalt nach der konkreten polizeilichen Funktion und Zuständigkeit zu unterscheiden. Die Datenübermittlung an zentrale Stellen ist restriktiv zu regeln; das gilt auch für Erkenntnisanfragen und deren Beantwortung.

2.2.3

Eine Übermittlung an andere als Polizeibehörden und sonstige öffentliche Stellen sowie an Privatpersonen ist nur im Einzelfall zulässig und nur

— zur Abwendung einer konkreten Gefahr, einer erheblichen sozialen Notlage oder

— zur Verfolgung von öffentlich-rechtlichen oder zivilrechtlichen Ansprüchen in Fällen von Beweisnot,

und nur, wenn hierfür eine ausdrückliche gesetzliche Regelung besteht. Bei Anfragen, deren Beantwortung in die Zuständigkeit anderer Stellen fällt, hat die Polizei grundsätzlich an diese Stellen zu verweisen. Die Vorschriften des Bundeszentralregistergesetzes dürfen nicht durch polizeiliche Auskunft unterlaufen werden.

Eine Datenübermittlung an Nachrichtendienste darf wegen der verfassungsrechtlich gebotenen Trennung von polizeilicher und nachrichtendienstlicher Tätigkeit entgegen der derzeitigen Praxis nur in engen Grenzen zugelassen werden. Ein geeigneter Maßstab sind die Übermittlungsregelungen nach dem Gesetz zu Art. 10 GG.

Bei der Übermittlung an ausländische Stellen ist durch geeignete Absprachen und durch die Vereinbarung internationaler Regelungen sicherzustellen, daß die innerstaatlichen Grundsätze des Datenschutzes nicht gefährdet werden.

2.2.4

Vor jeder Übermittlung hat die auskunftgebende Stelle grundsätzlich die Richtigkeit der vorhandenen Unterlagen und deren Erforderlichkeit für die eigene Aufgabenerfüllung zu überprüfen. Wenn ein Verfahren noch nicht abgeschlossen ist, ist darauf hinzuweisen. Eine Übermittlung hat zu unterbleiben, wenn die Unterlagen zu vernichten sind.

2.2.5

Tatsache und Inhalt der Übermittlung sind in der Akte festzuhalten. Bei Veränderung wesentlicher

Gesichtspunkte (z. B. Löschung) hat die übermittelnde Stelle die Änderung nachzuberichten, soweit dadurch nicht schutzwürdige Belange des Betroffenen beeinträchtigt werden.

2.3 Löschungs- und Überprüfungsvorschriften

Für die Aufbewahrung der Daten muß der Gesetzgeber differenziert Löschungs- und Überprüfungsvorschriften gesetzlich vorsehen. Insbesondere ist zu unterscheiden

— nach Alter des Betroffenen,

— nach der Schwere der Gefahr und der Straftat,

— nach der Art der Tatbegehung,

— nach der Art der Daten,

— nach dem Ausgang des Verfahrens.

Die gegenwärtig praktizierten Regelfristen (für Kinder 2 Jahre, für Jugendliche 5 Jahre, für Erwachsene 10 Jahre) dürfen nicht verlängert werden.

Daten, die allein zur Personenfeststellung erhoben wurden, sind unmittelbar nach Zweckerreichung zu vernichten.

2.4 Transparenz

Entsprechend der verfassungsmäßigen Garantie des Rechtsweges (Art. 19 Abs. 4 GG) hat der einzelne grundsätzlich ein Recht auf vollständige Auskunft. Dieses umschließt

— die zu seiner Person gespeicherten Informationen,

— Zweck, Rechtsgrundlage und vorgesehene Dauer der Speicherung,

— Art der Gewinnung oder Herkunft der Informationen,

— die Tatsache und den Inhalt der Übermittlung an andere Stellen.

Ausnahmen hiervon sollten nur dann zulässig sein, wenn hierdurch die Erfüllung polizeilicher oder anderer Sicherheitsaufgaben gefährdet oder erheblich erschwert wird, überwiegende Interessen Dritter entgegenstehen oder die Erfüllung des Auskunftsanspruchs nur mit unverhältnismäßigem Aufwand möglich wäre.

Die Bearbeitung von Auskunftsersuchen muß getrennt von polizeilichen Informationssammlungen erfolgen. Die Tatsache der Antragstellung darf nicht zum Nachteil des Betroffenen verwertet werden.

2.5 Notwendige organisatorische Maßnahmen

Für die Anlage neuer und für die Überprüfung vorhandener personenbezogener Sammlungen sowie für Verbunddateien muß der Erlaß von Errichtungsanordnungen gesetzlich vorgesehen werden, die Regelungen enthalten über

1. die Bezeichnung, den Zweck und die Rechtsgrundlage der Sammlung,
2. den in die Sammlung aufzunehmenden Personenkreis,
3. die Art und den Umfang der zu speichernden Informationen, die der Erschließung dienen können,
4. die Übermittlung von Informationen,
5. die Dauer der Aufbewahrung der Informationen und
6. die zuständige Stelle für die Anlage und Führung von Sammlungen.

Diese Errichtungsanordnungen sind zu veröffentlichen.

Daten, die zur Vorgangsverwaltung oder nur zum Nachweis polizeilichen Handelns geführt werden, sind von Datensammlungen zur Gefahrenabwehr und Strafverfolgung zu trennen.

Anlage 3 (zu Nr. 11.3.2)

Anforderungen an Datenschutzregelungen für den Verfassungsschutz

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 13. September 1985

I. Notwendigkeit bereichsspezifischer Regelungen

1. Gerade für die Datenverarbeitung der Verfassungsschutzbehörden sind präzise gesetzliche Grundlagen erforderlich, da sie in besonderem Maße in das informationelle Selbstbestimmungsrecht eingreift, weil sie fast vollständig im Geheimen und somit unter Ausschluß der Öffentlichkeit und der Kontrolle durch den Betroffenen stattfindet.

   Ebenso wie im Polizeirecht kann es auch beim Verfassungsschutz nicht darum gehen, die derzeitige Praxis gesetzlich festzuschreiben. Vielmehr muß der Umfang zulässiger Informationsverarbeitung der Verfassungsschutzbehörden auf der Grundlage des Volkszählungsgesetz-Urteils des Bundesverfassungsgerichts überprüft und durch spezielle Aufgaben- und Befugnisnormen konkretisiert und begrenzt werden. Die Neuregelung muß zumindest die nachfolgenden Grundsätze beachten.

2. Ähnliche Regelungen für den MAD und den BND sind unter Berücksichtigung der Besonderheiten der jeweiligen Aufgabenstellung geboten.

II. Allgemeine Grundsätze der Datenverarbeitung durch den Verfassungsschutz

1. Die Regelung der Informationsverarbeitung durch den Verfassungsschutz muß den Anforderungen der Normenklarheit entsprechen. Da über die Datenverarbeitung im einzelnen meist nichts bekannt wird, ist es für den Bürger von besonderer Bedeutung, daß er den gesetzlichen Bestimmungen entnehmen kann, aus welchem Anlaß, in welcher Form und zu welchem Zweck der Verfassungsschutz personenbezogene Daten verarbeiten darf.

2. Diese Vorschriften müssen zwischen den unterschiedlichen Aufgaben der Verfassungsschutzbehörden differenzieren. Was beispielsweise für die Abwehr von Spionen vertretbar ist, ist nicht auch für die Mitwirkung an Sicherheitsüberprüfungen angemessen.

3. Der Grundsatz der Zweckbindung gilt auch für die Verfassungsschutzbehörde. Das bedeutet: Angesichts der Vielfalt ihrer Aufgaben reicht eine pauschale Bindung an „Zwecke des Verfassungsschutzes" nicht aus. Vielmehr dürfen die für die unterschiedlichen Aufgaben erhobenen Daten grundsätzlich nur für die jeweilige Aufgabe verwendet werden.

4. Die Regelung der Verarbeitung personenbezogener Daten durch den Verfassungsschutz muß die Erhebung sowie jegliche andere Art der Verarbeitung und Verwendung einbeziehen.

5. Regelungsbedürftig sind auch die Voraussetzungen für die jeweilige Form der Datenverarbeitung: Wesentliche Schritte der Automatisierung sollen beispielsweise nur zugelassen werden, wenn diese für die Erfüllung der jeweiligen Aufgabe gerechtfertigt sind und hierdurch schutzwürdige Belange der Betroffenen nicht unverhältnismäßig beeinträchtigt werden. Dies gilt insbesondere für Systeme der Datenverarbeitung, die über einen Aktennachweis hinausgehen oder durch Übernahme von Akteninhalten neue Verwendungs- und Verknüpfungsmöglichkeiten eröffnen.

6. Für jede automatisierte oder manuelle Datei ist eine detaillierte Errichtungsanordnung zu erlassen.

III. Erheben und Sammeln personenbezogener Daten

1. Der Einsatz nachrichtendienstlicher Mittel muß klar geregelt sein. Dies gilt sowohl für die Voraussetzung der Anwendung als auch für die Frage, gegen wen nachrichtendienstliche Mittel eingesetzt werden dürfen. Die nachrichtendienstlichen Mittel sollten soweit wie möglich gesetzlich festgelegt werden. Zumindest sollten die Verfassungsschutzbehörden verpflichtet werden, alle in Frage kommenden Mittel im einzelnen intern zu beschreiben und ihren Einsatz zu dokumentieren. Die Anwendung nachrichtendienstlicher Mittel entbindet nicht von der Beachtung der allgemeinen Rechtsordnung.

2. Holt der Verfassungsschutz bei anderen Behörden Auskünfte ein, so soll er sein Ersuchen begründen, wenn nicht besondere Gründe entgegenstehen (z. B. schutzwürdige Belange des Betroffenen oder Sicherheitsinteressen des Staates). Entfällt danach die Begründung, so sind die Gründe des Ersuchens intern zu dokumentieren. Für Kontrollzwecke sollte ein eigenes Verzeichnis eingerichtet werden.

3. Eine Verpflichtung anderer Behörden, dem Verfassungsschutz von sich aus Informationen zu übermitteln, muß auf solche Bestrebungen beschränkt werden, die auf Anwendung von Gewalt oder geheimdienstlicher Tätigkeit gerichtet sind. Darüber hinaus dürfen Behörden von sich aus nur unter weiteren gesetzlich festzulegenden

Einschränkungen den Verfassungsschutz über personenbezogene Vorgänge informieren. Übermittlungen „auf Verdacht" sind unzulässig und können sich schädlich für das Verhältnis des Bürgers zu den Behörden auswirken.

4. Bei der Regelung der Informationsbeziehungen zwischen Polizei und Verfassungsschutz ist das verfassungskräftige Trennungsgebot zu beachten, das inhaltlicher ebenso wie organisatorischer Natur ist. Der Verfassungsschutz darf deshalb die Polizei z. B. nicht um Maßnahmen ersuchen, die die Anwendung polizeilicher Befugnisse erfordern. On-line-Verbindungen zwischen Polizei und Verfassungsschutz sind mit dem Trennungsgebot nicht vereinbar. Ein geeigneter Maßstab für Datenübermittlungen der Polizei an den Verfassungsschutz im Einzelfall sind die Verwertungsregelungen nach dem Gesetz zu Art. 10 GG.

5. Es ist sicherzustellen, daß spezielle Verwertungsbestimmungen — z. B. des Strafverfahrensrechts — beachtet werden: dies gilt z. B. für Erkenntnisse, die im Rahmen der Telefonüberwachung oder bei Durchsuchungen gewonnen wurden.

IV. Speichern personenbezogener Daten

1. Die Befugnis zur Speicherung ist differenziert nach den unterschiedlichen Aufgabenbereichen zu regeln.

   So muß der Extremismusbezug in der Person desjenigen erfüllt sein, dessen Daten personenbezogen auswertbar im Rahmen der Extremismusbeobachtung gespeichert werden sollen. Hierbei ist außerdem zu beachten, daß Personendaten nur gespeichert werden dürfen, wenn dies zum Zwecke der Beobachtung extremistischer Bestrebungen erforderlich ist. Der Praxis, die immer mehr von der Beobachtung von Organisationen zur Erfassung von Einzelpersonen übergeht, muß entgegengewirkt werden.

2. Die Gründe für eine Speicherung müssen aus den Unterlagen des Verfassungsschutzes nachvollziehbar sein. Werden Bewertungen gespeichert, so muß erkennbar sein, wer sie vorgenommen hat und welche Unterlagen ihnen zugrundeliegen.

3. Es sind gesetzliche Regelfristen für die Überprüfung und Löschung der gespeicherten Daten festzulegen. Dabei ist zwischen den einzelnen Aufgabenbereichen (etwa Extremismusbeobachtung/Spionageabwehr), nach der Relevanz der einzelnen Informationen (etwa: vager Verdacht/gesicherte Informationen) sowie nach dem Alter der Betroffenen zu differenzieren. Dies gilt auch für die Speicherung in Akten.

V. Mitwirkung an Personenüberprüfungen

(Sicherheitsüberprüfungen — § 3 Abs. 2 BVerfSchG)

1. Im Rahmen von Sicherheitsüberprüfungen werden sowohl beim Verfassungsschutz als auch bei einer Reihe weiterer Stellen Daten erhoben und verarbeitet. Hierfür sind besondere gesetzliche Grundlagen erforderlich.

2. Für die Mitwirkung des Verfassungsschutzes sind folgende Prinzipien zu beachten:

   — Die Sicherheitsüberprüfungen sind auf das erforderliche Maß zu beschränken. Dies gilt insbesondere für die Intensität der Prüfung, die sich nach der Gefährdung im Einzelfall richten muß.

   — Die Sicherheitsüberprüfung soll erst durchgeführt werden, wenn nur noch davon die Aufnahme der sicherheitsrelevanten Tätigkeit abhängig ist. Für den personellen Sabotageschutz ist zudem die exakte Beschreibung der sicherheitsempfindlichen Bereiche und die Begrenzung der Überprüfung auf tatsächlich in diesem Bereich eingesetzte Personen zu fordern.

   — Die Verfahrensregelungen müssen andere Ermittlungsformen ausschließen.

   — Die Voraussetzungen, unter denen im Rahmen der Sicherheitsüberprüfung auch Nachforschungen über Dritte angestellt werden dürfen, sind gesetzlich festzulegen. Soweit Dritte z. B. Ehegatten, einbezogen werden, ist deren Einwilligung erforderlich. Die Speicherung von Daten über diese Personen ist auf ein Minimum zu beschränken und darf grundsätzlich nicht personenbezogen erschließbar sein.

   — Das Verfahren muß für die Betroffenen (einschließlich der Dritten) transparent sein. Sie sind über die Tatsache, den Ablauf, die beteiligten Stellen und das Ergebnis der Sicherheitsüberprüfung zu unterrichten. Im Fall von Sicherheitsbedenken ist dem Überprüften Gelegenheit zur Stellungnahme zu geben. Ausnahmen von dieser Unterrichtungspflicht sind eng zu fassen. Auch Auskunftspersonen sind über den Zweck der Befragung zu unterrichten, um Fehlschlüsse zu Lasten des Betroffenen zu vermeiden, und auf die Freiwilligkeit ihrer Angaben hinzuweisen.

   — Stellt der Betroffene einen Auskunftsantrag nach den Datenschutzgesetzen, so ist diesem zu entsprechen, soweit die Speicherung im Rahmen der Sicherheitsüberprüfung erfolgt ist.

   — Die speziell für die Sicherheitsüberprüfung beim Betroffenen oder bei anderen Stellen erhobenen Daten dürfen in der Regel nur für diesen Zweck verwendet werden. Die Trennung von Sicherheits- und Personalakten ist strikt zu zu wahren.

VI. Übermittlung von Daten durch Verfassungsschutzbehörden

1. Verfassungsschutzbehörden dürfen untereinander personenbezogene Daten nur austauschen, soweit dies zu ihrer jeweiligen gesetzlich festge-

legten Aufgabenerfüllung erforderlich und verhältnismäßig ist.

2. Die Übermittlung personenbezogener Daten durch den Verfassungsschutz an andere Sicherheitsbehörden (z. B. Polizei, Staatsanwaltschaft, BND u. a.) muß unter Beachtung des Zweckbindungsgrundsatzes präziser und restriktiver als in den derzeit praktizierten Zusammenarbeitsrichtlinien in Staatsschutzsachen geregelt werden. Die Voraussetzungen einer Übermittlung müssen konkret festgelegt werden. Allein die Begründung, daß die Übermittlung mit „dem Zweck des Verfassungsschutzes" vereinbar sei, ist nicht ausreichend. An Strafverfolgungsbehörden darf der Verfassungsschutz Informationen, die er mit nachrichtendienstlichen Mitteln erlangt hat, nur weitergeben, wenn tatsächliche Anhaltspunkte für die Einleitung eines Ermittlungsverfahrens wegen einer Straftat der in § 7 Abs. 3 Gesetz zu Art. 10 GG genannten Art vorliegen.

3. Eine Übermittlung an andere Behörden kann nur zur Erfüllung eigener Aufgaben des Verfassungsschutzes in Betracht kommen. Ausnahmen bedürfen einer gesetzlichen Regelung.

4. Eine Übermittlung von personenbezogenen Daten an private Stellen (z. B. Firmen, Gewerkschaften, Parteien) ist nur im Rahmen der gesetzlich vorgesehenen Sicherheitsüberprüfungen und nur in dem dafür unerläßlichen Rahmen oder aus Gründen der Spionage- und Terrorismusabwehr zulässig. Bei Übermittlungen außerhalb der Sicherheitsüberprüfung ist außerdem die Zustimmung der obersten Dienstbehörde einzuholen.

5. Eine Übermittlung an ausländische Dienststellen einschließlich der Nachrichtendienste ist an besonders enge Voraussetzungen zu knüpfen. Es ist — längerfristig durch völkerrechtliche Übereinkommen — zu gewährleisten, daß im Inland geltende Schutzrechte des Betroffenen nicht gefährdet werden.

6. Vor jeder Übermittlung hat die auskunftgebende Verfassungsschutzbehörde die Richtigkeit der vorhandenen Unterlagen und deren Erforderlichkeit für die eigene Aufgabenerfüllung zu überprüfen. In allen Fällen ist die Übermittlung personenbezogen zu dokumentieren. Über die Änderung wesentlicher Gesichtspunkte ist die Empfängerbehörde zu unterrichten, soweit dadurch nicht schutzwürdige Belange des Betroffenen beeinträchtigt werden.

7. Eine Unterrichtung der Öffentlichkeit über personenbezogene Erkenntnisse des Verfassungsschutzes ist grundsätzlich ausgeschlossen.

VII. Auskunft an den Betroffenen

Die Verfassungsschutzbehörden dürfen Auskunftsersuchen der Bürger nicht, wie dies derzeit die meisten Ämter handhaben, schematisch ablehnen. Der Gesetzgeber sollte daher von folgenden Grundsätzen ausgehen:

Die Auskunft ist zu erteilen

— in aller Regel, wenn die Speicherung nur auf einer Sicherheitsüberprüfung beruht,

— im übrigen nach Abwägung im Einzelfall.

Im Falle einer Auskunftsverweigerung sind die Gründe im einzelnen zu dokumentieren.

Die Bearbeitung von Auskunftsersuchen muß getrennt von anderen Informationssammlungen erfolgen. Die Tatsache der Antragstellung darf nicht zum Nachteil der Betroffenen verwertet werden.

VIII. Rechte der Datenschutzbeauftragten

Die Kontrollkompetenz der Datenschutzbeauftragten erstreckt sich auf die gesamte Datenverarbeitung der Verfassungsschutzbehörden und umfaßt auch Akten und sonstige Unterlagen. Auch die Datenverarbeitung im Rahmen des Gesetzes zur Art. 10 GG muß der Kontrolle der Datenschutzbeauftragten unterliegen. Dies ist unerläßlich für die Durchsetzung des Rechts auf informationelle Selbstbestimmung gerade im Bereich des Verfassungsschutzes.

Anlage 4 (zu Nrn. 11.4.2 und 18.2)

Beschluß der Internationalen Datenschutzkonferenz in Luxemburg vom 23. bis 26. September 1985 zu Grundsätzen der polizeilichen Datenverarbeitung

Auf der Internationalen Konferenz der Datenschutzbeauftragten vom 12. bis 14. September 1984 in Wien wurde beschlossen, eine Arbeitsgruppe einzusetzen, die sich mit den von der Polizei verarbeiteten personenbezogenen Daten befaßt. Einige der Aspekte, die behandelt werden sollten, waren:

— Erhebung und Speicherung personenbezogener Daten durch die Polizei,

— Datenlöschung,

— Anforderungen an die Sicherheit der bei der Polizei vorhandenen Datensammlungen.

Die Internationale Datenschutzkonferenz erkennt an, daß es für die Polizei notwendig ist, die für die Erfüllung ihrer Aufgaben erforderlichen personenbezogenen Daten schnell sammeln zu können.

Die Befugnisse und Ermittlungsmaßnahmen der Polizei versetzen diese jedoch in eine privilegierte Lage hinsichtlich des Umfangs und des Inhalts der vorhandenen Datenbestände. Wegen der möglichen Nutzungen und der potentiellen Sensibilität der zur Erfüllung polizeilicher Aufgaben gesammelten Daten sind daher besondere Schutzvorkehrungen erforderlich für Erhebung, Speicherung, Nutzung und Übermittlung dieser Daten.

Die Konferenz ist deshalb der Auffassung, daß folgende Mindestgrundsätze beachtet werden sollten:

1. Die von der Polizei erhobenen und verarbeiteten personenbezogenen Daten sollten stets auf das beschränkt sein, was zur Erfüllung der Aufgaben erforderlich und verhältnismäßig ist.

2. Es sollten Regelungen getroffen werden, die die Erhebung und Speicherung personenbezogener Daten begrenzen. Hierbei sollte unterschieden werden nach den Mitteln der Erhebung, der Art der Daten, der Art ihrer Verarbeitung sowie nach dem Zweck, für den die Daten genutzt werden dürfen.

3. Es sollten verschiedene Regelungen getroffen werden für die Grenzen der Übermittlung personenbezogener Daten nach der Art des Empfängers — andere Polizeibehörden, öffentliche Behörden, Privatunternehmen oder Einzelpersonen — und nach der Art der Übermittlung. Die übermittelten Daten sollten richtig, erforderlich und verhältnismäßig in bezug auf die vom Empfänger beabsichtigte Nutzung sein. Die Übermittlung von Daten durch die Polizei sollte nur zulässig sein auf der Grundlage gesetzlicher Regelungen; soweit solche fehlen, sollte die Einwilligung des Betroffenen eingeholt werden.

   Die Übermittlung an ausländische Stellen sollte grundsätzlich auf Polizeibehörden beschränkt werden. Sie sollte nur zulässig sein, wenn innerstaatliche Regelungen für den Schutz des Betroffenen nicht gefährdet werden und unter der Voraussetzung einer klaren gesetzlichen Regelung des nationalen Rechts oder des Völkerrechts oder wenn es erforderlich ist zur Verhütung einer konkreten Gefahr oder zur Verfolgung einer bestimmten Straftat.

4. Der Betroffene sollte ein Recht auf Auskunft in geeigneter Form über die zu seiner Person bei der Polizei vorhandenen Daten haben, sofern hierdurch nicht die Erfüllung der polizeilichen Aufgaben oder Rechte und Interessen Dritter ernsthaft gefährdet werden könnten. Die Tatsache, welche Dateien bestehen, sollte öffentlich bekannt sein.

5. Die polizeilichen personenbezogenen Daten sollten grundsätzlich nach Wegfall der Erforderlichkeit gelöscht werden. Die Voraussetzungen der Löschung sollten sich auf Vorschriften und nicht auf individuelle Entscheidungen im Einzelfall stützen. Diese Vorschriften sollten unterscheiden nach den verschiedenen Arten von Daten und dem Erhebungszweck und sie sollten regelmäßige Überprüfungen der Erforderlichkeit der Daten vorsehen.

   Außerdem sollten sie Bestimmungen über die Dauer der Aufbewahrung und der Berichtigung der Daten enthalten.

6. Es sollten interne Überwachungs- und Kontrollverfahren für die Verarbeitung personenbezogener Daten durch die Polizei in Übereinstimmung mit den vorgenannten Prinzipien durch die Polizeibehörden jedes Landes entsprechend den jeweils bestehenden Regelungen über die Zusammenarbeit mit dem Datenschutzbeauftragten erlassen werden.

7. Die Polizeibehörden sollten alle möglichen organisatorischen und technischen Maßnahmen treffen, um die notwendige und geeignete physische und logische Sicherheit der Daten zu gewährleisten und um unberechtigten Zugang oder unerlaubte Übermittlung zu verhindern.

Die Konferenz schlägt vor, daß diese allgemeinen Regeln in den Abschlußgesprächen über die Löschung der beim Interpol-Generalsekretariat verarbeiteten Daten sowie über den Informationsaustausch zwischen den Nationalen Zentralbüros von Interpol beachtet werden.

Die Konferenz unterstützt die laufenden Arbeiten beim Europarat über polizeiliche Datensammlungen. Die Konferenz hofft, daß der Europarat eine Empfehlung verabschieden wird, die den o. a. Prinzipien Rechnung trägt.

Anlage 5 (zu Nr. 12.3)

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 15. November 1985 zur Speicherung personengebundener Hinweise im INPOL-System

Personengebundene Hinweise, d. h. Daten, die über die Identifizierungsfunktion hinausgehen und eine erste Einschätzung der gespeicherten Person ermöglichen sollen, finden sich zunehmend in polizeilichen Dateien. Im Bereich des Bundeskriminalamtes sind personengebundene Hinweise beispielsweise in den Dateien KAN, Haftdatei, Erkennungsdienst, Daktyloskopie, in den Falldateien sowie in anderen Dateien gespeichert. Auch in den Dateien der Länderpolizei sind derartige Hinweise enthalten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist der Auffassung, daß die Speicherung derartiger Hinweise die Gefahr der Ergreifung polizeilicher Maßnahmen nur aufgrund des Dateiinhalts hervorruft und daß sie ganz allgemein zu einer sozialen Abstempelung der betroffenen Person führen kann. Sie ist der Ansicht, daß polizeiliche Entscheidungen und insbesondere polizeiliches Einschreiten nur ausnahmsweise auf den Inhalt von Nachweisdateien gestützt werden dürfen, in der Regel jedoch Auskunft aus der Akte eingeholt werden muß. Die PHW's sind keine geeignete Entscheidungsgrundlage, weil sie nur bruchstückhafte Informationen darstellen und ihre ständige Aktualisierung nicht gewährleistet ist.

Die Datenschutzbeauftragten halten die Speicherung derartiger Hinweise allenfalls dann für zulässig, wenn dies zur Erreichung des mit der betreffenden Datei verfolgten Zwecks im jeweiligen Einzelfall unabdingbar ist. Nach derzeitigem Erkenntnisstand dürfen personengebundene Hinweise also nur noch in solchen Dateien niedergelegt werden, die als alleinige Grundlage für ein polizeiliches Einschreiten in Betracht kommen (z. B. die Personenfahndungsdatei).

Die benutzten Begriffe müssen präzise definiert werden, um eine einheitliche Handhabung sicherzustellen und unangemessenè Typisierungen von Betroffenen so weit wie möglich zu vermeiden. Es ist sicherzustellen, daß die vorgenommenen Bewertungen durch Tatsachen belegbar und nachvollziehbar sind. Die Aktualität der Hinweise muß innerhalb kurzer Fristen regelmäßig überprüft werden.

Nach derzeitigem Kenntnisstand sehen die DSB bei einer Abwägung der erkennbaren Interessen der Polizei an schnell verfügbaren Informationen mit der Gefahr unangemessener Stigmatisierungen der Betroffenen insbesondere die folgenden PHW's nicht als erforderlich an:

— geistesschwach

— entmündigt

— Prostitution

— Internationaler Rechtsbrecher

— häufig wechselnder Aufenthalt

— Land- und Stadtstreicher.

Diese Aufzählung ist nicht abschließend. Vielmehr müssen alle Kataloge zulässiger personengebundener Hinweise in den Informationssystemen der Polizei in Bund und Ländern auf ihre Erforderlichkeit hin überprüft werden.

Anlage 6 (zu Nr. 18.1)

Empfehlung Nr. R (85) 20 des Ministerkomitees an die Mitgliedsstaaten zum Schutz personenbezogener Daten bei der Verwendung für Zwecke der Direktwerbung

Präambel

Das Ministerkomitee, gemäß Artikel 15 (b) der Satzung des Europarats,

in der Erwägung, daß das Ziel des Europarats die Herbeiführung einer größeren Einheit unter seinen Mitgliedern ist;

in der Überzeugung, daß die Anwendung der Grundprinzipien des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten unter Berücksichtigung der Anforderungen in besonderen Tätigkeitsbereichen wünschenswert ist;

im Bewußtsein der Notwendigkeit des Schutzes des Persönlichkeitsbereichs des einzelnen angesichts des zunehmenden Einsatzes der Datenverarbeitung in der Direktwerbung;

in der Überzeugung, daß die Verwendung personenbezogener Daten für die Erhaltung und Entwicklung der Direktwerbung von wesentlicher Bedeutung ist;

in der Erkenntnis, daß der Bereich der Direktwerbung seine eigenen Regeln entwickelt, um die Rechte und Interessen des einzelnen zu schützen;

in der Erwägung, daß es zweckmäßig ist, in diesem Bereich die Entwicklung von Regeln zu fördern, sei es, daß sie rechtlich bindend oder selbstregelnd sind;

empfiehlt den Regierungen der Mitgliedsstaaten

— in ihrem innerstaatlichen Recht und in der Praxis im Hinblick auf die Verwendung personenbezogener Daten für Zwecke der Direktwerbung die Leitlinien im Anhang zu dieser Empfehlung zu berücksichtigen;

— sicherzustellen, daß diese Empfehlung eine weite Verbreitung findet, und daß das Bewußtsein und das Wissen in Bezug auf den Datenschutz in diesem Bereich gefördert wird.

Anhang zur Empfehlung Nr. R (85) 20

Richtlinien

1. Anwendungsbereich und Definitionen

1.1

Die Leitlinien in diesem Anhang gelten für die Verwendung personenbezogener Daten für Zwecke der Direktwerbung, wenn diese Daten automatisch verarbeitet werden.

1.2

Im Sinne dieser Empfehlung bedeutet „personenbezogene Daten" jede Information, die sich auf eine bestimmte oder bestimmbare Person (den Betroffenen) bezieht. Eine Person gilt nicht als „bestimmbar", wenn die Identifizierung einen unangemessen hohen Aufwand an Zeit, Geld und Arbeit erfordert;

umfaßt der Ausdruck „Direktwerbung" alle Aktivitäten, die es ermöglichen, einem Teil der Bevölkerung durch Post, Telefon oder andere Direktmedien Waren oder Dienstleistungen anzubieten oder sonstige Mitteilungen zu übersenden, die den Betroffenen informieren oder eine Reaktion bei ihm hervorrufen sollen, ebenso wie jegliche Hilfstätigkeit hierzu.

2. Das Sammeln von Daten für Zwecke der Direktwerbung

2.1

Jeder sollte bei der Erstellung von Listen für Werbezwecke, insbesondere Listen mit Namen und Adressen, für eigene Werbezwecke von Daten Gebrauch machen können, die er im Zuge vorheriger Geschäftsverbindungen mit tatsächlichen oder möglichen Kunden/Beitragszahlern zusammengestellt hat.

2.2

Personenbezogene Daten, die für die Direktwerbung verwendet werden sollen, sollten von jedermann aus allgemein zugänglichen Unterlagen oder anderen Veröffentlichungen gesammelt werden können, wenn dabei die durch das innerstaatliche Recht vorgesehenen Einschränkungen berücksichtig werden.

2.3

Das Erheben der Namen und Anschriften von Privatpersonen bei anderen Privatpersonen mit dem

Ziel, Listen für die Direktwerbung zu erweitern, sollte nur dann erlaubt sein, wenn es unter Wahrung der zum Schutz des Persönlichkeitsbereichs des Betroffenen vorgesehenen angemessenen Vorkehrungen erfolgt. Das innerstaatliche Recht kann dieses Verfahren verbieten oder strengeren Anforderungen unterwerfen.

2.4

Wenn das Erheben von Daten bei einer Privatperson einem anderen Ziel als dem der normalen Beziehungen zu Kunden/Beitragszahlern dient, sollte dies für Zwecke der Direktwerbung nur unter der Bedingung erlaubt sein, daß darauf bei der Datenerhebung ausdrücklich hingewiesen wurde.

Das Erheben von Daten bei einer Privatperson unter falschem Vorwand sollte nicht erlaubt sein.

2.5

In Fällen, in denen dies nach innerstaatlichem Recht zulässig ist, sollten personenbezogene Daten, die unter die besonderen in Artikel 6 des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten genannten Arten fallen, nur unter Wahrung der jeweiligen nach innerstaatlichem Recht vorgesehenen Vorkehrungen und gegebenenfalls nur mit der ausdrücklichen Einwilligung des Betroffenen für Zwecke der Direktwerbung erhoben und verwendet werden.

3. Die Zur-Verfügung-Stellung von Marketinglisten an Dritte

3.1

Nach Maßgabe der in Abs. 2.5 enthaltenen Bestimmungen sollten Marketinglisten Dritten für Zwecke der Direktwerbung unter der Voraussetzung zur Verfügung gestellt werden dürfen, daß der Betroffene unmittelbar oder mit anderen geeigneten Mitteln bei der Erhebung oder zu einem späteren Zeitpunkt davon in Kenntnis gesetzt worden ist, daß die Daten Dritten übermittelt werden können, und unter der Voraussetzung, daß er keinen Widerspruch erhoben hat.

Die Listen sollten keine Informationen enthalten, die den Persönlichkeitsbereich des Betroffenen verletzten könnten, es sei denn, dieser habe seine Einwilligung gegeben.

3.2

Die Zur-Verfügung-Stellung von Marketinglisten an Dritte für deren Werbezwecke muß Gegenstand eines Vertrages sein, der die Bedingungen festlegt, unter denen sie verwendet werden dürfen.

3.3

Die Inhaber von Marketingdateien sollten über alle Benutzer ihrer Listen Buch führen, um die Ausübung der in Kapitel 4 aufgeführten Rechte zu erleichtern.

4. Rechte des Betroffenen

4.1

Jeder sollte in der Lage sein, soweit angemessen, entweder

i. die Aufnahme von Daten zu seiner Person in Marketinglisten zu untersagen oder

ii. die Übermittlung von Daten auf solchen Listen an Dritte zu untersagen oder

iii. uneingeschränkt und auf Verlangen die Löschung oder sonstige Entfernung solcher Daten aus einigen oder allen von Benutzern geführten Listen zu veranlassen.

Außerdem sollte jeder das Recht haben, Daten zu seiner Person, die auf einer Liste für Direktwerbung stehen oder in einer Marketingdatei gespeichert sind, zu erfahren und zu berichtigen.

4.2

Geeignete Maßnahmen sollten ergriffen werden, die es dem Betroffenen ermöglichen, die in Absatz 4.1 aufgeführten Rechte auszuüben und den Inhaber der Marketingdatei zu übermitteln.

Der Inhaber der Marketingdatei sollte verpflichtet sein, alle Maßnahmen mit dem Ziel zu ergreifen, den aufgrund von Absatz 3.3 erfaßten Benutzern mitzuteilen, daß der Betroffene seine Rechte nach Absatz 4.1 ausgeübt hat, damit notwendige Änderungen an den Listen vorgenommen werden können.

5. Form der Werbemitteilungen und des Werbematerials

5.1

Die angebotenen Güter und Dienstleistungen sowie die Mitteilungen sollten in einer Art und Weise dargeboten werden, daß der Persönlichkeitsbereich der Empfänger nicht verletzt wird.

6. Datensicherheit

Bei der Zusammenstellung von Unterlagen mit personenbezogenen Daten für Zwecke der Direktwerbung sollten alle im Hinblick auf die Anforderungen dieses Bereichs angemessenen technischen und organisatorischen Vorkehrungen zur Gewährleistung der Sicherheit und Vertraulichkeit der Daten getroffen werden.

Die Inhaber der Unterlagen und das bei der Verarbeitung der Daten beschäftigte Personal sollten von diesen Anordnungen und der Notwendigkeit, sie zu befolgen, fortlaufend unterrichtet werden.

7. Maßnahmen zur Anwendung der Empfehlung

7.1

Die Entwicklung von Maßnahmen zur Selbstregulierung im Bereich der Direktwerbung sollte gefördert werden, um die Lösung von Problemen im Zusammenhang mit den in dieser Empfehlung vorgesehenen Vorkehrungen, insbesondere der Entfernung von Namen aus Direktwerbungslisten, zu erleichtern.

7.2

Geeignete Maßnahmen sollten ergriffen werden, um die Einhaltung der Bestimmungen dieser Empfehlung durch Adressenmittler und -dienste sicherzustellen.

7.3

Den Betroffenen sollten geeignete Informationen über die in dieser Empfehlung niedergelegten Vorkehrungen zur Verfügung gestellt werden.

Sachregister

Adressenweitergabe 23
Ärztliche Gutachten und Atteste 14f., 15, 31, 32
Ärztliche Schweigepflicht 32f., 53f.,
Aktennachweis des BKA 35, 41, 42, 44
Amtsgeheimnis 23
Amtshilfe 36, 37
Arbeitslosenhilfe 30
Arbeitsvermittlung 30
Archivgesetz 26
Auskunft an den Betroffenen 40, 59
Ausländische Dienste 36
Ausländerzentralregister 10
Autotelefon 19

Baugesetzbuch 13
Beihilfe 13f., 15
Berufsangabe 24
Beurteilungen 16
Bildschirmtext (Btx) 19f.
Bundesadreßregister 22
Bundesamt für Verfassungsschutz 36, 40, 47ff.
Bundesbahn 16ff., 25f.
Bundesdruckerei 10

Bundesgrenzschutz 36
Bundeskriminalamt 35f., 40, 41ff.
Bundesnachrichtendienst 37
Bundespost 19ff.
Bundesverfassungsschutzgesetz 38
Bundeswahlordnung 11
Bundeswehr 50
Bundeszentralregister 11f.

Datenträgerverwaltung 55f., 57
Dialyse-Patienten 34
Düsseldorfer Kreis 8

Einkommensnachweis 30
Erkennungsdienstliche Unterlagen 43
Erziehungsgeld 29
Europarat 40, 60
Extremismusbeobachtung 38, 47ff.

Fahndung 36, 39, 41, 45
Fahrzeugregister 23f.
Familienkrankenhilfe 31f.
Fangschaltung 22
Fernmeldeordnung 21
Fernsprechauskunft 22

Gefahrenvorsorge 38
Geheimschutz 36
Gerichtsverfassungsgesetz 12
Grenzaktennachweis (GAN) 36, 45
Grenzkontrolle 39
Grenzschutzdirektion 10, 36

Hacker 20
Haftdatei 41
Hochschulstatistikgesetz 28
Homecomputer 56
Homebanking 19
Hotelmeldepflicht 10

INPOL 35, 41, 44
Interpol 35, 41ff.

Kaufpreissammlung 13
Kennwort, persönliches → Paßwort
Kontrollbefugnis des BfD 19, 38, 40, 54f., 59
Kontrolle von Abfragen 53, s. auch Protokollierung
Krankenhausmeldepflicht 10
Krankenkasse 31f.
Kriegsdienstverweigerer 11, 51
Kredit 52f.
Kriminalaktennachweis (KAN) 35, 43f., 45
Kryptographische Verschlüsselung 17, 58
Kurentlassungsbericht 32ff.

Leistungskontrolle 16, 17
Löschungsfrist 35, 40, 42f., 47f.

MAD-Gesetz 38
Mahnbescheid 53
Maschinenlesbarkeit 8f.
Melderechtsrahmengesetz 10
Melderegister 9
Mikrozensus 27
Militärischer Abschirmdienst (MAD) 36, 50
Mitbestimmung 18f.
Mitteilungen in Strafsachen (MiStra) 12
Mitteilungen in Zivilsachen (MiZi) 12

Nachberichtspflicht 35
NADIS 47, 49
Novellierung des BDSG 4, 59f.

Online-Anschluß 24

Paß 8
Paßgesetz 10, 38
Paßwort 20, 55
Personal
-akten 10, 15
-daten 13ff.
-informationssysteme 16ff.
Personalausweis 8ff., 38
-gesetz 38
Personal Computer (PC) 17f., 56ff.
Personelle Vorbeugung 36, 50
Personengebundene Hinweise 35, 37, 41, 44f.
PIOS 37, 44, 45f.
Polizeirecht 37
Postgeheimnis 23
Postreklame 22f.
Protokollierung von Abfragen 9, 24

Rauschgiftkriminalität 35, 40f., 43, 44
Rehabilitation 32

Relevanzprüfung 35
Rentenversicherungsnummer 29f.
Rentenversicherungsträger 33
Repräsentativstatistik 27
Reservisten 51f.

Scheidungsurteil 16, 51
Schuldnerverzeichnis 12f.
Schufa 52f.
Schwangerschaft 34
Seriennummer 9
Sicherheitsbehörden 10, 35ff.
Sicherheitsüberprüfung 36, 39, 49, 50
Sozialversicherungsnummer 29f.
Spionageabwehr 50
Spurendokumentationssystem (SPUDOK) 44, 45f.
Staatsschutz 37, 46
Statistik 27f.
Steuergeheimnis 40f.

Telefonbuch 19, 21f.
Telefonüberwachung 35, 38
Telefonverbindungsdaten 22
Telekommunikationsordnung (TKO) 20
Telekonto 20
TEMEX 20f.
Terrorismus 46
Textverarbeitung 56

Urlaubsanschrift 16

Verhaltenskontrolle 16, 17
Verkartungsplan 48
Verkehrszentralregister 25
Verlaufsstatistik 28
Verwertungsverbot nach § 51 BZRG 35
Videoüberwachung 25
Virusprogramm 56
Volkszählung 27

Wehrersatzbehörden 50
Werbung 60

Zentraler Personenindex 42
Zentrales Verkehrsinformationssystem (ZEVIS) 23f.
Zivildienst 11
Zollkriminalinstitut 38
Zusammenarbeitsgesetz (ZAG) 38
Zwangseintrag 21
Zweckbindung 17, 36, 39, 50

Abkürzungsverzeichnis

ADV	Automatisierte Datenverarbeitung
AGB	Allgemeine Geschäftsbedingungen
AO	Abgabenordnung
AVG	Angestelltenversicherungsgesetz
AZR	Ausländerzentralregister
BBG	Bundesbeamtengesetz
BDSG	Bundesdatenschutzgesetz
BfA	Bundesversicherungsanstalt für Angestellte
BfD	Bundesbeauftragter für den Datenschutz
BfV	Bundesamt für Verfassungsschutz
BGB	Bürgerliches Gesetzbuch
BGBl	Bundesgesetzblatt
BGS	Bundesgrenzschutz
BKA	Bundeskriminalamt
BKAG	Gesetz über die Errichtung eines Bundeskriminalpolizeiamtes
BMA	Bundesminister für Arbeit und Sozialordnung
BMBau	Bundesminister für Raumordnung, Bauwesen und Städtebau
BMBW	Bundesminister für Bildung und Wissenschaft
BMF	Bundesminister der Finanzen
BMI	Bundesminister des Innern
BMJ	Bundesminister der Justiz
BMJFG	Bundesminister für Jugend, Familie und Gesundheit
BMP	Bundesminister für das Post- und Fernmeldewesen
BMV	Bundesminister für Verkehr
BMVg	Bundesminister der Verteidigung
BND	Bundesnachrichtendienst
BStatG	Bundesstatistikgesetz
BT	Bundestag
BetrVG	Betriebsverfassungsgesetz
Btx	Bildschirmtext
BVerfG	Bundesverfassungsgericht
BVerfGE	Bundesverfassungsgerichtsentscheidung
BVerfschG	Bundesverfassungsschutzgesetz
BZR	Bundeszentralregister
BZRG	Bundeszentralregistergesetz
DA	Dienstanweisung für die Standesbeamten und ihre Aufsichtsbehörden
DATEX	DATa EXchange
DB	Deutsche Bundesbahn
DBP	Deutsche Bundespost
DEVO	Datenerfassungsverordnung
DÜVO	Datenübermittlungsverordnung
DV	Datenverarbeitung
ed	erkennungsdienstlich
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
ETB	Elektronisches Telefonbuch
G 10	Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses
GAN	Grenzaktennachweis
GG	Grundgesetz
GMBl	Gemeinsames Ministerialblatt
GSD	Grenzschutzdirektion
INPOL	Informationssystem der Polizei
IRG	Gesetz über die Internationale Rechtshilfe in Strafsachen

KAN	Kriminalaktennachweis
KBA	Kraftfahrt-Bundesamt
KDV	Kriegsdienstverweigerer
KDVNG	Kriegsdienstverweigerungs-Neuordnungsgesetz
MAD	Militärischer Abschirmdienst
MiStra	Mitteilungen in Strafsachen
MiZi	Mitteilungen in Zivilsachen
MRRG	Melderechtsrahmengesetz
NADIS	Nachrichtendienstliches Informationssystem
PC	Personal Computer
PIOS	Auskunftssystem über Personen, Institutionen, Objekte und Sachen
PostVwG	Postverwaltungsgesetz
RKG	Reichsknappschaftsgesetz
RVO	Reichsversicherungsordnung
SCHUFA	Schutzgemeinschaft für allgemeine Kreditsicherung GmbH
SGB	Sozialgesetzbuch
SGB X	Sozialgesetzbuch Zehntes Buch
SPUDOK	Spurendokumentationssystem
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
StVG	Straßenverkehrsgesetz
StVZO	Straßenverkehrs-Zulassungs-Ordnung
TB	Tätigkeitsbericht*)
TEMEX	Telemetry Exchange (Fernwirkdienst der DBP)
TKO	Telekommunikationsordnung
TV	Tarifvertrag
VwVfG	Verwaltungsverfahrensgesetz
VZG	Volkszählungsgesetz
VZR	Verkehrszentralregister
VZRG	Verkehrszentralregistergesetz
WEWIS	Wehrersatzweseninformationssystem
ZEVIS	Zentrales Verkehrsinformationssystem
ZKI	Zollkriminalinstitut
ZPO	Zivilprozeßordnung

*) 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