Deutscher Bundestag
9. Wahlperiode

Drucksache 9/93

09. 01. 81

Sachgebiet 204

Unterrichtung

durch den Bundesbeauftragten für den Datenschutz

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

Gliederung

		Seite
1	**Überblick**	4
1.1	Erwartungen und Ergebnisse	4
1.2	Schwerpunkte der Tätigkeit im Berichtsjahr	4
1.3	Verhältnis zu anderen Stellen	6
1.4	Eingaben	7
1.5	Kooperation mit anderen Datenschutzinstanzen	7
1.6	Arbeitskontakte mit Spitzenorganisationen	8
1.7	Öffentlichkeitsarbeit	8
1.8	Dateienregister	8
2	**Fortentwicklung des Datenschutzrechts**	9
2.1	Novellierung des BDSG — Anhörung am 21./22. April 1980 —	9
2.2	Entwurf von Verwaltungsvorschriften	10
2.3	Melderechtsrahmengesetz	12
2.4	Personalausweisgesetz	13
2.5	Sozialgesetzbuch X (Verwaltungsverfahren) — Neuordnung des Sozialdatenschutzes	14
2.6	Bundesstatistikgesetz	16
3	**Stand des Datenschutzes in ausgewählten Bereichen**	16
3.1	Allgemeine innere Verwaltung	16
3.1.1	Bundesverwaltungsamt/Ausländerzentralregister	16
3.1.2	Umweltbundesamt	16
3.1.2.1	Dateien des Amtes	16
3.1.2.2	Hausmülluntersuchung	17
3.1.3	Bundesamt für die Anerkennung ausländischer Flüchtlinge	17
3.1.4	Eingliederung von Spätaussiedlern	17
3.1.5	Datenschutz im Bereich des Zivildienstes	18
3.1.6	Übersicht über Verfassungsstreitsachen vor dem Bundesverfassungsgericht	18

Gemäß § 19 Abs. 2 Satz 2 des Bundesdatenschutzgesetzes zugeleitet mit Schreiben des Bundesbeauftragten für den Datenschutz — I — 192 111/2 — vom 9. Januar 1981.

		Seite
3.2	Rechtswesen/Justizverwaltung	19
3.2.1	Bundeszentralregister	19
3.2.2	Anordnung über Mitteilungen in Strafsachen	19
3.2.3	Akteneinsicht für Betroffene in Strafverfahren	19
3.2.4	Prozeßkostenhilfegesetz	20
3.2.5	Schuldnerverzeichnis	20
3.2.6	Mietpreisspiegel	20
3.3	Steuerverwaltung	21
3.3.1	Bundesamt für Finanzen	21
3.3.2	Zollkriminalinstitut (ZKI) und Zollfahndungsdienst	22
3.4	Statistik und Forschung	23
3.4.1	Statistisches Bundesamt	24
3.4.2	Sozialhilfestatistik	24
3.4.3	Wehrmedizinalstatistik	24
3.4.4	Forschung	25
3.5	Personalwesen	25
3.5.1	Bewerbungsunterlagen und Personalbögen	26
3.5.2	Personalaktenrecht	26
3.5.3	Bundespersonalausschuß	27
3.5.4	Beihilfen	27
3.5.5	Automatisierte Datenverarbeitung	27
3.5.5.1	Personalinformationssysteme	27
3.5.5.2	Gleitzeiterfassung	28
3.5.5.3	Telephonkontrolle	28
3.5.5.4	Leistungskontrolle	29
3.5.5.5	Zugangs- und Zugriffskontrolle	29
3.6	Bibliothekswesen	30
3.7	Deutsche Bundespost	30
3.7.1	Aufzeichnungen über Telephongespräche	31
3.7.2	Eintrag ins Fernsprechbuch	31
3.7.3	Antrag auf Fernmeldehauptanschluß, Datenübermittlung an die Deutsche Postreklame	32
3.7.4	Anschriftenprüfung	32
3.7.5	Gehaltskontoverfahren	32
3.8	Medien	33
3.8.1	Deutsche Welle	33
3.8.2	Datenschutzprobleme bei neuen Medien	33
3.9	Verkehrswesen	34
3.9.1	Kraftfahrt-Bundesamt (KBA)	34
3.9.1.1	Kfz-Halter-Datei	35
3.9.1.2	Verkehrszentralregister (VZR)	35
3.9.1.3	Übermittlung aus dem VZR	36
3.9.1.4	Datei der versicherungspflichtigen Fahrzeuge	37
3.9.1.5	ZEVIS	37
3.9.2	Auto-Notfunk	38
3.9.3	Schwarzfahrer bei der Deutschen Bundesbahn (DB)	38
3.10	Sozialverwaltung, Gesundheitswesen	38
3.10.1	Allgemeines	38
3.10.2	Rentenversicherung	39
3.10.2.1	Sozialbericht bei Abhängigkeitskranken	39
3.10.2.2	Verband Deutscher Rentenversicherungsträger e. V. (VDR)	39
3.10.3	Krankenversicherung	40
3.10.3.1	Weitergabe von Daten aus der Ersatzkasse an eine private Krankenversicherung	40
3.10.3.2	Hamburgische Zimmererkrankenkasse	40
3.10.3.3	Techniker-Krankenkasse	40
3.10.3.4	Hamburg-Münchener Ersatzkasse	40
3.10.3.5	DVDIS	41
3.10.4	Unfallversicherung	41
3.10.4.1	Verwaltungs-Berufsgenossenschaft	41
3.10.4.2	Arbeitskreis „Arbeitsmedizin" der Bau-Berufsgenossenschaften	41
3.10.5	Arbeitsverwaltung	43
3.10.5.1	Stellung des internen Datenschutzbeauftragten der BA	43
3.10.5.2	Anmeldungen der BA und interne Übersicht gem. § 15 Nr. 1 BDSG	43
3.10.5.3	Neuregelung des Auskunftsverfahrens der BA, insbesondere aus Beratungs- und Übermittlungsunterlagen	43
3.10.5.4	Einzelfälle	43
3.10.6	Gesundheitswesen	45
3.10.6.1	„Modellprogramm Psychiatrie"	45
3.10.6.2	Bundesgesundheitsamt	45
3.11	Öffentliche Sicherheit, Verteidigung	45
3.11.1	Grenzen der informationellen Zusammenarbeit der Sicherheitsbehörden	45
3.11.1.1	Abriß der Problematik	45
3.11.1.2	Zur Frage meiner Kontrollkompetenz im G 10-Bereich	47
3.11.1.3	Allgemeine Prüfung einiger ausgewählter Fälle bei den Sicherheitsbehörden	48
3.11.2	Bundeskriminalamt	48
3.11.2.1	INPOL-Neukonzeption	48
3.11.2.2	Dateienrichtlinien für das BKA und Richtlinien über Kriminalpolizeiliche Sammlungen (KpS)	50
3.11.2.3	BKA-Datei „Bundeswahlkampf"	50
3.11.2.4	BKA-Rasterfahndung	50
3.11.2.5	Polizeiliche Beobachtung	52
3.11.2.6	Arbeitsdatei PIOS — Rauschgift	52
3.11.3	Bundesgrenzschutz	53
3.11.4	Bundesnachrichtendienst	54
3.11.5	Bundesamt für Verfassungsschutz	55
3.11.6	Militärischer Abschirmdienst (MAD)	56

Seite

3.11.6.1 Sicherheitsüberprüfung Wehrpflichtiger unter Mithilfe des BfV 56
3.11.6.2 Sicherheitsüberprüfung von Reservisten .. 56
3.11.6.3 Kriterien für die Speicherung und Löschungsrichtlinien 56
3.11.6.4 Dateienübersicht beim MAD 56
3.11.7 Weitergabe von Unterlagen über Kriegsdienstverweigerer an das BfV 56

4 Allgemeine Erfahrungen 57

4.1 Prüfungskompetenz des BfD 57

4.2 Formulargestaltung 58

4.3 Grenzen der Automatisierung 58

4.4 Maßnahmen zur Gewährleistung des Datenschutzes 59
4.4.1 Die Bedeutung der Übersicht 59
4.4.2 Probleme der Durchsetzung von Maßnahmen 60
4.4.3 Reaktion auf Alarmmeldungen 60

5 Datenschutz im Ausland, internationale Zusammenarbeit 61

5.1 Stand der Datenschutzgesetzgebung im Ausland 61

Seite

5.2 Internationale Übereinkommen 61
5.2.1 Europarat 61
5.2.2 OECD 61
5.2.3 Europäische Gemeinschaft 61

5.3 Internationale Zusammenarbeit in Fragen des Datenschutzes 62

Anhang 1

(Bundesministerium für Verkehr

Mitteilungen zur Anpassung der empirischen Forschung an die Bestimmungen des Bundesdatenschutzgesetzes [BDSG] vom 18. 6. 1980
— Auszug —) 63

Anhang 2

(Grundsätze für den Datenschutz bei den Neuen Medien [insbesondere bei Bildschirmtext und Kabelfernsehen]

Beschluß der 7. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in Berlin am 11. Dezember 1980) 66

Abkürzungsverzeichnis 69
Sachregister 72

1 Überblick

1.1 Erwartungen und Ergebnisse

Von den Datenschutzbeauftragten erwarten manche, daß sie in regelmäßigen Abständen „Datenskandale" aufdecken und öffentlich anprangern, also offensichtliche Verstöße gegen die Datenschutzbestimmungen, Mißbrauch und Veruntreuung personenbezogener Daten, schwere Verstöße gegen die Pflicht zur Datensicherung. In der Tat werden durch Datenschutzprüfungen immer wieder Fälle rechtswidrigen Umganges mit Daten bekannt. Im Berichtsjahr waren insbesondere einige Komplexe unzulässiger oder zumindest bedenklicher Speicherung oder Übermittlung und Mängel in der Datensicherung bestimmter Bundesbehörden zu beanstanden; außerdem wurde die Pflicht zur Aufklärung der Betroffenen über die vorgesehenen und praktizierten Formen von Datenverarbeitung und über die Rechtsgrundlagen häufig nur ganz unzulänglich erfüllt.

Eindeutige Verstöße gegen klare, nicht weiter auslegungsbedürftige Datenschutzbestimmungen sind jedoch insgesamt selten. Kern von Auseinandersetzungen war vielmehr in aller Regel eine Meinungsverschiedenheit über das richtige Verständnis von Rechtsgrundsätzen und Grundrechten. Nicht vorsätzliche Mißachtung von Bürgerrechten durch die bei der Datenverarbeitung beschäftigten Mitarbeiter der öffentlichen Verwaltung, sondern zu geringe Einschätzung dieser Rechte insbesondere bei Systemplanungen war meist die Ursache von Fehlentscheidungen. Jede Verwaltung neigt dazu, ihr Interesse an der bestmöglichen Aufgabenerfüllung sehr hoch, verglichen mit den Interessen Betroffener zu hoch, zu bewerten — so kommt es z. B. dazu, daß Systeme zur Abrechnung erbrachter Leistungen (z. B. Telefondienst) vorrangig darauf ausgerichtet werden, die Beweislage der forderungsberechtigten Verwaltung zu verbessern, während der Gesichtspunkt, die Entstehung großer Bestände sensibler Daten möglichst zu vermeiden, unterbewertet wird, oder daß die Gefahren aus der zentralen Sammlung von Kriminalaktenhinweisen zu gering gewichtet werden.

Die Verantwortung für den richtigen Umgang mit personenbezogenen Daten liegt bei der jeweiligen Verwaltungsspitze und den Fachaufsichtsbehörden (vgl. § 15 BDSG); *hier* — in meinem Prüfungsbereich bei den Behördenleitungen und den obersten Bundesbehörden — sind Verzögerungen oder Versäumnisse festzustellen, die zum Teil Unsicherheiten bei den ausführenden Organen und die Fortsetzung rechtlich nicht mehr zulässiger Praktiken zur Folge hatten. So ist nach wie vor das Problem der polizeilichen Beobachtung und zollrechtlichen Überwachung ungelöst, die künftige Ausgestaltung des kriminalpolizeilichen Informationssystems INPOL (insbesondere des geplanten Kriminalaktennachweises) ist offen, und die bisher auf die unzulängliche Rechtsgrundlage des allgemeinen Amtshilfegebots gestützten Informationsbeziehungen zwischen Polizei und Nachrichtendiensten bedürfen immer dringender einer (restriktiven) rechtlichen Regelung, wozu auch Gesetzesänderungen und -ergänzungen gehören. Die entsprechenden Absichtserklärungen der politisch Verantwortlichen liegen vor, und es ist zu hoffen, daß nunmehr bald Gesetzesvorlagen folgen werden — der gegenwärtige Zustand ist nicht mehr lange erträglich.

Möglicherweise hätte eine noch intensivere Prüfungstätigkeit in Rechenzentren der Bundesverwaltung die eine oder andere weitere Feststellung unzulässigen Umgangs mit personenbezogenen Daten gebracht. Die Wahrscheinlichkeit dafür, daß ungewöhnliche Fälle der bewußten Gesetzesverletzung aufgedeckt worden wären, ist aber nicht so hoch, daß sie den Aufbau einer umfassenden Datenschutzbürokratie rechtfertigen würden. Anreiz für rechtswidrigen Umgang mit Daten besteht immer nur dort, wo die Handelnden sich davon einen materiellen oder sonstigen Gewinn versprechen können. Dies ist zum einen dort der Fall, wo Angaben über Mitarbeiter oder „Kunden" der öffentlichen Verwaltung (z. B. Mitglieder von Krankenkassen) für kommerzielle Auswertungen von Interesse sind, zum anderen dort, wo die Verletzung des Datenschutzrechts eine wesentliche Vereinfachung oder Verbesserung der eigenen Arbeit ermöglicht, was für den einzelnen Mitarbeiter der öffentlichen Verwaltung unter Umständen einen Machtzuwachs oder eine Verbesserung seiner Karrierechancen bedeuten kann. Andererseits ist aber zu beachten, daß die bestehenden Schwellen relativ hoch sind und gerade in letzter Zeit noch erhöht worden sind. Nicht nur Strafrecht und vor allem Disziplinarrecht wirken abschreckend, sondern auch eine Besonderheit der automatischen Datenverarbeitung: bei richtiger Organisation kann kaum jemals ein einzelner allein in das System zu seinem Vorteil eingreifen, und größer angelegte Umgehungsversuche sind ohne mehrere Mitwisser nicht möglich. Es spricht wenig dafür, daß es in der öffentlichen Verwaltung „Verschwörungen" zum bewußten Verstoß gegen Grundrechte der Bürger und zur Täuschung der Kontrollinstanzen gibt. Die gleichwohl vorkommenden Verstöße müssen ernst genommen und konkret beim Namen genannt werden; Verallgemeinerungen sind aber schon deswegen nicht angebracht, weil sie die Motivation der Mitarbeiter der Verwaltung für ein engagiertes Umsetzen des Datenschutzes in die Praxis beeinträchtigen können.

1.2 Schwerpunkte der Tätigkeit im Berichtsjahr

Schwerpunkte der Tätigkeit meiner Dienststelle im Berichtsjahr lagen in den Bereichen der Post, der Si-

cherheitsbehörden einschließlich Ausländerzentralregister, der Verkehrsverwaltung des Bundes (Kraftfahrt-Bundesamt) und der Personalverwaltung (ein Personalinformationssystem). Ich habe beratend an den großen datenschutzrechtlichen Gesetzesvorhaben der vergangenen Legislaturperiode (Melderechtsrahmengesetz und Sozialgesetzbuch X. Buch) mitgewirkt und im Bereich der Justizverwaltung mehrere wichtige Fragenkomplexe aufgegriffen.

Über Einzelheiten wird in den Sachabschnitten dieses Berichts referiert; als Überblick sei hier jedoch vorangestellt:

— Die Deutsche Bundespost bestreibt Datenverarbeitung in großem Umfang und nutzt dabei auch Möglichkeiten, die unter Datenschutzaspekten kritisch zu beurteilen sind. Auf die von mir geäußerte und in der Öffentlichkeit aufgegriffene Kritik hin hat der Bundesminister für das Post- und Fernmeldewesen den besonders bedenklichen Versuch beendet, im Rahmen des elektronischen Wählsystems die geführten Telefongespräche auch mit den Nummern der Angerufenen aufzuzeichnen (s. u. 3.7.1). In diesem Zusammenhang sind aber weitere Einzelheiten klärungs- und lösungsbedürftig, insbesondere die künftige Methode der Aufzeichnung von Nutzungsdaten der Neuen Medien.

  Mehrere Beschwerden veranlaßten mich zu einer Kritik an der Praxis der Post, die Eintragung von Fernsprechteilnehmern im Telefonbuch trotz entgegenstehender Geheimhaltungsgründe durchzusetzen (s. u. 3.7.2). Das Verfahren der „Anschriftenprüfung" (Mitteilung neuer Anschriften an Absender von Postsendungen) war ebenso Gegenstand datenschutzrechtlicher Auseinandersetzung wie die Übermittlung von Kundendaten an die Deutsche Postreklame GmbH; in beiden Fällen werden die Interessen der Betroffenen jetzt besser geschützt als früher (s. u. 3.7.3 und 4).

— Datenschutzrechtliche Prüfungen fanden beim Bundeskriminalamt, bei der Grenzschutzdirektion, bei einzelnen Grenzschutzämtern und -stellen, beim Bundesamt für Verfassungsschutz, beim Militärischen Abschirmdienst und beim Bundesnachrichtendienst statt. Beim Bundeskriminalamt wurde die Datenverarbeitung aus Anlaß von Rasterfahndungen kontrolliert. Die Informationsflüsse zwischen den verschiedenen Sicherheitsbehörden (vor allem zwischen dem Bundesgrenzschutz und anderen Dienststellen einschließlich Ausländerzentralregister) wurden durch eine größere Anzahl von Prüfungen weiter aufgeklärt; dabei wurden einige Notierungen festgestellt, die gelöscht werden mußten und nach unserer Aufforderung tatsächlich gelöscht wurden. Gleichzeitig konnten durch solche systematischen Prüfungen die Grundlagen für eine sachgerechte Beurteilung der Amtshilfeproblematik aus der Sicht des Datenschutzes erheblich verbessert werden; diese Ergebnisse fließen in die Gespräche mit den zuständigen obersten Bundesbehörden über diesen Fragenkomplex ein. Thema zahlreicher Besprechungen mit dem Bundesministerium des Innern und dem Bundeskriminalamt waren die Richtlinien über kriminalpolizeiliche personenbezogene Sammlungen und die Dateienrichtlinien für das Bundeskriminalamt; einige wesentliche Verbesserungen wurden durchgesetzt, andere Fragen sind nach wie vor kontrovers (s. u. 3.11.2).

  Bei verschiedenen Sicherheitsbehörden wurden die Dateienübersichten kontrolliert und die Voraussetzungen und Fristen für die Löschung personenbezogener Daten eingehend besprochen. In einer Reihe von Fällen konnte trotz des Auskunftsverweigerungsrechts der Sicherheitsbehörden (§ 13 Abs. 2 BDSG) eine Auskunft über gespeicherte Daten an die Betroffenen vermittelt werden (s. u. 3.11.1 und Näheres in den dann folgenden Abschnitten zu den einzelnen Sicherheitsbehörden).

— Zusammen mit den Landesbeauftragten für den Datenschutz habe ich mich im Berichtsjahr auch der Überprüfung jener Informationsströme zugewandt, die zwischen der Strafjustiz und anderen Stellen aufgrund der Anordnung über Mitteilungen in Strafsachen (MiStra) fließen. Die Datenschutzbeauftragten haben gegenüber dieser Anordnung erhebliche rechtliche Bedenken geltend gemacht und in einer parallelen Aktion auf Bundes- und Landesebene Abhilfe gefordert (s. u. 3.2.2).

— Kritische Beobachtung war auch dem Verkehrsinformationssystem ZEVIS gewidmet, dessen generelle Problematik ich bereits im zweiten Tätigkeitsbericht (2. TB S. 41 f., siehe dort auch S. 39 f.) angesprochen habe und dessen weitere Entwicklung ich sorgfältig beobachten werde (s. u. 3.9.1.5).

— Die Dienststelle hat sich im Berichtsjahr erstmals näher mit dem Problem der Personalinformationssysteme befaßt und eines davon, das des Bundesministeriums der Verteidigung, einer ersten Prüfung unterzogen. Da diese Prüfung erst in den letzten Wochen des Jahres stattfand, werden hier nur einige Hinweise gegeben (s. u. 3.5.5.1). Weitere Aspekte des Datenschutzes im Personalwesen sind im Abschnitt 3.5 behandelt.

— Sowohl durch intensive Besprechung der organisatorischen Fragen wie durch Ausübung des Akteneinsichtsrechts in Einzelfällen konnte der Datenschutz bei der Arbeitsverwaltung weiter verbessert werden. Die Bundesanstalt für Arbeit hat im Berichtsjahr beachtliche Anstrengungen unternommen, den Datenschutz in ihrem Bereich mit größerer Effektivität durchzusetzen. Die bei mir eingegangenen Beschwerden über den Umgang mit Daten in der Arbeitsverwaltung, die zum Teil als begründet erkannt wurden, haben die Bundesanstalt auch zu verstärkten Schulungsbemühungen in Sachen Datenschutz veranlaßt (zum ganzen Bereich s. u. 3.10.5).

— An den Beratungen des Gesetzgebers über das Melderechtsrahmengesetz, den Datenschutz in der Sozialverwaltung (SGB X) und das Personalausweisgesetz war ich durch mündliche und

schriftliche Stellungnahmen in verschiedenen Phasen beteiligt. Es ist gelungen, in alle diese Gesetze über die ohnehin vorgesehenen Sicherungen hinaus zusätzliche Datenschutzbestimmungen einzufügen. Einige Fragen sind nicht so entschieden worden, wie ich es vorgeschlagen habe; auch die Landesbeauftragten für den Datenschutz haben an manchen Vorschriften insbesondere des Sozialgesetzbuches Kritik geübt. Insgesamt stellen jedoch diese Gesetze erhebliche Fortschritte für den bereichsspezifischen Datenschutz dar. Die verbliebenen Zweifelsfragen werden wahrscheinlich im Rahmen der weiteren Prüfungstätigkeit behandelt werden müssen.

Über eine Reihe anderer Initiativen, die von meiner Dienststelle ausgegangen sind (z. B. in den Bereichen von Justiz- und Steuerverwaltung sowie Statistik und Forschung, Bibliothekswesen und Medien), kann in diesem Überblick nicht berichtet werden; dazu sei auf die entsprechenden folgenden Abschnitte verwiesen. Doch sind drei Querschnittsaufgaben besonders anzusprechen, die einen erheblichen Teil der Arbeitskapazität meiner Dienststelle in Anspruch genommen haben:

— Nicht nur in den Bereichen, die öffentliche Diskussionen ausgelöst haben, sondern auch in „normalen" Behörden wurden datenschutzrechtliche Prüfungen vorgenommen. Zur Datensicherung ergaben sie, kurz gesagt, daß insgesamt das Bewußtsein für die Notwendigkeit umfassender Datenschutzkonzeptionen gewachsen ist und daß die vorgesehenen Sicherungsmaßnahmen im großen und ganzen ausreichen. Doch wurde, wie in den Vorjahren, eine Reihe von Schwachstellen aufgedeckt. Nach wie vor fehlt es auch in vielen Behörden an der notwendigen Übersicht über alle Datenverarbeitungsvorgänge in ihrem eigenen Bereich. In einem Fall war dieses Defizit gravierend.

  Außerdem zeigten einige Eingaben, daß die „Schnittstelle Maschine/Mensch" nicht immer richtig gestaltet ist. Der für eine ordnungsgemäße Datenverarbeitung unverzichtbare Änderungsdienst weist gelegentlich deutliche Mängel auf; Mitteilungen von Betroffenen an Behörden werden wegen mangelhafter Organisation nicht oder zu spät verarbeitet. In einem Falle wurde schlaglichtartig erkennbar, daß der automatischen Verarbeitung von der Aufgabe her Grenzen gesetzt sind: Ein Verfahren, das auf die Aufdeckung der Doppelvergabe von Versicherungsnummern abzielte, war unter Ausschluß menschlicher Tätigkeit so organisisert, daß zumindest in einem Fall, der uns von einem Betroffenen mitgeteilt wurde, die Daten zweier verschiedener Personen zusammengefügt waren und nur unter Schwierigkeiten wieder auseinandergezogen werden konnten. Die betroffene Verwaltungsstelle hat auf unsere Aufforderung hin das Verfahren bereinigt.

— Die Öffentlichkeitsarbeit mit dem Ziel, die Probleme von Datenverarbeitung und Datenschutz einem breiten Publikum bewußt zu machen und weiterführende Informationen an Rat- und Auskunftsuchende zu vermitteln, hat mich und meine Mitarbeiter im Berichtsjahr wiederum stark beschäftigt. Die verschiedenen Broschüren, die wir herausgegeben haben, finden Anklang; in Vorträgen und Diskussionen wird an vielen Orten über den Datenschutz und seine Verwirklichung gesprochen.

— Ich habe mich bemüht, auch die internationale Zusammenarbeit auf dem Gebiet des Datenschutzes weiter zu pflegen (vgl. Abschnitt 5). Heute kann man sagen, daß die Bundesrepublik Deutschland im internationalen Vergleich der Datenschutzpraxis eine allgemein anerkannte Position einnimmt.

Wenn dieser Bericht mit einem relativ günstigen Gesamtergebnis abschließt, darf nicht übersehen werden, daß nach wie vor Sorgen wegen der weiteren Entwicklung der Informationstechnologie begründet sind. Schließt man aus dem bisherigen Verlauf auf die Zukunft, so muß mit weiteren großen Veränderungen in Technik und Organisation der Informationsverarbeitung gerechnet werden. Neue Medien sind bereits in der Erprobung oder stehen kurz davor. „Heimcomputer" drängen auf den Markt, und manche möglichen Entwicklungen auf dem Gebiet der Datenübertragung und -auswertung sind wahrscheinlich noch kaum bekannt. Die Chance, solche Veränderungen rechtlich in den Griff zu bekommen, indem man ihnen grundrechtschützende und machtverteilende Grenzen setzt, ist gegeben. Um sie zu nutzen, müssen die Geschehnisse in vielen Bereichen des Wirtschafts- und Soziallebens sorgfältig verfolgt werden. Dazu ist insbesondere auch die wissenschaftliche Erforschung der vorhersehbaren sozialen Folgen technischen Fortschritts unverzichtbar. Ich unterstütze deshalb Bestrebungen der verschiedenen wissenschaftsfördernden Institutionen, angefangen beim Bundesministerium für Forschung und Technologie, solche Vorhaben anzuregen und zu fördern, und bedauere, daß die nötige Förderung in einem wichtigen Falle bisher nicht gewährleistet ist (s. u. 3.8.2).

1.3 Verhältnis zu anderen Stellen

Die Arbeitskontakte zu den zu kontrollierenden und zu beratenden Bundesbehörden waren überwiegend von Offenheit und dem beiderseitigen Bestreben geprägt, die anstehenden Probleme in argumentativer Auseinandersetzung zu lösen. Bei einigen Stellen war jedoch im Berichtsjahr die Tendenz erkennbar, die Befugnisse meines Amtes einengend auszulegen, und die Beantwortung meiner Fragen zog sich in manchen Fällen zu lange hin. So hatte ich Veranlassung darauf hinzuweisen, daß das Datenschutzgesetz mir die Kontrolle auch der Einhaltung „anderer Vorschriften über den Datenschutz" zuweist (s. u. 4.1). Außerdem mußte einige Male nachdrücklich auf die Befugnisse nach § 19 Abs. 3 BDSG hingewiesen werden. Das Bundeskanzleramt hat erstmals in zwei Einzelfällen von dem Sicherheitsvorbehalt des § 19 Abs. 3 Satz 4 BDSG Gebrauch gemacht (s. u. 3.11.4). Die Auseinandersetzung mit der Finanzverwaltung über das Verhältnis von Steuergeheimnis und meiner Prüfungsbefugnis dauert an (s. u. 3.3.3).

1.4 Eingaben

Auch in diesem Berichtsjahr haben sich wieder sehr viele Bürger an mich gewandt, um Beschwerden vorzubringen oder Auskunft zu Rechtsfragen und allgemeine Informationen zu erhalten. Die Eingaben betrafen insbesondere die Bundespost, die Arbeitsverwaltung, die Sozialversicherung und die Sicherheitsbehörden.

Daneben erreichen mich nach wie vor fast täglich Anfragen, wo eigene Daten der Betroffenen gespeichert sein könnten. Konkrete Hinweise kann ich in diesen Fällen nur geben, wenn mir Anhaltspunkte für bestimmte Verwaltungsbeziehungen vom Betroffenen selbst genannt werden. In den meisten Fällen muß ich mich darauf beschränken, den anfragenden Bürgern durch allgemeine Hinweise oder Übersendung der Broschüre „Der Bürger und seine Daten" eine Hilfe für weitere eigene Überlegungen zu geben.

In einem Fall wurde ein Beamter gerügt, weil er bei einer Eingabe an mich den Dienstweg nicht eingehalten habe. Die parallele Problematik eines Eingriffs in das Petitionsrecht gem. § 7 des Gesetzes über den Wehrbeauftragten vom 26. Juni 1957 (BGBl. I S. 652) hat auch schon den Wehrbeauftragten des Deutschen Bundestages beschäftigt (vgl. Jahresbericht 1979, BT-Drucksache (8/3800, S. 9 unter 2.3).

Ebensowenig wie der Ausübung des Petitionsrechts nach Artikel 17 GG grundsätzlich die Einhaltung des Dienstweges entgegengehalten werden darf, darf dies bei der Anrufung des Bundesbeauftragten für den Datenschutz gemäß § 21 BDSG geschehen. § 21 gibt *jedermann* dieses Recht ohne Einschränkungen. Zwar sind Anträge und Beschwerden des Beamten auf dem Dienstwege vorzulegen — vgl. § 171 BBG, § 59 BRRG, § 12 Abs. 1 Gemeinsame Geschäftsordnung der Bundesministerien, Allgemeiner Teil (GGO I); das gilt aber nicht bei Instanzen, die gesetzliche Unabhängigkeit genießen, einerlei, ob es sich dabei um Gerichte oder um Beauftragte — wie den Wehrbeauftragten, den Bundesbeauftragten für den Datenschutz usw. — handelt.

1.5 Kooperation mit anderen Datenschutzinstanzen

Die mir durch § 19 Abs. 5 BDSG aufgegebene Kooperation mit anderen Datenschutzkontrollinstanzen hat sich weiterhin als nützliche Hilfe für die Bewältigung übergreifender Probleme des Datenschutzes erwiesen. Es zeigt sich immer wieder, daß nicht nur Auslegungsfragen zu den allgemeinen Bestimmungen des BDSG, die nahezu gleichlautend auch in den Landesdatenschutzgesetzen enthalten sind, sondern auch die rechtspolitischen Anliegen des Datenschutzes, Gesetzgebungsvorhaben, zu denen Beratung notwendig oder erwünscht ist, oder länderübergreifende Informationssysteme allgemein interessierenden Diskussionsstoff liefern oder sogar gemeinsames Vorgehen oder abgestimmte Stellungnahmen erfordern.

Die Ständige Konferenz der Datenschutzbeauftragten der Länder und des Bundes hat im Berichtsjahr viermal getagt. Behandelt wurden u. a. folgende Themen:

— Ausbau des INPOL-Systems

— Rasterfahndung des Bundeskriminalamts

— Gesetzgebungsvorhaben zum Melderechtsrahmengesetz, zum Personalausweisgesetz und zum Zehnten Buch des Sozialgesetzbuchs (Sozialdatenschutz)

— datenschutzrechtliche Probleme bei den Neuen Medien (Bildschirmtext, Kabelfernsehen)

— Anordnung über Mitteilungen in Strafsachen

— Datenschutzkonvention des Europarats.

Die Beratungen wurden teilweise durch ad hoc gebildete Arbeitsgruppen vorbereitet. Die Ergebnisse fanden in unterschiedlicher Weise ihren Niederschlag in übereinstimmenden Stellungnahmen gegenüber den jeweiligen Regierungen, gemeinsamen Presseerklärungen oder der Verabredung einheitlichen Vorgehens in bestimmten Kontroll- oder Beratungsaktivitäten.

Im Berichtszeitraum habe ich — wie im Vorjahr — an der Koordinierung zwischen den obersten Datenschutzaufsichtsbehörden der Länder im Rahmen des „Düsseldorfer Kreises" teilgenommen. Im Vordergrund der Beratungen standen Fragen der Anwendung des BDSG auf einzelne Berufs- und Wirtschaftszweige (z. B. Kreditschutzorganisationen, Auskunfteien, Wirtschafts-/Steuerberater, Markt- und Meinungsforschungsinstitute, Partnerschaftsvermittlungen) sowie allgemeine Fragen zur Auslegung der gesetzlichen Regelungen im ersten, dritten und vierten Abschnitt des BDSG (z. B. Umfang des Auskunftsanspruchs, Zeitpunkt der Benachrichtigung, Datenverarbeitung im Auftrag).

In zahlreichen Fällen zeigten sich Überschneidungen zu Problemen der Datenverarbeitung im öffentlichen Bereich, z. B. Einwilligung des Betroffenen in die Datenverarbeitung; Abgrenzung des Medienprivilegs; Übermittlung an kirchliche Einrichtungen; Weitergabe von Informationen an Strafverfolgungsbehörden; Verwendung von Daten aus öffentlichen Verzeichnissen; Datenschutz im Archivwesen; Konkretisierung des Begriffs „schutzwürdige Belange".

Die Zusammenarbeit hat sich bewährt; in fast allen Fällen wurden Lösungen gefunden, die von allen Beteiligten getragen werden. Es besteht gute Aussicht, in den wesentlichen Grundsätzen des Datenschutzrechts die Einheitlichkeit der Auslegung und Anwendung auch in Zukunft zu erhalten.

Ich habe im Berichtsjahr auch eine gemeinsame Sitzung mit den Landesbeauftragten und den Vertretern der obersten Aufsichtsbehörden der Länder einberufen, um deren Auffassungen zur Novellierung des BDSG kennenzulernen. Da die Sitzung im zeitlichen Zusammenhang mit der vom Innenausschuß des Bundestages veranstalteten Anhörung zu den aus der Mitte des Bundestages eingebrachten Änderungsentwürfen (s. u. 2.1) stand, waren mir die

so gewonnenen zusätzlichen Erfahrungen eine wertvolle Hilfe bei meiner Argumentation im Hearing.

Schließlich habe ich auch wieder die innerbehördlichen Datenschutzbeauftragten der obersten Bundesbehörden (§ 15 BDSG) zu einem Erfahrungsaustausch eingeladen. Dabei ging es mir vor allem darum, Reaktionen auf meinen zweiten Tätigkeitsbericht zu erhalten, Kritik zu hören, aber auch zu erfahren, inwieweit meine Bemerkungen zu konkreten Maßnahmen geführt haben. Bei dieser Gelegenheit stellte sich heraus, daß in den Bundesministerien nach wie vor bei der Anwendung des BDSG in der Zusammenarbeit mit den Personalräten Probleme auftreten, die sich wohl nur durch bereichsspezifische Gesetzgebung befriedigend lösen lassen werden (vgl. dazu 2. TB S. 24). Auch Stellung und Befugnisse der innerbehördlichen Datenschutzbeauftragten wurden diskutiert.

Insgesamt läßt sich feststellen, daß sich die für die Kooperation mit den anderen Datenschutzkontrollinstanzen gefundenen Formen bewährt haben und es mir ermöglichen, dem Auftrag des § 19 Abs. 5 BDSG gerecht zu werden.

1.6 Arbeitskontakte mit Spitzenorganisationen

Das Datenschutzrecht ist auch ein Schutzrecht für die Beschäftigten, sei es im öffentlichen Dienst, sei es in der Wirtschaft. Deshalb habe ich Gespräche mit den Spitzenorganisationen der Beschäftigten im öffentlichen Dienst geführt, nämlich mit dem Vorstand des Deutschen Beamtenbundes und dem Geschäftsführenden Vorstand des Deutschen Gewerkschaftsbundes. Sinn derartiger Gespräche ist nicht die Behandlung von Einzelfragen, sondern die Erörterung grundsätzlicher Probleme.

1.7 Öffentlichkeitsarbeit

Die Broschüre „Was bringt das Datenschutzgesetz?" ist, wie im letzten Berichtsjahr, stark nachgefragt worden. Diese Informationsschrift hat inzwischen eine Auflage von 63 000 Exemplaren erreicht. Nach nunmehr fast dreijähriger Tätigkeit meiner Dienststelle erschien es mir notwendig, sie inhaltlich zu überarbeiten und dabei einige Ergänzungen aufzunehmen, um dem Leser noch mehr Informationen über die Grundzüge des Datenschutzrechts zu bieten. Auch sollten einige Erfahrungen aus der praktischen Arbeit mit dem Gesetz einfließen. Die überarbeitete Neuauflage ist unter dem Titel „Bürgerfibel Datenschutz?" soeben erschienen und kann bei mir kostenlos bezogen werden.

Auch von der neuen Broschüre „Der Bürger und seine Daten", die ich in Gemeinschaftsarbeit mit den Landesbeauftragten für den Datenschutz, der Datenschutzkommission Rheinland-Pfalz sowie den Aufsichtsbehörden der Länder erstellt habe, sind bereits ca. 50 000 Exemplare versandt worden. Die Schrift gibt — ausgehend von typischen Verwaltungsbeziehungen und den sich aus den verschiedensten Lebensbereichen ergebenen Sozialkontakten des Bürgers — einen Überblick über daraus folgende Datenspeicherungen. Sie soll so dem Bürger helfen, die Stellen ausfindig zu machen, bei denen er sein Recht auf Auskunft über die zu seiner Person gespeicherten Daten geltend machen kann.

Beide Broschüren werden vor allem von Schulen, Universitäten, Vereinigungen und Verbänden in großem Umfange angefordert.

Mein zweiter Tätigkeitsbericht wurde als Sonderdruck in 3 000 Exemplaren an Interessierte abgegeben.

Ich halte es auch weiterhin für eine meiner wichtigsten Aufgaben, das Anliegen Datenschutz in der Bevölkerung zu verbreiten und dem Bürger deutlich zu machen, daß er selbst ein wichtiger Garant für einen rechtmäßigen und fairen Umgang mit seinen Daten ist, indem er sein Auskunftsrecht als primäres Kontrollmittel wahrnimmt. Solche Appelle an den Bürger sind immer dann am wirkungsvollsten, wenn sie sich aus praktischen Fallgestaltungen entwickeln lassen oder ihnen aktuelle Feststellungen aus meiner Kontrolltätigkeit zugrunde gelegt werden können. Ich habe deshalb auch in diesem Berichtszeitraum das immer wieder feststellbare breite Interesse der Medien an Fragen des Datenschutzes genutzt und zahlreiche Presse- und Rundfunkinterviews gegeben. Die mir daraufhin zugegangenen Zuschriften bestätigen, daß in der Bevölkerung ein Bedürfnis nach aktueller Information besteht und diese auch „ankommt". Daneben habe ich einige Presseveröffentlichungen zu aktuellen Fragen herausgegeben und darin meine zum Teil kritische Beurteilung von Datenverarbeitungsmaßnahmen oder -planungen einer breiten Öffentlichkeit zugänglich gemacht.

1.8 Dateienregister

Der Umfang der Anmeldungen zum Register der automatisch betriebenen Dateien der Behörden und sonstigen öffentlichen Stellen des Bundes ist im Laufe des Jahres 1980 auf ca. 1 000 angestiegen. Für örtliche Kontrollen sind diese Meldungen neben den von den Bundesstellen selbst zu führenden Übersichten über die Art der gespeicherten personenbezogenen Daten nach § 15 BDSG eine erste Grundlage. Als Mangel hat es sich erwiesen, daß die manuell geführten Dateien nicht zum Register angemeldet zu werden brauchen. Die Veröffentlichungen dieser Dateien nach § 12 BDSG füllen diese Lücke nicht; sie sind oft unzulänglich, weil die dazu abgegebenen Meldungen der datenverarbeitenden Stellen inhaltlich ungeprüft übernommen werden. Ich wiederhole deshalb meinen Vorschlag (vgl. 2. TB S. 65 f.), die Zuständigkeiten für Veröffentlichungen und Dateienregister beim Bundesbeauftragten zusammenzufassen. Dies wäre nur durch eine Novellierung der gesetzlichen Vorschriften erreichbar. Sie könnte zu größerer Transparenz und einer noch effektiveren Nutzung der Dateienmeldungen führen.

Auch im Berichtsjahr 1980 haben nur ganz wenige Bürger ihr Recht auf Einsichtnahme in das Register

genutzt. Einige Bürger haben einen Gesamtabdruck des Registers angefordert. Solchen Wünschen konnte ich wegen des damit verbundenen Aufwands nicht entsprechen. Auszüge aus dem Register habe ich vereinzelt versandt, obwohl dies im BDSG nicht vorgeschrieben ist.

An eine Umstellung der manuellen Führung des Registers auf ein automatisiertes Verfahren ist zur Zeit nicht gedacht. Ich bin jedoch weiterhin darum bemüht, die Meldungen inhaltlich aufzubereiten und durch unterschiedliche Sortierfolgen und Zugriffsmethoden die Aussagekraft des Registers zu verbessern.

2 Fortentwicklung des Datenschutzrechts

2.1 Novellierung des BDSG — Anhörung am 21./22. April 1980 —

Nachdem die CDU/CSU-Fraktion und die Koalitionsfraktionen des Deutschen Bundestages in der vergangenen Legislaturperiode je einen Gesetzentwurf zur Änderung des BDSG eingebracht hatten (Drucksachen 8/3608 und 8/3703), veranstalteten die Berichterstatter des federführenden Innenausschusses zusammen mit Vertretern der übrigen beteiligten Ausschüsse eine interne Anhörung von Sachverständigen zu den Schwerpunkten beider Entwürfe. Eingeladen waren dazu die Datenschutzbeauftragten des Bundes und eines Landes, Aufsichtsbehörden der Länder für den Datenschutz, Vertreter der Exekutive, Verbände und einzelne Wissenschaftler. Ich habe zu den mir gestellten Fragen eine schriftliche Stellungnahme eingereicht und hatte darüber hinaus Gelegenheit, sie in der Anhörung, die am 21. und 22. April 1980 stattfand, eingehend zu erläutern. Ich habe dabei die vorgelegten Gesetzentwürfe als einen ersten begrüßenswerten Schritt zur Fortentwicklung des BDSG gewürdigt, zugleich aber deutlich gemacht, daß sie nur einen Teil des Notwendigen darstellen und der Ausbau des bereichsspezifischen Datenschutzes dadurch keineswegs überflüssig wird. Ferner habe ich auf meine im zweiten Tätigkeitsbericht (2. TB S. 60 ff.) dargestellten Überlegungen zur Fortentwicklung des Datenschutzrechts verwiesen.

Meine Stellungnahme zu den einzelnen in der Anhörung behandelten Punkten wiederhole ich hier in verkürzter Form:

— Die Schaffung eines *Schadensersatzanspruchs ohne Verschuldensvoraussetzung* ist grundsätzlich positiv zu bewerten. Der Anspruch sollte aber nicht auf den öffentlichen Bereich beschränkt, sondern auch auf den nicht-öffentlichen Bereich erstreckt werden. Eine aktuelle Notwendigkeit für eine solche Regelung ist allerdings nicht dadurch zu begründen, daß etwa eine Vielzahl von Schadensersatzklagen wegen der Verschuldungsvoraussetzung abgewiesen worden wäre. Jedenfalls im Bereich des Bundes konnte bisher ein dringendes Bedürfnis nicht festgestellt werden. Andererseits wäre die zweifellos entstehende mittelbare Wirkung einer Schadensersatzregelung zu begrüßen, insofern nämlich, als drohende Schadensersatzansprüche zu mehr Vorsicht bei der Datenverarbeitung führen dürften.

— Die Beseitigung der *Gebührenpflichtigkeit* bzw. Entgeltlichkeit der Auskunft im öffentlichen *und* im nicht-öffentlichen Bereich ist unbedingt zu bejahen. Ein Mißbrauch eines kostenfreien Auskunftsanspruchs ist nicht zu befürchten.

— Eine Änderung oder Aufhebung des *Dateibegriffs* gehört nach meinem Dafürhalten zu den schwierigsten Problemen, die bei einer Novellierung des BDSG zu bedenken wären. Lösungsansätze müssen einerseits gewährleisten, daß der Anwendungsbereich des BDSG überschaubar bleibt, sie dürfen andererseits nicht Erscheinungsformen der Datenverarbeitung ausklammern, die nach den praktischen Erfahrungen schutzbedürftig sind. Eine Beschränkung des BDSG auf automatisierte Verfahren wäre jedenfalls nicht akzeptabel (S. u. 3.10.5, vgl. auch 2. TB S. 60 f.).

— Eine *Ausweitung des Datenverarbeitungsbegriffes*, der dann z. B. die Datenerhebung und die Datennutzung insbesondere durch Bekanntgabe innerhalb der speichernden Stelle als geschützte Phasen der Datenverarbeitung einbeziehen würde, ist aus meiner Sicht positiv zu beurteilen.

— Die *Ausdehnung des Zweckbestimmungsprinzips* in der Weise, daß der Empfänger übermittelter Daten diese grundsätzlich nur für den Zweck verwenden darf, zu dessen Erfüllung sie ihm übermittelt wurden, wäre nachhaltig zu begrüßen. Die vorgeschlagene Regelung sollte für Datenübermittlungen nach dem zweiten, dritten und vierten Abschnitt des Gesetzes gelten.

— Die *Anlage zu § 6 Abs. 1 Satz 1 BDSG* ist daraufhin zu überprüfen, inwieweit sich als Folge der vorgesehenen Neuregelungen Änderungen als notwendig erweisen.

— Eine aktuelle Notwendigkeit für eine *Streichung des § 7 Abs. 3* mit der Folge, daß auf Personaldaten der zweite Abschnitt des BDSG anzuwenden wäre, ist aus meiner Sicht nicht erkennbar.

— Die *Verrechtlichung der Aufgaben*, zu deren Erfüllung Daten verarbeitet werden dürfen, ist grundsätzlich zu begrüßen. Es wäre sogar zu überlegen, ob nicht die Regelung des bayerischen Datenschutzgesetzes übernommen werden sollte, die nicht nur fordert, daß die Aufgaben, zu de-

ren Erfüllung Datenverarbeitung betrieben wird, durch Rechtsnorm „geregelt" sind, sondern darüber hinaus verlangt, daß die Aufgaben der speichernden/übermittelnden Stelle bzw. dem Empfänger durch Rechtsnorm „zugewiesen" sind.

— Eine *Benachrichtigung im öffentlichen Bereich* halte ich nicht für zweckmäßig. Es wäre abzusehen, daß dadurch Benachrichtigungen in solchen Massen erforderlich würden, daß die öffentliche Verwaltung überfordert, die Bürger aber eher irritiert als auf die wirklich bedeutsamen Fälle aufmerksam gemacht würden. Die notwendige Transparenz ließe sich auch durch verbesserte Formulare, Merkblätter und sonstige Formen der allgemeinen Unterrichtung über Informationswege und Speicherungsmethoden herstellen.

— Wenn im Rahmen regelmäßiger Datenübermittlungen Empfänger unrichtiger Daten von einer *Berichtigung unverzüglich verständigt* werden, so ist dies zu begrüßen. Andererseits ist darauf zu achten, daß unnötige Datenübermittlungen unterbleiben. So sollte die Mitteilung einer Berichtigung den Empfänger nicht dazu veranlassen, bereits erledigte Vorgänge wieder aufzugreifen. Dies wäre denkbar, wenn die Berichtigung schon gesperrte oder gelöschte Daten betrifft.

— Gegen die vorgeschlagene *Pflicht zur Löschung* nicht mehr benötigter Daten könnten sich Bedenken insofern ergeben, als schutzwürdige Belange Betroffener möglicherweise gerade dadurch beeinträchtigt werden, daß die Daten im Falle einer späteren Beweisnot nicht mehr zur Verfügung stehen würden. Auch wichtige Interessen der Archivierung könnten berührt sein.

— Je früher der Bundesbeauftragte über *Automationsprojekte und Planungen für Informationssysteme* unterrichtet wird, um so effektiver kann er seine Beratungsaufgabe wahrnehmen. Eine gesetzliche Benachrichtigungspflicht wird daher nachdrücklich unterstützt.

— Die Streichung des Geburtsdatums und des Berufs aus dem Katalog der sog. *freien Daten* in § 24 BDSG ist grundsätzlich zu begrüßen. Problematisch erschiene allerdings die Freigabe des gemeinsamen Gruppenmerkmals. Dieser Vorschlag würde die Übermittlung einer beliebigen, im Gesetz auch nicht andeutungsweise genannten Zusatzangabe ermöglichen. Nach meiner Auffassung begegnet die freie Übermittlung von Daten, die im Regelfall im Rahmen eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses gespeichert werden und damit ebenfalls den Prinzipien vertraglicher Rechtsbeziehungen unterliegen, grundsätzlichen Bedenken.

— Die Einführung eines *Widerspruchsrechts des Betroffenen gegen Datenübermittlungen für Zwecke der Werbung oder der Markt- und Meinungsforschung* wäre zu begrüßen. Auch der vorgesehene Anspruch auf Löschung der für Zwecke der Werbung gespeicherten Daten entspricht einem Anliegen vieler Bürger und ist positiv zu werten. Wünschenswert wäre außerdem, die gleiche Regelung auch im dritten Abschnitt vorzusehen, um den Löschungsanspruch auch gegenüber Unternehmen zu gewähren, die Daten für eigene Werbezwecke speichern.

  Wichtig wäre darüber hinaus eine Vorschrift, durch die das werbende Unternehmen verpflichtet würde, die Herkunft der Daten anzugeben, und zwar nicht erst im Rahmen des Auskunftsanspruchs des Betroffenen, sondern schon zugleich mit der Werbesendung.

— Die Einführung einer Pflicht zur Unterrichtung des Betroffenen über Maßnahmen, die aufgrund *negativer Kreditauskünfte* getroffen werden, wäre zu begrüßen. Wichtig wäre darüber hinaus eine ergänzende Vorschrift, die dazu verpflichtet, in diesen Fällen auch die Herkunft der (negativen) Daten mitzuteilen.

— Die *Absicherung des betrieblichen Datenschutzbeauftragten* durch einen besonderen Kündigungsschutz würde die Unabhängigkeit des Datenschutzbeauftragten stärken und könnte dazu beitragen, daß er die Interessen des Personals und des Datenschutzes gegenüber der Unternehmensleitung nachdrücklicher vertreten kann. Die vorgeschlagene Regelung ist daher positiv zu beurteilen. Die Beschränkung auf diejenigen Datenschutzbeauftragten, die Arbeitnehmer sind und keine weiteren Aufgaben wahrnehmen, halte ich allerdings für sehr problematisch.

Ich hoffe, daß die in der Anhörung gewonnenen Erkenntnisse sich in der von der Bundesregierung angekündigten Novellierung des BDSG niederschlagen. Zur Vorbereitung erschiene es mir vordringlich, eine Bestandsaufnahme der Probleme vorzunehmen, die unter dem geltenden Recht entstanden sind. Das besondere Augenmerk müßte dabei auf die Frage gerichtet werden, ob Informationsbestände und Verarbeitungsformen, für die ein Regelungsbedürfnis vorliegt, vom BDSG bisher nicht erfaßt werden und dadurch ein Defizit an Datenschutz entsteht, das durch bereichsspezifische Bestimmungen nicht ausgeglichen werden kann.

2.2 Entwurf von Verwaltungsvorschriften

Um Schwierigkeiten und Zweifelsfragen bei der Anwendung des BDSG in den Behörden und sonstigen öffentlichen Stellen des Bundes so weit wie möglich generell zu klären, bereitet der Bundesminister des Innern unter maßgeblicher Beteiligung einer Arbeitsgruppe aus verschiedenen Ressorts einen Entwurf von Allgemeinen Verwaltungsvorschriften (VwV) zum BDSG für den Bereich der Bundesverwaltung vor. Ich habe mich im Rahmen dieser Arbeitsgruppe an den Arbeiten beteiligt, um meine Vorstellungen über die Auslegung des BDSG zur Geltung zu bringen und um dazu beizutragen, daß den datenverarbeitenden Stellen der Bundesverwaltung eine wirksame Hilfe bei der Umsetzung des Gesetzes in den Verwaltungsvollzug gegeben wird.

In vielen Problemfällen ist es dabei gelungen, Regelungen zu finden, die dem Schutzzweck des Gesetzes

angemessen sind. Ich habe meine Auffassungen, die ich auch weiterhin meinen Kontrollen zugrunde legen werde, jedoch nicht immer durchsetzen können. Manche Formulierungen vermitteln den Eindruck, als seien sie von dem Bestreben geprägt, durch das BDSG möglichst wenig Umstellungen oder gar Erschwernisse hinnehmen zu müssen.

Ein typisches Beispiel dafür ist die restriktive Eingrenzung des Schutzbereiches des Gesetzes. Nach § 1 Abs. 2 BDSG erstreckt sich dieser auf „... personenbezogene Daten, die in *Dateien* gespeichert, verändert, gelöscht oder aus Dateien übermittelt werden". Nach meiner Auffassung bedeutet dies: Wenn bestimmte personenbezogene Daten *sowohl* in Dateien gespeichert *als auch* in anderen Darstellungsformen, etwa in Listen, bei der speichernden Stelle vorhanden sind, dann unterliegen sie stets den Vorschriften des BDSG. So gelten die Übermittlungsvorschriften auch dann, wenn die Übermittlung nicht aus der Datei, sondern aus einem anderen Speichermedium stattfindet. Andernfalls wäre es leicht, durch Verwendung der nicht in der Datei gespeicherten Daten die Anwendung des BDSG zu umgehen. Der gegenwärtige Entwurf der VwV folgt dieser naheliegenden Auslegung nicht, sondern bezieht Daten in anderen Erscheinungsformen nur ein, soweit sie aus Dateien *entnommen* sind. Danach unterlägen z. B. zwar in einer Akte aufbewahrte Computerausdrucke den Schutzvorschriften, nicht aber die in derselben Akte abgehefteten, inhaltsgleichen Angaben des Betroffenen oder anderer Behörden, die erst zu der Datenspeicherung geführt haben. Für die Frage, ob eine Datenübermittlung aus dieser Akte nach dem BDSG zu beurteilen ist oder nicht, käme es dann darauf an, ob derjenige, der die Daten weitergibt, diese dem Computerausdruck entnimmt oder die etwas weiter vorn abgehefteten Unterlagen als Quelle benutzt. Auch die Durchführung einer gesetzlich vorgeschriebenen Löschung der Daten dürfte sich bei dieser Auslegung darauf beschränken, daß nur die Daten in der Datei gelöscht und die Computerausdrucke aus der Akte entfernt werden, die nunmehr „gelöschten" Daten aber in anderer Form in der Akte enthalten bleiben und der Behörde weiterhin zur Verfügung stehen. Die Auswirkungen der in den VwV vorgesehenen wenig bürgerfreundlichen Auslegung machen deutlich, daß dadurch der Datenschutz in nicht mehr erträglichem Maße verkürzt würde.

Ein weiteres Beispiel für eine Lösung, die möglicherweise die Verwaltung entlastet, aber wenig datenschutz- und bürgerfreundlich ist, findet sich in der Regelung über die Pflicht zur Aufklärung des Bürgers in den Fällen, in denen eine Behörde von ihm selbst personenbezogene Daten erhebt. § 9 Abs. 2 BDSG schreibt dafür vor, daß der Bürger auf die entsprechende Rechtsvorschrift oder auf die Freiwilligkeit seiner Angaben hinzuweisen ist. Der derzeitige Entwurf der VwV trifft die Aussage, daß ein solcher Hinweis entfallen kann, wenn die Daten nicht in Dateien gespeichert werden sollen.

Ich halte diese Interpretation, die damit begründet wird, daß das BDSG nur in Dateien gespeicherte Daten schützt, für falsch und habe dies schon in meinem zweiten Tätigkeitsbericht (2. TB. S. 61) näher ausgeführt. Da sie nunmehr Aufnahme in die VV finden soll, sehe ich mich veranlaßt, meinen Standpunkt nochmals zu verdeutlichen. § 9 Abs. 2 BDSG ist eine Grundsatzvorschrift, in der der Gesetzesvorbehalt für den Umgang mit personenbezogenen Daten und das Selbstbestimmungsrecht des Betroffenen klar zum Ausdruck kommen. Sie war im Regierungsentwurf zum BDSG nicht enthalten, sondern ist erst während des Gesetzgebungsverfahrens im Bundestag in den Entwurf eingefügt worden. Dafür gab es gewichtige Gründe: Die Datenerhebung beim Betroffenen ist in vielen Fällen die Basis für jede weitere Verarbeitung seiner Daten; ihre Rechtmäßigkeit oder Rechtswidrigkeit wirkt in der weiteren Verwendung der Daten fort. Ist schon die Erhebung der Daten rechtswidrig, so kann ihre anschließende Verarbeitung nicht rechtmäßig sein. Die eigentliche Bedeutung des § 9 Abs. 2 besteht aber darin, für den Betroffenen die Datenverarbeitung auch hinsichtlich ihrer Rechtsgrundlagen transparent werden zu lassen und ihm Anhaltspunkte dafür zu liefern, ob er Daten, die ihm abverlangt werden, hergeben muß oder nicht, worauf sich eine eventuell bestehende Rechtsverpflichtung stützt und welche Verwendungszwecke verfolgt werden. Mit dem Sinn einer solchen Aufklärungspflicht, die weitergreifend auch in § 25 Verwaltungsverfahrensgesetz ihren Ausdruck gefunden hat, wäre es nicht zu vereinbaren, wenn sie davon abhängig gemacht würde, in welchem technischen oder organisatorischen Verfahren die weitere Verarbeitung erfolgt. Abgesehen davon, daß dies häufig bei der Erhebung noch nicht feststehen wird und bei einer erst nachträglichen Entscheidung, die Daten in Dateien zu übernehmen, die fehlende Aufklärung des Betroffenen nicht mehr nachgeholt werden kann, würde eine solche Auslegung auch Umgehungen insbesondere in den Fällen ermöglichen, in denen vermutet wird, daß der Betroffene freiwillig Angaben nicht machen würde. Im übrigen ist der Dateibezug in § 1 Abs. 2 Satz 1 ausdrücklich nur für die Speicherung, Veränderung, Löschung und Übermittlung personenbezogener Daten enthalten. Die Datenerhebung gehört zu keiner dieser Verarbeitungsformen, sie ist ihnen vielmehr vorgelagert. Diese Überlegungen bleiben in der gegenwärtig vorliegenden Fassung der VwV leider unberücksichtigt.

Schließlich hat sich der Bundesminister des Innern auch nicht meine Auffassung zu eigen gemacht, wonach die im BDSG mehrfach wiederkehrende Formulierung „... andere Vorschriften über den Datenschutz" (gemeint sind andere Vorschriften als die des BDSG) auch solche Bestimmungen erfaßt, die den Schutz personenbezogener Daten außerhalb von Dateien regeln. Vielmehr ist vorgesehen, in den VwV zu § 15 BDSG, der diese Formulierung verwendet, auszuführen, daß nur solche Vorschriften gemeint seien, die — wie das BDSG — Regelungen zur Datenverarbeitung in Dateien treffen. Abgesehen davon, daß dadurch das besondere Gebot, die Ausführung von Datenschutzvorschriften sicherzustellen, in weiten Anwendungsgebieten der Datenverarbeitung wieder aufgehoben wird und damit die beabsichtigte Wirkung verliert, hat ein solches Verständnis des Gesetzestextes auch unmittelbare Auswir-

kungen auf meine Kontrollzugehörigkeit, da diese in § 19 Abs. 1 Satz 1 BDSG durch die gleiche Formulierung beschrieben ist. Ich kann eine solche Einschränkung meiner Kompetenz nicht hinnehmen (s. u. 4.1) und muß im Interesse der Rechtsklarheit, die eine einheitliche Ausdeutung gleicher Gesetzesformulierungen verlangt, den Entwurf der VwV zu § 15 insoweit als Fehlinterpretation kritisieren.

2.3 Melderechtsrahmengesetz

Im Bundesgesetzblatt vom 22. August 1980 (BGBl. I S. 1429) ist das Melderechtsrahmengesetz (MRRG) verkündet worden, nachdem der Deutsche Bundestag in einer seiner letzten Sitzungen der 8. Legislaturperiode das Gesetz nach eingehenden Beratungen, an denen ich beteiligt war, beschlossen hat. Es ist nunmehr gelungen, für den Bereich des Meldewesens den diesem Verwaltungszweig und seinen Bedürfnissen angepaßten Datenschutz rahmengesetzlich zu schaffen. Ich hatte dies bereits in meiner gutachtlichen Stellungnahme zum Entwurf eines Bundesmeldegesetzes vom 15. Oktober 1978 gefordert. Da der Innenausschuß des Deutschen Bundestages mich zu seinen Beratungen hinzuzog, hatte ich Gelegenheit, meine Vorstellungen zu dem Gesetzentwurf aus der Sicht des Datenschutzes sowohl dem Ausschuß selbst als auch — in einer internen Anhörung am 10. Juni 1980 — den Berichterstattern vorzutragen. Ich habe mich darüber hinaus auch noch schriftlich gegenüber dem Ausschußvorsitzenden zu einigen mir wichtig erscheinenden Problemen, die sich aus dem Beratungsergebnis des Bundesrates ergaben, geäußert. Meine Vorschläge haben auch weitgehend Berücksichtigung gefunden.

Den Regierungsentwurf hatte ich bereits in meinem zweiten Tätigkeitsbericht eingehend gewürdigt (2 TB S. 13) und verzichte hier auf eine Wiederholung meiner Stellungnahme, soweit die angesprochenen Entwurfsvorschriften unverändert Gesetz geworden sind. Ich halte auch daran fest, daß das MRRG insgesamt gegenüber den bisher auch für dieses Spezialgebiet geltenden Auffangvorschriften der Datenschutzgesetze einen beachtlichen Fortschritt darstellt. In einigen Punkten ist es allerdings über Kompromißlösungen nicht hinausgekommen.

Im Regierungsentwurf zum MRRG (E-MRRG) war in § 1 (Aufgaben der Meldebehörden) festgelegt, daß die Meldebehörden die in ihrem Zuständigkeitsbereich wohnhaften Einwohner zu registrieren haben, um deren Identität und Wohnungen feststellen und nachweisen zu können. Im Absatz 2 war ferner folgendes vorgesehen:

„(2) Weitere Aufgaben dürfen die Meldebehörden nur wahrnehmen, wenn sie ihnen durch Rechtsvorschrift übertragen sind. Sie sollen ihnen nur übertragen werden, wenn ihre Erfüllung die Feststellung der Identität und der Wohnungen der Einwohner voraussetzt."

§ 1 Abs. 1 E-MRRG wurde unverändert Gesetz, § 1 Abs. 2 E-MRRG hingegen wurde gestrichen. Der Datenkatalog des § 2 Abs. 1 E—MRRG wurde trotz dieser Einschränkung aber nicht etwa reduziert, sondern sogar von 17 auf 19 Daten erweitert. Damit wird ein Datenkatalog, der vorher für viele Aufgaben bestimmt war, die sich im weitesten Sinne auf die Identitätsfeststellung und den Wohnungsnachweis beziehen sollten, jetzt auf die alleinige Aufgabe der Feststellung und des Nachweises der Identität und von Wohnungen der im Zuständigkeitsbereich der Meldebehörde wohnhaften Einwohner (§ 1 Abs. 1 MRRG) bezogen. Ich bezweifle, ob alle im § 2 Abs. 1 MRRG genannten Daten nur hierfür und nicht auch noch für andere, im MRRG nun nicht mehr bezeichnete Aufgaben der Meldebehörde bestimmt sind. § 1 Abs. 3 MRRG verlangt zwar, daß *alle* Daten, die die Meldebehörde im Melderegister speichert, nur nach dem MRRG selbst oder anderen Rechtsvorschriften erhoben, verarbeitet oder sonst genutzt werden, sorgt somit für eine rechtliche Begrenzung der Nutzung der Melderegister, enthält aber nicht die von mir geforderte Zweckbindung aller Daten, die die Meldebehörde speichern darf, an die Identitätsfeststellung und den Wohnungsnachweis. (Ausnahmen sind die nach § 2 Abs. 2 MRRG erlaubten Datenspeicherungen für Wahlen, Lohnsteuerkarten, Wehr- und Zivildienstüberwachung.) Es ist zu hoffen, daß die Landesgesetzgeber gleichwohl diese Zweckbindung berücksichtigen, wenn sie von der Ermächtigung des § 2 Abs. 3 MRRG Gebrauch machen. Nach § 2 Abs. 3 MRRG kann durch Landesgesetz bestimmt werden, daß für die Erfüllung der Aufgaben der Länder weitere als die in § 2 Abs. 1 und 2 MRRG bereits vorgesehenen Daten gespeichert werden.

Die Regelung über die Datenübermittlung an die öffentlich-rechtlichen Religionsgesellschaften (§ 19 MRRG) geht erheblich über das hinaus, was der Regierungsentwurf zu diesem Punkt vorsah. An die Religionsgesellschaft, der der Betroffene angehört, dürfen nunmehr zusätzlich zu den im Regierungsentwurf vorgesehenen Grunddaten auch noch Staatsangehörigkeit, Tag des Ein- und Auszugs aus einer Wohnung, Familienstand und Kinderzahl übermittelt werden. Von Familienangehörigen eines Kirchenmitglieds, die selbst nicht der gleichen oder gar keiner Religionsgesellschaft angehören, dürfen Daten übermittelt werden, auch ohne daß ein öffentliches Interesse vorliegt. Zwar ist das Recht des Betroffenen, in diesem Fall eine Übermittlungssperre zu verlangen, beibehalten worden; es ist jedoch in seiner datenschutzrechtlichen Wirkung kein voller Ausgleich für die von Amts wegen festzustellende Voraussetzung eines öffentlichen Interesses an der Datenübermittlung. Meine Bedenken gegen die Vorschrift insgesamt gründen sich auf die Verfassungsbestimmung, wonach niemand verpflichtet ist, seine religiöse Überzeugung zu offenbaren, und die Behörden nur soweit das Recht haben, nach der Religionszugehörigkeit zu fragen, als davon Rechte und Pflichten abhängen oder eine gesetzlich angeordnete statistische Erhebung dies erfordert. Die öffentlich-rechtlichen Religionsgesellschaften sind berechtigt, aufgrund der bürgerlichen Steuerlisten Steuern zu erheben (Artikel 140 GG in Verbindung mit Artikeln 136 Abs. 3 und 137 Abs. 6 Weimarer Reichsverfassung). Die Datenübermittlungen an die

Kirchen dienen jedoch nur ausnahmsweise der Erhebung der Kirchensteuer, diese wird fast überall durch die staatliche Finanzverwaltung eingezogen. Insoweit bleibt zweifelhaft, ob die vorgesehenen Datenübermittlungen überhaupt erforderlich und damit zulässig sind. Fehlt es aber an einer Rechtfertigung der Datenübermittlungen, wäre bereits die Datenerhebung verfassungsrechtlich bedenklich, wenn sie sich allein auf diesen Zweck stützte. Die Kirchen selbst begründen ihre Datenwünsche in erster Linie mit ihren Aufgaben der Seelsorge und der sozialen Betreuung. Da die Kirchen für diese Zwecke kein eigenes kirchliches Meldewesen unterhalten, ist ihr Bedürfnis, von den Meldebehörden Grunddaten ihrer Mitglieder zu erfahren, kaum zu bestreiten. Aus dem Staatskirchenrecht läßt sich eine Legitimation der staatlichen Behörden herleiten, den Kirchen solche Daten zur Verfügung zu stellen. Es würde jedoch genügen, die Übermittlungsregelung auf solche Daten zu beschränken, die nur die Mitglieder betreffen und die die kirchlichen Stellen in die Lage versetzen, an ihre Mitglieder heranzutreten, um von diesen selbst die für die Erfüllung kirchlicher Aufgaben erforderlichen weiteren Angaben zu erhalten.

Die Vorschrift über die sogenannte erweiterte Melderegisterauskunft (§ 21 Abs. 2 MRRG) an Private weicht insofern vom Regierungsentwurf ab, als vom Auskunftssuchenden lediglich ein „berechtigtes" Interesse glaubhaft gemacht zu werden braucht, während ursprünglich ein „rechtliches" Interesse verlangt wurde. Da ein berechtigtes Interesse schon immer dann angenommen werden kann, wenn es sich aus vernünftigen, von der Rechtsordnung nicht mißbilligten Überlegungen ergibt, während das rechtliche Interesse eindeutige Rechtspositionen voraussetzt, wurde der Zugang zu den der erweiterten Melderegisterauskunft unterliegenden Daten erheblich erleichtert. Zwar ist nunmehr vorgesehen, daß der Betroffene durch Nachweis eines seinerseits vorhandenen berechtigten Interesses die Auskunft verhindern kann, jedoch schmälert diese Regelung schon deshalb seinen Datenschutz, weil von ihm aktives Handeln verlangt wird. Abgesehen davon erscheint die Praktikabilität der Regelung fraglich, da die Meldebehörde eine im Einzelfall häufig schwierige Abwägung der beiderseitigen berechtigten Interessen vornehmen muß, die nach dem Regierungsentwurf bereits durch den Gesetzgeber getroffen werden sollte. Der Gesetzgeber ist hier einem Vorschlag des Bundesrates gefolgt, der die vorgesehene Regelung als überzogenen Schutz des Betroffenen zu Lasten der Wirtschaft bewertet hat. Ich teile diese Einschätzung nicht.

Eine nach meinem Eindruck problematische Regelung wurde in § 24 MRRG getroffen. Hier wird den Ländern gestattet, für eine Übergangsfrist bis zum 31. Dezember 1985 ein Einsichtsrecht der Polizeibehörden selbst, also ohne Mitwirkung der Meldebehörde, zu begründen. § 24 MRRG gilt allerdings nur dann, wenn Datenübermittlungen „wegen der besonderen Art der Speicherung im Melderegister nicht oder nur mit unverhältnismäßig hohem Aufwand möglich sind"; gemeint ist die manuelle Registerführung, die einen Zugang zu den Daten außerhalb der Dienstzeiten des Personals häufig ausschließt.

Damit würde den Polizeibehörden faktisch der gesamte Datenbestand zur Verfügung gestellt. Zwar sind sie an die Übermittlungsvoraussetzungen des § 18 Abs. 1 und 2 MRRG gebunden, jedoch wird die Prüfung dieser Voraussetzungen im Gegensatz zur „normalen Datenübermittlung" hier dem Datenempfänger allein überlassen. Dadurch entfällt der Kontrolleffekt, der sonst dadurch entsteht, daß die Meldebehörde zumindest mitprüft, ob die verlangten Daten zur rechtmäßigen Erfüllung der in der Zuständigkeit des Empfängers liegenden Aufgaben erforderlich sind. Diese Prüfung braucht sich nicht auf die besonderen Umstände des Einzelfalls zu beziehen, sie gewährleistet jedoch, daß der Umfang der Datenübermittlung nicht unverhältnismäßig ist. Wird — wie in § 24 MRRG vorgesehen — der gesamte Datenbestand des Meldewesens zur Verfügung gestellt, ist das Fehlen einer solchen Sicherung bedenklich.

Die Übergangsregelung des § 24 MRRG wurde geschaffen, weil zu erwarten ist, daß die automatisierten Verfahren, mit denen die Meldebehörden überwiegend bereits arbeiten, spätestens nach Ablauf der Frist so weit entwickelt sind, daß der Polizei ein kontrollierter begrenzter Zugriff auf die für sie erforderlichen Daten ermöglicht werden kann. Sofern es sich hierbei um Verfahren der Datenfernverarbeitung handelt, sind dies regelmäßige Datenübermittlungen. Regelmäßige Datenübermittlungen bedürfen übrigens nach § 18 Abs. 4 MRRG einer Rechtsgrundlage, die Anlaß und Zweck der Übermittlung festlegt.

2.4 Personalausweisgesetz

Das Gesetz zur Änderung des Bundespersonalausweisgesetzes ist am 6. März 1980 verabschiedet worden (BGBl. I S. 270). Die von mir und den Landesbeauftragten für den Datenschutz sowie der Datenschutzkommission Rheinland-Pfalz geforderten Inhalts- und Verwendungsbeschränkungen (vgl. 2 TB S. 11 f.) sind eingearbeitet worden. Das Ergebnis ist insgesamt zufriedenstellend. Gegenwärtig wird das Verfahren der automatisierten Herstellung des Ausweises bei der Bundesdruckerei in Berlin vorbereitet. Auch darauf haben die Datenschutzbeauftragten der Bundesländer und ich Einfluß genommen und bewirkt, daß die Verarbeitungsdauer bei der Bundesdruckerei erheblich verkürzt wird. Für eine kurze Zeitspanne müssen die Daten bei der Bundesdruckerei gespeichert werden, und zwar zunächst — für einige Sekunden — die Angaben für die Vorderseite, die sogleich automatisch auf das Formblatt übertragen und anschließend gelöscht werden, darüber hinaus bis zu etwa einer Stunde die Angaben, die für den Druck der Rückseite vorgehalten werden müssen (auch sie werden nach dem Druck sogleich gelöscht). Ich sehe darin einen formellen Verstoß gegen das Verbot der Speicherung des § 2 Abs. 3 des Bundespersonalausweisgesetzes. Um späteren Berufungsfällen vorzubeugen, habe ich dieses Verfahren beanstandet. Der Bundesminister des Innern hält demgegenüber im Einvernehmen mit den Innenministern/-senatoren der Bundesländer diese

kurzfristige Zwischenspeicherung für zulässig, weil sie ausschließlich dem Zwecke der Herstellung des Personalausweises diene. Die Daten würden unmittelbar nach dem Herstellungsvorgang gelöscht. Das in § 2 Abs. 3 des Bundespersonalausweisgesetzes festgelegte Verbot sei im Zusammenhang mit der zugelassenen zentralen Speicherung der Seriennummer zu sehen. Der Gesetzgeber habe hier die dauernde Speicherung von Daten über alle Ausweisinhaber gemeint. Das gegenwärtig vorgesehene Verfahren erlaube es hingegen sogar, auch auf die zentrale Speicherung der Seriennummer zu verzichten.

Ich werde das vorgesehene Verfahren in allen Entwicklungsstadien sorgfältig im Auge behalten, um zu gewährleisten, daß es tatsächlich jedenfalls bei dieser vorübergehenden Zwischenspeicherung bleibt und keinerlei technische und organisatorische Vorkehrungen getroffen werden, um das Speicherungsverbot zu umgehen.

Auf meine Anregung hin wird auf der Rückseite des Ausweises ferner ein Hinweis auf die wichtigste Verwendungsbeschränkung aufgenommen werden. Geplant ist, den Text des § 5 Abs. 4 des Bundespersonalausweisgesetzes zu übernehmen: „Der Personalausweis darf nicht zur automatischen Erschließung von Dateien verwendet werden. Dies gilt nicht für Dateien, die für Zwecke der Grenzkontrolle und der Fahndung aus Gründen der Strafverfolgung und der Gefahrenabwehr durch die hierfür zuständigen Behörden betrieben werden". Ich betrachte dies als eine wirkungsvolle Maßnahme, um jeden Ansatz, Dateien mittels des Personalausweises zu erschließen, im Keime zu ersticken. Der Hinweis wendet sich nicht nur an Betreiber von Dateien; er ist auch geeignet, den betroffenen Bürger zu veranlassen, kritische Fragen zu stellen, wenn er vermutet, daß sein Ausweis für eine verbotene Erschließung verwendet werden könnte.

Der neue Personalausweis soll ab 1. Oktober 1981 ausgegeben werden. Inzwischen erscheint es jedoch fraglich, ob dieser Termin eingehalten werden kann. Mögen dafür auch in erster Linie Finanzierungsschwierigkeiten ursächlich sein, so bietet dieser Aufschub doch die Gelegenheit, auch die noch offenen Datenschutzfragen erneut aufzugreifen.

2.5 Sozialgesetzbuch X (Verwaltungsverfahren) — Neuordnung des Sozialdatenschutzes

Am 18. August 1980 ist im Bundesgesetzblatt (BGBl. I S. 1469) das X. Buch des Sozialgesetzbuchs (SGB) — Verwaltungsverfahren — verkündet worden. Dieses Gesetz bringt nach langen Beratungen, an denen auch meine Dienststelle beteiligt war, auf einem besonders wichtigen Gebiet eine bereichsspezifische Datenschutzregelung; in einem besonderen Kapitel wird der Schutz der Sozialdaten umfassend und abschließend geordnet. Im Regierungsentwurf fehlten entsprechende Bestimmungen noch völlig. Erst auf die Initiative einiger weniger Abgeordneter wurde das 2. Kapitel „Schutz der Sozialdaten" in das SGB X eingefügt. Zahlreiche meiner Vorschläge (vgl. 2. TB S. 26) konnten dabei berücksichtigt, sich abzeichnende Verschlechterungen des Entwurfs konnten verhindert werden. Wegen der grundsätzlichen Bedeutung dieser Neuordnung sei über die wichtigsten Ergebnisse hier berichtet.

— Der neugefaßte § 35 SGB I hat den Geheimnisbegriff als Tatbestandsvoraussetzung des Geheimhaltungsgebots aufgegeben. Geschützt sind nunmehr personenbezogene Daten i. S. des BDSG (= Einzelangaben über die persönlichen und sachlichen Verhältnisse eines Betroffenen) sowie Betriebs- und Geschäftsgeheimnisse. Personenbezogene Daten sowie Betriebs- und Geschäftsgeheimnisse bilden zusammen die Sozialdaten im Sinne der Neuordnung.

— Der Anspruch jedermanns auf Schutz dieser Sozialdaten ist ausgebaut worden; war er bisher auf die Unterlassung unbefugter Offenbarung gerichtet, so ist nunmehr die Verpflichtung hinzugekommen, die Sozialdaten „als Sozialgeheimnis" zu wahren. Hierdurch werden den „Sozialgeheimnis-Trägern" auch positive Vorkehrungen zum Schutz der Sozialdaten auferlegt.

— § 35 SGB I zählt abschließend die Stellen auf, denen die Verpflichtung zur Wahrung des Sozialgeheimnisses obliegt. Gegenüber dem bisherigen Recht ist der Kreis der Verpflichteten erweitert worden. Hinzugekommen sind:

  — die Arbeitsgemeinschaften der Leistungsträger,
  — die Künstlersozialkasse (das diesbezügliche Gesetz ist allerdings noch nicht verabschiedet worden),
  — die Deutsche Bundespost, soweit sie mit der Berechnung oder Auszahlung von Sozialleistungen betraut ist,
  — die rechnungsprüfungs- oder weisungsberechtigten Behörden.

— Der neue § 35 SGB I bestimmt weiter, daß *nur* unter den im SGB selbst geregelten Voraussetzungen eine Offenbarung von Sozialdaten durch die in § 35 genannten Stellen zulässig ist. Diese Bestimmung dient der Rechtsklarheit für Bürger und Verwaltung: an einer Stelle, eben im SGB, soll feststellbar sein und bleiben, welche Fälle zulässiger Offenbarung es gibt. Sollte sich in der Praxis erweisen, daß die Neuregelung Lücken enthält, so müssen diese *im SGB* geschlossen werden.

— Von besonderer Tragweite ist, daß in allen Fällen, in denen eine Offenbarung nicht zulässig ist, für die in § 35 SGB I genannten Stellen keine Auskunftspflicht, keine Zeugnispflicht und keine Pflicht zur Vorlegung oder Auslieferung von Schriftstücken, Akten, Dateien und sonstigen Datenträgern besteht.

— Durch die Verweisung in § 35 Abs. 2 SGB I auf die §§ 67 bis 77 SGB X wird erreicht, daß die äußerlich auf zwei Bücher des SGB verteilten Regelungen der Neuordnung des Sozialdatenschutzes als Einheit angewendet werden.

— Wichtig ist, daß der Gesetzgeber der Regelung der Einwilligung besondere Bedeutung beigemessen hat. Sie muß *im Einzelfall* erfolgen (§ 67 Satz 1 Nr. 1 SGB X). Sie muß sich demnach auf konkret erkennbare Datenflüsse aus einem konkreten Anlaß beziehen. Pauschalermächtigungen sind unzulässig.

— Der abschließende Katalog gesetzlicher Offenbarungsbefugnisse gemäß §§ 68 bis 77 SGB X differenziert nach der Art und dem Umfang der Daten, nach der Art der Aufgabe, nach der Art eines Anspruchs, nach dem Sitzland des Empfängers usw. Durch Anknüpfung an eines oder mehrere dieser Kriterien wird ein sachnahes System von ausnahmsweise zulässigen Offenbarungen geschaffen. Dieses System wird durch Kautelen zusätzlich abgesichert, die einzeln oder vereint greifen, nämlich:

  — die Erforderlichkeit der Offenbarung ist stets zu prüfen,

  — schutzwürdige Belange des Betroffenen können einer Offenbarung entgegenstehen,

  — verfahrensmäßige Sicherungen sorgen für eine Entscheidung über die Offenbarung an zentraler Stelle mit besonderem Verantwortungsgrad,

  — die Beschränkung auf den Einzelfall und Subsidiaritätsklauseln verhindern eine pauschale Freigabe von Sozialdaten für die Aufgabenerfüllung anderer Verwaltungen und sorgen für die Wahrung des Regel-Ausnahme-Verhältnisses zwischen Geheimhaltung und Offenbarung.

— §§ 76 bis 78 enthalten Beschränkungen der in §§ 68 bis 75 genannten Offenbarungsbefugnisse. Hervorzuheben ist die Einschränkung der Offenbarungsbefugnis bei besonders schutzwürdigen personenbezogenen Daten — das sind alle Daten, die einer in § 35 SGB I von einem Arzt oder einer anderen in § 203 Abs. 1 und 3 StGB genannten Person zugänglich gemacht worden sind (§ 76 Abs. 1 SGB X).

— Von den gesetzlichen Offenbarungsbefugnissen sei nur die für Zwecke der Forschung oder Planung — § 75 SGB X — erwähnt. Die Befugnis zur Offenbarung wird hier an eine Reihe inhaltlicher und verfahrensmäßiger Voraussetzungen geknüpft; dies sind vor allem:

  — die Offenbarung muß für die wissenschaftliche Forschung im Sozialleistungsbereich oder für die Planung im Sozialleistungsbereich durch eine öffentliche Stelle im Rahmen ihrer Aufgaben erforderlich sein;

  — schutzwürdige Belange des Betroffenen dürfen nicht beeinträchtigt werden oder

  — das öffentliche Interesse an der Forschung oder Planung muß das Geheimhaltungsinteresse des Betroffenen erheblich überwiegen. Ein erhebliches Überwiegen kann nur nach Abwägung der in Rede stehenden Interessen festgestellt werden. Dazu ist in der Regel eine Befragung des Betroffenen über seine schutzwürdigen Belange erforderlich. Im allgemeinen wird die Einwilligung des Betroffenen der einfachste Weg sein, um zum Ziele zu kommen.

Bereits im Januar 1980 habe ich den Bundesminister für Arbeit und Sozialordnung, den Bundesminister für Jugend, Familie und Gesundheit und den Bundesminister für Forschung und Technologie darauf aufmerksam gemacht, daß Richtlinien für die Behandlung von Forschungsanträgen im Bereich der Sozialverwaltung erarbeitet werden müssen. Seit Erlaß des SGB X kann über die Notwendigkeit derartiger Richtlinien kein Zweifel mehr bestehen. Ab 1. Januar 1981 werden die zuständigen Ressorts gemäß § 75 SGB X über die Zulässigkeit der Offenbarung personenbezogener Daten zu entscheiden haben. Ich habe daher nach Erlaß des SGB X die obengenannten Ressorts erneut angeschrieben und auf die Dringlichkeit der Angelegenheit hingewiesen. Bisher hat jedoch keines der Ressorts eine Lösung erarbeitet, so daß die Gefahr besteht, daß Anträge verzögert werden, daß falsch entschieden wird oder widersprüchliche Entscheidungen ergehen.

— Eine der wichtigsten datenschutzrechtlichen Bestimmungen der Neuordnung ist § 76 SGB X. Er „verlängert" den Schutz der unter § 203 StGB fallenden Privatgeheimnisse in den Bereich der Sozialverwaltung hinein: sind personenbezogene Daten einer der in § 203 Abs. 1 und 3 StGB genannten Personen zugänglich gemacht worden, so darf die Offenbarung, die nach §§ 68 bis 75 SGB X an sich zulässig wäre, gleichwohl nur unter den Voraussetzungen erfolgen, unter denen die in § 203 Abs. 1 und 3 StGB genannten Personen selbst offenbarungsbefugt wären. Das sind sie außer in Fällen gesetzlicher Mitteilungspflichten oder eines rechtfertigenden Notstandes, die zahlenmäßig nicht ins Gewicht fallen, nur bei Einverständnis des Betroffenen.

Dies bedeutet, daß z. B. eine Offenbarung medizinischer Daten für die Erfüllung einer gesetzlichen Aufgabe nach dem SGB (§ 69 Abs. 1 Nr. 1 SGB X) oder für die wissenschaftliche Forschung oder die Planung im Sozialleistungsbereich (§ 75 SGB X) fast ausschließlich nur noch mit Einwilligung des Betroffenen zulässig ist. Der Gesetzgeber hat hier aufgrund einer Güterabwägung entschieden, daß etwa der Schutz von Daten, die aus der ärztlichen oder psychologischen Behandlung oder der Betreuung durch Sozialarbeiter stammen, einen so hohen Stellenwert haben soll, daß selbst berechtigte Interessen der Verwaltung, der Forschung oder der Planung dahinter zurückstehen müsssen.

Nachdem das SGB nunmehr die Fälle zulässiger Offenbarung durch die in § 35 SGB I genannten Stellen, kurz: die Sozialverwaltung, untereinander oder gegenüber Dritten abschließend und differenziert geregelt hat, muß dasselbe mit den Offenbarungsbefugnissen der in § 203 Abs. 1 und 3

StGB genannten Personen gegenüber den in § 35 SGB I genannten Stellen geschehen. Die gleiche Sorgfalt, die der Gesetzgeber des SGB X der Wahrung des Sozialgeheimnisses angedeihen ließ, sollte er z. B. den Offenbarungsbefugnissen der Ärzte gegenüber den in § 35 SGB I genannten Stellen widmen. § 76 regelt nur eine Seite einer Medaille; die andere bleibt vorerst eine nur teilweise gesicherte Flanke des Betroffenenschutzes. Auch hier muß der Schritt von mehr oder weniger vagen Generalklauseln zu einem System durchdachter Offenbarungsbefugnisse führen, das sich an den vom Gesetzgeber des SGB befolgten Leitlinien orientieren kann.

— Während § 35 SGB I i. V. mit §§ 67 bis 78 SGB X nur die Offenbarung von Sozialdaten — als das bereichsspezifische Pendant zur Übermittlung nach dem BDSG — (unabhängig vom Vorliegen einer Datei) regelt, erfassen die §§ 79 bis 85 SGB X („Schutz der Sozialdaten bei der Datenverarbeitung") die Datenverarbeitung allgemein, also auch die Speicherung, Veränderung und Löschung von Sozialdaten, allerdings beschränkt auf Dateien. Die §§ 79 ff. ergänzen für den Anwendungsbereich des SGB das BDSG, das als Auffanggesetz dem bereichsspezifischen Datenschutz Raum läßt.

Besonders hervorzuheben ist, daß die in § 35 SGB I genannten Stellen, soweit sie Sozialdaten in Dateien verarbeiten, nach Maßgabe der §§ 80 bis 85 SGB X den Vorschriften des Ersten und Zweiten Abschnittes sowie den §§ 41, 42 Abs. 1 Nr. 2 und 45 BDSG unterliegen. Hier wird also nicht mehr nach Bundes- und Landesstellen unterschieden: für Bundes- und Landesbehörden sowie sonstige öffentliche Stellen gilt im Anwendungsbereich des SGB nunmehr einheitliches Recht. Dem liegt die Auffassung zugrunde, dem Bürger sei nicht verständlich zu machen, daß der Sozialdatenschutz vom Bund zum Land oder von Land zu Land unterschiedlich sein darf.

Hinzuweisen ist schließlich auf die Verpflichtung der in § 35 SGB I genannten Stellen, einen Datenschutzbeauftragten zu bestellen; die §§ 28, 29 BDSG sind insoweit entsprechend anzuwenden.

2.6 Bundesstatistikgesetz

Das Bundesstatistikgesetz, bei dessen Novellierung ich die Gesetzgebungsorgane beraten habe (vgl. 2. TB S. 20, 1. TB S. 19 f.) ist im Berichtszeitraum in Kraft getreten. Die praktische Umsetzung seiner datenschutzrechtlichen Bestimmungen hat nunmehr Priorität (s. u. 3.4).

3 Stand des Datenschutzes in ausgewählten Bereichen

3.1 Allgemeine Innere Verwaltung

3.1.1 Bundesverwaltungsamt/Ausländerzentralregister

Das Bundesverwaltungsamt erfüllt die Funktion einer zentralen Verwaltungsbehörde des Bundes. Ihm sind vielfältige unterschiedliche Verwaltungsaufgaben zugewiesen worden, die unter der Fachaufsicht des jeweils zuständigen Bundesministeriums erledigt werden.

Ich habe eine dieser Aufgaben, nämlich die Führung des Ausländerzentralregisters an Ort und Stelle überprüfen lassen. Nach § 6 des Gesetzes über die Errichtung des Bundesverwaltungsamts dient das Ausländerzentralregister „der Erfassung von im Bundesgebiet wohnhaften Ausländern". Tatsächlich werden aber auch Daten über Ausländer gespeichert, die nie in die Bundesrepublik Deutschland eingereist sind. Für die Speicherung dieser Daten gibt es keine Rechtsgrundlage. Das Ausländerzentralregister ist als Hinweisdatei konzipiert. Es besteht aus der Hauptdatei und der Erkenntnisdatei. Beide Dateien sind in dem von mir geführten Register nach Maßgabe der Datenschutz-Registerordnung beschrieben. Die Erkenntnisdatei unterscheidet sich von der Hauptdatei dadurch, daß sie Angaben zur Person des Ausländers enthält, die für ausländerrechtliche Entscheidungen bedeutsam sein können. Die datenschutzrechtliche Brisanz dieser Datei liegt darin, daß die dort gespeicherten Angaben für sich allein als Basis für Entscheidungen genutzt werden könnten. Es ist auch zweifelhaft, ob alle dort registrierten Daten noch von der Ermächtigung in § 6 des Errichtungsgesetzes gedeckt werden. Dies ist für mich der Grund, die Notwendigkeit der Eintragungen sehr sorgfältig zu prüfen. In diesem Zusammenhang sei auch erwähnt, daß die gegenwärtig geübte Praxis, das Ausländerzentralregister als Informationsschiene für andere Behörden zu nutzen, ernsthafte datenschutzrechtliche Bedenken ausgelöst hat, die ich dem Bundesminister des Innern mitgeteilt habe und über die ich mit ihm im Gespräch bin.

3.1.2 Umweltbundesamt

3.1.2.1 Dateien des Amtes

Beim Umweltbundesamt haben sich meine Mitarbeiter im Frühjahr 1980 einen ersten Überblick über die Aufgaben des Amtes und der dort geführten Dateien sowie die Art der gespeicherten Daten verschafft.

Das Kernstück der Dateien des Umweltbundesamtes bildet das Informations- und Dokumentationssystem (UMPLIS). Es handelt sich hierbei um ein rechnergestütztes Informationssystem, das mit seinem Datenbestand und einem Verweissystem Grundlage für eine effektive Umweltplanung und Umweltpolitik sein soll. Es besteht aus mehreren Teilsystemen.

Sie werden, wenn das System voll in Betrieb genommen worden ist, aus bereichsübergreifenden und bereichsbezogenen Datenbanken, einer Umwelt-, Literatur- und Rechtsdokumentation und einer Umwelt-Fachbibliothek bestehen.

Diese Datenbanken enthalten auch personenbezogene Daten. Ich habe feststellen können, daß das Umweltbundesamt bei der Speicherung solcher Daten sorgfältig vorgegangen ist. So sind z. B. bei der Datenerfassung für die Broschüre „Bürger im Umweltschutz" alle Personen und Einrichtungen, die in die Broschüre aufgenommen werden sollten, einzeln angeschrieben und auf die Freiwilligkeit der Angabe von Daten für diese Broschüre hingewiesen worden.

Ferner habe ich mich über die in sonstigen Datenbanken des Umweltbundesamtes gespeicherten personenbezogenen Daten unterrichtet. Aus diesen Informationen haben sich datenschutzrechtliche Bedenken nicht ergeben.

3.1.2.2 Hausmülluntersuchung

Ein besorgter Bürger teilte mir seine Beobachtung mit, daß sein Hausmüll seit einiger Zeit nicht mehr von der allgemeinen Müllabfuhr, sondern von einem offensichtlich privaten Lkw abgeholt wurde. Auf seine Frage habe er von der Gemeindeverwaltung die Auskunft erhalten, sein Haushalt sei in ein Forschungsvorhaben einbezogen, das im Auftrag eines Bundesministeriums den Müll aus verschiedenen Haushaltsstrukturen untersuchen solle. Er befürchtete nun, daß durch die Untersuchung und Auswertung seines Hausmülls auf Grund weggeworfener Medizinschachteln, Kontoauszüge, Lieferscheine, Flaschen u. a. Rückschlüsse auf seinen Gesundheitszustand, seine Lebensgewohnheiten und seinen Lebensstandard gezogen werden könnten.

Ich habe festgestellt, daß es sich hier um ein Forschungsvorhaben handelt, daß als „Bundesweite Hausmülluntersuchung" vom Umweltbundesamt in Berlin im Rahmen des Abfallwirtschaftsprogramms 1975 der Bundesregierung durchgeführt wird. Ziel und Aufgabe des Hausmüllanalysenprogramms ist, die Hausmüllmenge und -zusammensetzung in der Bundesrepublik Deutschland zu ermitteln. Eine Gewinnung personenbezogener Daten oder eine Zuordnung der Untersuchungsergebnisse zu Einzelpersonen oder Einzelhaushalten ist dabei weder beabsichtigt noch nach den angewandten Forschungsmethoden möglich. Die Auswahl der in das Forschungsvorhaben einzubeziehenden Haushalte und der einzusammelnden Müllbehälter erfolgt — unter Berücksichtigung bestimmter Bevölkerungs- und Siedlungsstrukturen — nach dem Lotterieprinzip, also rein zufällig. Bereits an Ort und Stelle werden die Abfälle aus verschiedenen Haushalten in Großbehältern vermischt, so daß die genaue Herkunft einzelner Müllbestandteile nicht mehr bestimmbar ist.

Einige Müllbestandteile lassen allerdings den Personenbezug unmittelbar erkennen, z. B. Kontoauszüge oder Briefumschläge. Der beste Datenschutz „in eigener Sache" wäre in diesem Fall, den Personenbezug unkenntlich zu machen. Meine Forderung geht deshalb dahin, bei der Durchführung derartiger Forschungsvorhaben die betroffenen Haushalte rechtzeitig vorher entsprechend zu informieren, um Bedenken und Befürchtungen des einzelnen hinsichtlich des Mißbrauchs personenbezogener Daten von vornherein auszuräumen. In der fehlenden Information der Betroffenen sehe ich einen datenschutzrechtlichen Mangel bei der Durchführung dieses Forschungsvorhabens. Eine durch Vorab-Information möglicherweise eintretende „Verfälschung" der Müllmenge und -zusammensetzung dürfte bei entsprechender Aufklärung kaum ins Gewicht fallen und müßte im übrigen im Hinblick auf vorrangige Datenschutzinteressen hingenommen werden.

Ich habe das Umweltbundesamt und den Bundesminister des Innern als die zuständige oberste Bundesbehörde auf diese Gesichtspunkte hingewiesen. Es besteht Einvernehmen darüber, daß die entstandenen Fragen — auch im Hinblick auf künftige derartige Forschungsvorhaben — einer Klärung bedürfen, um den Belangen des Datenschutzes auch in diesem Bereich gerecht zu werden.

3.1.3 Bundesamt für die Anerkennung ausländischer Flüchtlinge

Das Bundesamt für die Anerkennung ausländischer Flüchtlinge in Zirndorf ist die erste Instanz für die Entscheidung über Asylanträge ausländischer Flüchtlinge. Es verarbeitet dazu eine Fülle von personenbezogenen Daten mit teilweise hohem Sensibilitätsgrad. Die Daten werden aber — wie ich anläßlich einer Überprüfung festgestellt habe — nicht in Dateien, sondern ausschließlich in Akten verarbeitet. Eine zentrale Namenskartei dient dem internen Zweck, die zu einer Person geführten Akten aufzufinden. Geplant ist, dieses System zu automatisieren und seinen Verwendungszweck zu erweitern (z. B. Feststellung des jeweiligen Verfahrensstandes, Statistik). Sollten dabei zusätzlich personenbezogene Daten gespeichert und anderen Stellen der Zugriff eröffnet werden, müssen vorher die datenschutzrechtlichen Fragen erneut geprüft werden.

3.1.4 Eingliederung von Spätaussiedlern

Spätaussiedler, die aus Staaten des Ostblocks in die Bundesrepublik Deutschland kommen, sehen sich bei ihrer Eingliederung in die politischen, gesellschaftlichen und wirtschaftlichen Verhältnisse mit einer Fülle von Problemen konfrontiert, die sie ohne fremde Hilfe nicht lösen können. Diese Unterstützung kann ihnen aber in effektiver Form nur gewährt werden, wenn den damit betrauten öffentlichen und nicht-öffentlichen Stellen die dafür erforderlichen Daten verfügbar gemacht werden. Für die Aussiedler ihrerseits ist Datenschutz weitgehend ein Fremdwort. Sie sind an rascher, unbürokratischer Hilfe interessiert; es kümmert sie wahrscheinlich wenig, welche Daten dafür erhoben und wie sie verarbeitet werden.

Dies kann aber nicht bedeuten, daß dem Datenschutz insoweit keine Beachtung zu schenken wäre.

Vielmehr sehe ich gerade hier eine wichtige Funktion der Datenschutzbeauftragten des Bundes und der Länder, als Sachwalter der Datenschutzinteressen dieser Menchen tätig zu werden.

Mit dem Bundesminister des Innern erörtere ich zur Zeit, welche Angaben in die Registrierscheine, die die Aussiedler bei ihrer Ankunft auszufüllen haben, aufgenommen werden müssen. Sie dienen primär als Grundlage für Entscheidungen über die Anerkennung als Deutscher, für die Erteilung des Vertriebenen-Ausweises und für die Arbeitsbeschaffung, um nur einige zu nennen.

Bisher wurden Kopien der ausgefüllten Registrierscheine auch an private Betreuungsorganisationen übermittelt. Diese erhielten damit Daten, die sie zur Erfüllung ihrer Betreuungsaufgaben nicht benötigten. Ich habe daher dem Bundesminister des Innern vorgeschlagen, auf ein Verfahren hinzuwirken, durch das den Betreuungsorganisationen nur diejenigen Daten übermittelt werden, die sie für eine gezielte Kontaktaufnahme benötigen. Dazu ist sicher mehr notwendig als nur der Name und die gegenwärtige Anschrift. Es ist ein berechtigtes Anliegen zu verhindern, daß sämtliche an einem Ort tätigen Betreuungsorganisationen zu allen eintreffenden Aussiedlern Kontakt aufnehmen müssen, um festzustellen, ob sie für eine Betreuung überhaupt in Betracht kommen. Die tatsächliche Betreuung könnte sich dadurch erheblich verzögern, was weder im öffentlichen noch im Interesse des betroffenen Aussiedlers liegt. Vorbehaltlich anderer Entscheidung der Länder müssen daher weitere Daten übermittelt werden, aus denen die Betreuungsorganisationen ersehen können, ob der einzelne Aussiedler für eine Betreuung durch sie in Betracht kommt. Wird damit dann gleichzeitig sichergestellt, daß die übermittelten Daten nur für Zwecke der Betreuung verwendet werden dürfen, dann werden nach meiner Einschätzung schutzwürdige Belange der Betroffenen nicht beeinträchtigt. Kommt es aufgrund der ersten Kontaktaufnahme tatsächlich zu einer Betreuung, kann dann der Aussiedler selbst entscheiden, welche weiteren Daten er an die Betreuungsorganisation weitergeben möchte.

3.1.5 Datenschutz im Bereich des Zivildienstes

Mit dem Bundesbeauftragten für den Zivildienst habe ich im Berichtsjahr ein der gegenseitigen Information und dem Erfahrungsaustausch dienendes Gespräch geführt. Es wurden datenschutzrechtliche Problembereiche angesprochen, die noch der vertieften Bearbeitung bedürfen. Einige führe ich auf:

— Das Bundesamt für den Zivildienst erhält nach § 2 Abs. 3 Zivildienstgesetz die Personalunterlagen der anerkannten Kriegsdienstverweigerer. Dazu gehören auch die Akten aus dem Anerkennungsverfahren. Diese Unterlagen können zwar in Einzelfällen nützlich sein, wenn über den Einsatz des Zivildienstleistenden zu entscheiden ist und dieser selbst keine Wünsche geäußert hat. Sie sind aber für die Erfüllung der Aufgaben des Bundesamtes für den Zivildienst nicht erforderlich. Es benötigt lediglich die Bestätigung, daß der Betroffene als Kriegsdienstverweigerer anerkannt worden ist. Verwendungswünsche sollten bei den Kriegsdienstverweigerern besonders erfragt werden. Zwar handelt es sich nicht um Dateien, so daß das Bundesdatenschutzgesetz nicht anwendbar ist. Der „Erforderlichkeitsgrundsatz" des Bundesdatenschutzgesetzes kann aber bereits heute als ein allgemeiner Rechtsgrundsatz angesehen werden, der Anlaß genug sein sollte, die bisherige Praxis zu überprüfen.

— In der vergangenen Legislaturperiode haben dem Deutschen Bundestag zwei Gesetzentwürfe zur Neuordnung des Anerkennungsverfahrens vorgelegen. Beide Entwürfe sahen vor, die Gewissensentscheidung des Kriegsdienstverweigerers von Amts wegen zu überprüfen. Zur Verabschiedung ist es nicht mehr gekommen. Dies bietet die Chance, in der neuen Legislaturperiode nach gesetzlichen Lösungen zu suchen, die den Betroffenen nicht in die Rolle eines „Angeklagten" versetzen. Dieser macht mit der Verweigerung des Kriegsdienstes mit der Waffe ein ihm vom Grundgesetz gewährtes Recht geltend. Ich halte es für fragwürdig, ob der Staat das Recht hat, die Gewissensentscheidung des Betroffenen einer vielfach peinlichen Überprüfung zu unterwerfen. Nach dem Urteil des Bundesverfassungsgerichts vom 13. April 1978 reicht zwar die einfache Erklärung, den Kriegsdienst verweigern zu wollen, nicht aus; das Überprüfungsverfahren sollte aber zumindest so ausgestaltet werden, daß der Betroffene weitgehend mitbestimmt, welche Einzelheiten eingebracht und erörtert werden. Denkbar wäre, daß er für seine Gewissensentscheidung Beweise anbietet und zunächst nur sie Gegenstand der Verhandlung sind. Hält der Prüfungsausschuß weitere Beweise für erforderlich, könnte dem Betroffenen vorab Gelegenheit zur Äußerung gegeben werden. Durch eine solche Verfahrensweise ließen sich unnötige Beweiserhebungen weitgehend vermeiden.

  Ich verkenne nicht, daß dadurch u. U. für den Betroffenen günstige Tatsachen gar nicht erst erhoben werden. Der Betroffene, der sich dieses Risikos bewußt ist, hat aber zumindest die Möglichkeit zu entscheiden, ob weitere Ermittlungen angestellt werden sollen oder nicht.

3.1.6 Übersicht über Verfassungsstreitsachen vor dem Bundesverfassungsgericht

In den Übersichten über die dem Deutschen Bundestag zugeleiteten Streitsachen vor dem Bundesverfassungsgericht werden bisher bei Verfassungsbeschwerden u. a. die Namen und Anschriften der Beschwerdeführer angegeben. Damit wird einer relativ breiten Öffentlichkeit nicht nur bekannt, daß diese Personen eine Verfassungsbeschwerde eingeleitet haben, sondern zum Teil auch deren Gegenstand. Es handelt sich dabei um personenbezogene Daten von einer gewissen Sensibilität, da sie Aufschlüsse über persönliche Verhältnisse der Betroffenen geben. Diesen wird in den wenigsten Fällen bekannt sein,

daß ihre Daten auf diese Weise und in diesem Zusammenhang an die Öffentlichkeit gelangen.

Wenn auch das Bundesdatenschutzgesetz hier nicht unmittelbar anzuwenden sein wird, da kaum anzunehmen ist, daß die Angaben in einer Datei gespeichert sind, so besteht hier doch ein datenschutzrechtliches Problem. Ich habe daher gegenüber dem Deutschen Bundestag angeregt zu prüfen, ob der Zweck der Übersicht nicht auch zu erreichen wäre, wenn auf die Angabe der Namen der Beschwerdeführer verzichtet würde. Ich habe ferner zu erwägen, gegeben, lediglich den Anfangsbuchstaben des Namens und den Wohnort des Beschwerdeführers aufzuführen. Der einzelne Abgeordnete hätte dann noch die Möglichkeit, den Verfahren, die in seinem Wahlkreis angestrengt worden sind, seine besondere Aufmerksamkeit zuzuwenden.

Der Vorsitzende des Rechtsausschusses des Deutschen Bundestages hat diesem Vorschlag zugestimmt und mir mitgeteilt, daß künftig bei der Übersicht über Verfassungsstreitsachen vor dem Bundesverfassungsgericht nur die Anfangsbuchstaben und der Wohnort des Beschwerdeführers aufgeführt werden.

3.2 Rechtswesen/Justizverwaltung

Die nachstehend aufgeführten Einzelthemen habe ich zum Teil bereits im vergangenen Jahr aufgegriffen. Bewegt hat sich in der Zwischenzeit wenig. Zwar wird die Berechtigung meiner datenschutzrechtlichen Forderungen und Anregungen nicht bezweifelt, fiskalische Bedenken und Kompetenzaufteilung haben sich aber bisher als stärker erwiesen. Ich bin jedoch zuversichtlich, daß es auch hier gelingen wird, schrittweise dem Ziel eines verbesserten Datenschutzes näher zu kommen.

3.2.1 Bundeszentralregister

Die Verarbeitung personenbezogener Daten im Bundeszentralregister in Berlin habe ich eingehend und systematisch überprüft. Dabei habe ich nicht nur kontrolliert, ob die Daten in Übereinstimmung mit den Bestimmungen des Bundesdatenschutzgesetzes und des Bundeszentralregistergesetzes verarbeitet werden, sondern auch, wie sie verarbeitet werden, also die Datensicherung mit einbezogen. Die Daten über Vorstrafen der Bundesbürger sind besonders sensibel. Ein Zugriff Unbefugter könnte unabsehbare Folgen für die Betroffenen auslösen. Die Daten müssen daher nicht nur rechtlich geschützt, sondern auch technisch einwandfrei gesichert sein. Das Ergebnis war insgesamt positiv. Es gab keinen Anlaß zu einer formellen Beanstandung nach § 20 BDSG. Einige Verbesserungen des Datenschutzes habe ich angeregt und angekündigt, im nächsten Jahr zu überprüfen, ob und inwieweit sie aufgegriffen und umgesetzt worden sind.

3.2.2 Anordnung über Mitteilungen in Strafsachen

Auf die datenschutzrechtliche Problematik der Anordnung über Mitteilungen in Strafsachen (MiStra) und die Reaktion der beteiligten obersten Bundesbehörden habe ich in meinem 2. Tätigkeitsbericht (2. TB S. 16 f.) hingewiesen. Die MiStra wird vor allem im Verkehr zwischen Gerichten/Staatsanwaltschaften einerseits und Landesbehörden andererseits angewendet. Meine Kollegen in den Bundesländern haben sich des Themas daher ebenfalls angenommen; es wurde sodann auf der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 29. September 1980 ausführlich behandelt. Die Mitteilungen nach der MiStra lösen in zahlreichen Fällen unmittelbare oder mittelbare Rechtswirkungen aus, durch die in die vom Grundgesetz geschützte Persönlichkeitsphäre des Betroffenen eingegriffen wird. Die Justizverwaltungen des Bundes und der Länder werden in dem Beschluß des Bundesbeauftragten und der Landesbeauftragten für den Datenschutz daher gebeten, die MiStra zu überprüfen und nur noch die Vorschriften fortbestehen zu lassen, für die eine Rechtsgrundlage besteht, oder eine solche gesetzliche Grundlage zu schaffen und die Datenschutzbeauftragten von dem beabsichtigten Vorgehen zu unterrichten. Der Beschluß enthält ferner Anregungen zur Änderung einzelner Vorschriften der MiStra, die weitgehend denen entsprechen, die ich im vergangenen Jahr vorgelegt habe.

3.2.3 Akteneinsicht für Betroffene in Strafverfahren

Die niederländische Stiftung „Landelijk Comité Waakzaamheid Personenadministratie" hat sich an mich gewandt und mir folgendes vorgetragen: Ein in den Niederlanden lebender Holländer sei im Jahre 1943 in Berlin wegen des Diebstahls von einigen Paar Socken zu einer Zuchthausstrafe von 18 Monaten verurteilt worden. Seine Bemühungen, nach dem Krieg Entschädigung in Holland zu erlangen, seien bisher vergeblich gewesen. Nach Auffassung der zuständigen Stellen sei er wegen einer kriminellen Handlung, nicht jedoch wegen seiner Rasse, seines Glaubens oder seiner Weltanschauung verurteilt worden. Er hat sich in der Vergangenheit mehrfach vergeblich um Einsicht in die Strafakten bemüht.

Diesen Sachverhalt habe ich dem Bundesminister der Justiz mitgeteilt und gleichzeitig darauf hingewiesen, daß nach Nr. 185 der Richtlinien für das Strafverfahren und das Bußgeldverfahren vom 1. Januar 1977 eine Akteneinsicht dem Betroffenen grundsätzlich versagt ist. Ich habe ferner zum Ausdruck gebracht, daß ich diese Regelung für unbefriedigend halte und es begrüßen würde, wenn über die Erweiterung der Akteneinsicht zugunsten von Privatpersonen eine Diskussion eingeleitet werden könnte.

Der Bundesminister der Justiz hat mir daraufhin mitgeteilt, daß diese Frage im Unterausschuß der Justizministerkonferenz am 28./29. Februar 1980 in Berlin erörtert worden ist. Ergebnis dieser Besprechung war, daß mein Vorschlag, die Vorschriften der Richtlinien für das Strafverfahren und das Bußgeldverfahren über die Akteneinsicht zugunsten von Privatpersonen (vor allem der von einem Verfahren Betroffenen) zu erweitern, bei den Landesjustizverwaltungen auf Ablehnung gestoßen sei. Gegen ihn seien

Bedenken aus § 203 Abs. 2 Satz 2 StGB geltend gemacht worden. Auch wurde darauf hingewiesen, daß bei einer Verwirklichung des Vorschlags die „Unversehrtheit des Aktenguts" nicht gewährleistet sei. Darüber hinaus befürchteten die Länder, eine Ausdehnung der Akteneinsicht in dem vorgeschlagenen Rahmen führe zu einem unverhältnismäßigen Arbeitsaufwand und störe den Arbeitsablauf bei den — ohnehin überlasteten — Gerichten und Staatsanwaltschaften. Die geltende Regelung erlaube im übrigen, bei Ersuchen um Akteneinsicht berechtigte Interessen ausreichend zu berücksichtigen. Fälle nicht sachgerechter Bearbeitung solcher Anträge könnten im Wege der Dienstaufsicht korrigiert werden.

Bei dieser Haltung der Länder will sich der Bundesminister der Justiz zunächst darauf beschränken, die weitere Entwicklung der Praxis zu beobachten. Aufgrund der Erörterungen dieser Sache kann erwartet werden, daß die Gerichte und Staatsanwaltschaften den mit der Akteneinsicht durch Privatpersonen verbundenen Problemen ihre besondere Aufmerksamkeit widmen. Sollten weitere Fälle bekannt werden, in denen die geltende Regelung der Richtlinien für das Strafverfahren und das Bußgeldverfahren über die Akteneinsicht zu unbefriedigenden Ergebnissen führt, will der Bundesminister der Justiz erneut an die Länder herantreten.

Aus der Sicht des Datenschutzes (Auskunft über die eigenen Daten!) halte ich es für wichtig, die Diskussion über diesen Problemkreis fortzuführen. Daher habe ich die Landesbeauftragten für den Datenschutz gebeten, die Entwicklung in ihrem Bereich zu beobachten und das Ihre dazu beizutragen, daß die Landesjustizverwaltungen ihren Standpunkt überdenken.

3.2.4 Prozeßkostenhilfegesetz

Mit dem Gesetz über die Prozeßkostenhilfe vom 13. Juni 1980 (BGBl. I S. 677) sind verschiedene Mängel des bisherigen Armenrechts beseitigt worden. Auch nach dem neuen Recht muß jedoch derjenige, der Prozeßkostenhilfe beantragt, seine persönlichen und wirtschaftlichen Verhältnisse offenlegen. Dagegen ist auch nichts einzuwenden. Es kann aber nicht der Sinn des Prozeßkostenhilfegesetzes sein, dem Antragsteller einerseits helfen zu wollen, ihn aber gleichzeitig dadurch zu diskriminieren, daß er seine persönlichen und sachlichen Verhältnisse gegenüber allen Personen und Stellen, die das Recht der Akteneinsicht haben (§ 299 ZPO), offenlegen muß. Aus datenschutzrechtlicher Sicht sollte daher alles unternommen werden, um den Kreis derjenigen, die von den so dargelegten persönlichen und wirtschaftlichen Verhältnissen Kenntnis erhalten müssen, so klein wie möglich zu halten. Ich habe noch im Verlaufe der parlamentarischen Beratungen des Gesetzentwurfs dem Bundesminister der Justiz gegenüber angeregt, darauf hinzuwirken, daß die Angaben des Betroffenen nur dem Gericht zur Kenntnis gelangen. Praktisch hätte dies bedeutet, das Prozeßkostenhilfeverfahren als eigenes neben dem eigentlichen Streitverfahren auszugestalten, wie dies auch im Patentverfahren nach §§ 46a bis 46k Patentgesetz der Fall ist. Dieses Anliegen ist jedoch im Gesetzgebungsverfahren nicht mehr berücksichtigt worden.

Nach der Verabschiedung des Prozeßkostenhilfegesetzes habe ich in einem Gespräch mit Vertretern des Bundesministers der Justiz und der Landesjustizverwaltungen auszuloten versucht, ob und inwieweit nach dem nunmehr geltenden Recht die Prüfung der wirtschaftlichen Verhältnisse auf das Gericht beschränkt bleiben kann. Dies hat sich als unmöglich erwiesen. Das Verfahren zur Gewährung der Prozeßkostenhilfe ist Teil des Streitverfahrens. Nach § 118 ZPO (i. d. F. des Artikel I Nr. 4 des Gesetzes über die Prozeßkostenhilfe) ist dem Gegner vor der Bewilligung der Prozeßkostenhilfe Gelegenheit zur Stellungnahme zu geben, wenn dies nicht aus besonderen Gründen unzweckmäßig erscheint. Ich neige zwar zu der Auffassung, daß diese Stellungnahme sich auf die Streitsache und damit auf die Erfolgsaussichten des Gerichtsverfahrens bezieht; es kann dem Prozeßgegner aber nicht verwehrt werden, sich auch zu den persönlichen und wirtschaftlichen Verhältnissen des Antragstellers zu äußern und gegebenenfalls auch diesen Teil der Gerichtsakten einzusehen.

Angesichts der gesetzlich gegebenen Lage wird es weitgehend bei den Gerichten liegen, inwieweit sie dem Gedanken des Datenschutzes dadurch Rechnung tragen, daß sie die Aufgaben, die der Rechtsuchende im Prozeßkostenhilfeverfahren offen legt, so diskret wie möglich behandeln und sie den sonstigen Prozeßbeteiligten nur dann zur Kenntnis gelangen lassen, wenn dies unumgänglich notwendig ist. Das vom Antragsteller auszufüllende Formular ist unter meiner Mitwirkung so ausgestaltet worden, daß nur die notwendigen Daten erhoben werden.

3.2.5 Schuldnerverzeichnis

In meinem zweiten Tätigkeitsbericht (2. TB S. 18) habe ich auf die datenschutzrechtliche Problematik bei der Übermittlung von Angaben aus dem Schuldnerverzeichnis nach § 915 ZPO hingewiesen und angeregt, die Zahl der Stellen, die vollständige Namenslisten aus dem Schuldnerverzeichnis erhalten, stark zu reduzieren. Der Bundesminister der Justiz, der meine Anregungen positiv aufgenommen hat, hat inzwischen Stellungnahmen der beteiligten Behörden und Verbände eingeholt. Die Landesjustizverwaltungen und die befragten Wirtschaftsverbände haben sich gegen meine Vorschläge ausgesprochen. Da jede Änderung der zu § 915 ZPO erlassenen Verwaltungsvorschriften der Zustimmung des Bundesrates bedarf, besteht wenig Aussicht, daß meine Anregungen in absehbarer Zeit verwirklicht werden. Es bedarf weiterer geduldiger Überzeugungsarbeit, um den Datenschutz hier schrittweise zu verbessern.

3.2.6 Mietpreisspiegel

Durch mehrere Eingaben bin ich auf ein datenschutzrechtliches Problem im Mietrecht aufmerksam gemacht worden. Nach dem Zweiten Wohnraumkündigungsschutzgesetz vom 18. Dezember

1974 (BGBl. I S. 3603) kann eine Miete erhöht werden, wenn der verlangte Mietzins die üblichen Entgelte für vergleichbare Wohnungen nicht übersteigt. Vielfach wird die Vergleichsmiete auf der Grundlage von sogenannten Mietwerttabellen — auch Mietpreisspiegel genannt — ermittelt. Wo es Mietpreisspiegel nicht gibt, ist der Vermieter auf Sachverständigengutachten angewiesen, oder er muß die Mieten von drei vergleichbaren Wohnungen anderer Vermieter angeben.

Zur Erstellung der Mietpreisspiegel oder von Sachverständigengutachten werden Daten über Art, Größe, Ausstattung, Beschaffenheit, Lage und Mietpreis von Wohnungen erhoben. Dies sind personenbezogene Daten über den Mieter oder den Hauseigentümer, auch wenn sie ohne Namensnennung übermittelt werden. Zwar ist nach einer Entscheidung des Bundesverfassungsgerichts (BVerfGE 37, 147) niemand verpflichtet, über den Zustand und den Mietpreis seiner Wohnung Auskunft zu geben, er kann aber nicht verhindern, daß sein Vertragspartner diese Angaben macht. Sowohl der Mieter als auch der Vermieter können ein legitimes Interesse daran haben, daß der Inhalt ihres Mietvertrages und vor allem die genauen Wohnverhältnisse nicht bekannt werden. Wie jemand wohnt, das sagt unter Umständen viel über ihn aus. Durch den Mietvertrag kann man sozusagen in die Wohnung hineinschauen — ohne den Grundrechtsschutz der Wohnung zu verletzen — und Schlüsse auf Einkommen und Lebensstil des Mieters ziehen. Wieviel jemand von seinen Wohnverhältnissen erkennen lassen will, muß er im Prinzip selbst entscheiden können. Die Abwägung zwischen den Belangen des Betroffenen und dem gewiß nicht gering zu veranschlagenden Interesse an der Feststellung der ortsüblichen Miete wird in solchen Fällen möglicherweise dazu führen müssen, eine anonymisierte Angabe von Vergleichswohnungen genügen zu lassen.

Der Bundesminister der Justiz, den ich in dieser Frage angesprochen habe, ist mit mir der Auffassung, daß dem Persönlichkeitsschutz auch im Rahmen der Vorschriften über die Ermittlung der Vergleichsmiete so weit wie möglich Rechnung getragen werden müsse. Es sei aber auch darauf zu achten, daß die Berücksichtigung der Belange einzelner Mietparteien nicht dazu führe, das System der Ermittlung der Vergleichsmieten, das sich bewährt habe, insgesamt zu gefährden oder in Frage zu stellen. Unter dieser Voraussetzung sieht der Bundesminister der Justiz in den Mietpreisspiegeln einen besonderen Vorteil, weil sie nicht punktuelle Informationen über gezahlte Entgelte für einzelne Wohnungen liefern, sondern auf breiter Informationsbasis lediglich Anhaltspunkte für die Ermittlung der Vergleichsmiete im Einzelfall bieten. Auch bei Sachverständigengutachten ist meiner Forderung nach einer möglichst weitgehenden Anonymisierung der Angaben bereits ansatzweise Rechnung getragen worden. Die Bundesregierung hat zusammen mit den Landesjustizverwaltungen und den Verbänden der Wohnungswirtschaft sowie dem Deutschen Industrie- und Handelstag ein Muster-Sachverständigengutachten erstellt, in dem vorgesehen ist, die Wohnungen in ihrer Belegenheit nur so grob zu bezeichnen, daß nur die Lage des Objektes nachvollziehbar ist, das konkrete Vergleichsobjekt aber nicht benannt wird.

Trotz dieser begrüßenswerten Ansätze bleiben bei der Erstellung von Mietpreisspiegeln und Sachverständigengutachten Probleme, die kurzfristig nicht lösbar sind, ohne das gesamte System der Erstellung von Vergleichsmieten in Frage zu stellen. Nur schrittweise werden hier Verbesserungen des Datenschutzes erreichbar sein. Wünschenswert wäre dies vor allem bei der Spruchpraxis der Gerichte. Diese fordern bei der Angabe über Wohnungen anderer Vermieter teilweise sehr detaillierte Informationen. Auch hier zeichnet sich indessen eine positive Entwicklung ab. Einzelne Gerichte sind schon dazu übergegangen, im Falle der Beweiserhebung die Zustimmung des Mieters zur Besichtigung von Wohnräumen durch das Gericht zu fordern.

3.3 Steuerverwaltung

In meinem letzten Tätigkeitsbericht (2. TB, S. 19 f.) habe ich auf Meinungsverschiedenheiten mit dem Bundesminister der Finanzen über den Umfang meiner Kontrollbefugnisse hingewiesen.

Der Bundesminister der Finanzen sieht sich durch das Steuergeheimnis daran gehindert, mir bei meinen Kontrollen Einblick in Dateien, Akten und Unterlagen zu gewähren, wenn die Identität des Steuerpflichtigen dadurch preisgegeben würde. Im Bundesdatenschutzgesetz sei die Befugnis zur Offenbarung gemäß § 30 Abs. 4 Nr. 3 der Abgabenordnung nicht ausdrücklich geregelt. Ich bin im Einvernehmen mit den Landesbeauftragten für den Datenschutz und der Datenschutzkommission Rheinland-Pfalz der gegenteiligen Auffassung. Die Meinungsverschiedenheiten bestehen nach wie vor. Zwar war es möglich, im Bundesamt für Finanzen eine systematische Kontrolle durchzuführen, ohne daß personenbezogene Daten offenbart werden mußten (dazu sogleich 3.3.1), die Grenzen einer solchen eingeschränkten Prüfung zeigten sich aber bereits im Anschluß an die Überprüfung des Zollkriminalinstituts und des Zollfahndungsdienstes (s. u. 3.3.2). Letztlich wird die Frage doch durch den Gesetzgeber geklärt werden müssen.

3.3.1 Bundesamt für Finanzen

Im Berichtsjahr habe ich eine Überprüfung der Datenverarbeitung beim Bundesamt für Finanzen durchführen lassen.

Die datenschutzrechtliche Prüfung konzentrierte sich auf die Informationszentrale Ausland und das Verfahren zur Vergütung bzw. Erstattung von Körperschaft- und Kapitalertragsteuer. Ich habe dabei auch Einzelvorgänge eingesehen und mich über Art und Umfang der gespeicherten Daten orientiert. Die Namen der jeweils betroffenen Steuerpflichtigen blieben dabei abgedeckt.

Ich konnte mich davon überzeugen, daß der Umgang des Bundesamtes für Finanzen mit personenbezoge-

nen Daten, von geringfügigen Mängeln abgesehen, den aus datenschutzrechtlicher Sicht zu stellenden Anforderungen entspricht.

Wenn auch diese Überprüfung keinen Anlaß bot, die Kontroverse wegen des Umfangs meiner Kontrollbefugnisse erneut aufleben zu lassen, so will ich doch keinen Zweifel darüber lassen, daß ich aus den Gründen, die ich in meinem 2. Tätigkeitsbericht dargelegt habe, nach wie vor meine, auch Einzelvorgänge überprüfen zu können, ohne daß der betroffene Steuerpflichtige mich dazu ausdrücklich ermächtigt hat. Diese Befugnis hat der Bundesbeauftragte nach meiner Auffassung, und er muß sie haben, um wirksam sein zu können.

3.3.2 Zollkriminalinstitut (ZKI) und Zollfahndungsdienst

3.3.2.1

Im Rahmen einer Überprüfung des Zollkriminalinstituts in Köln habe ich mir einen ersten Überblick über die dort geführten Dateien und die Art der gespeicherten Daten verschafft. Dabei wurde erneut die Problematik des Umfangs meiner Kontrollbefugnis im Finanzbereich angesprochen. Zwar habe ich wiederum die Dateien überprüft, ohne die Namen der betroffenen Steuerpflichtigen zur Kenntnis zu nehmen. Ich konnte aber nicht feststellen, ob Daten zulässigerweise an Dritte übermittelt worden sind. Ich muß aber die Namen kennen, um die Verarbeitung beim Empfänger kontrollieren zu können.

3.3.2.2

Der Zollfahndungsdienst betreibt das *Informationssystem INZOLL*. Dieses System soll den Zollfahndungsämtern und Zollfahndungszweigstellen (nicht den Grenzzollstellen) nachweisen, welche Informationen sich bei welchen anderen Zollfahndungsstellen über die Personen befinden, deren Fall jeweils zu bearbeiten ist. INZOLL hatte zunächst die Funktion eines zentralen Hinweissystems ähnlich wie der geplante Kriminalaktennachweis (s. u. 3.11.2.1); inzwischen ist es zu einer Straftaten-/Straftäter-Datei für den Zollfahndungsdienst geworden.

Da INZOLL ein in sich relativ abgeschlossenes Informationssystem darstellt, bietet es sich an, dafür eine besondere Datenschutzregelung zu erlassen, in der die Zweckbestimmung festgeschrieben und außerdem bestimmt wird, welche Arten von Daten gespeichert und verarbeitet werden dürfen. Zu regeln wäre, wer innerhalb oder außerhalb der speichernden Stelle Zugang zu den Daten haben darf. Ferner wären Verfahren für die Auskunftserteilung an den Betroffenen, die Berichtigung, Sperrung, Löschung und Archivierung der Daten einzuführen und in der Datenschutzregelung für verbindlich zu erklären; schließlich müßte festgelegt werden, wie in Ausnahmefällen sowie bei tatsächlichen oder vermuteten Verstößen zu verfahren ist.

3.3.2.3

Die Tätigkeit der Zollfahndungsämter und des ZKI selbst auf den Gebieten der Gefahrenabwehr und der Strafverfolgung wirft zum Teil ähnliche Rechtsprobleme auf wie die polizeiliche Beobachtung durch die allgemeinen Polizeibehörden.

— Die Zollfahndungsämter sind über das ZKI an der polizeilichen Personenfahndung beteiligt, die durch das Informationssystem INPOL technisch unterstützt wird. So wie Gerichte und Staatsanwaltschaften die Eingabe von Haftbefehlen oder Aufenthaltsermittlungsersuchen in diese Fahndungsdatei veranlassen können, ist der Zollfahndungsdienst nach den geltenden Verwaltungsvorschriften befugt, Daten über Personen in dieses Informationssystem einzugeben, die zollrechtlich überwacht oder polizeilich beobachtet werden sollen. In dem einen Fall werden durch diese Art der Ausschreibung zollrechtliche Maßnahmen (Anhalten, Durchsuchen u. ä.), in dem anderen Fall Maßnahmen der polizeilichen Beobachtung ausgelöst. Die polizeiliche Beobachtung ist bei Verdacht des Verstoßes gegen Vorschriften des Betäubungsmittelrechts und des Waffenrechts zugelassen; die entsprechenden Angaben der Zollbehörden werden in die vom BKA geführte Datei „polizeiliche Beobachtung Rauschgift und Waffen" (eine logische Unter-Datei der Personenfahndungsdatei von INPOL) eingestellt; dadurch können die Reisebewegungen der betroffenen Personen registriert und an die Zollfahndungsstellen gemeldet werden.

Die Voraussetzungen für die verschiedenen Ausschreibungsarten sind in der Polizeidienstvorschrift 384.2 enthalten (hierzu s. u. 3.11.2.5). Das ZKI nimmt seine Ausschreibungen aufgrund eines innerdienstlichen Errichtungserlasses des Bundesministers der Finanzen vor. Dieser Erlaß ermächtigt das ZKI zur Sammlung aller Nachrichten, die für den Zollfahndungsdienst von Bedeutung sein können. Die rechtliche Problematik ist hier dieselbe wie bei der polizeilichen Beobachtung durch allgemeine Polizeibehörden. Zu den dagegen geäußerten Bedenken kommt hinzu, daß das ZKI — anders als das BKA — nicht auf der Grundlage einer gesetzlichen Aufgabenzuweisung arbeitet.

Soweit die dargestellten Maßnahmen der vorbeugenden Verbrechensbekämpfung und damit der *Gefahrenabwehr* dienen sollen, ist zur Rechtfertigung auf § 208 Abgabenordnung verwiesen worden. Er vermag jedoch eine Rechtsgrundlage nicht zu ersetzen, weil er ersichtlich nur eine Aufgabe umschreibt, nicht aber Befugnisse festlegt. Eine Generalklausel über die Befugnisse der Finanzbehörden ist in der Abgabenordnung und im Zollgesetz nicht enthalten. Vielmehr sind die Befugnisse — wie in der Strafprozeßordnung — jeweils speziell zugewiesen.

§ 208 AO enthält aus denselben Gründen auch keine ausreichende Rechtsgrundlage für eingreifende Maßnahmen zu Zwecken der *Strafverfolgung*. Auch § 404 AO, der auf die Befugnisse nach der Strafprozeßordnung verweist, vermittelt keine Rechtsgrundlage: hierfür käme nämlich allein § 163 StPO in Frage, auch dieser enthält jedoch nur eine Aufgaben- und keine Befugnisnorm (s. u. 3.11.2.5).

Für das ZKI und die Zollfahndungsbehörden gibt es bisher auch keine der Dateienrichtlinien für das BKA vergleichbaren Richtlinien, die insbesondere Löschung und Auskunft regeln. Zu fordern ist, daß für den Finanzbereich gleiche Regelungen in Kraft gesetzt werden wie für die Polizeibehörden.

3.3.2.4

Die vom ZKI in die polizeiliche Beobachtung und zollrechtliche Überwachung eingestellten Informationen sind auch durch das Steuergeheimnis geschützt. Eine Offenbarung dieser Erkenntnisse ist nur dann zulässig, wenn ein Ausnahmetatbestand nach § 30 AO gegeben ist. Das ist hier nicht der Fall.

Offenbarung ist jedes Verfahren, das es ermöglicht, daß steuerliche Erkenntnisse einem anderen bekannt werden oder bekannt werden können. Das INPOL-Personenfahndungssystem ermöglicht dem angeschlossenen Teilnehmerkreis einen sofortigen Direktzugriff auf den Datenbestand. Deshalb ist *vor* der Einstellung steuerlicher Erkenntnisse in das INPOL-System zu prüfen, ob die Voraussetzungen für die Zulässigkeit dieser Offenbarung nach § 30 AO *generell* vorliegen werden.

Nach § 30 Abs. 4 Nr. 1 AO ist die Offenbarung u. a. dann zulässig, wenn sie zur Durchführung eines *Steuerverfahrens* dient. Die Übermittlung an die an INPOL angeschlossenen Polizeibehörden ist danach nicht zulässig.

Ein weiterer Tatbestand zulässiger Offenbarung ist gegeben, wenn diese für ein konkretes *Strafverfahren* erforderlich ist. Das ist bei der polizeilichen Beobachtung und der zollrechtlichen Überwachung zumindest nicht immer der Fall. So ist in Nummer 1.1 der Polizeidienstvorschrift 384.2 ausdrücklich die Gefahrenabwehr als ein zulässiger Ausschreibungszweck benannt; das geht über die Strafverfolgung hinaus. Der Bundesminister der Finanzen beruft sich demgegenüber darauf, daß an der Kenntnis dieser Daten ein zwingendes öffentliches Interesse bestehe und die Offenbarung daher nach § 30 Abs. 4 Nr. 5 AO zulässig sei. Der Gesetzgeber hat zwar in dieser Bestimmung die Delikte, die eine Offenbarung rechtfertigen, nur beispielhaft aufgezählt, doch zeigt diese Aufzählung, daß es sich um Taten von erheblicher Bedeutung handeln muß. Bei einer der von mir geprüften zwei Personenakten aus diesem Bereich konnte ich diese Voraussetzung für die Einstellung bisher nicht erkennen.

Soweit dem Steuergeheimnis unterliegende Daten zur *zollrechtlichen Überwachung* in das INPOL-System eingestellt werden, erscheint mir eine generelle Zulässigkeit der Offenbarung ebenfalls bedenklich. Für die Verfolgung von Zoll- und Steuervergehen im Rahmen des § 208 AO sind ausschließlich die Zollfahndungsdienststellen zuständig. Diese haben aber im Gegensatz zu den Polizeidienststellen keinen direkten Zugriff auf diesen Datenbestand. Polizeidienststellen sind mit der Verfolgung dieser Delikte nicht betraut. Für sie ist die Kenntnis dieser Daten somit nicht erforderlich. Überdies darf die zollrechtliche Überwachung allein zollrechtliche Maßnahmen nach sich ziehen. Der Bundesminister der Finanzen hat inzwischen aufgrund meiner Bedenken die Weisung erteilt, solange keine Ausschreibung zur zollrechtlichen Überwachung in das INPOL-System mehr vorzunehmen, bis das Bundeskriminalamt eine getrennte Bestandsführung der zollrechtlichen Daten realisiert hat.

3.3.2.5

Das BDSG nimmt die Sicherheitsbehörden generell und „Bundes- und Landesfinanzbehörden, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung in Dateien speichern," von der Veröffentlichungs- und Auskunftspflicht aus (§ 12 Abs. 2 Nr. 1, § 13 Abs. 2). Der Begriff der Bundes- und Landesfinanzbehörden ist in § 6 AO abschließend definiert. Er ist auch bei Anwendung des BDSG zugrundezulegen. Das Zollkriminalinstitut ist in § 6 AO nicht erwähnt. Die Ausnahmetatbestände des BDSG sind also für diese Stelle nicht anwendbar.

Eine Veröffentlichung von Dateien des ZKI im Bundesanzeiger ist bisher nicht erfolgt, Meldungen des ZKI zu meinem Register (§ 19 Abs. 4 BDSG) liegen mir nicht vor. Ich werde darauf hinwirken, daß das ZKI diesen Verpflichtungen nach dem BDSG nachkommt.

3.4 Statistik und Forschung

In den aus der Sicht des Datenschutzes seit jeher besonders problematischen Bereichen der statistischen, planerischen und wissenschaftlichen Datenverarbeitung haben sich im Berichtszeitraum auf Teilgebieten praktibable Lösungen ergeben oder doch abgezeichnet.

Zur Frage, unter welchen Voraussetzungen und in welcher Form die statistischen Ämter wissenschaftlichen Instituten und anderen Interessenten statistisches Datenmaterial überlassen dürfen, hat § 11 Abs. 5 Bundestatistikgesetz eine grundsätzliche Klärung gebracht: Nicht nur aggregierte Daten (d. h. vor allem Tabellen) sondern auch Einzelangaben (Mikrodaten), an denen die Wissenschaft wegen ihrer vielfältigen Auswertbarkeit besonders interessiert ist, dürfen übermittelt werden, wenn sie „so anonymisiert" sind, „daß sie Auskunftspflichtigen oder Betroffenen nicht mehr zuzuordnen sind". Die Grenzlinie zwischen Datenschutz und Informationsbedürfnis ist damit genau an der richtigen Stelle gezogen: Die Betroffenen sind davor geschützt, daß die Datenempfänger etwas über ihre Verhältnisse erfahren, andererseits ist sichergestellt, daß der Datenschutz nicht dadurch diskreditiert wird, daß die Bereitstellung von Datenbeständen abgelehnt wird, obwohl die gewünschten Daten keinen Personenbezug aufweisen. Das Problem besteht nun in der praktischen Durchführung dieses Grundsatzes. Es ist eine vorrangige Aufgabe der statistischen Ämter, auf der Basis einschlägiger ausländischer Erfahrungen geeig-

nete Methoden zu entwickeln, die die vom Gesetz vorausgesetzte Anonymisierung von Mikrodaten-Beständen leisten. Ich befürworte und unterstütze entsprechende Forschungsprojekte wissenschaftlicher Institute und begrüße es, daß die Stiftung Volkswagenwerk im Rahmen ihres Förderungsprogramms „Datenschutz und Informationsbedarf — Forschungen zur Anwendung und Weiterentwicklung rechtlicher Regelungen" Mittel auch für diese Aufgabe bereitgestellt hat.

Die Bundestatistiken werden durchweg bundesweit erhoben; die Aufbereitung, Speicherung und Auswertung erfolgt überwiegend arbeitsteilig durch die statistischen Ämter der Länder und das Statistische Bundesamt. Daraus ergibt sich die Notwendigkeit einer möglichst einheitlichen datenschutzrechtlichen Beurteilung von Problemfällen. Die Konferenz des Bundes- und der Landesbeauftragten für den Datenschutz hat deshalb einen Arbeitskreis mit dem Auftrag eingerichtet, für die Anwendung und Auslegung der Datenschutzvorschriften des BDSG und der Statistikgesetze einheitliche Grundsätze zu entwickeln und Erfahrungen auch unter dem Gesichtspunkt der Fortentwicklung des Datenschutzrechts zusammenzutragen.

Ich begrüße es, daß die statistischen Ämter diese Koordinierungsbemühungen durch Information und Beratung unterstützen.

3.4.1 Statistisches Bundesamt

In meinem zweiten Tätigkeitsbericht hatte ich unter 2.4.3 (2. TB S. 20) über die Überprüfung des Statistischen Bundesamtes und die dabei festgestellten Mängel berichtet.

Zwischenzeitlich hat das Amt eine Reihe technischer und organisatorischer Maßnahmen zur Verbesserung des Datenschutzes in Angriff genommen und zum Teil auch umgesetzt. Dabei wurden die von mir ausgesprochenen Anregungen weitgehend berücksichtigt: Die interne Übersicht zur Darstellung der vorhandenen Datenbestände und Informationsflüsse wird überarbeitet und so erweitert, daß sie den Gesamtnachweis für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten beim Statistischen Bundesamt sowie Hinweise auf sicherheitsrelevante Tatbestände liefern kann; die Vervollständigung der Verfahrensdokumentation erfolgt fortlaufend; die Sicherheit im EDV-Bereich wird bis zum Neubau des Rechenzentrums durch organisatorische Maßnahmen verbessert. Außerdem wird an der Realisierung eines umfassenden Sicherheitskonzepts gearbeitet, das auch die Sicherung archivierter Daten einschließt.

Die Gesamtentwicklung beurteile ich positiv; auf einzelne noch bestehende Mängel habe ich das Amt hingewiesen.

3.4.2 Sozialhilfestatistik

Nach § 2 des Gesetzes über die Durchführung von Statistiken auf dem Gebiet der Sozialhilfe, der Kriegsopferfürsorge und Jugendhilfe vom 15. Januar 1963 (BGBl. I S. 49) werden in der Jahresstatistik der Sozialhilfe „die Zahl der Empfänger der Hilfe und die Aufwendungen im Berichtsjahr, aufgegliedert nach Empfängergruppen und Hilfearten", erfragt. Auskunftspflichtig sind die Träger der Sozialhilfe. Der Landesbeauftragte für den Datenschutz Nordrhein-Westfalen hat mich darauf aufmerksam gemacht, daß die amtlichen Zählblätter Namen und Anschriften sowie weitere personenbezogene Daten der Hilfeempfänger enthalten. Die statistischen Ämter hatten ohne Rücksicht auf das Fehlen einer entsprechenden gesetzlichen Ermächtigung eine namentliche Erfassung vorgesehen, weil angeblich nur so die Fälle ermittelt werden könnten, in denen ein Empfänger sowohl von örtlichen als auch von überörtlichen Sozialhilfeträgern Leistungen erhalten hat; dies sei zur Errechnung der genauen Zahl der Hilfempfänger erforderlich. Den betroffenen Personen wurden die Übermittlungen nicht bekannt, da die auskunftspflichtigen Sozialhilfeträger alle Angaben aus ihren Unterlagen entnehmen.

Auf meinen Wunsch hat der Bundesminister für Jugend, Familie und Gesundheit die zuständigen Stellen der Länder auf die datenschutzrechtlichen Bedenken, die auch von anderen Landesbeauftragten geteilt wurden, hingewiesen und erreicht, daß die Erfassung von Namen und Anschriften in der Sozialhilfestatistik künftig unterbleibt. Die Frage, ob die gesetzliche Ermächtigung überhaupt eine Verwendung von auf den Einzelfall bezogenen Zählblättern erlaubt, wenn dabei Betroffene bestimmbar sind, ist Gegenstand weiterer Beratungen.

3.4.3 Wehrmedizinalstatistik

Beim Institut für Wehrmedizinalstatistik und Berichtswesen der Bundeswehr in Remagen werden die ärztlichen Unterlagen aller Soldaten sowie ziviler Patienten der Sanitätseinrichtungen zentral archiviert und aufgrund einer Dienstvorschrift fünfzig Jahre lang aufbewahrt. Sie dienen sowohl der Verwendung in Einzelfällen, insbesondere für medizinische und versorgungsrechtliche Zwecke, als auch der Erarbeitung von zusammenfassenden Berichten und Statistiken. Aufgrund von Beschwerden Betroffener habe ich festgestellt, daß die ärztlichen Unterlagen aus der Musterung auch von denjenigen Wehrpflichtigen aufbewahrt werden, die wegen Wehrdienstuntauglichkeit ausgemustert worden sind; dies betrifft etwa 40 000 Personen jährlich. Für eine einzelfallbezogene Weiterverwendung besteht in diesen Fällen jedoch keinerlei Bedarf. Auf meine Einwendungen hin hat der Bundesminister der Verteidigung umgehend angeordnet, daß die ärztlichen Unterlagen der ausgemusterten Wehrdienstpflichtigen dem Institut für Wehrmedizinalstatistik nur noch in anonymisierter Form übersandt werden. Ein — theoretisch denkbarer — Mißbrauch dieser besonders sensiblen Unterlagen ist damit ausgeschlossen. Wehrpflichtige, die schon früher ausgemustert wurden, können die Löschung von Namen und Anschrift beim Institut für Wehrmedizinalstatistik verlangen.

3.4.4 Forschung

Der Bundesminister für Verkehr hat mich um Beratung gebeten, nachdem es bei demoskopischen Erhebungen, die Institute in seinem Auftrag durchführten, mehrfach zu Protesten von befragten Bürgern und zu kritischen Kommentaren in den Medien gekommen war. Das Ergebnis dieser Beratungen sind Richtlinien, die bei Forschungsvorhaben im Geschäftsbereich des Verkehrsministeriums künftig zugrunde gelegt werden sollen; sie sind auszugsweise im Anhang 1 zu diesem Bericht abgedruckt.

Ich habe mich bei der Beratung von dem Grundsatz leiten lassen, daß es nicht das Ziel des Datenschutzes sein kann, Informationsquellen auszutrocknen, auf die die Wissenschaft angewiesen ist, wenn sie ihren Auftraggebern tragfähige Entscheidungsgrundlagen liefern soll. Andererseits rechtfertigen weder die staatlichen Aufgaben noch die wissenschaftlichen Arbeitsmethoden, die Anforderungen des Datenschutzes zu ignorieren oder weniger ernst zu nehmen. Dies bedeutet für die Praxis demoskopischer Umfragen vor allem, daß die Institute und ihre staatlichen Auftraggeber nicht länger allein mit dem Ziel an den Betroffenen herantreten dürfen, eine möglichst hohe Antwortquote zu erreichen; vielmehr muß das Persönlichkeitsrecht der Betroffenen unter allen Umständen gewahrt bleiben. Das heißt konkret vor allem, daß jederzeit eine hinreichend tiefe und sachlich einwandfreie Aufklärung gegeben werden muß, ehe um eine freiwillige Teilnahme und — soweit erforderlich — um die Einwilligung zur Datenverarbeitung gebeten wird.

Die Richtlinien sind im übrigen mit den Grundsätzen abgestimmt, die zwischen den Verbänden der Markt- und Sozialforschungsinstitute und den obersten Datenschutz-Aufsichtsbehörden der Länder vereinbart worden sind. Ich empfehle den übrigen Geschäftsbereichen, die Richtlinien des Verkehrsministeriums und die damit gemachten Erfahrungen auch für ihre Forschungsvorhaben zu berücksichtigen. Ich bin zuversichtlich, daß auf diesem Wege zumindest ein Teil der Probleme im Bereich „Datenschutz und Forschung" bewältigt werden kann.

Um so dringender ist es freilich, die datenschutzrechtlichen Bedingungen der unabhängigen wissenschaftlichen Forschung zu überprüfen. Hochschulforschern sowie wissenschaftlichen Vereinigungen, die mir im vergangenen Jahr in großer Sorge darüber berichtet haben, daß ihnen der Zugang zu wichtigen Informationsquellen in zunehmendem Umfang unter Berufung auf den Datenschutz verwehrt wird, habe ich zugesagt, ihren Wunsch zu unterstützen, bei einer Novellierung des BDSG oder anderer datenschutzrechtlicher Bestimmungen von den gesetzgebenden Organen gehört zu werden.

In vielen Fällen zeigt sich allerdings auch, daß der Datenschutz lediglich als bequemer Vorwand angeführt wird, wenn Stellen, die über forschungsrelevante Daten verfügen, den Wissenschaftlern keinen Einblick in ihre Tätigkeit gewähren wollen. Ich rate deshalb allen Forschern, Konfliktfälle auszutragen und dabei auch die Hilfe der Datenschutz-Kontrollinstanzen in Anspruch zu nehmen. Nur wenn zwischen den Beteiligten um die richtige Anwendung des Datenschutzrechts gerungen wird, kann Klarheit gewonnen werden, ob die gesetzlichen Regelungen oder nur deren fehlerhafte Anwendung für die zunehmenden Informationsprobleme der Wissenschaft verantwortlich sind. Diese Klärung aber ist Voraussetzung für gesetzgeberische Korrekturen.

3.5 Personalwesen

Datenschutz ist für die Personalverwaltung nichts grundlegend Neues. Schon die traditionellen Aufgaben des Personalwesens wie Einstellung, Beförderung, Personalplanung usw. wurden nicht ohne die Pflicht zur Verschwiegenheit einerseits und ohne Einsichtsrechte in die Personalakten andererseits wahrgenommen. Es gibt — im großen und ganzen bewährte — Regeln, wie zwischen den Anforderungen der Aufgabenerfüllung des Dienstherrn/Arbeitgebers und den Interessen der Beschäftigten ein angemessener Ausgleich herzustellen ist.

Ich sehe indessen die Gefahr, daß als Folge einer zunehmenden Technisierung des Personalwesens tendenziell einseitige Veränderungen zu Lasten der Beschäftigten erfolgen. Hierauf habe ich bereits in meinem zweiten Tätigkeitsbericht (2. TB S. 24) hingewiesen.

Die Anwendungen der Informationstechnologie für Zwecke der Personalverwaltung stecken in der öffentlichen Verwaltung gegenwärtig zwar noch in den Anfängen — von einigen Anwendern sowie Standardauswertungen einmal abgesehen. Erfahrungsgemäß übernehmen jedoch öffentliche Verwaltungen mit zeitlicher Verzögerung häufig Konzepte, die in der Privatwirtschaft bereits praktiziert werden. Damit kommen datenschutzrechtliche Probleme auf die Verwaltungen zu, wie sie bisher nur aus diesem Bereich bekannt geworden sind. Vor einer Übernahme ergibt sich so aber die Chance, rechtzeitig die möglichen Gefahren einer Technisierung des Personalwesens zu erkennen und dem Einsatz der Informationstechnologie als Instrument übermäßiger Verhaltenskontrolle vorzubeugen. Für meine Bewertung sind vor allem zwei Gesichtspunkte entscheidend:

— Verknüpfbarkeit unterschiedlicher Anwendungen

  Schon heute eingesetzte Techniken wie z. B. Stechuhren, Aufzeichnung von dienstlichen oder privaten Telefongesprächen sowie Zugangskontrollen sind für sich genommen häufig wenig spektakulär und unbedenklich. Zum Teil ist ihr Einsatz aus Gründen der Datensicherung sogar sachlich geboten. Mit den zunehmenden Möglichkeiten, diese Techniken untereinander zu verknüpfen, ergibt sich jedoch eine neuartige Problemdimension: Quantität droht in Qualität umzuschlagen, weil eine Vielzahl von Einzelinformationen durch Zusammenführung zu einem Gesamtbild („Persönlichkeitsprofil") des Beschäftigten führen kann.

— Formalisierung menschlichen Verhaltens
Mir bekannte Konzepte von Personalinformationssystemen versuchen die Eigenschaften der Beschäftigten in unterschiedlich vielen und unterschiedlich differenzierten Merkmalen auszudrücken, z. B. um Grundlagen für Beförderungsentscheidungen oder innerbetriebliche Umsetzungen zu schaffen. Keine noch so gute Abbildung dieser Eigenschaften kann einen Menschen jedoch vollständig beschreiben. Im Gegenteil — jede Abbildung ist zwangsläufig mit einem Informationsverlust verbunden. Ich verkenne nicht, daß Verwaltungen, bei denen Personalentscheidungen Massenprobleme sind, auf den Einsatz technischer Instrumente schon aus Kostengründen ungern verzichten. Dies könnte hingenommen werden, wenn die begrenzte Tragfähigkeit maschinell gestützter Entscheidungen allen Beteiligten deutlich wäre. Ich habe aber Zweifel, ob die unterstützende Funktion derartiger Entscheidungshilfen allgemein erkannt wird und die Entscheidung immer beim Personalbearbeiter verbleibt.

Auch wenn mir bis jetzt nur wenige, zudem geringfügige Verstöße gegen Datenschutzbestimmungen bekannt geworden sind, scheint mir eine kritische Beobachtung der Entwicklung geboten. Der Weg zu sachgerechten Lösungen ist datenschutzrechtlich bis jetzt kaum ausgeschildert. Der Gesetzgeber, vor allem aber die Sozialpartner sind aufgerufen, rechtzeitig zu handeln.

3.5.1 Bewerbungsunterlagen und Personalbögen

Aufgrund mehrerer Eingaben habe ich mich mit der Problematik der Erhebung von Personaldaten in der öffentlichen Verwaltung befaßt. Im Rahmen der Bewerbung und Einstellung von Beschäftigten werden eine Vielzahl von Daten erhoben. Diese dienen zum Zeitpunkt der Bewerbung dem Bedürfnis, sich über den potentiellen Beschäftigten ein möglichst genaues Bild zu machen, vom Zeitpunkt der Einstellung an dienen sie der Personalführung und -bewirtschaftung. Aufgrund der zum Teil hohen Sensibilität dieser Daten ist dem Grundsatz der Verhältnismäßigkeit hier besonders Rechnung zu tragen. Ich strebe deshalb an, daß je besondere Regeln für Bewerbungsunterlagen und Einstellungsunterlagen angewendet werden. Inhalt der Bewerbungsunterlagen sollen nur die für die Entscheidung über die Einstellung eines Bewerbers erforderlichen Informationen sein, während die Einstellungsunterlagen darüber hinausgehende Informationen enthalten können, die z. B. für die Berechnung der Besoldung, der Vergütung oder des Lohns erforderlich sind. Ferner ist sicherzustellen, daß Bewerber, die nicht eingestellt werden, ihre Bewerbungsunterlagen zurückerhalten.

Personalbögen, die meist den Personalakten vorgeheftet werden, sind ein geeignetes Hilfsmittel, sich über den Beschäftigten eine kurze, schnelle Information zu beschaffen. Diesem Zweck, aber auch nur diesem, sollen sie dienen. Regelmäßig dürfen sie den Blick in die Personalakte zur Vorbereitung von Personalentscheidungen nicht ersetzen. Eine generelle Aussage über den Inhalt der Personalbögen ist nur bedingt möglich, weil ein nach der Behördenaufgabe unterschiedliches Informationsbedürfnis bestehen kann und auch aufgrund nicht einheitlicher Vorschriften des Beamten- und Tarifrechts in Bund, Ländern und Gemeinden im Detail unterschiedliche Informationen erhoben werden können. Deshalb wird es eine einheitliche, abschließende Antwort darauf, welchen Inhalt Personalbögen haben sollen, nicht geben können. Um der Vielfalt der unterschiedlichen Behördenaufgaben und Regelungen gerecht werden zu können, muß es bei generalklauselartigen Aussagen bleiben. Jedoch sind die Personal- und Betriebsräte aufgefordert, im Rahmen ihres Mitbestimmungsrechts den Inhalt der Personalbögen den jeweiligen Bedürfnissen der Behörde und dem Interesse der Beschäftigten anzupassen. Darüber hinaus halte ich eine Präzisierung des Inhalts von Personalbögen für einzelne Verwaltungsbereiche, z. B. auf dem Erlaßwege, für möglich und erstrebenswert. Angaben wie z. B. über die Religionszugehörigkeit oder über Namen und Beruf des Ehepartners sollten nur in solchen Fällen in den Personalbogen aufgenommen werden, in denen sie für die Personalbewirtschaftung und -führung von Bedeutung sind. Die Tatsache, daß diese Informationen zum Teil auch aus anderen Unterlagen (z. B. Heiratsurkunde, Steuerkarte) hervorgehen, spricht eher gegen als für die Notwendigkeit, diese Informationen auch in den Personalbogen aufzunehmen.

3.5.2 Personalaktenrecht

Im Personalwesen werden unzählige personenbezogene Daten erhoben und verarbeitet. Herkömmlich geschieht dies in *Personalakten*. Lediglich ein Teil der Verwaltung verwendet für einen Teil seines Personals und/oder für einen Teil der Daten aus Personalakten automatische und/oder manuelle Dateien.

Die personenbezogenen Daten in Personalakten unterliegen verstärktem Schutz: das Personalaktengeheimnis ist ein *besonderes* Amtsgeheimnis i. S. des Datenschutzrechts (vgl. z. B. §§ 10, 11, 24 BDSG). Die Vorschriften über den Schutz des Amtsgeheimnisses (z. B. § 61 BBG, § 39 BRRG) gelten folglich nur nach Maßgabe der besonderen in der Rechtsprechung entwickelten Grundsätze zum Schutze des Personalaktengeheimnisses. So dürfen z. B. Mitteilungen im dienstlichen Verkehr, die gemäß den Vorschriften über das Amtsgeheimnis zulässig sind, bei Daten, die unter das Personalaktengeheimnis fallen, nur erfolgen, wenn die spezifischen Regeln des Personalaktenrechts eine derartige Mitteilung erlauben. Generell ist aber eine Mitteilung im dienstlichen Verkehr aus Personalakten nicht zulässig. Das Bundesverwaltungsgericht vertritt in ständiger Rechtsprechung den Standpunkt, daß Personalakten ohne Einwilligung des Beamten grundsätzlich nur von einem eng begrenzten Personenkreis mit besonderer dienstlicher Verantwortung (Personalreferent, Behördenleiter) eingesehen werden dürften; sie genössen sowohl im dienstlichen Interesse als auch im schutzwürdigen persönlich-privaten In-

teresse des Beamten einen besonderen Vertrauensschutz, der sich auch auf den Verkehr der Behörden untereinander erstrecke. Personalakten gehörten grundsätzlich zu den Vorgängen, die gemäß § 99 Abs. 1 Satz 2 VwGO ihrem Wesen nach geheimgehalten werden müßten (BVerwGE 19, 179, 185 m. w. N.; 35, 225, 227).

Die Befugnis und Pflicht zur Führung von Personalakten wird in den bundesgesetzlichen Regelungen (z. B. § 90 BBG, § 56 BRRG) vorausgesetzt. Eine gesetzliche Regelung hierzu fehlt — im Gegensatz zu einigen Landesbeamtengesetzen. Nun zeichnet sich das Beamtenrecht sonst durch eine besonders große Regelungsdichte aus. Um so mehr muß es verwundern, daß Befugnis und Pflicht zur Führung von Personalakten, also Regelungsgegenstände, bei denen es sich um die Erhebung und Verarbeitung zum Teil sensibelster Daten handelt, bisher keine bundesgesetzliche Grundlage gefunden haben. Angesichts eines gewachsenen Problembewußtseins im Bereich der Informationsverarbeitung sollte dies bald nachgeholt werden. Bei dieser Gelegenheit sind auch endlich Regelungen zur Tilgung oder Löschung von Daten aus Personalakten zu treffen. Auch insoweit sollte der Bund nicht hinter den auf diesem Wege vorangegangenen Landesbeamtengesetzen zurückbleiben.

Der Entwurf eines Bereinigungsgesetzes — Stand: Januar 1980 —, der im Mai 1980 Gegenstand eines Beteiligungsgesprächs gemäß § 94 BBG, war, aber in der 8. Legislaturperiode nicht mehr verabschiedet wurde, fand insoweit nicht den Beifall zweier großer Spitzenorganisationen der zuständigen Gewerkschaften, nämlich des Deutschen Beamtenbundes und des Deutschen Gewerkschaftsbundes. Auch ich halte den Entwurf unter datenschutzrechtlichen Gesichtspunkten für verbesserungsbedürftig. Insbesondere sollte er dazu führen, daß das Vorhalte- und Verwertungsverbot gemäß §§ 49, 50 Bundeszentralregistergesetz auch im Personalaktenrecht in einer Weise implementiert wird, die der Bedeutung des Resozialisierungsgebots gerecht wird. Das ist in der bisherigen Fassung nicht der Fall, auf Grund einer sorgfältigen Abwägung zwischen dem Persönlichkeitsschutz des Beamten und etwaigen Grundsätzen der Aktenführung wie dem sogenannten Vollständigkeitsgrundsatz aber erforderlich.

3.5.3 Bundespersonalausschuß

In meinem zweiten Tätigkeitsbericht habe ich über Verfahrensordnungen des Bundespersonalausschusses, nach denen ihm „die Personalakten" vorzulegen seien (2. TB S. 23 f.), und darüber berichtet, daß der Meinungsaustausch zwischen dem Bundesminister des Innern, dem Bundespersonalausschuß und mir hierüber noch nicht abgeschlossen sei.

Inzwischen hat der Bundespersonalausschuß die Vorlagepflicht auf die Personalhauptakten (also ohne Vor- und Nebenakten) beschränkt. Er hat sich darüber hinaus bereit erklärt, in den einschlägigen Verfahrensordnungen den Umfang der Vorlagepflicht klarzustellen. Der Verzicht auf die Vorlage von Vor- und Nebenakten ist eine zu begrüßende Einschränkung im Sinne des in § 102 Abs. 2 BBG normierten Erforderlichkeitsprinzips.

3.5.4 Beihilfen

Aufgrund mehrerer Eingaben und einer Anregung der Datenschutzkommission Rheinland-Pfalz habe ich die Frage der Erforderlichkeit eines ärztlichen Schlußberichts bei Sanatoriumsaufenthalten und Heilkuren geprüft. Nach § 6 Abs. 1 Beihilfevorschriften sind u. a. die Kosten der Unterbringung und Verpflegung in einem Sanatorium sowie die Auslagen für Kurtaxen und die Kosten des ärztlichen Schlußberichtes beihilfefähig, wenn ein amts- oder vertrauensärztliches Gutachten darüber vorgelegt wird, daß die Sanatoriumsbehandlung dringend notwendig und nicht durch stationäre Behandlung in einer anderen Krankenanstalt oder durch eine Heilkur mit gleicher Erfolgsaussicht ersetzbar ist, und die Festsetzungsstelle die Beihilfefähigkeit vorher anerkannt hat. Der genannte ärztliche Schlußbericht fällt sehr unterschiedlich aus. Er kann den Behandlungsplan für einen Kurverlauf wiedergeben, d. h. alle während der Kur getroffenen Verordnungen und verabreichten Anwendungen; er kann aber darüberhinaus personenbezogene Daten enthalten, z. B. Diagnosedaten, die teilweise sehr sensibel sein können. Der Schlußbericht kann schließlich so inhaltsarm sein, daß er nicht einmal für den Zweck der Abrechnung der Beihilfe ausreicht, so daß Rückfragen erforderlich werden. Je nach dem beschriebenen Inhalt stellt sich die datenschutzrechtliche Problematik unterschiedlich.

Ich habe anerkannt, daß die Beihilfestelle für die Abrechnung der Beihilfe diejenigen Informationen benötigt, aus denen hervorgeht, ob die abgerechneten Leistungen mit den angeordneten und durchgeführten Verordnungen des Arztes übereinstimmen oder ob bzw. warum Änderungen in der Durchführung vorgenommen wurden. Soweit der ärztliche Schlußbericht darüber hinausgehende Informationen gibt, sind diese für die Beihilfestelle nicht erforderlich. Hält der Sanatoriums- oder Kurarzt ärztliche Hinweise für die weitere Behandlung des Beihilfeberechtigten für erforderlich, so sind diese — mit Einwilligung des Beschäftigten — dem behandelnden Arzt oder dem Personalarzt in einem Arztbrief mitzuteilen.

Das für Beihilfefragen zuständige Grundsatzreferat des Bundesministeriums des Innern und der Leitende Arzt des Ärztlichen und Sozialen Dienstes der obersten Bundesbehörden werden in Übereinstimmung mit mir darauf hinwirken, daß der ärztliche Schlußbericht in Zukunft nur noch die für die Abrechnung der Beihilfe erforderlichen Daten enthält, während darüber hinausgehende Informationen mit Einwilligung des Beschäftigten dem Hausarzt oder ggf. dem Personalarzt zugeleitet werden.

3.5.5 Automatisierte Datenverarbeitung

3.5.5.1 Personalinformationssysteme

Es gibt keine gesicherte Definition für das in der öffentlichen Diskussion zunehmend gebrauchte

Schlagwort „Personalinformationssystem". Ein Lehrwerk über Personalinformationssysteme (G. Reber [Hg.], Personalinformationssysteme, Stuttgart 1979, S. V) gibt folgende Aufgabenbeschreibung: „Die Grundvorstellung für den Einsatz von Personaldaten im Sinne der Aufgaben eines Management-Informationssystems liegt in der Lösung eines Zuordnungsproblems zwischen Arbeitsplatzanforderungen einerseits und personalen Eigenschaften andererseits zur Optimierung der mit der Erfüllung der Arbeitsplatzanforderungen angestrebten betrieblichen Leistung". Mir ist für den Bereich meiner Zuständigkeit kein einziges System bekannt, das diesen Wunschvorstellungen ganz entspricht. Allerdings gibt es in einer Reihe von Verwaltungen Bemühungen, Personaldaten, die in der Vergangenheit automatisiert lediglich für den Zweck „Lohn- und Gehaltsabrechnung" verarbeitet wurden, auch für andere Zwecke zu benutzen, z. B. für automatisierte Erstellung von Reihungen (Listen) für Beförderungsentscheidungen oder zur Unterstützung von Planungs- und Führungsentscheidungen.

Das nach meiner Kenntnis am weitesten entwikkelte System im Bereich des Bundes ist das System PERFIS, das „Personalführungs- und -informationssystem Soldaten" des Bundesministers der Verteidigung. Ich habe dieses System Ende 1980 zwei Wochen lang überprüfen lassen. Da das Verfahren dieser Prüfung noch nicht abgeschlossen ist, habe ich mit den zuständigen Stellen eine Fortsetzung Anfang des Jahres 1981 vereinbart. Ich möchte deshalb hier auf die Wiedergabe von Details verzichten (zum Problem der Speicherung von Beurteilungsnoten vgl. schon 2. TB S. 21 f.) und lediglich auf einige klärungsbedürftige Probleme hinweisen, nämlich

— das System der Zugriffe auf PERFIS,
— Inhalt und Verfahren empirischer, insbesondere psychologischer Forschungen und ihre Abgrenzung von den eigentlichen Aufgaben des Personalwesens,
— Sicherheitsanforderungen an ein System wie PERFIS, das auch im Ernstfall einsatzfähig sein muß, insbesondere höchste Anforderungen an Transparenz und Beherrschbarkeit des Systems,
— die Organisation des Datenschutzes im Bereich des Personalwesens.

Allgemein sei festgestellt, daß das System PERFIS wegen seines verteidigungspolitischen Auftrags als Beispiel nur bedingt verallgemeinerungsfähig ist. Was für dieses System mit einem besonders in die Pflicht genommenen Adressatenkreis vertretbar sein mag, kann für andere öffentliche Verwaltungen eine problematische Lösung sein. Bei dem gegenwärtigen Stand des Aufbaus von Personalinformationssystemen kann ich vorerst nur allgemein darauf aufmerksam machen, die auftretenden Probleme grundsätzlich zu durchdenken, bevor mit der Anwendungsphase von Personalinformationssystemen begonnen wird.

3.5.5.2 Gleitzeiterfassung

Mehrere Eingaben betreffen Fragen der Gleitzeiterfassung.

Eine maschinelle Gleitzeiterfassung scheint mir nur dann erforderlich zu sein, wenn eine Selbstaufzeichnung durch die betroffenen Mitarbeiter aus konkreten arbeitsbedingten Gründen nicht möglich ist oder aber wenn sich herausstellt, daß solche Aufzeichnungen nicht korrekt geführt werden. Wird ein Erfassungsgerät eingesetzt, muß sichergestellt sein, daß folgende Forderungen berücksichtigt werden:

— Es sollen nur die für die Abrechnung erforderlichen Daten aufgezeichnet werden.
— Die Zeitdaten der Mitarbeiter dürfen nicht von anderen eingesehen werden können. Dies kann z. B. bei Aufzeichnungskarten dadurch erreicht werden, daß die Kartei beaufsichtigt wird (z. B. durch den Pförtner); dies wurde in einem Fall auf meine Empfehlung veranlaßt. Auch dadurch, daß die Namen auf den Karten nicht ausgewiesen werden, wird das Aufnehmen von Informationen durch andere als den Betroffenen erschwert. Bei anderen Aufzeichnungsarten ist durch andere organisatorische und technische Maßnahmen eine unbefugte Kenntnisnahme zu verhindern.
— Es muß sichergestellt sein, daß die erhobenen Daten ausschließlich für die Gleitzeitberechnung verwandt werden. So wäre vor allem die Aufnahme dieser Daten in ein Personalinformationssystem problematisch.
— Die aufgezeichneten Daten sind nach Abrechnung und Anerkenntnis durch den Betroffenen zu löschen.

Der Personal-/Betriebsrat ist in allen die maschinelle Gleitzeiterfassung betreffenden Fragen zu beteiligen (vgl. §§ 68 Abs. 2, 75 Abs. 3 Nr. 1 u. 17 BPersVG; § 87 Abs. 1 Nr. 2 u. 6 BetrVerfG). Der interne Datenschutzbeauftragte sollte jedenfalls kontrollieren, daß die Daten nur für den Zweck Zeitabrechnung verwandt werden.

3.5.5.3 Telefonkontrolle

Im Rahmen einer Prüfung und in mehreren Eingaben wurde die Frage der automatischen Erfassung von Ferngesprächen aufgeworfen. Hierüber gibt es in den allermeisten Fällen weder Rechtsvorschriften noch Vereinbarungen zwischen Dienstherrn und Personalrat bzw. Unternehmensleitung und Betriebsrat. Es ist daher von den allgemeinen Grundsätzen der Erforderlichkeit (für die Aufgabenerfüllung) und der Verhältnismäßigkeit auszugehen.

Bei der Klärung von Art und Umfang einer Speicherung ist zwischen dienstlichen und privaten Gesprächen zu unterscheiden. Daten über dienstliche Gespräche sollten grundsätzlich nur dann registriert werden, wenn dies für die Aufgabenerfüllung, über private Gespräche nur, wenn und soweit es zu Abrechnungszwecken erforderlich ist. Im einzelnen vertrete ich dazu folgende Auffassung:

Im ersten Falle sollte sich die Registrierung auf die Angabe der Nebenstellennummer des Beschäftigten sowie des Datums und der Dauer des Telefonats (Gebühreneinheiten) beschränken. Weitergehende Informationen (z. B. Verbuchungsstelle, Aktenzeichen) sollten nur dann registriert werden, wenn sich dies

aus der Aufgabenstellung der Behörde ergibt. Die Angabe des Gesprächsteilnehmers wird nur in Ausnahmefällen erforderlich sein, weil der Beschäftigte regelmäßig Aufzeichnungen über den Gesprächspartner und den Gesprächsinhalt in einer Aktennotiz zu machen hat. Eine wörtliche Registrierung des Gesprächsinhalts wird sich aus der Aufgabenerfüllung nur selten rechtfertigen lassen (z. B. im Sicherheitsbereich).

Eine Auswertung der Aufzeichnungen über dienstliche Telefongespräche zu Zwecken der Kontrolle der Beschäftigten oder die Verknüpfung dieser Aufzeichnungen mit anderen Informationen über die Beschäftigten darf nicht stattfinden. Wenn zur Reduzierung des Gebührenaufkommens zeitlich befristete Kontrollaufzeichnungen vorgenommen werden, sollten die Beschäftigten vorher unterrichtet und die Maßnahme mit dem Personal-/Betriebsrat und gegebenenfalls dem internen Datenschutzbeauftragten abgestimmt werden. Die Auswertung dieser Aufzeichnungen ist auf die hierfür Zuständigen zu beschränken. Nach Ende der befristeten Maßnahme sind die Aufzeichnungen zu löschen.

Die Registrierung von Angaben über *private* Telefongespräche ist nur zulässig, soweit diese für Abrechnungszwecke erforderlich sind. Dazu genügen die Nebenstellennummer des Beschäftigten, das Datum sowie die Dauer des Telefonats (Gebühreneinheiten). Eine Aufzeichnung des Teilnehmers (Angerufenen) ist nicht erforderlich. Sollte der Beschäftigte dies verlangen, so sollte ihm geraten werden, diese Informationen selbst in geeigneter Form festzuhalten. Eine Auswertung der genannten Angaben zu anderen als Abrechnungszwecken und die Verknüpfung mit anderen Informationen über die Beschäftigten muß unterbleiben.

Die Beschäftigten sind aus Gründen der Transparenz über den Umfang der Registrierung und darüber, welche Stellen die Unterlagen zu Abrechnungszwecken erhalten, zu informieren. Die Aufzeichnungen sind nach erfolgter Abrechnung zu löschen.

3.5.5.4 Leistungskontrolle

Bei vielen Bildschirmarbeitsplätzen werden Aufzeichnungen über die Arbeit des „Bedieners" geführt. Die dabei gesammelten Angaben werden u. a. zu Abrechnungszwecken benötigt. Zum Beispiel wird die Arbeit eines Programmierers, der am Bildschirm Software entwickelt, in solchen Aufzeichnungen beschrieben, um die Entwicklungskosten für die jeweiligen Programme den verursachenden Sachgebieten anlasten zu können.

Mir ist ein Fall bekannt geworden, in dem derartige Aufzeichnungen nicht nur für Abrechnungszwecke benutzt wurden, sondern einem Vorgesetzten zur Leistungsbewertung vorlagen. Abgesehen davon, daß Aufzeichnungen, die für einen bestimmten andersartigen Bereich erfolgen, in der Regel nicht geeignet sind, sich ein Bild von der Leistungsfähigkeit eines Mitarbeiters zu machen, halte ich es für problematisch, Daten, die zweckbestimmt erhoben wurden, anderweitig zu benutzen.

3.5.5.5 Zugangs- und Zugriffskontrolle

Aus Sicherheitsgründen ist für viele Bereiche eine Zugangskontrolle erforderlich. Auch das BDSG fordert in der Anlage zu § 6 Abs. 1 Satz 1, „Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren."

Wie die Zugangskontrolle realisiert werden kann, ist in einer Reihe von Fachzeitschriften beschrieben worden. Darüber hinaus sind Zugangskontrollsysteme vielerorts Praxis. Sowohl in Veröffentlichungen als auch in der Praxis ist bisher zwei Problemen zu wenig Aufmerksamkeit entgegengebracht worden:

— Bei Einsatz von *Zugangskontrollsystemen* entstehen Aufzeichnungen mit naturgemäß personenbezogenem Inhalt. Es muß sichergestellt werden, daß diese Informationen nur für den Zweck „Zugangskontrolle" ausgewertet werden. Die Auswertung sollte daher nur durch den Datenschutzbeauftragten erfolgen. Er sollte auch darüber mitentscheiden, welche Daten überhaupt aufgezeichnet werden. So kann es erforderlich sein, alle Zutritte bzw. Zutrittsversuche aufzuzeichnen; je nach organisatorischer „Flankensicherung" kann es aber auch genügen, nur unbefugte Zutrittsversuche (ohne Aufzeichnung) zu melden.

— Die technische Entwicklung hat ermöglicht, *Computerunterstützung an den Arbeitsplatz* zu bringen. Bürocomputer, die heute eine Leistungsfähigkeit und eine Speicherkapazität haben wie vor einigen Jahren nur Großanlagen, werden in stark wachsender Anzahl in Büroräumen aufgestellt. Wie ich bei Überprüfungen festgestellt habe, führt das — nicht nur in Ausnahmefällen — zu folgender Situation:

  Behörden und andere Organisationen sichern ihre Rechenzentren mit erheblichem technischen Aufwand ab. Nahezu perfekte Zugriffs- und Zugangskontrollsysteme sind eingesetzt. In der gleichen Stelle stehen Bürocomputer in nicht oder nur mangelhaft gesicherten Büroräumen, obwohl hier ähnlich sensible Daten, wenn auch in geringerer Menge als im Rechenzentrum, verarbeitet werden. Die hier durchgeführten Zugriffs- und Zugangskontrollen sind oft unzureichend. Eine Lösung dieses Problems kann ich auch noch nicht anbieten. Hersteller und Anwender sind jedoch aufgerufen, dazu beizutragen, auch die Datenverarbeitung am Arbeitsplatz sicherer zu machen.

Um kontrollieren zu können, ob tatsächlich nur Berechtigte auf die ihrer *Zugriffsberechtigung* unterliegenden personenbezogenen Daten zugreifen, wird in der Regel aufgezeichnet, welche Berechtigten auf welche Datensätze zugreifen. Dies geschieht teilweise durch Ausdruck auf Papier, in großen Systemen jedoch in elektronischen Dateien. Demgegenüber wird beim Bundeskriminalamt bewußt auf die Protokollierung der Zugriffe verzichtet, da hier zusätzliche Dateien mit sehr sensiblem Inhalt entstünden. Von Ausnahmen dieser Art abgesehen, halte ich eine Protokollierung jedoch für erforderlich.

Die dabei entstehenden Dateien müssen entsprechend gesichert werden. Zu nutzen sind sie allein durch den Datenschutzbeauftragten, soweit nicht eine Nutzung für systemtechnische Zwecke unumgänglich ist (Wiederanlauf des EDV-Systems). Nach Durchführung der Kontrollen durch den Datenschutzbeauftragten sind die Dateien zu löschen.

Im übrigen sind solche Dateien bei mir zur Aufnahme in das Register gemäß § 19 Abs. 4 BDSG anzumelden.

3.6 Bibliothekswesen

Bei der *Deutschen Bibliothek* in Frankfurt wurde eine zweitägige Prüfung durchgeführt. Als zentrale Archivbibliothek hat die Deutsche Bibliothek im wesentlichen die Aufgabe, sämtliche deutschsprachigen Druckwerke, soweit sie nach dem 8. Mai 1945 hergestellt worden sind, zu sammeln, zu inventarisieren und bibliographisch zu verzeichnen. Sie dient gleichzeitig der Allgemeinheit als Präsenzbibliothek.

Das Ergebnis der Prüfung läßt sich folgendermaßen zusammenfassen:

Die Bedeutung des Datenschutzes für die eigene Tätigkeit war in der Deutschen Bibliothek noch kaum erkannt. Im Hinblick darauf, daß die im Rahmen des gesetzlichen Auftrags verarbeiteten personenbezogenen Daten ausnahmslos zur Veröffentlichung bestimmt sind und auch tatsächlich veröffentlicht werden, war man davon ausgegangen, daß ein sachliches Bedürfnis für Datenschutz nicht gegeben sei. Ein Verzeichnis der Dateien war zwar vorhanden, aber nicht auf die in § 15 BDSG definierten Anforderungen abgestimmt. Weiterhin waren die nach § 12 vorgeschriebene Veröffentlichung und die nach § 19 Abs. 4 erforderliche Anmeldung zum Dateienregister versäumt worden. Eine Verpflichtung auf das Datengeheimnis hatte nicht stattgefunden.

Im Verlauf der Prüfung und der Beratungsgespräche in verschiedenen Abteilungen ergab sich jedoch bald volle Übereinstimmung darin, daß der Datenschutz auch für die Deutsche Bibliothek erhebliche Bedeutung hat. Auch wenn die bibliographischen Daten durchweg keines Schutzes gegen unbefugte Kenntnisnahme bedürfen, so besteht doch ein klar erkennbares Interesse der Betroffenen (vor allem Autoren und Herausgeber) an wirksamen Kontrollmöglichkeiten im Hinblick auf die Richtigkeit der verarbeiteten Daten. Darüber hinaus gibt es auch in der Deutschen Bibliothek Dateien, wie Personal- oder Benutzer- und Entleiher-Karteien, die umfassend datenschutzbedürftig sind.

Mein Besuch hatte zur Folge, daß die versäumten Maßnahmen nachgeholt und eine Reihe weiterer von mir festgestellter Mängel und Schwachstellen behoben wurden oder Verbesserungen von der Deutschen Bibliothek fest eingeplant sind. Der Zugang zum Sondermagazin, das u. a. Druckwerke mit nicht allgemein zugänglichen personenbezogenen Daten (z. B. Fahndungsbüchern, Auszügen aus Schuldnerverzeichnissen in Druckwerken der Industrie- und Handelskammern) enthält, wurde auf zwei Personen beschränkt. Die Benutzerkartei wird von Angaben, deren dauerhafte Speicherung nicht zwingend ist (etwa: Beruf, Geburtstag, Geburtsort, Personalausweis-Nummer) befreit; ähnliches gilt für die Ausleihzettel. Die Sicherheit der in der Personalabteilung gespeicherten Angaben wird durch organisatorische und technische Maßnahmen verbessert. Bezogen auf die Hauptaufgabe der Deutschen Bibliothek, die bibliographische Verzeichnung und katalogmäßige Erschließung von Druckwerken, waren wesentliche datenschutzrechtliche Mängel nicht festzustellen. Insbesondere habe ich mich vergewissert, daß den hin und wieder eingehenden Berichtigungsverlangen Betroffener in korrekter Weise nachgekommen wird.

Insgesamt ist festzustellen, daß die Beanstandungen durchweg zu positiven und angemessenen Reaktionen geführt haben und nunmehr zu erwarten ist, daß der Datenschutz in absehbarer Zeit weitestgehend gewährleistet sein wird.

3.7 Deutsche Bundespost

Die Datenverarbeitung bei der Deutschen Bundespost bildete im vergangenen Jahr einen Schwerpunktbereich meiner Kontrolltätigkeit. Dies rührt einmal daher, daß anteilmäßig die meisten Eingaben die Datenverarbeitung durch die Post betrafen, wenn man von den Eingaben im privaten Bereich, die ich an die Länder weitergeleitet habe, absieht. Damit soll nicht gesagt werden, daß die Deutsche Bundespost den Datenschutz nicht genügend beachtete. Der Bundesminister für das Post- und Fernmeldewesen hat bereits frühzeitig umfangreiche Erläuterungen und detaillierte Anweisungen für die Gewährleistung des Datenschutzes im Bereich der Deutschen Bundespost erlassen. Datenschutz ist überdies für die Post nichts Neues. Das Post- und Fernmeldegeheimnis wird nicht nur generell strikt beachtet; es wird auch mir bei meiner Kontrolltätigkeit entgegengehalten. Dies muß ich akzeptieren, weil das Bundesdatenschutzgesetz keine ausdrückliche (‚benannte') Ausnahmeregelung zugunsten meiner Kontrollbefugnisse enthält, wie sie in Artikel 19 Abs. 1 Satz 2 GG vorgeschrieben ist. Die Rechtslage ist insoweit anders als im Bereich der Steuerverwaltung (s. o. 3.3). Während es dort nur einer Klarstellung bedarf, daß das Steuergeheimnis meine Kontrolltätigkeit nicht beschränkt, muß für das Post- und Fernmeldegeheimnis der Gesetzgeber entscheiden, ob ich die darunter fallenden Unterlagen einsehen kann oder nicht.

Der wesentliche Grund, mich der Datenverarbeitung bei der Post verstärkt zuzuwenden, liegt darin, daß hier gegenwärtig die technologischen Grundlagen für die Ausgestaltung der Informationslandschaft der Zukunft geschaffen werde. Ich nenne als Beispiele das Kabel- und Dialogfernsehen, den elektronisch übermittelten Brief (Telefax), das Bildschirmtelefon und andere Dienstleistungen, die alle dem Zweck dienen, mehr Informationen schneller und sicherer zu befördern. Daß hier Datenschutzüberlegungen eingebracht werden müssen, ehe voll-

endete Tatsachen geschaffen sind, dürfte unmittelbar einleuchten.

3.7.1 Aufzeichnungen über Telefongespräche

Die Deutsche Bundespost führt Aufzeichnungen über Ferngespräche nur in Ausnahmefällen. In der Regel werden lediglich die anfallenden Gebühren addiert und dem Fernsprechteilnehmer die Summe in Rechnung gestellt. Beanstandet er seine Rechnung, kann das Fernmeldeamt einen sogenannten befristeten Zählvergleich durchführen, bei dem die rufende Nummer, die gerufene Nummer, Datum und Uhrzeit sowie die Zahl der Gesprächseinheiten während eines befristeten Zeitraums auf einem Zählvergleichsstreifen festgehalten werden. Die so erfaßten Daten unterliegen dem Fernmeldegeheimnis, sie werden entsprechend geschützt und nach Ablauf des Erstattungsanspruches bzw. nach Abschluß des Streitfalles vernichtet.

Einige Fernmeldeämter der Deutschen Bundespost sind mit dem sogenannten elektronischen Wählsystem (EWS) ausgestattet, das technische Verbesserungen gegenüber der herkömmlichen Technik aufweist. Auch im EWS werden im Regelfall die Gebühren lediglich addiert. Bei Beanstandungen bzw. auf Antrag des Teilnehmers wird ein befristeter Zählvergleich durchgeführt.

In der Vergangenheit ist die Deutsche Bundespost häufig aufgefordert worden, ausführlichere Telefonrechnungen in Form einer Auflistung der Gebühren für einzelne Gespräche zu erstellen. Das EWS-System bot erstmals die technische Möglichkeit, dieser Forderung ohne allzu großen Mehraufwand zu entsprechen. Daher wurden seit 1978 bei einigen Fernmeldeämtern, die an das EWS angeschlossen waren, die Daten, die sonst im befristeten Zählvergleich gespeichert wurden, nunmehr vorbeugend festgehalten. Dem Teilnehmer, der seine Rechnung beanstandete, sollte damit nachgewiesen werden, daß die ihm in Rechnung gestellten Gespräche tatsächlich von seinem Anschluß aus geführt worden waren. Die bei diesem sogenannten vorbeugenden Zählvergleich anfallenden Daten wurden in einem zentralen Rechner in Neuss gespeichert und nach Ablauf einer bestimmten Frist gelöscht. Die dabei entstehenden Dateien sind nicht zu dem von mir geführten Register angemeldet worden.

Ich habe den Bundesminister für das Post- und Fernmeldewesen um nähere Informationen gebeten und auf die Gefahren hingewiesen, die in der Speicherung so riesiger Mengen von personenbezogenen Daten liegen. Es handelt sich dabei um Daten von hohem Sensibilitätsgrad, die, wenn sie Unbefugten zur Kenntnis gelangen, in vielfältiger Weise mißbraucht werden können. Dies gilt namentlich für die Speicherung der Rufnummer des angerufenen Teilnehmers. Wenn auch das Fernmeldegeheimnis einen starken Schutz bietet, so könnte es doch nicht verhindern, daß Polizei und Nachrichtendienste sich dieser ergiebigen Datenquelle im Rahmen der ihnen gesetzlich zugewiesenen Befugnisse bedienen. Der vorbeugende Zählvergleich ist eine nützliche und akzeptierbare Einrichtung, solange er in den Grenzen der zugewiesenen Zweckbestimmung genutzt wird. Er kann jedoch zu einem gefährlichen Überwachungsinstrument werden. Darauf hinzuweisen halte ich für meine Pflicht.

Ein öffentlicher Vortrag in der Evangelischen Akademie in Bad Boll, in dem ich erneut auf die Gefahren aufmerksam gemacht habe, löste ein lebhaftes Echo in den Medien aus. Der Bundesminister für das Post- und Fernmeldewesen sah sich daraufhin veranlaßt, die Maßnahme für beendet zu erklären. Er wird nach Auswertung der vorliegenden Ergebnisse die weiteren Schritte mit mir und dem Bundesminister des Innern abstimmen.

3.7.2 Eintrag ins Fernsprechbuch

§ 39 Abs. 2 der Fernmeldeordnung (FO) enthält den Grundsatz, daß jeder Fernsprechteilnehmer in das amtliche Fernsprechbuch aufzunehmen ist. Ausnahmen werden nur „auf begründeten Antrag" zugelassen. Ein möglichst vollständiges Verzeichnis aller Fernsprechteilnehmer liegt nach Auffassung des Bundesministers für das Post- und Fernmeldewesen im öffentlichen Interesse. „Gelegentliche" Belästigungen der Teilnehmer mittels des Telefons seien zumutbar. Wer heute vom Eintrag in das Fernsprechbuch ausgenommen werden will, muß entweder zu denjenigen gehören, die aufgrund ihres besonderen Bekanntheitsgrades zahlreichen Anrufen fremder Personen ausgesetzt sind, oder er muß seinerseits begründen und beweisen, daß die Belästigungen ein solches Maß angenommen haben, daß das angebliche öffentliche Interesse an der Vollständigkeit des Fernsprechbuches zurücktreten muß.

Diese Rechtsauffassung vermag nicht zu überzeugen. Die große Mehrzahl der Haushalte in der Bundesrepublik Deutschland ist heute mit Fernsprechapparaten ausgestattet. Das Telefon ist ein Medium, mittels dessen jeder praktisch mit jedem Kontakt aufnehmen kann, mag der andere es wollen oder nicht. Nur mit Hilfe der Gerichte ist es gelungen, die Telefonwerbung in Grenzen zu halten. Daß sie ungeachtet dessen auch heute noch praktiziert wird, ist bekannt. Hinzu kommen Belästigungen anderer Art. Der betroffene Anschlußinhaber kann sich ihnen nicht entziehen; denn bei keinem Anruf ist erkennbar, ob er wichtig (z. B. nächtliche Unterrichtung über den Unfall eines Angehörigen) ist oder nicht. Der datenschutzbewußte Bürger ist nicht mehr ohne weiteres bereit, das öffentliche Interesse an der Vollständigkeit des Fernsprechbuches anzuerkennen und die damit verbundenen Belästigungen hinzunehmen.

Folgendes kommt hinzu: Die Wohnung steht unter dem besonderen Schutz des Grundgesetzes (Artikel 13 GG). Zwar schützt Artikel 13 die Wohnung gegen Eingriffe durch die staatliche Gewalt. Hier hingegen geht es um Informationseingriffe durch Personen oder andere private Stellen mittels des Telefons. Sie werden jedoch erst durch das in einer Rechtsverordnung des Bundespostministeriums (§ 39 Abs. 2 FO) festgelegte Prinzip der Vollständigkeit des Fernsprechbuches ermöglicht. Nach der

Rechtsprechung des Bundesverfassungsgerichts ist aber die Rechtsordnung so auszugestalten, daß sie einer Verletzung von Grundrechten nicht Vorschub leistet.

Eine datenschutzkonforme Lösung ließe sich im Rahmen des geltenden Rechts finden, wenn der Bundesminister für das Post- und Fernmeldewesen die zuständigen Stellen in seinem Geschäftsbereich anweisen würde, ihr Ermessen bei der Entscheidung über Anträge auf Nichteintrag in das Fernmeldebuch zugunsten der Antragsteller großzügiger zu handhaben. Dies habe ich als eine Sofortmaßnahme gefordert. Längerfristig ist daran zu denken, § 39 Abs. 2 FO zu ändern. Dabei ist auch zu erwägen, ob dem Betroffenen nicht nach dem Vorbild des englischen Telefonsystems die Wahl gelassen werden sollte, ob er eingetragen werden will oder nicht. Die nicht im Fernsprechbuch erscheinenden Namen und Anschlüsse müssen deswegen nicht unauffindbar bleiben.

Der Bundesminister für das Post- und Fernmeldewesen hat in einer Stellungnahme seine bisher vertretene Rechtsauffassung bestätigt. Die Diskussion ist damit aber noch nicht beendet.

3.7.3 Antrag auf Fernmeldehauptanschluß, Datenübermittlung an die Deutsche Postreklame

In meinem ersten Tätigkeitsbericht (1. TB S. 40) habe ich darauf hingewiesen, daß das Antragsformular für die Einrichtung eines Fernmeldeanschlusses den Erfordernissen des Bundesdatenschutzgesetzes nicht entspreche. Der Bundesminister für das Post- und Fernmeldewesen hat daraufhin veranlaßt, daß bis zur Entwicklung eines neuen Formulars dem alten Formblatt besondere Hinweise beigefügt wurden, in denen die von mir geforderte Aufklärung enthalten war. Seit Anfang 1980 liegt nunmehr das neue Antragsformular vor. Es benennt die Angaben, die zur Bearbeitung des Antrags erforderlich sind, und bezeichnet die dafür geltende Rechtsgrundlage. Die freiwilligen Angaben sind ebenfalls als solche gekennzeichnet. In dem Formular wird ferner darauf hingewiesen, daß der Name, die Anschrift und gegebenenfalls die Berufs-/Branchenangabe an die Deutsche Postreklame für Werbezwecke weitergegeben werden können. Dem Antragsteller wird Gelegenheit gegeben, sich damit einverstanden zu erklären oder durch Ankreuzen des entsprechenden Kästchens sein Einverständnis zu verweigern. Damit ist den Belangen des Datenschutzes hinlänglich Rechnung getragen. Erste Auswirkungen sind bereits erkennbar geworden. Während im vergangenen Jahr die Mehrzahl der Eingaben sich gegen das alte Formular selbst richtete, erreichten mich in diesem Jahr vornehmlich Beschwerden von Bürgern, die der Übermittlung ihrer Daten zwar widersprochen hatten, dennoch aber Werbesendungen erhielten. Nun ist es natürlich möglich, daß hier — wie überall, wo Menschen tätig sind — Fehler vorkommen und der Postreklame Namen und Anschriften entgegen dem Wunsch des Kunden übermittelt wurden. Die Post bemüht sich aber erkennbar, die Fehlerquoten möglichst gering zu halten. Hinzu kommt, daß die Deutsche Postreklame nur ein Unternehmen neben zahlreichen weiteren des Adreßhandels ist. Es ist also nicht mit letzter Sicherheit zu sagen, ob eine Anschrift von der Postreklame stammt oder nicht. Ich weise die Betroffenen stets darauf hin, daß sie sich gegen unerwünschte Direktwerbung weiter absichern können, indem sie sich in die sogenannte „Robinsonliste" eintragen lassen. Diese Liste wird vom Verband der Adressenverleger und Direktwerbeunternehmer (Postfach 1206, 6370 Oberursel) geführt. Die dem Verband angeschlossenen Unternehmen streichen dann den Namen aus ihren Anschriftenkollektionen.

3.7.4 Anschriftenprüfung

Einige Bürger fühlen sich in ihren schutzwürdigen Belangen beeinträchtigt, weil sie — z. B. nach einem Umzug — unerwünschte Postsendungen erhielten. Sie vermuteten, daß die Post den Absendern die neue Anschrift mitgeteilt haben könnte. Nach § 38 der Postordnung kann die Post in der Tat im Wege der Anschriftenprüfung die neue Anschrift mitteilen. Sie hat bisher im mutmaßlichen Interesse des Empfängers dessen Anschrift dann regelmäßig mitgeteilt, wenn der Absender dies durch den Aufdruck „Wenn Empfänger verzogen, mit neuer Anschrift zurück" verlangte.

Die in dieser Sache an mich gerichteten Eingaben zeigen, daß das Interesse des Empfängers an der Weitergabe seiner Anschrift keineswegs stets vermutet werden kann. Empfängerinteressen können einer Übermittlung der neuen Anschrift vielmehr entgegenstehen; so hat das Oberverwaltungsgericht Koblenz in einem kürzlich bekannt gewordenen Beschluß der Post verboten, die vorübergehende Anschrift eines Inhaftierten an Dritte weiterzugeben.

Ich habe gegenüber dem Bundesminister für das Post- und Fernmeldewesen angeregt, durch geeignete bereichsspezifische Regelungen sicherzustellen, daß eine Anschriftenprüfung unterbleibt, wenn der Betroffene es verlangt. Der Anregung wurde entsprochen und die Oberpostdirektionen wurden angewiesen, von der Übermittlung der neuen Anschrift abzusehen, wenn der Empfänger schriftlich widersprochen hat. Der Widerspruch kann jederzeit bei der Post eingelegt werden. Er ist auch im Rahmen der Anschriftenprüfung nach § 38 der Postordnung zu beachten.

3.7.5 Gehaltskontoverfahren

Die Deutsche Bundespost eröffnet ihren Bediensteten, die ihr Gehalt auf ein Postscheckkonto überweisen lassen, einige Vergünstigungen, die normale Postscheckkunden nicht genießen: So kann der Bedienstete auch bei anderen Postscheckämtern (z. B. bei Dienstreisen, Urlaub, Krankheit) seinen Zahlungsverkehr abwickeln. Das Verfahren im einzelnen regelt sich nach einer Dienstanweisung, die im Amtsblatt des Bundesministers für das Post- und Fernmeldewesen veröffentlicht ist (Amtsbl. 1974 Nr. 151 S. 2009). Überzieht der Bedienstete sein Konto über ein bestimmtes Limit hinaus, wird eine Sperre veranlaßt, durch die sichergestellt werden

soll, daß künftig Zahlungen nur bei Deckung geleistet werden. Darüber hinaus wird die für den Bediensteten zuständige Personalstelle unterrichtet. Diese vermerkt den Grund und die Dauer der Sperre in einer Kartei und wirkt auf den Bediensteten ein, daß er künftig sein Konto nicht mehr überzieht. Ich sehe darin eine deutliche Schlechterstellung der sich an diesem Verfahren beteiligenden Postbediensteten gegenüber denjenigen, die ihr Gehalt auf ein Gehaltskonto bei einem anderen Kreditinstitut überweisen lassen. Im geltenden öffentlichen Dienstrecht gibt es für eine Maßnahme dieser Art keine Rechtsgrundlage. Die Mitteilung an die Personalstelle ist ein Mittel der Disziplinierung des Bediensteten, das weder dienstrechtlich zu rechtfertigen ist noch im Rahmen dieses Gehaltskontoverfahrens angemessen erscheint. Die Benachteiligung liegt einmal darin, daß eine Sperre und Mitteilung bereits bei einer Überziehung ab 500 DM erfolgt. Andere Kreditinstitute gewähren in der Regel einen Überziehungskredit in Höhe eines Monatsgehalts. Die Mitteilung an die Personalstelle des Bediensteten ist auch sachlich nicht geboten. Das Postscheckamt kann seine Interessen dadurch wahren, daß es den Betroffenen selbst über die Überziehung unterrichtet und gegebenenfalls eine Sperre verfügt. Der damit verbundene Mehraufwand ist möglicherweise höher, er trifft das Postscheckamt aber nicht härter als andere gehaltskontoführende Stellen auch. Datenschutzrechtlich handelt es sich hier um eine nicht zu rechtfertigende Übermittlung personenbezogener Daten vom Kreditinstitut (Postscheckamt) an die Beschäftigungsbehörde. Auf die Beschwerde eines Postbediensteten habe ich dieses Verfahren daher beanstandet. Eine endgültige Stellungnahme des Bundesministers für das Post- und Fernmeldewesen steht noch aus.

3.8 Medien

3.8.1 Deutsche Welle

Im November 1980 habe ich die Datenverarbeitung bei der Deutschen Welle überprüfen lassen. Die Deutsche Welle ist eine bundesunmittelbare Anstalt des öffentlichen Rechts mit der Aufgabe, den Hörern im Ausland ein Bild des Lebens in Deutschland zu vermitteln sowie die vielfältigen internationalen Beziehungen der Bundesrepublik darzustellen.

Für den 24stündigen Sendebetrieb werden in großem Umfang Informationen gesammelt, archiviert und für redaktionelle Zwecke aufbereitet.

Der weitaus größte Teil der bei dieser Rundfunkanstalt verarbeiteten Daten wird ausschließlich zu eigenen publizistischen Zwecken genutzt. Für diese Daten gelten die Regelungen des BDSG nach § 1 Abs. 3 BDSG nur insoweit, als durch geeignete technische und organisatorische Maßnahmen diese Verwendungsbeschränkung durch die Erfüllung der Sicherungsanforderungen (§ 6 und Anlage) zu gewährleisten ist.

Meine Mitarbeiter haben bei verschiedenen Organisationseinheiten des Hauses die Einhaltung der Zweckbestimmung und die dort bestehenden Sicherungsvorkehrungen überprüft. Dabei haben sich keine Anhaltspunkte für eine zweckfremde Nutzung ergeben.

Auf die Verarbeitung personenbezogener Daten außerhalb des Programmbetriebes sind die Regelungen des BDSG voll anzuwenden. Dies gilt z. B. für die Personal-, Lieferanten-, Hörerdateien, EDV-mäßig erstellte Leistungsnachweise und automatisch geführte Telefonaufzeichnungen (s. o. 3.5.5.3). Im Verwaltungsbereich traten einige Mängel beim Vollzug der datenschutzrechtlichen Vorschriften auf: die Übersicht über die Art der gespeicherten personenbezogenen Daten nach § 15 war nicht vollständig; einige der darin erfaßten Dateien waren unzureichend beschrieben; die Meldungen zum Dateienregister nach § 19 waren unvollständig; Veröffentlichungen nach § 12 waren nicht erfolgt. Darüber hinaus habe ich die Deutsche Welle auf weitere nicht schwerwiegende Unzulänglichkeiten und Schwachstellen hingewiesen.

3.8.2 Datenschutzprobleme bei Neuen Medien

Nach Verabschiedung entsprechender Landesgesetze wurden im Juni 1980 in Berlin und Düsseldorf Pilotprojekte des *Bildschirmtext-Dienstes* gestartet. Ein speziell ausgerüstetes Fernsehgerät ermöglicht dem Teilnehmer in Verbindung mit dem Telefon auf einfache Weise den Zugang zu einem zentralen Rechner (Bildschirm-Zentrale), auf dessen Dateien der Teilnehmer entweder direkt zugreifen kann oder mit dessen Hilfe er sich mit einem externen Rechner, z. B. dem eines Versandhauses verbinden lassen kann. Die z. Z. etwa 2 500 Teilnehmer können auf Dienste verschiedenster Art von etwa 900 Anbietern zurückgreifen. Schwerpunktmäßig werden Informationsseiten (z. B. Werbetexte, aktuelle Nachrichten, Fahrpläne) angeboten, in beschränktem Umfang ist jedoch auch schon die Kommunikation mit dem externen Rechner möglich. So kann sich der Teilnehmer z. B. einen individuellen Kreditplan errechnen lassen oder Versandhausbestellungen aufgeben.

Eine besondere Problematik ergibt sich daraus, daß die Deutsche Bundespost als Betreiber des Systems das Inkasso für die kostenpflichtig angebotenen Dienste übernimmt. In den Bildschirmtext-Zentralen fallen dadurch zwangsläufig solche Betriebsdaten an, die es ermöglichen würden, mit geringstem Aufwand sehr genaue Benutzerprofile zu erstellen: Es wäre lückenlos nachweisbar, welcher Benutzer zu welcher Zeit welchen Dienst in Anspruch genommen und in welcher Weise er das getan hat. Die Erstellung von Benutzerprofilen aus diesen Daten würde Grundsätzen des Datenschutzes zuwiderlaufen. Schon der Sammlung solcher Daten muß entgegengetreten werden.

Erheblich entschärft werden könnte dieses Problem dadurch, daß die anfallenden persönlichen Benutzungsdaten nicht zentral, sondern dezentral, nämlich beim Teilnehmer gespeichert würden. Analog zum Vorbild des Gas- und Stromzählers hätte der Teilnehmer dadurch einen aktuellen und detaillier-

ten Überblick über Art und Kosten der Nutzung seines Gerätes z. B. in den vergangenen vier Wochen. Darüber hinaus hätte er hiermit auch ein Kontrollinstrument gegen unbefugte Benutzung seines Gerätes in der Hand. Die Deutsche Bundespost würde bei dieser Verfahrensweise — je nach technischer Realisierung — nur noch die Summe der aufgelaufenen Gebühren zentral speichern bzw. aus den dezentralen Registriergeräten abrufen. Die Kosten, die bei einer solchen dezentralen Gebührenerfassung zusätzlich für die Teilnehmergeräte entstehen, könnten sich bei großen Produktionszahlen auf eine tragbare Höhe reduzieren. Hier ist die einschlägige Industrie aufgerufen, durch entsprechende Neuentwicklungen einen aktiven Beitrag zur datenschutzgerechten Gestaltung der Neuen Medien zu leisten.

Wegen der Öffentlichkeit des Dienstes kommt — mehr noch als in privaten Datennetzen — der Datensicherung besondere Bedeutung zu. Der Schwerpunkt muß bei Maßnahmen liegen, die Schutz vor fehlerhaft oder mißbräuchlich geschalteten Verbindungen sowie vor unbefugter Benutzung des Teilnehmergerätes bieten.

Ein Informationsbesuch meiner Mitarbeiter bei der von der Deutschen Bundespost betriebenen Bildschirmtext-Zentrale Düsseldorf sollte einen ersten Überblick über die Art der eingesetzten Programme sowie die organisatorischen und technischen Maßnahmen zur Datensicherheit bringen. Unter Verweis auf das Fernmeldegeheimnis wurde mir allerdings kein Einblick in die personenbezogenen Datensätze gewährt (dazu s. o. 3.7). Die Datenschutzkontrolle weist hier eine Lücke auf, die im Hinblick auf die wissenschaftlichen Begleituntersuchungen während der Testphase besonders bedenklich erscheint. Um die wissenschaftliche Auswertung zu unterstützen, wird nämlich jede 100. Anschaltung in ihrem Gesamtverlauf protokolliert. Festgehalten werden insbesondere die Nummer des Teilnehmers, Zeit und Dauer der Verbindung sowie jeder Aufruf einer Bildschirmtextseite mit Nummer der Seite und der Art des Aufrufs, also z. B. als Folgeseite, als Auswahlschritt in einem Suchbaum oder als Direktaufruf durch Eingabe der Seitennummer. Diese Daten sind nicht anonymisiert. Es ist noch nicht detailliert festgelegt, in welcher Form (anonymisiert, aggregiert) diese Daten den wissenschaftlichen Begleitern zur Verfügung gestellt werden sollen.

Über Ordnungsmäßigkeit und Sicherheit der Datenverarbeitung bei der Bildschirmtext-Zentrale werde ich nach weiteren Kontrollen im Zusammenhang berichten.

Bereits 1978 haben sich die Ministerpräsidenten der Länder auf vier durchzuführende Pilotprojekte *Kabelfernsehen* geeinigt, deren erstes frühestens 1981 in Betrieb genommen wird. Die datenschutzrechtliche Relevanz ergibt sich hier besonders durch den Rückkanal. Er ermöglicht — wie beim Bildschirmtext — dem Teilnehmer eine direkte Kommunikation mit der Netzzentrale bzw. dem Informationsanbieter. Besonders für dieses neue Medium stehen noch zahlreiche datenschutzrechtliche Aspekte offen. Dies gilt z. B. für die Anwendung des Fernmeldegeheimnisses und die Bedeutung der Einwilligung bei Verwendung des Rückkanals.

Die Landesbeauftragten und der Bundesbeauftragte für den Datenschutz haben sich in einer Arbeitsgruppe mit der besonderen Datenschutzproblematik der Neuen Medien befaßt und ein gemeinsames Thesenpapier erarbeitet (vgl. Anhang 2 zu diesem Bericht). Meine Vorstellungen wurden dabei weitgehend berücksichtigt.

Die Deutsche Bundespost geht davon aus, daß voraussichtlich 1983 Bildschirmtext als ständiger Dienst angeboten werden wird. Zu diesem Zeitpunkt werden auch schon Versuchsergebnisse von Kabelfernseh-Pilotprojekten zur Verfügung stehen und andere Verfahren der Neuen Medien im Laborzustand erprobt sein. Es ist zu erwarten, daß bereits mittelfristig die neuen Telekommunikationsdienste — nicht nur im Medienbereich — eine große Rolle spielen werden. Die angedeuteten Gefahrenpotentiale haben mich zu zahlreichen Kontakten zu solchen Institutionen veranlaßt, die im Bereich der technisch-organisatorischen Planung und soziologischen Forschung zur Vorbereitung und Realisierung entsprechender Projekte tätig sind. Insbesondere ist hier meine Mitarbeit im Beirat des Forschungsprojekts „Datenschutz bei rechnerunterstützten Telekommunikationssystemen" (DARUTS) des Instituts für Zukunftsforschung, Berlin, zu nennen. Das Projekt ist in seiner Voruntersuchungsphase vom Bundesminister für Forschung und Technologie gefördert worden. Da ich mir davon wichtige Erkenntnisse für die Lösung datenschutzrechtlicher Probleme bei den Neuen Medien verspreche, sehe ich eine weitere Förderung mit Bundesmitteln als unerläßlich an. Der Bundesminister für Forschung und Technologie hat mir jedoch mitgeteilt, daß dies frühestens im Jahre 1982 möglich sein werde. Unter diesen Bedingungen könnte das Projekt wahrscheinlich nicht fortgesetzt werden, und der Anschluß an die technische Entwicklung ginge verloren. Ich meine, eine unmittelbare Anschlußfinanzierung aus Mitteln des „Förderungsprogramms Informationstechnik" müßte möglich sein.

Dieses Programm, an dessen Formulierung ich mitwirke, will erstmals Forschungen über technische Entwicklungen und ihre sozialen Konsequenzen fördern. Gerade der zweite Aspekt darf nicht zu kurz kommen. Bei der Entscheidung über die Förderungswürdigkeit von Projekten im Bereich Datenschutz und Datensicherungstechniken wirken meine Mitarbeiter beratend mit.

3.9 Verkehrswesen

3.9.1 Kraftfahrt-Bundesamt (KBA)

Im Frühjahr 1980 fand eine Anschlußprüfung beim KBA statt, um den Fortgang der technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes zu ermitteln. Ich habe mich davon überzeugen können, daß seit der ersten Überprüfung im August 1979 eine Anzahl der damals erkannten Probleme gelöst oder zumindest in Angriff

genommen wurde. Der Datenschutz wurde insbesondere verbessert durch den Umbau im Rechenzentrum, die Entwicklung einer prüffähigen Verfahrensdokumentation für automatisierte Anwendungen sowie durch die Arbeiten an der Zusammenstellung und detaillierten Aufbereitung der Dateibeschreibungen zur internen Übersicht.

Das KBA hatte in der Zwischenzeit besondere Anstrengungen unternommen, um Schwachstellen und mögliche Risiken bei der Verarbeitung personenbezogener Daten in den Griff zu bekommen. Ein Schutz- und Sicherheitskonzept befindet sich in Vorbereitung. Das bedeutet, daß auch weiterhin ausreichende Kapazitäten zur Verfügung gestellt werden müssen, um bei einer Behörde mit derart umfangreichen Datensammlungen und Datenübermittlungen die erforderlichen Schutzmaßnahmen in die Wege leiten und überwachen zu können. Eine besondere Rolle spielen dabei der Ausbau automatisierter Datenverarbeitung bis hin zur Einrichtung von Direktabfragemöglichkeiten durch dritte Stellen sowie die im eigenen Hause vorzunehmende Koordinierung und Abstimmung zwischen DV- und Fachbereichen.

Trotz dieser im ganzen positiven Entwicklung gibt es eine Reihe datenschutzrechtlicher Probleme, die sich vornehmlich auf den Umfang der Speicherung in einzelnen Dateien und das Bereithalten dieser Daten für Auskunftszwecke beziehen.

3.9.1.1 Kfz-Halter-Datei

Bei der Zulassung von Fahrzeugen wird im Anmeldeantrag u. a. nach dem Beruf bzw. nach der Art einer gewerblichen Tätigkeit des Halters gefragt. Die Zulassungsstellen melden diese Daten zur zentralen Speicherung an das KBA. Die Erhebung von Beruf und Gewerbe ist zwar nach § 23 Abs. 1 Nr. 1 Straßenverkehrszulassungsordnung (StVZO) vorgeschrieben; ich habe aber gegenüber dem Bundesminister für Verkehr (BMV) als dem Verordnungsgeber Bedenken angemeldet, ob diese Bestimmung insoweit durch die Verordnungsermächtigung nach § 6 Straßenverkehrsgesetz (StVG) gedeckt ist. Danach ist der BMV ermächtigt, für die Kraftfahrzeugzulassung Rechtsverordnungen und allgemeine Verwaltungsvorschriften zu erlassen. Ich kann jedoch nicht erkennen, inwiefern die Angaben zum Beruf oder zum Gewerbe für die Kfz-Zulassung erforderlich sind. Zweifel an der Notwendigkeit dieser Daten für die Verwaltungstätigkeit der Zulassungsstellen wurden auch von mehreren Landesbeauftragten für den Datenschutz erhoben.

Sofern die Daten der statistischen Auswertung durch das KBA dienen und damit über das für den Verwaltungsvollzug Erforderliche hinausgehen, ist für die Begründung einer Auskunftspflicht des Halters eine spezielle gesetzliche Grundlage bzw. eine weitergehende Verordnungsermächtigung erforderlich. Solange eine solche Rechtsgrundlage fehlt, dürfen die Angaben nur auf freiwilliger Basis mit entsprechendem Hinweis nach § 9 Abs. 2 BDSG erhoben werden.

Außerdem habe ich festgestellt, daß für die Berufestatistik der Kfz-Halter keine konkreten Berufsbezeichnungen benötigt werden, da die Auswertung nur nach vier Kategorien (Beamte, Angestellte, Arbeiter, Nichterwerbspersonen) erfolgt. Der BMV begründet die Erhebung dieser Daten u. a. damit, daß die Angaben zur Auskunftserteilung an die Polizei- und Bußgeldbehörden für Zwecke der Ahndung von Ordnungswidrigkeiten benötigt würden. Diese ebenso wie andere angeführte Verwendungen gehören jedoch nicht zur Ausführung der §§ 1—5 StVG. Sie entsprechen auch nicht den tatsächlichen Erfordernissen der Verwaltung, wie der Niedersächsische Datenschutzbeauftragte nach Ermittlungen bei verschiedenen Zulassungsstellen festgestellt hat.

Auch die Begründung, daß konkrete Berufs- bzw. Gewerbeangaben zur Ausführung des Bundesleistungsgesetzes (BLG) erforderlich seien, vermag nicht zu überzeugen. Nach § 4 BLG können alle natürlichen und juristischen Personen sowie Personenvereinigungen herangezogen werden, um im Verteidigungsfall oder zur beschleunigten Herstellung der Verteidigungsbereitschaft (§ 1 Abs. 2) Vermögensgegenstände zu überlassen (§ 2 BLG). Von dieser Leistungspflicht sind nach § 4 Abs. 2 und 3 BLG bestimmte Berufe, Gewerbe und Einrichtungen (z. B. Parteien, Gewerkschaften, Kirchen, Betriebe der öffentlichen Versorgung) ausgenommen. Wenn aber die Kenntnis lediglich einzelner Berufe und Einrichtungen erforderlich ist, so hat sich die Erhebung an diesen speziellen Erfordernissen auszurichten. Eine Aufzeichnung der Berufs-/Gewerbeangaben aller Fahrzeughalter läßt sich damit nicht rechtfertigen.

Ich habe den Bundesminister für Verkehr um eine ergänzende Stellungnahme gebeten. Kann die Rechtmäßigkeit der Erhebung nicht nachgewiesen werden, so sind die Vordrucke zu ändern und die bereits erhobenen und gespeicherten Angaben zu löschen.

3.9.1.2 Verkehrszentralregister (VZR)

Bei Entziehung oder Versagung einer Fahrerlaubnis werden zum Verkehrszentralregister aufgrund § 13 Abs. 1 Nr. 1 und 2 StVZO in Verbindung mit § 28 StVG die Entscheidung von Gerichten und Verwaltungsbehörden gemeldet. Für die Datenübermittlung an das KBA dient ein vom Bundesminister für Verkehr entwickelter bundeseinheitlicher Vordruck („Vordruck A Nr. 5701"). In diesem Vordruck sind die Entscheidungsgründe anhand eines Kennziffernkatalogs verschlüsselt einzutragen. Danach bedeutet z. B. 11: Mangelndes Sehvermögen; 13: Körperbehinderung; 20: Mangelnde geistige Fähigkeiten; 31: Neigung zur Trunk- und Rauschgiftsucht; 32: Sonstige charakterliche Mängel; 41: Verkehrsunfallflucht; 50: Sonstige Vorstrafen; 71/72: Theoretische/praktische Prüfung nicht bestanden; 80: Sonstige Entscheidungsgründe (stichwortartig erläutern).

Gegen die Übermittlung dieser Entscheidungsgründe bestehen datenschutzrechtliche Bedenken. Weder im Straßenverkehrsgesetz noch in der Straßenverkehrszulassungsordnung ist die Übermitt-

lung von Begründungen vorgesehen. § 13 Abs. 1 StVZO bestimmt lediglich, daß die Tatsache der Entziehung oder Versagung einer Fahrerlaubnis im VZR eingetragen wird. Die Mitteilungsvorschrift des § 13b StVZO sieht ebenfalls nur die Meldung von Entscheidungen vor. Erst der nach § 13d StVZO vorgeschriebene Vordruck A Nr. 5701 geht darüber hinaus und sieht Angaben über die Entscheidungsgründe vor.

Der Bundesminister für Verkehr (als vorgesetzte Behörde) hat die Überprüfung meiner Bedenken noch nicht abgeschlossen. Er hat mich aber vorab über die grundsätzlichen Überlegungen informiert, die zu einer Pflicht zur Mitteilung der Entscheidungsgründe auch im Entwurf des VZR-Gesetzes geführt haben. Danach benötigt das KBA Hinweise auf die Entziehungs- bzw. Versagungsgründe für die Tilgung von VZR-Eintragungen. Der Ablauf der Tilgungsfristen wird solange gehemmt, wie eine Fahrerlaubnis z. B. wegen wiederholter Verkehrsverstöße (= sog. charakterlicher Eignungsmangel) entzogen ist (§ 29 Abs. 2 StVG i. V. m. § 13a Nr. 5 StVZO; § 18 VZRG-E). Diese Regelung beruht auf dem Gedanken der Bewährung, der allen Tilgungsvorschriften zugrunde liegt; solange eine zulässige Teilnahme am Straßenverkehr nicht möglich ist, kann auch keine Bewährung, die zur Tilgung vorhandener Eintragungen führt, stattfinden. Erst nach Wiedererteilung der Fahrerlaubnis läuft der Bewährungs-(Tilgungs-)Zeitraum weiter. Eine Ausnahme soll nach dem Entwurf eines VZR-Gesetzes lediglich gelten, wenn die Entziehung ausschließlich auf körperlichen oder geistigen Gebrechen des Fahrerlaubnisinhabers beruht: Hier spielt nicht die Bewährung, sondern der Sicherungszweck der Eintragung eine Rolle, so daß Tilgungsfristen eventuell vorhandener weiterer Eintragungen auch während der Dauer der Entziehung weiterlaufen. Im Falle der Wiedererteilung — wenn also die oben genannten Gebrechen nicht mehr vorliegen — wird die Eintragung über die vorherige Entziehung der Fahrerlaubnis sofort gelöscht. Für die Aufgaben des KBA würde es genügen, diese Fälle entsprechend zu kennzeichnen.

Der Bundesminister für Verkehr hat die Meldung der Entscheidungsgründe darüber hinaus mit der Notwendigkeit von Geschäftsstatistiken für das KBA begründet. Die Aufstellung von Geschäftsstatistiken bei den jeweiligen Ressorts ist jedoch nach § 9 Abs. 1 Bundesstatistik-Gesetz (BStatG) an die Voraussetzung geknüpft, daß die dafür benötigten „Unterlagen ausschließlich im Geschäftsgang der Bundesbehörden anfallen ...". Gerade dies ist bei der Meldung der Entscheidungsgründe nicht der Fall. Die Daten kommen weder aus dem Geschäftsbereich von Bundesbehörden noch fallen sie im Geschäftsgang an. Als Rechtsgrundlage für die Übermittlung und Speicherung weitergehender Daten kann daher diese Begründung nicht herangezogen werden.

Die bisher angeführten Argumente haben meine datenschutzrechtlichen Bedenken bezüglich der Übermittlung und Speicherung der Entscheidungsgründe nicht beseitigt. Sowohl nach der geltenden Rechtslage als auch nach dem in Vorbereitung befindlichen VZR-Gesetz ist die Übermittlung der Entscheidungsgründe in der bisher praktizierten Form nicht erforderlich. Aus gegenwärtiger Sicht fehlt es daher an der notwendigen Rechtsgrundlage für die Speicherung dieser Daten beim KBA sowie für ihre Übermittlung durch das KBA. Bevor ich eine Beanstandung ausspreche, habe ich dem Bundesminister für Verkehr jedoch Gelegenheit zu einer ergänzenden Stellungnahme gegeben.

3.9.1.3 Übermittlungen aus dem VZR

Bereits in meinem Zweiten Tätigkeitsbericht (z. TB S. 40) hatte ich die Praxis der Auskunftserteilung aus dem Verkehrszentralregister bemängelt.

Das KBA und mit ihm der Bundesminister für Verkehr beharren weiterhin auf ihrem Standpunkt, daß es die Regelung in § 30 Straßenverkehrsgesetz (StVG) rechtfertige, bei jeder Anfrage durch Gerichte und Behörden Ablichtungen *aller* Eintragungen zu übersenden, ohne den jeweiligen Anlaß und das konkrete Informationsbedürfnis zu berücksichtigen. Das KBA vertritt die Auffassung, daß für die Anwendung des BDSG auf das VZR kein Raum sei, da § 30 Abs. 2 StVG als bereichsspezifische Regelung dem BDSG vorgehe.

Ich bestreite das nicht; gleichwohl bleibt die Praxis der Auskunftserteilung aus dem VZR bedenklich. § 30 Abs. 2 Satz 1 StVG legt abschließend fest, welche Stellen auskunftsberechtigt sind. Satz 2 regelt darüber hinaus, wie die Auskunft zu erteilen ist, und zwar so, „daß die anfragende Stelle die Akten über die den Eintragungen zugrundeliegenden Entscheidungen beiziehen kann". Die Auffassung, daß der Gesetzgeber damit im Sinne der unterschiedslosen Erteilung von Vollauskünften entschieden habe, läßt sich auf diese Regelung nicht stützen. Der Wortlaut des Satzes 2 spricht — im Gegenteil — für eine Beschränkung auf die zur Aktenbeiziehung *erforderlichen* Angaben. Das Erforderlichkeitsprinzip des § 10 BDSG ist nur eine Ausprägung des allgemeinen, im Verfassungsrecht wurzelnden Verhältnismäßigkeitsgrundsatzes, den die Verwaltung auch im bereichsspezifischen Datenschutzrecht zu beachten hat. Er verlangt, bei Eingriffen in die Rechte des Bürgers jeweils das mildeste Mittel zu wählen; dazu gehört auch, belastende Informationen nicht weiterzuleiten, wenn die Empfängerbehörde sie nicht konkret benötigt.

Ich habe dem Bundesminister für Verkehr mitgeteilt, daß die bisherige Verfahrensweise vom KBA nicht beibehalten werden kann, weil es dafür keine sachliche Rechtfertigung und keine gesetzliche Ermächtigung gibt.

Das neuerdings vorgetragene Argument, bei dem Verkehrszentralregister handele es sich nicht um eine Datei, sondern um eine Aktensammlung, auf die das BDSG nicht anwendbar sei, ist schon deshalb wenig überzeugend, weil das KBA selbst dieses Register als Datei nach § 12 BDSG im Bundesanzeiger veröffentlicht hat (Bekanntmachung Nr. 1 über gespeicherte personenbezogene Daten nach § 12 Abs. 1 BDSG, Bundesanzeiger vom 21. Dezember 1978 Nr. 34/78). Die von mir erbetene Begründung für die

in Nr. 7 der Veröffentlichungen erfolgte ersatzlose Streichung (Bundesanzeiger vom 27. Mai 1980 Nr. 19/80) steht noch aus.

Zur Sache ist festzustellen: Das KBA erhält zwei Arten von Meldungen von Gerichten und Behörden, die — jeweils für sich gesehen — einen weitgehend gleichartig aufgebauten Formularkopf mit Angaben zur Person enthalten und lediglich bei den Mitteilungen Unterschiede aufweisen. Die Auswertung nach diesen beiden Arten (Bußgeldbescheide bzw. andere Eintragungen) ist ohne weiteres möglich.

Darüber hinaus gilt für alle Vordrucke, daß sie selbst unter Berücksichtigung ihrer gegenwärtigen Aufbewahrungsform auch „nach anderen bestimmten Merkmalen umgeordnet und ausgewertet werden können" (§ 2 Abs. 3 Nr. 3 BDSG). Denn die Angaben zur Person befinden sich aufgrund der Formulargestaltung jeweils an der gleichen Stelle und sind deutlich von den übrigen Angaben getrennt.

Daß die Datensammlung in Lose-Blatt-Form geführt und die einzelnen Vordrucke in Gruppen zu je 10 in einem numerierten Aktendeckel zusammengefaßt werden, kann an der rechtlichen Beurteilung nichts ändern. Der Aktendeckel ist kein geeignetes Mittel zur Umgehung des BDSG, da die Möglichkeit des Umsortierens und gezielten Auswertens nicht beeinträchtigt wird.

Ich habe den Bundesminister für Verkehr um eine erneute Stellungnahme gebeten.

3.9.1.4 Datei der versicherungspflichtigen Fahrzeuge

Zur Überwachung des Versicherungsschutzes bei Kleinkrafträdern, Fahrrädern mit Hilfsmotor und maschinell angetriebenen Krankenfahrstühlen wird eine zentrale Datei geführt. Die Versicherer haben dem Amt dazu nach § 29 f StVZO bestimmte Daten zu melden.

Bei der Überprüfung habe ich festgestellt, daß die Meldungen einiger Versicherer mehr personenbezogene Angaben enthalten, als vorgesehen und für den Versicherungsnachweis erforderlich sind, so z. B. Geburtsdatum, Geburtsort und Beruf des Halters, Höhe des Versicherungsbeitrags.

Das KBA erhält die Versicherungsmeldungen auf vorgedruckten Postkarten bzw. auf Magnetbändern. Während der Inhalt der Magnetbänder in den Datenbestand des Amtes übertragen wird, werden die Postkartenrückseiten unmittelbar als Karteikarten benutzt. Bei der bisherigen Verarbeitungspraxis führt jede Meldung von Versicherern beim KBA zu einer Datenspeicherung gleichen Inhalts wie die Meldung. Das bedeutet, daß die Meldung weitergehender Angaben zwangsläufig zu einer unzulässigen Speicherung führt. Dies war zu beanstanden.

Für die über die Erfordernisse der Rechtsvorschrift hinausgehende und damit ebenfalls unzulässige Datenübermittlung durch die Versicherer tragen diese die Verantwortung. Ich habe deshalb die für den Datenschutz im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörden informiert.

Die Versicherer dürfen bei der Meldung nur Karteikarten verwenden, „deren Muster vom Kraftfahrt-Bundesamt genehmigt ist" (§ 29 f. Abs. 1 Satz 1 StVZO). Erfolgt die Meldung auf Magnetbändern, so gilt für deren Inhalt — dem Sinn der Vorschrift entsprechend — gleiches. Ich habe deshalb das KBA aufgefordert, auf eine Korrektur der Praxis seitens der Versicherer hinzuwirken. Das KBA hat die Änderung des Verfahrens in Angriff genommen und die zuviel gemeldeten Daten gesperrt, so daß sie bei der Aufgabenerfüllung des Amtes nicht mehr genutzt werden; insbesondere wurde sichergestellt, daß diese Daten bei Auskünften an Dritte nicht mitgeteilt werden.

3.9.1.5 ZEVIS

In meinem vorigen Tätigkeitsbericht (2. TB S. 41 f.) hatte ich über das geplante und im Aufbau befindliche Zentrale Verkehrsinformationssystem ZEVIS berichtet. Anläßlich meines Kontrollbesuchs im Frühjahr 1980 ließ ich mich über den neuesten Stand und die weiteren Entwicklungsschritte unterrichten. Nach der laufenden Planung war noch für 1980 vorgesehen, den bereits automatisierten Teildatenbestand des VZR — erweitert um die Anschriften der Betroffenen — mehreren Polizeidienststellen im Direktzugriff zur Verfügung zu stellen. Ferner sollte ein Teil des Halterdatenbestandes in den Direktzugriff übernommen und in einer Pilotanwendung die integrierte Verarbeitung beider Datenbestände erprobt werden. Durch diese Integration kann z. B. die gleichzeitig direkte Anfrage an beide Datenbestände ermöglicht und innerhalb von Sekunden die Antwort gegeben werden, welche Angaben insgesamt zu einem bestimmten Namen oder zu einem bestimmten Kfz-Kennzeichen und dem Fahrzeughalter vorliegen.

Wegen der weitreichenden Bedeutung dieser Planung für den Datenschutz der davon betroffenen Bürger bat ich den Bundesminister für Verkehr um Zwischenberichte, um schon vor der Einrichtung des Direktabfragebetriebes die datenschutzrechtliche Zulässigkeit sowie die Wirksamkeit der Schutzvorkehrungen beurteilen zu können. Die verlangten Informationen habe ich jedoch bis heute trotz Anmahnung nicht erhalten, obwohl die Realisierung — wie ich von anderer Seite erfahren habe — weit fortgeschritten ist. Die Erfüllung meiner gesetzlichen Aufgabe, die Einhaltung des Datenschutzes zu überwachen, wird mir dadurch auf einem wichtigen Gebiet erschwert.

Darüber hinaus habe ich förmlich nach § 20 BDSG beanstandet, daß die Einrichtung der Direktabfrage für bestimmte Polizeidienststellen nicht rechtzeitig und (nach Anmahnung) nicht ordnungsgemäß zum Dateienregister gemeldet worden ist. So halte ich beispielsweise die bloße Angabe „Polizeidienststellen" als Empfänger regelmäßiger Übermittlungen für unzureichend, wenn feststeht, daß es sich um ganz bestimmte Dienststellen in einem ganz bestimmten geographischen Bereich handelt. Auch sollte im eigenen Interesse der verarbeitenden Stelle zum Ausdruck kommen, daß es sich um eine begrenzte Pilotanwendung handelt. Sonst könnte in

der Öffentlichkeit, deren Information das Register auch dient, das Mißverständnis entstehen, daß bereits zum jetzigen Zeitpunkt alle Polizeidienststellen der Bundesrepublik auf die beim KBA gespeicherten Daten direkt zugreifen können.

3.9.2 Auto-Notfunk

Im Rahmen meiner Beratungsfunktion nach § 19 Abs. 1 BDSG unterstütze ich die Bundesanstalt für Straßenwesen in Fragen des Datenschutzes bei dem Projekt ‚Auto-Notfunk'.

Es handelt sich dabei um ein mobiles Nótrufsystem, dessen Entwicklung vom Bundesminister für Forschung und Technologie sowie vom Hessischen Minister des Innern gefördert wird. Die Bundesanstalt für Straßenwesen koordiniert die nicht-technische Begleitforschung und läßt durch eine Projektgruppe, die aus mehreren Wissenschaftlern besteht, derzeit eine Probeanalyse vornehmen, um darauf aufbauend notwendige Untersuchungen vorzunehmen.

Neben Fragen der Zulässigkeit der Datenspeicherung und der Datenübermittlung an eine Pannenhilfszentrale wurde das Problem der Kennung der einzelnen mobilen Sende- und Empfangsgeräte beraten. Diese Kennung sollte so gewählt werden, daß die Verwendung einer fremden Kennung und unbefugtes Mithören möglichst reduziert werden.

Das technische System soll bis 1983 in einem Modellversuch im Raum Darmstadt getestet werden. Auch der Hessische Datenschutzbeauftragte ist an den Beratungen beteiligt.

3.9.3 Schwarzfahrer bei der Deutschen Bundesbahn (DB)

Sogenannte Schwarzfahrerdateien werden bei den Generalvertretungen und Direktionen der DB geführt. Sie bestehen aus den Durchschriften der Nachlösezettel, die vom Zugbegleitpersonal ausgefüllt werden, wenn jemand ohne gültigen Fahrausweis angetroffen wird und den vollen Fahrpreis nicht an Ort und Stelle bezahlt.

Die Schwarzfahrerdatei dient der Überwachung des Zahlungseingangs, der Geltendmachung zivilrechtlicher Ansprüche, wenn der Schuldner nicht innerhalb der eingeräumten Frist zahlt, sowie der Überprüfung im Einzelfall, ob es sich um einen „Wiederholungstäter" handelt. Sofern ein Strafverfahren eingeleitet werden soll, wird der Vorgang an den Fahndungsdienst der DB bei der Zentralen Transportleitung in Mainz abgegeben.

Ich habe erreicht, daß die Erhebung der Berufsangabe unterbleibt, da kein Zusammenhang mit der Fahrpreisnachforderung erkennbar ist. Ebenso soll künftig auf die Angabe der Personalausweisnummer verzichtet werden. Art und Nummer des Personalausweises werden zwar vom Fahndungsdienst bei Verdacht einer strafbaren Handlung erhoben, bei dem Ausfüllen des Nachlösezettels handelt es sich jedoch nicht um polizeiliche Ermittlungstätigkeit, so daß es auf die dort verwendeten Formulare nicht ankommt. Als Nachweis, daß die Personenangaben vom Zugpersonal anhand des Personalausweises überprüft wurden, reicht es aus, ein entsprechendes Feld im Vordruck anzukreuzen.

Die DB hat zugesagt, den Vordruck zu ändern. Die Mitarbeiter sind angewiesen, in der Zwischenzeit bereits entsprechend zu verfahren.

Bezüglich der Angaben über den Arbeitgeber habe ich verlangt sicherzustellen, daß diese Daten nur bei Lohn- und Gehaltspfändungen benutzt werden. Eine vorherige Kontaktaufnahme mit dem Arbeitgeber, etwa um Druck auf den Fahrpreisschuldner auszuüben, ist unzulässig. Eine Datenspeicherung zu diesem Zweck wäre unverhältnismäßig und von § 23 BDSG nicht gedeckt.

Die Nachlösezettel werden zur Ermittlung von Wiederholungstätern im Hinblick auf eine eventuelle Einschaltung des Fahndungsdienstes fünf Jahre aufgehoben und anschließend vernichtet.

3.10 Sozialverwaltung, Gesundheitswesen

3.10.1 Allgemeines

Wie im Vorjahr fand auch im Berichtsjahr eine Besprechung mit den Geschäftsführern der Spitzenverbände der Sozialversicherung statt. Wichtigste Beratungspunkte waren die sich auf die Sozialverwaltung, insbesondere die Sozialversicherung, beziehenden Teile meines 2. Tätigkeitsberichtes und die Neuordnung des Sozialdatenschutzes durch das Sozialgesetzbuch (s.o. 2.5). Dabei ging es nicht um die Klärung von Einzelfragen, sondern um einen Meinungsaustausch zu grundsätzlichen Fragen des Datenschutzes im Bereich der Sozialverwaltung. Es wurde vereinbart, die Zusammenarbeit fortzusetzen.

Eine große Zahl von Eingaben betraf den Umfang der *Mitwirkungspflicht* des Leistungsberechtigten. Wer Sozialleistungen beantragt oder erhält, hat gemäß § 60 SGB I alle Tatsachen anzugeben, die für die Leistung erheblich sind, und auf Verlangen des zuständigen Leistungsträgers der Erteilung der erforderlichen Auskünfte durch Dritte zuzustimmen. Diese Vorschrift wird häufig als Grundlage dafür benutzt, eine pauschale, umfassende Zustimmung des Betroffenen zur Erteilung aller nur denkbaren Auskünfte einzuholen. Demgegenüber stellt § 60 SGB I auf die Erheblichkeit und Erforderlichkeit ab, will also die Mitwirkung des Leistungsberechtigten gerade begrenzen. Sicherlich kann diese Grenzziehung im Einzelfall schwierig sein, sie ist aber nur nach Prüfung des konkreten Falles möglich. Wenn der Gesetzgeber für die Offenbarung personenbezogener Daten in § 67 SGB X eine Einwilligung des Betroffenen *im Einzelfall* (s. o. 2.5) verlangt, so macht dies seine grundsätzliche Einstellung deutlich. Sie kann auch bei der Bestimmung des Umfangs der Mitwirkung des Leistungsberechtigten gemäß § 60 SGB I nicht unbeachtet bleiben. Hier ist unter strik-

ter Wahrung des Verhältnismäßigkeitsgrundsatzes nur ein solches Maß an Mitwirkung zu verlangen, wie § 60 SGB I es gewährt. Pauschale Ermächtigungen, etwa bei Sparkassen, Banken, der Deutschen Bundespost, bei allen Ärzten und Krankenhäusern usw. Erkundigungen einzuholen, sind in der Regel gemäß § 60 SGB I nicht gerechtfertigt. Gleiches gilt für in diesem Zusammenhang erteilte pauschale Entbindungen von den jeweiligen Schweigepflichten, durch die z. B. alle Ärzte, die den Antragsteller jemals behandelt haben, von ihrer Schweigepflicht entbunden werden.

Falls ein Leistungsberechtigter geltend macht, er habe bestimmte anspruchsbegründende Angaben von Familienangehörigen oder Dritten, die ihm gegenüber nicht auskunftspflichtig seien, auch bei wiederholten Versuchen nicht in Erfahrung bringen können, so wäre eine dennoch geforderte Mitwirkung auf etwas gerichtet, was der Leistungsberechtigte unmöglich erbringen kann. Hier sind die Grenzen der gemäß § 60 SGB I gegebenen Mitwirkungsobliegenheiten erreicht. Die Verwaltung wird in einem solchen Fall zu prüfen haben, ob sie die anspruchsbegründenden Angaben von Amts wegen (vgl. § 20 SGB X) auf andere Weise ermitteln kann.

3.10.2 Rentenversicherung

3.10.2.1 Sozialbericht bei Abhängigkeitskranken

Wiederholt haben mich Eingaben erreicht, welche die Prüfung des Umfangs der Fragen und der Verwendung des Sozialberichts — psychosoziale Grunddaten — zum Gegenstand hatten. Der Sozialbericht wird seit 1979 von den Rentenversicherungsträgern im Rehabilitationsverfahren Abhängigkeitskranker eingesetzt und dient als Grundlageninformation zur Vorbereitung der Entscheidung über Anträge auf Rehabilitationsmaßnahmen. Der Bericht ist eine der Entscheidungshilfen, die es dem Leistungsträger ermöglichen sollen, sowohl die voraussichtliche Erhaltung, wesentliche Besserung oder Wiederherstellung der Erwerbsfähigkeit abschätzen zu können als auch den Gesamtplan (§ 5 Abs. 3 Rehabilitations-Angleichungsgesetz) zur Rehabilitation aufzustellen. Um dieser Aufgabe entsprechen zu können, enthält der Bericht neben den Angaben zur Person eine Vielzahl sensibler Informationen, z. B. Angaben zu den finanziellen und Wohnverhältnissen, zur Vorgeschichte und zum derzeitigen Zustand (u. a. Suizidversuche, verwendete Suchtmittel, ihre Dosis und Häufigkeit der Einnahme, Verhalten unter Einfluß von Suchtmitteln), zu Zahl und Zeitpunkt durchgeführter Entgiftungen und Entwöhnungen, zur Sozialanamnese des Betreuten, insbesondere zum sozialen Umfeld, und Hinweise zur Motivation und Behandlungsfähigkeit.

Die genannten Daten werden von dem betreuenden Sozialarbeiter der Beratungsstelle beim Betroffenen erhoben.

Der Sozialbericht enthält über diese Angaben hinaus auch deren Würdigung durch den betreuenden Sozialarbeiter; er wird von diesem unterschrieben. Der Betreute wird gebeten, in einer dem Sozialbericht beigefügten Erklärung zu bestätigen, daß er über dessen Inhalt unterrichtet wurde und mit der Übermittlung des Berichts an den Leistungsträger und die Behandlungsstätte zum Zwecke der Antragserledigung und zur Durchführung der Behandlung einverstanden ist.

Datenschutzrechtlich problematisch ist insbesondere der Umfang der Erhebung von Daten beim Betreuten durch den Sozialarbeiter der Beratungsstelle und die Übermittlung des Sozialberichts an den jeweilig zuständigen Leistungsträger. Da die angesprochenen Probleme sowohl in meine als auch in die Zuständigkeit der Datenschutzbeauftragten der Länder fallen, hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder auf ihrer Sitzung am 29. April 1980 beschlossen, dieses Problem gemeinsam in einer Arbeitsgruppe unter meinem Vorsitz zu erörtern. Die Arbeitsgruppe hat Vertreter der Rentenversicherung und einiger gemeinnütziger und freier Einrichtungen beratend hinzugezogen. Neben der Erörterung des Sozialberichts wird wegen des engen Sachzusammenhangs auch über den „Entlassungsbericht nach stationärer Heilbehandlung" beraten.

Die Arbeitsgruppe ist bisher zweimal zusammengetreten. Die Beratungen werden im nächsten Berichtsjahr fortgesetzt werden. Nach ihrem Abschluß werde ich zusammenfassend berichten. Schon jetzt zeichnet sich jedoch ab, daß kaum wesentliche datenschutzrechtliche Bedenken bleiben werden, wenn in Einzelheiten eine Klarstellung erfolgt.

3.10.2.2 Verband Deutscher Rentenversicherungsträger e.V. (VDR)

Im Berichtszeitraum sind der VDR und meine Dienststelle in mehreren Gesprächen zu einer zunehmend guten Zusammenarbeit gelangt. Gemeinsam konnten erste Ergebnisse erzielt werden.

Anläßlich meiner Überprüfung im Jahre 1979 hatte ich folgende Forderungen an den Verband gestellt:

— eine Risiko- und Schwachstellenanalyse auf der Basis einer zu verbessernden Übersicht nach § 15 Nr. 1 BDSG,

— eine Verbesserung der organisatorischen Transparenz,

— eine Begrenzung der Datenverarbeitungsaufgaben beim VDR,

— eine Überprüfung des Umfangs und Inhalts der vorhandenen Datensammlung auf ihre Erforderlichkeit.

Diese Forderungen konnten vom VDR inzwischen zum Teil erfüllt werden, zum Teil ist ihre Realisierung eingeleitet:

— Die Übersicht nach § 15 Nr. 1 BDSG wurde verbessert. Sie entspricht jetzt meinen Anforderungen. Eine Risiko- und Schwachstellenanalyse wird gegenwärtig durchgeführt. Erste Maßnahmen wie eine Verbesserung der Zugangskontrolle sind getroffen.

— Die Hauptabteilung IV des VDR wird entsprechend meiner Forderung nach mehr Transparenz neu organisiert.

— Laufende Arbeiten am Projekt „Raucherentwöhnungstherapie", für das aus meiner Sicht fraglich ist, ob der VDR es durchführen darf, werden bald beendet. Ob derartige Arbeiten auch künftig vom Verband wahrgenommen werden dürfen, wird angesichts der Neuregelungen des SGB X, insbesondere § 75, noch zu klären sein.

— Die Überprüfung der Erforderlichkeit der Datensammlung durch den Verband hat ergeben, daß die DEVO/DÜVO-Sicherungsdatei mit insgesamt bis zu 75 Millionen personenbezogenen Datensätzen Ende 1981 eingestellt wird.

— Ein Verfahren, in dem genau festgelegt wird, wer dem Rechenzentrum Arbeitsaufträge erteilen darf, konnte noch nicht realisiert werden. Ich kann jedoch davon ausgehen, daß ein solches Verfahren im Jahre 1981 eingeführt wird. Für diese Neuregelung wird es darauf ankommen, ob der VDR für die Träger der Rentenversicherung Daten im Auftrag verarbeitet (§ 8 BDSG i. V. m. §§ 69, 80 SGB X) oder ob es sich um eigene Aufgaben des VDR handelt. Diese Frage wird in erster Linie von den Trägern der Rentenversicherung und vom VDR gemeinsam zu entscheiden sein.

3.10.3 Krankenversicherung

3.10.3.1 Weitergabe von Daten aus der Ersatzkasse an eine private Krankenversicherung

In einem Fall hat mir eine Bürgerin mitgeteilt, sie habe bei einer Ersatzkasse einen Auslandskrankenschein beantragt; anläßlich dieses Antrags müsse ihre Adresse an eine private Krankenversicherung weitergegeben worden sein. Die private Krankenversicherung habe ihr Werbeunterlagen übersandt. Ein Anruf bei der Ersatzkasse habe dann ergeben, daß der zuständige Mitarbeiter die Anschrift tatsächlich übermittelt habe. Auf diese Möglichkeit sei sie jedoch beim Anfordern ihres Auslandskrankenscheins nicht hingewiesen worden.

Die Nachforschungen des internen Datenschutzbeauftragten der Ersatzkasse, die auf meine Bitte angestellt wurden, haben ergeben, daß der genaue Sachverhalt nicht mehr festzustellen ist. Die Kasse geht jedoch davon aus, daß die Anschrift übermittelt worden ist. Sie teilte mir mit, sie halte es zwar für ihre Pflicht, im Rahmen ihrer Betreuungsaufgaben die Mitglieder ausführlich auf die ungedeckten Risiken bei einem Auslandsaufenthalt und auf die Möglichkeiten, sie abzudecken, hinzuweisen; es sei jedoch ein Fehlverhalten des Mitarbeiters gewesen, die Anschrift an die private Krankenversicherung zu übermitteln. Die Mitarbeiter der Ersatzkasse seien nochmals über die bestehenden diesbezüglichen Anweisungen belehrt worden, um solche Fehler künftig zu unterbinden.

Ich halte es für angebracht, solche Übermittlungen auch dann zu unterlassen, wenn sie in guter Absicht geschehen. Die sicherlich sehr sinnvolle Beratung der Mitglieder läßt sich auch durchführen, ohne das Selbstbestimmungsrecht des einzelnen zu beeinträchtigen.

3.10.3.2 Hamburgische Zimmererkrankenkasse

Ich habe den Stand des Datenschutzes bei der Kasse in einem eintägigen, unangemeldeten Besuch überprüfen lassen. Der Besuch hat gezeigt, daß auch eine sehr kleine Verwaltung — die Kasse hat bei ca. 50 000 Mitgliedern ca. 170 Mitarbeiter — angemessene Lösungen bei der Umsetzung des Datenschutzes finden kann. Dies gilt z. B. für die ideenreiche interne Übersicht gem. § 15 Nr. 1 BDSG. Mängel, die die Kontrollierbarkeit der DV-Programme (§ 15 Nr. 2 BDSG) betrafen, hat die Kasse inzwischen abgestellt.

3.10.3.3 Techniker-Krankenkasse

Im Januar des Berichtsjahres wurde eine eintägige Kontrolle der Techniker-Krankenkasse (TK) durchgeführt.

Bei dieser Kasse gab es keinen internen Datenschutzbeauftragten, sondern einen Fachausschuß Datenschutz, der sich aus Abteilungsleitern und Vertretern der Geschäfts- und Abrechnungsstellen zusammensetzt. Ich habe meine Bedenken, bei der internen Meinungsbildung in diesem Ausschuß sei ein Dominieren der Interessen der Fachabteilungen zu befürchten, deutlich gemacht und geraten, einen internen Datenschutzbeauftragten zu bestellen. Die Kasse meint jedoch, der Ausschuß habe sich bewährt und solle weiter bestehen bleiben. Gleichwohl hat sie eine Planstelle „Sachbearbeiter Datenschutz" geschaffen und besetzt. Dieser Mitarbeiter arbeitet direkt mit dem Fachausschuß zusammen. Ich halte dies für eine interessante Konstruktion. Die TK wird mich weiter über Arbeits- und Wirkungsweise informieren.

Der Arbeitsablauf, insbesondere das Auftragsverfahren für EDV-Arbeiten, die Verwaltung der Datenträger, die Programmdokumentation sowie der Objektschutz im Rechenzentrum sind nach meinem Eindruck gut geregelt.

Einige Mängel, wie das offene Versenden der Versicherten-Nummer (und damit des Geburtsdatums) mit Postkarten, sind inzwischen abgestellt.

Bei der Realisierung des Projekts „DEVAS", Mitgliederbestandsführung und Beitragswesen im Dialogverkehr, wird mich die TK beteiligen.

3.10.3.4 Hamburg-Münchener Ersatzkasse

Im Berichtszeitraum wurde eine eintägige Überprüfung der Hamburg-Münchener Ersatzkasse durchgeführt. Dabei wurde festgestellt, daß der erreichte Stand der Umsetzung des Datenschutzes, gemessen am Stand der Automatisierung und verglichen mit Anwendern gleicher Größe, relativ gut ist.

Ein Datenschutzbeauftragter war noch nicht bestellt. Ich kann jedoch nach gegenwärtigem Stand

davon ausgehen, daß dies Anfang 1981 der Fall sein wird.

In die interne Übersicht gem. § 15 Nr. 1 BDSG und in die Auskunftsregelung gem. § 13 BDSG waren manuell geführte Dateien nicht aufgenommen. Beides hat die Kasse inzwischen geändert.

Auch die Praxis, Anschriften von Auszubildenden zu Werbezwecken zu erheben, wurde inzwischen eingestellt.

3.10.3.5 DVDIS

In meinem 2. Tätigkeitsbericht (S. 35) habe ich über das Projekt „Datenerfassung, Verarbeitung, Dokumentation und Informationsverbund in den sozialärztlichen Diensten mit Hilfe der elektronischen Datenverarbeitung" — DVDIS — der Arbeitsgemeinschaft für Gemeinschaftsaufgaben der Krankenversicherung (AGK) in Essen berichtet und Kriterien angegeben, die das Projekt aus datenschutzrechtlicher Sicht zu erfüllen hat. Anfang 1980 habe ich das Projekt mehrere Tage lang untersuchen lassen und mich davon überzeugt, daß DVDIS entgegen meinem ursprünglichen Eindruck keine zentrale medizinische Datenbank werden soll. Der Schwerpunkt der gegenwärtigen Arbeiten liegt vielmehr lediglich bei Veränderungen in den Informationsprozessen der einzelnen sozialärztlichen Dienste. Inwieweit das DVDIS-Konzept, einmal eingesetzt, Auswirkungen auf die Arbeit der jeweiligen Krankenkassen haben wird, bedarf noch näherer Prüfung. Die AGK hat für DVDIS ein eigenes Datenschutzkonzept entwickelt, das insgesamt einen Fortschritt darstellt und keine wesentlichen Lücken enthält. Für die künftige datenschutzrechtliche Einschätzung von DVDIS wird es entscheidend darauf ankommen, welchen Satzaufbau die geplanten Dateien erhalten werden. Die Diskussion zwischen der AKG und meiner Dienststelle ist insoweit noch nicht abgeschlossen.

3.10.4 Unfallversicherung

3.10.4.1 Verwaltungs-Berufsgenossenschaft

Eine eintägige Kurzüberprüfung bei der Verwaltungs-Berufsgenossenschaft in Hamburg ergab ein insgesamt sehr erfreuliches Bild: Die Unterlagen des internen Datenschutzbeauftragten waren vorbildlich und ideenreich geführt. Die Art und Weise der Organisation des Verhältnisses von EDV- und Fachabteilung war entsprechend der Verantwortlichkeit der Fachabteilung für die Verarbeitung ihrer Daten geregelt. Unwesentliche Datensicherungsmängel und unbestrittene Unzulänglichkeiten beim Objektschutz, welche die Berufsgenossenschaft im Jahr 1981 beheben will, konnten diesen positiven Gesamteindruck nicht verwischen.

3.10.4.2 Arbeitskreis „Arbeitsmedizin" der Bau-Berufsgenossenschaften

Der Arbeitskreis „Arbeitsmedizin" der Bau-Berufsgenossenschaften erwägt, ob eine zentrale „Clearingstelle" der überbetrieblichen ärztlichen Dienste bei der Bayerischen Bau-Berufsgenossenschaft, einer landesunmittelbaren Berufsgenossenschaft, für die ich nicht zuständig bin, in München eingerichtet werden soll. Hierüber und über den Stand der Arbeiten an einem Projekt betriebsärztlicher Betreuung aller Arbeitnehmer im Baugewerbe habe ich mich bei einem mehrtägigen Besuch informiert.

§ 1 des Arbeitssicherheitsgesetzes (ASiG) von 1973 hat den Arbeitgebern die Bestellung von Betriebsärzten zur Pflicht gemacht, zugleich aber die Möglichkeit zugelassen (§ 19 ASiG), daß der Arbeitgeber einen überbetrieblichen Dienst von Betriebsärzten mit der Wahrnehmung der Aufgaben nach § 3 ASiG*) betraut.

Wegen der besonderen Probleme des Baugewerbes (viele kleine Betriebe; häufiger Wechsel des Arbeitsplatzes) lag es nahe, diese Möglichkeit zu ergreifen. Die Bau-Berufsgenossenschaften haben von der in § 719a RVO eröffneten Befugnis Gebrauch gemacht, einen überbetrieblichen arbeitsmedizinischen Dienst zu schaffen und für die Mitglieder, die Unternehmer der Bauwirtschaft, einen Anschlußzwang nach den jeweiligen Satzungen einzuführen.

Die gesetzliche Aufgabenzuweisung im ASiG sagt wenig darüber aus, mit welchen Mitteln die dort genannten Aufgaben erfüllt werden sollen und können. Um Struktur und Schwerpunkte der künftigen Aufgaben der Arbeitsmedizinischen Dienste (AMD) näher zu konkretisieren, haben die Bau-Berufsgenossenschaften zwei sog. Pilotstudien in Angriff genommen.

Bei der Pilotstudie 1, die abgeschlossen ist, wurden über 30 000 Fragebögen mit etwa 80 Fragen zu gesundheitlichen Verhältnissen an Bauarbeiter versandt (Eigen-Anamnese). Dabei sind folgende Dateien entstanden:

— bei jeder Bau-BG eine, also insgesamt sieben Dateien mit personenbezogenen Daten,

— ein anonymisierter zusammengeführter Bestand aller Dateien, der beim Rechenzentrum der Bayerischen Bau-Berufsgenossenschaft geführt wird.

---

*) Gesetz über Betriebsärzte, Sicherheitsingenieure und andere Fachkräfte für Arbeitssicherheit vom 12. Dezember 1973, BGBl. I S. 1885

§ 3
Aufgaben der Betriebsärzte

(1) Die Betriebsärzte haben die Aufgabe, den Arbeitgeber beim Arbeitsschutz und bei der Unfallverhütung in allen Fragen des Gesundheitsschutzes zu unterstützen. Sie haben insbesondere

1. den Arbeitgeber und die sonst für den Arbeitsschutz und die Unfallverhütung verantwortlichen Personen zu beraten, insbesondere bei
   a) der Planung, Ausführung und Unterhaltung von Betriebsanlagen und von sozialen und sanitären Einrichtungen,
   b) der Beschaffung von technischen Arbeitsmitteln und der Einführung von Arbeitsverfahren und Arbeitsstoffen,

Bei der Pilotstudie 2, deren Erhebungsphase abgeschlossen ist und deren Auswertung bald beendet sein wird, ist nahezu derselbe Personenkreis vom AMD untersucht worden. Es sollen u. a.

— eine Arbeitnehmerdatei und
— eine Befunddatei (z. B. mit den Daten der Eigenanamnese, ärztlichen Untersuchungsergebnissen und Labordaten)

entstehen.

Als Identitätszeichen verwenden die Berufsgenossenschaften die Rentenversicherungsnummer der Arbeitnehmer. Es wird erörtert, den aufgebauten Datenbestand in folgender Weise zu nutzen:

— Bei jeder einzelnen Bau-Berufsgenossenschaft wird eine Datei aufgebaut, die festhält, wer wann von welchem AMD untersucht wurde. Diese Datei soll nur einen Index enthalten, mit dessen Hilfe es möglich ist, die Stelle aufzufinden, bei der Befunde gespeichert werden.
— Die Tatsache der Untersuchung eines bestimmten Arbeitnehmers wird durch den AMD an die „Clearingstelle" bei der Bayerischen Bau-Berufsgenossenschaft gemeldet.
— Bei der „Clearingstelle" kann dann nachgefragt werden, ob ein bestimmter Arbeitnehmer von einem AMD untersucht wurde.

Die Beratungen zwischen dem Arbeitskreis „Arbeitsmedizien" der Bau-Berufsgenossenschaften und meiner Dienststelle haben nach anfänglich unterschiedlichen Auffassungen inzwischen erfreulicherweise zu einem vom Arbeitskreis gemachten Vorschlag einer einwandfreien Fassung der Datenschutzklausel gemäß § 9 Abs. 2 BDSG auf den Fragebögen geführt. Diese Klausel soll nunmehr wie folgt lauten:

„Aufgrund des § 3 Abs. 1 Nr. 2 des Arbeitssicherheitsgesetzes und der Satzung der Berufsgenossenschaft obliegt dem Arbeitsmedizinischen Dienst u. a. die Aufgabe, die Arbeitnehmer der Bauwirtschaft zu untersuchen, arbeitsmedizinisch zu beurteilen und zu beraten sowie die Untersuchungsergebnisse zu erfassen und auszuwerten.

Indem Sie freiwillig diesen Fragebogen ausfüllen und sich anschließend arbeitsmedizinisch untersuchen lassen, dienen sie nicht nur Ihrer eigenen Gesundheit, sondern auch den Interessen aller Arbeitnehmer der Bauwirtschaft.

Ihre Angaben und die Untersuchungsergebnisse unterliegen der ärztlichen Schweigepflicht."

Dagegen sind einige andere Fragen noch nicht endgültig geklärt:

— Der Fragebogen der ärztlichen Untersuchung enthält Fragen, deren Erforderlichkeit zweifelhaft erscheint. So wird z. B. unter dem Punkt „Psyche" lediglich die Einteilung „unauffällig", „im Grenzbereich", „weitere Untersuchung empfohlen" angeboten. Diese Daten sind so wenig ergiebig, daß ihre Erhebung für den angestrebten Zweck nicht geeignet sein dürfte.
— Ich halte die Verwendung der Rentenversicherungsnummer als Identifizierungsmerkmal für den AMD für bedenklich; die Bau-Berufsgenossenschaften haben mir bisher keine überzeugenden Gründe genannt, welche die Verwendung gerade dieses Schlüssels erforderlich machen. Ich verkenne nicht die Notwendigkeit der Verwendung eines Identifizierungsschlüssels; es sollte jedoch ein Schlüssel gewählt werden, der die Gefahr der Verknüpfung mit Datenbeständen anderer Bereiche der Verwaltung nicht erhöht.
— Zu den Erörterungen, eine „Clearingstelle" zu errichten, kann ich abschließend noch nicht Stel-

---

c) der Auswahl und Erprobung von Körperschutzmitteln,

d) arbeitsphysiologischen, arbeitspsychologischen und sonstigen ergonomischen sowie arbeitshygienischen Fragen, insbesondere

des Arbeitsrhythmus, der Arbeitszeit und der Pausenregelung,

der Gestaltung der Arbeitsplätze, des Arbeitsablaufs und der Arbeitsumgebung,

e) der Organisation der „Ersten Hilfe" im Betrieb,

f) Fragen des Arbeitsplatzwechsels sowie der Eingliederung und Wiedereingliederung Behinderter in den Arbeitsprozeß,

2. die Arbeitnehmer zu untersuchen, arbeitsmedizinisch zu beurteilen und zu beraten sowie die Untersuchungsergebnisse zu erfassen und auszuwerten,

3. die Durchführung des Arbeitsschutzes und der Unfallverhütung zu beobachten und im Zusammenhang damit

a) die Arbeitsstätten in regelmäßigen Abständen zu begehen und festgestellte Mängel dem Arbeitgeber oder der sonst für den Arbeitsschutz und die Unfallverhütung verantwortlichen Person mitzuteilen, Maßnahmen zur Beseitigung dieser Mängel vorzuschlagen und auf deren Durchführung hinzuwirken,

b) auf die Benutzung der Körperschutzmittel zu achten,

c) Ursachen von arbeitsbedingten Erkrankungen zu untersuchen, die Untersuchungsergebnisse zu erfassen und auszuwerten und dem Arbeitgeber Maßnahmen zur Verhütung dieser Erkrankungen vorzuschlagen,

4. darauf hinzuwirken, daß sich alle im Betrieb Beschäftigten den Anforderungen des Arbeitsschutzes und der Unfallverhütung entsprechend verhalten, insbesondere sie über die Unfall- und Gesundheitsgefahren, denen sie bei der Arbeit ausgesetzt sind, sowie über die Einrichtungen und Maßnahmen zur Abwendung dieser Gefahren zu belehren und bei der Einsatzplanung und Schulung der Helfer in „Erster Hilfe" und des medizinischen Hilfspersonals mitzuwirken.

(2) Die Betriebsärzte haben auf Wunsch des Arbeitnehmers diesem das Ergebnis arbeitsmedizinischer Untersuchungen mitzuteilen; § 8 Abs. 1 Satz 2 bleibt unberührt.

(3) Zu den Aufgaben der Betriebsärzte gehört es nicht, Krankmeldungen der Arbeitnehmer auf ihre Berechtigung zu überprüfen.

lung nehmen, weil die mir bekanntgewordenen Pläne zu wenig konkret sind. Schon jetzt möchte ich jedoch auf die Problematik des etwaigen Aufbaus zentraler personenbezogener oder personenbeziehbarer Bestände dieser Art hinweisen.

Ich werde mit der Arbeitsgemeinschaft in nächster Zeit ein weiteres Gespräch führen.

3.10.5 Arbeitsverwaltung

In meinem zweiten Tätigkeitsbericht (S. 30) hatte ich der Bundesanstalt für Arbeit (BA) „teilweise gravierende Mängel bei der Konzeption des Datenschutzes" bescheinigen müssen. Die intensive Zusammenarbeit zwischen der Bundesanstalt und meiner Dienststelle hat inzwischen zu Ergebnissen geführt, die nicht nur datenschutzfreundlich sind, sondern darüber hinaus beispielhaft auch für andere Verwaltungen sein könnten. An diesem sehr positiven Gesamtbild vermögen auch die Einzelfälle, über die ich berichten werde, nichts zu ändern.

Ich habe im übrigen durch Mitarbeiter meines Hauses einen Schulungskurs „Grundfragen des Datenschutzes" für Führungskräfte der BA veranstalten lassen — ein Beispiel dafür, daß sich meine Aufgaben nicht in Kritik erschöpfen, sondern in eine konstruktive Zusammenarbeit münden können.

3.10.5.1 Stellung des internen Datenschutzbeauftragten der BA

In meinem zweiten Tätigkeitsbericht hatte ich kritisiert, daß die Funktion des internen Datenschutzbeauftragten personell und qualifikationsmäßig nicht optimal ausgestattet war. Die Bundesanstalt hat aus dieser Kritik folgende Konsequenzen gezogen:

— Mit Wirkung vom 1. April 1980 ist der Direktor des Vorprüfungsamtes der BA zum Beauftragten für Datenschutz und Datensicherheit bestellt worden. So ist es möglich, das mit Revisionsaufgaben betraute „Vorprüfungsamt" auch für Zwecke der Kontrolle des Datenschutzes in den einzelnen Arbeitsämtern zu nutzen.

— Ein Referat der Zentralabteilung der BA hat die Bearbeitung „gemeinsamer Angelegenheiten des Datenschutzes" übernommen.

Die auf dieser Grundlage seit dem 1. April 1980 erfolgte Zusammenarbeit mit den zuständigen Stellen der BA hat sich hervorragend bewährt. Vorbehaltlich einer endgültigen Stellungnahme nach längerer Erprobung habe ich in diesem Fall nichts dagegen einzuwenden, daß das Vorprüfungsamt auch Kontrollaufgaben nach dem BDSG wahrnimmt.

3.10.5.2 Anmeldungen der BA und interne Übersicht gem. § 15 Nr. 1 BDSG

Die Dateienmeldungen der BA gemäß §§ 19 Abs. 4 Satz 3 und 12 Abs. 1 BDSG sowie die interne Übersicht gemäß § 15 Nr. 1 BDSG waren unvollständig, insbesondere weil die manuellen Dateien der Arbeitsverwaltung nicht erfaßt waren.

Die BA hat das Versäumte inzwischen nachgeholt. Die Übersicht enthält nunmehr eine Zusammenstellung

— aller maschinell betriebenen Dateien (ca. 50),

— aller manuell betriebenen Dateien mit personenbezogenen Daten, die zur Übermittlung an Dritte bestimmt sind (ca. 10),

— aller manuell betriebenen Dateien mit personenbezogenen Daten, die *nicht* zur Übermittlung an Dritte bestimmt sind (ca. 70).

Die Übersicht entspricht noch nicht restlos den Kriterien, die ich in meinem zweiten Tätigkeitsbericht (S. 56 f.) festgelegt habe. Ich bin mit der BA im Gespräch, inwieweit diesen Kriterien Rechnung getragen werden kann.

3.10.5.3 Neuregelung des Auskunftsverfahrens der BA, insbesondere aus Beratungs- und Vermittlungsunterlagen

In einer Reihe von Eingaben hatten Bürger die unzureichende und schleppende Beantwortung ihrer Auskunftsersuchen gem. § 13 BDSG kritisiert. Die Bundesanstalt ist meiner Anregung gefolgt und hat das Verfahren der Auskunftserteilung grundlegend neu geregelt:

— Die Eingaben werden seit 1. April 1980 wie Petitionen an den Deutschen Bundestag behandelt. Der Petitionsausschuß hat eine Frist von sechs Wochen zur Stellungnahme gesetzt. Petenten können jetzt in der Regel mit einer Antwort innerhalb weniger Wochen rechnen.

— Die Unterscheidung zwischen Akten und Dateien, die das BDSG trifft, ist aus der Sicht des Bürgers unverständlich, zumal in der Arbeitsverwaltung, wo wichtige Unterlagen nur in Akten untergebracht sind. Diese oft ziemlich zufällige Differenzierung kann überdies dazu verführen, die für den Bürger wichtigsten Daten, wie z. B. ärztliche Gutachten, in Akten zu verbringen und so dem Auskunftsrecht des § 13 BDSG zu entziehen. Die Bundesanstalt hat in einem beispielhaften Erlaß diesen auf dem BDSG selbst beruhenden Zustand beseitigt. Der — gebührenfreien — Auskunft unterliegen neben den Eintragungen in den Dateien nunmehr sämtliche, einen konkreten Vorgang betreffende Unterlagen zu den Dateien. Die Auskunftserteilung bezieht sich — allerdings ohne Anerkenntnis einer gesetzlichen Verpflichtung — auch auf die internen Dateien der Arbeitsberatung und Arbeitsvermittlung.

Die Auskünfte werden grundsätzlich durch die zuständigen Fachkräfte gegeben, Auskünfte über medizinische oder psychologische Gutachten erfolgen durch Ärzte bzw. Psychologen. Die Auskünfte werden, den Wünschen der Betroffenen entsprechend, grundsätzlich mündlich oder durch Gewährung von Einsichtnahme erteilt. Mit Ausnahme der medizinischen und psychologischen Gutachten können auch Fotokopien der Unterlagen überlassen werden.

Dieses nachahmenswerte Beispiel zeigt mir, wie ideenreich und bürgerfreundlich eine nicht eben geglückte gesetzliche Regelung durch eine Verwaltung gestaltet werden kann.

3.10.5.4 Einzelfälle

Wie schon im Jahr 1979 habe ich auch im Berichtsjahr Einzeleingaben vor Ort und ohne vorherige An-

meldung überprüfen lassen. Alle Eingaben betrafen die Zulässigkeit von Eintragungen in den Vermittlungsunterlagen, insbesondere in der Vermittlungskartei (Bewerber-Angebots-Kartei, BAnK).

— Ein Arbeitsamt in Norddeutschland

Ein Ausländer hatte sich mit der Bitte an mich gewandt, seine Vermittlungsunterlagen zu überprüfen. Er wolle als technischer Zeichner vermittelt werden, habe aber den Verdacht, daß sich in seinen Unterlagen Bemerkungen befinden müßten, die ihm keine faire Chance einer Vermittlung einräumten. Meine Feststellungen ergaben, daß dieser Verdacht begründet war:

In der Vermittlungs-Kartei befand sich das Zeugnis eines Arbeitgebers, der ihm nach weniger als einem Monat fristlos gekündigt hatte. Es enthielt Aussagen wie „Herrn X fehlen die elementarsten Grundkenntnisse", „Herr X zeigte sich in äußerstem Maße uneinsichtig", „konsequente Unbelehrbarkeit". Ihm wurde weiter die Fähigkeit abgesprochen, einen geraden Strich zu ziehen — ein vernichtendes Urteil für einen technischen Zeichner.

In einem Vermerk des Fachgruppenleiters „technische Zeichner" stand: „Herr X ist nicht geeignet als Fachkraft, soll nur für gewerbliche Hilfsarbeiten verwendet werden". Der Vermerk, ein kleiner, mit Maschinenschrift beschriebener Zettel, war außen an die Karteikarte geheftet — wahrscheinlich für jeden, der diese Karte zum erstenmal aus der Kartei zieht, die erste Information, die überhaupt wahrgenommen wird. Dadurch wird möglicherweise von vornherein ein falscher Eindruck über den Betroffenen vermittelt. Das Arbeitsamt hat sich meinen Bedenken angeschlossen und hat Zeugnis und Vermerk vernichtet.

Der Petent ist seit Frühjahr 1980 auf eigene Bemühungen hin als technischer Zeichner beschäftigt. Sein Arbeitgeber bescheinigt ihm gute persönliche und fachliche Eigenschaften.

— Ein Arbeitsamt in Süddeutschland

Auch die folgende Eingabe zeigt, wie sich problematische Werturteile zu Vorurteilen gegen den betroffenen Arbeitslosen auswachsen können.

Ein Arbeitsuchender hatte mir in einem 20seitigen Brief sein Leben, insbesondere seine „Karriere" als Arbeitsloser geschildert. Der Tenor seiner Behauptungen war: Das Arbeitsamt behandle ihn als „verrückt", was er aber nicht sei.

Meine Feststellungen haben ergeben:

In der umfangreichen Vermittlungsunterlage von 1977 (die als Tasche ausgestaltet ist) befindet sich u. a. eine sog. Mitführungskarte von 1970. Auf dieser Karte hat unter der Rubrik „Erwerbsbehinderungen" ein Sachbearbeiter festgehalten: „nervlich belastet". In der Karte werden Hinweise auf ein psychologisches und ein ärztliches Gutachten aus 1970 gegeben. Das psychologische Gutachten von 1970 bescheinigt Herrn X überdurchschnittliche Arbeitseigenschaften; der Psychologe weist darauf hin, daß Herr X wegen seines ausdrücklichen Wunsches, in eine selbstbestimmte Arbeit vermittelt zu werden, schwer zu vermitteln sein werde. In dem sehr kurzen ärztlichen Gutachten von 1970 heißt es zweimal sinngemäß, Herr X sei „nicht in der Lage, sich der Realität anzupassen". Aus dem Gutachten ist nicht ersichtlich, auf welche tatsächlichen Feststellungen sich dieses Urteil gründet.

Herr X ist 1978 nochmals medizinisch und psychologisch untersucht worden. Der medizinische Gutachter bescheinigt dem Petenten — unter Hinzuziehung des Altgutachtens — eine „psychische Fehlhaltung"; für dieses Werturteil werden keine Belege angegeben. Gleichzeitig habe sich sein allgemeiner Gesundheitszustand seit 1970 verbessert. Das ausführliche psychologische Gutachten von 1978 enthält keine Hinweise auf etwaige psychische Erkrankungen. Der Psychologe, der eine insgesamt sehr positive Prognose gibt, schlägt vor, Herrn X wegen seiner Abneigung gegen den erlernten Beruf zum praktischen Betriebswirt ausbilden zu lassen.

Die beschriebene Mitführungskarte in der BAnK-Tasche hätte nach den Vorschriften der Bundesanstalt längst vernichtet sein müssen. Gerade sie enthält das problematische Urteil „nervlich belastet" mit dem Hinweis auf die veralteten Gutachten. Diese zu löschenden Informationen sind objektiv geeignet, ein Vorurteil über den Betroffenen aufzubauen oder zu verstärken. Es wurde deshalb zugesagt, diese Karte zu vernichten, denn es ist nicht auszuschließen, daß die zuständigen Bearbeiter des Arbeitsamtes sich eine feste — negative — Meinung über die Eigenschaften des Betroffenen gebildet hatten. Es wurde deshalb darüber hinaus zugesagt, daß der Betroffene einem Arbeitsvermittler zugewiesen wird, der ihn noch nicht kennt. Dieser Mitarbeiter soll neue Vermittlungsversuche ohne Kenntnis der Vermittlungsakte mit den Gutachten unternehmen.

Dieser Einzelfall, von dem alle Beteiligten hoffen, daß er zur Zufriedenheit des Betroffenen geklärt werden kann, weist einige Aspekte auf, die mich mit Sorge erfüllen: Es ist offenbar nicht ausgeschlossen, daß ein Arbeitsuchender in den Akten als „verrückt" geführt wird, ohne daß dieses gravierende Werturteil präzis nachprüfbar ist. Der Stellenwert ärztlicher und psychologischer Gutachten und Werturteile bei Fachaufgaben wird deshalb neu zu überdenken sein.

— Ein Arbeitsamt in Nordwestdeutschland

Ein Arbeitsloser hatte in einer Eingabe behauptet, das Arbeitsamt habe seine Gesundheitsdaten, insbesondere Daten über eine psychische Erkrankung, an Arbeitgeber weitergegeben. Als Folge dieses Datenmißbrauchs habe er keine feste Anstellung mehr bekommen.

Dieser Verdacht hat sich bei einer unangemeldeten Prüfung vor Ort, bei der neben der Hauptstelle auch die Nebenstelle eines Arbeitsamtes miteinbezogen wurde, nicht erhärtet. Im Gegenteil — alle Beteiligten hatten sich bemüht, einen sehr schwierigen Vermittlungsfall unbürokratisch und mit viel Einfühlungsvermögen gegenüber dem Betroffenen zu lösen.

Um die Eingabe im Rahmen meiner Zuständigkeit aufzuklären, habe ich zusätzlich eine Zweigstelle der Barmer Ersatzkasse unangemeldet überprüfen lassen. Auch dort waren die Mitarbeiter der Kasse mit der gebotenen Sorgfalt an diesen schwierigen Fall herangegangen.

Da ich am Rande der Prüfung erfahren habe, daß möglicherweise eine Stelle des betreffenden Landes Gesundheitsdaten weitergegeben hat, habe ich die Eingabe insoweit an den zuständigen Landesbeauftragten abgegeben.

3.10.6 Gesundheitswesen

3.10.6.1 „Modellprogramm Psychiatrie"

Datenschutz im Bereich des Gesundheits- und Sozialwesens kann exemplarisch verdeutlicht werden an dem Modellprogramm der Bundesregierung zur Reform der Versorgung der Bevölkerung im psychiatrischen und psychotherapeutisch/psychosomatischen Bereich. Hierzu liegen Sachverständigengutachten und eine Stellungnahme der Bundesregierung vor. Gemeinsam ist den vorhandenen Unterlagen, daß der Datenschutz nur vereinzelt in das Blickfeld der jeweiligen Verfasser getreten ist. Angesichts des betroffenen Personenkreises müssen aber gerade in diesem Zusammenhang besonders sorgfältige Überlegungen angestellt werden. Daten über die in Rede stehenden Mitbürger sind in höchstem Grade sensibel. Bei einem Teil der betroffenen Patienten ist davon auszugehen, daß sie geschäftsunfähig oder beschränkt geschäftsfähig sind, so daß die Einwilligung des Betroffenen in die Datenerhebung und Datenverarbeitung nicht oder nur unter erschwerenden Umständen zu erlangen ist. Rechtsvorschriften als Grundlage für die Datenerhebung und Datenverarbeitung fehlen oder reichen nicht aus; angesichts historischer Erfahrungen ist nicht damit zu rechnen, daß der Gesetzgeber umfassende Ermächtigungen erteilen wird.

Im Gegenteil: im Anwendungsbereich des Sozialgesetzbuches (s. o. 2.5) hat er gerade entschieden, bei den in § 76 SGB X angesprochenen, besonders schutzwürdigen personenbezogenen Daten eine Offenbarung nur noch unter sehr eingeschränkten Voraussetzungen zuzulassen. Aber auch bei den nicht unter § 76 SGB X fallenden personenbezogenen Daten, die unter den Schutz des Sozialgeheimnisses (§ 35 SGB I) fallen, ist die Offenbarung für Forschungs- oder Planungszwecke gemäß § 75 SGB X an eingrenzende Voraussetzungen geknüpft, die in einem besonderen Genehmigungsverfahren geprüft werden müssen.

Aus all diesen Gründen habe ich den Bundesminister für Jugend, Familie und Gesundheit auf seine Beratungsbitte hin gebeten, im weiteren Verlauf seiner Überlegungen sein besonderes Augenmerk auf die folgenen Fragen zu richten:

— die voraussichtlichen Informationsflüsse:
  welche Daten sollen von wem erhoben und verarbeitet werden?
  insbesondere: welche Daten sollen von wem an wen übermittelt werden?
— die Legitimationsgrundlagen der Datenerhebung und Datenverarbeitung:
  — Einwilligung
  — Rechtsvorschriften (SGB, Unterbringungsgesetze der Länder usw.),
— die Zweckentfremdung von Daten, die zur Heilung und Betreuung eines Patienten erhoben und verarbeitet werden, für Zwecke der Forschung oder Planung.

Ich werde die weitere Entwicklung auf diesem Gebiet sorgfältig beobachten.

3.10.6.2 Bundesgesundheitsamt

Bei einem Informationsbesuch des Bundesgesundheitsamtes im Frühjahr 1980 sind schwerwiegende Mängel bei der Umsetzung des Datenschutzes zutage getreten. So war keine Übersicht über die Dateien mit personenbezogenen Daten vorhanden. Auch gab es kein Verfahren, nach dem sich die ordnungsgemäße Anwendung der DV-Programme kontrollieren läßt. Diese Mängel wiegen um so schwerer, als im Bundesgesundheitsamt, teilweise unter Mitwirkung außenstehender Dritter, mit hochsensiblen medizinischen Daten geforscht wird. Nach diesem Besuch hat der Vizepräsident des Amtes die Funktion des internen Datenschutzbeauftragten selbst übernommen. Nach einem weiteren Besuch wurde mir die Fertigstellung der vollständigen internen Übersicht gemäß § 15 Nr. 1 BDSG für den 1. August, das verbesserte Datensicherungskonzept für den 1. Oktober 1980 zugesagt. Nach mehrmaliger Erinnerung und Fertigstellung dieses Berichts gingen umfangreiche Materialien ein, die ich für diesen Bericht noch nicht durcharbeiten konnte.

Ich werde das Bundesgesundheitsamt im Jahre 1981 einer Prüfung unterziehen.

3.11 Öffentliche Sicherheit, Verteidigung

3.11.1 Grenzen der informationellen Zusammenarbeit der Sicherheitsbehörden

3.11.1.1 Abriß der Problematik

Im demokratischen Rechtsstaat ist die staatliche Macht bewußt auf verschiedene Säulen verteilt. Machtkontrolle und Machtverteilung sind Eckpfeiler unserer demokratischen Ordnung. Unsere Rechtsordnung kennt neben der klassischen Dreiteilung der Staatsgewalt eine Vielzahl von Befugnisnormen, in denen, abgestimmt auf den jeweiligen Aufgabenbereich, Bürgerrecht und Staatsmacht in ein ungefähres Gleichgewicht gebracht sind.

Ein unverzichtbares Element dieses Gleichgewichts ist, grob gesagt, daß der Staat, insbesondere eine einzige staatliche Stelle, nicht alles über den Bürger wissen darf. Der staatliche Informationsanspruch ist eingebunden und gezügelt durch spezifische Kompetenzen und Befugnisse, die ihrerseits an der Aufgabenerfüllung orientiert sein müssen. Gewöhnlich werden diese Zusammenhänge unter dem Stichwort „informationelle Gewaltenteilung" diskutiert.

Die moderne Technik der Informationsverarbeitung droht diesen Rahmen zu sprengen. „Bandabgleich", „Gegenlauf", „Online-Anschluß", um nur einige gängige elektronische Verarbeitungsmethoden zu nennen, ermöglichen dort kompletten Informationsausgleich in kurzer Zeit, wo früher immenser Zeitaufwand nötig gewesen wäre. Die moderne Informationstechnologie hat jedenfalls die *technischen* Probleme eines umfassenden innerstaatlichen Informationsaustausches über den Bürger beseitigt. Umso mehr muß nunmehr darauf geachtet werden, daß die rechtlichen Sicherungen gegen ungehemmten Informationsaustausch zwischen den verschiedenen staatlichen Stellen verstärkt werden. Auch ein so traditionelles Institut wie die *Amtshilfe* bedarf vor dem Hintergrund dieser Entwicklung der weiteren rechtlichen Durchdringung. Die Amtshilfe ist ein subsidiäres Institut, das dort zum Tragen kommt, wo jenseits des geschriebenen Rechts im Einzelfall die ergänzende Hilfe einer Behörde für eine andere notwendig ist. Dies läßt deutlich werden, daß der gesetzlich geregelte Datenschutz als lex specialis Vorrang genießt.

Auch wenn also die Voraussetzungen für eine Amtshilfe vorliegen mögen, so ist damit nur ein allgemeiner Rechtmäßigkeitsrahmen gegeben. Daneben müssen zusätzlich die spezifischen datenschutzrechtlichen Bestimmungen eingehalten werden. Diese verlangen, wenn die Amtshilfe in der Übermittlung personenbezogener Daten liegen soll, daß dies zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Empfängers liegenden Aufgaben im Rahmen der Befugnisse erforderlich ist.

Hier bestehen nun gerade im Bereich der Sicherheitsbehörden erhebliche Probleme.

In diesem Bereich stellt praktisch jeder Schritt der Verarbeitung personenbezogener Daten, insbesondere die Übermittlung, eine Belastung des Betroffenen und damit einen Eingriff in eine grundrechtlich geschützte Position dar. So können durch Informationsaustausch zwischen Ämtern für Verfassungsschutz und anderen Behörden erhebliche Nachteile für die Betroffenen verursacht werden, z. B. bei Bewerbungen um Einstellung in den öffentlichen Dienst. Durch Übermittlung an Polizeibehörden können strafrechtliche Ermittlungsverfahren oder polizeiliche Maßnahmen gegen die Betroffenen ausgelöst werden. Schon die Registrierung von Handlungen und Äußerungen bei staatlichen Behörden kann einen Einschüchterungseffekt haben und damit Grundrechte beeinträchtigen. Staatliche Maßnahmen, die solche Wirkungen haben, können nicht durch das Gebot der Amtshilfe gerechtfertigt werden; dieses begründet nur eine Pflicht der Behörden untereinander, sich zu unterstützen, aber keine Eingriffsbefugnisse im Verhältnis von Staat und Bürger. Dafür bedarf es anderer gesetzlicher Grundlagen. Diese sind in den für die jeweilige staatliche Aufgabe einschlägigen Gesetzen zu finden. Soweit diese Vorschriften des besonderen Verwaltungsrechts keine entsprechenden Ermächtigungen enthalten, sind Maßnahmen der Datenverarbeitung ebensowenig zulässig wie andere Verwaltungshandlungen. § 10 BDSG reicht zur Rechtfertigung deshalb nicht aus, weil er die Bedingungen rechtmäßigen Verwaltungshandelns nicht nennt, sondern nur auf sie verweist und damit die jeweiligen Spezialbestimmungen implizit in Bezug nimmt.

BND und MAD arbeiten außerhalb des Anwendungsbereichs des Gesetzes zu Artikel 10 GG (G 10) bekanntlich ohne gesetzliche Grundlage. Dies wirft grundsätzliche Rechtsfragen nicht nur bei der Datenübermittlung an BND und MAD, sondern auch bei der übrigen Tätigkeit der beiden Dienste, etwa der eigenen Datenerhebung und Datenspeicherung auf (s. u. 3.11.4 und 3.11.6).

Es bleibt zu hoffen, daß der 9. Deutsche Bundestag aus der Arbeit des Untersuchungsausschusses zur Abhöraffäre Strauß/Scharnagl die Konsequenz zieht, die informationelle Amtshilfe für beide Dienste restriktiv gesetzlich zu regeln und für die Datenverarbeitung beider Dienste ebenfalls klare Bestimmungen zu schaffen.

Ein weiteres gravierendes Problem ergibt sich aus folgendem:

Das Bundesamt für Verfassungsschutz (BfV) verfügt zwar in Form von § 3 Abs. 3 Satz 2 BVerfSchG über eine Befugnisnorm zur Speicherung personenbezogener Daten im Rahmen der Aufgabenerfüllung. Aus § 3 Abs. 3 Satz 1 BVerfSchG erwachsen aber andere bedeutende Grenzen der Amtshilfe für das BfV. Dort ist nämlich bestimmt, daß dem BfV keine polizeilichen Befugnisse oder Kontrollbefugnisse zustehen. Gleichsam als zusätzliche Sicherung ist in § 3 Abs. 3 Satz 3 ein Anschluß des BfV an eine polizeiliche Dienststelle verboten (vgl. auch 1. TB S. 27 und 2. TB S. 44).

Diese Restriktionen gehen zurück auf den sog. Alliierten Polizeibrief, in dem der Bundesrepublik Deutschland nach den Erfahrungen des Dritten Reiches die strikte Trennung von Polizei und Nachrichtendiensten vorgeschrieben worden war. Da die Alliierten in ihrem Genehmigungsschreiben zum Grundgesetz auf diesen Polizeibrief ausdrücklich Bezug genommen haben, darf von Verfassungs wegen von der Möglichkeit des Artikel 87 Abs. 1 Satz 2 GG, Zentralstellen für Zwecke des Verfassungsschutzes zu errichten, nur in einer Form Gebrauch gemacht werden, die dem Trennungsgebot Rechnung trägt.

Das Trennungsgebot will dem Verfassungsschutz nicht nur polizeiliche Befugnisse vorenthalten, es bezieht sich auch auf die bei Anwendung derartiger Befugnisse gewonnenen Informationen. Die Anwendung polizeilicher Befugnisse geschieht nicht um ihrer selbst willen. In aller Regel soll sie der Gewinnung von Informationen dienen. Es würde deshalb auf eine Aushöhlung des Trennungsgebots hinauslaufen, wenn dem Verfassungsschutz zwar die Anwendung von polizeilichen Befugnissen verboten wäre, der Zugang zu Informationen, die bei der Anwendung dieser Befugnisse gewonnen werden, aber offen wäre.

Es dürfte deshalb kaum bestreitbar sein, daß gezielte Amtshilfeersuchen des BfV, die auf die Anwendung polizeilicher Befugnisse gerichtet sind, einen Verstoß gegen das Trennungsgebot darstellen würden und damit rechtswidrig wären, denn stets

handelt es sich hierbei um Erkenntnisse, die mittels polizeilicher Befugnisse und für die Erfüllung polizeilicher Aufgaben gewonnen wurden. Vor dem Hintergrund dieser Rechtslage bedarf die Praxis der Grenzüberwachung zugunsten der Nachrichtendienste der gründlichen Durchforstung. In diesem Zusammenhang wird auch ganz allgemein die Frage zu erörtern sein, unter welchen Kriterien die Anordnung von Grenzüberwachungsmaßnahmen zulässig ist.

Etwas schwieriger liegen die Dinge, wenn die Polizei im Rahmen eigener Aufgabenerfüllung ihre Befugnisse einsetzt und hierbei Kenntnisse erlangt, die auch für das BfV von Interesse sind. Schon wegen der großen Mißbrauchsgefahr wird man die Weitergabe derartiger „Zufallsfunde" nicht von vornherein für unbedenklich halten können. Möglicherweise ist hier eine Lösung analog § 7 Abs. 3 G 10 denkbar. Die dort genannten Straftaten hat der Gesetzgeber offenbar als derart gravierend angesehen, daß das Interesse an ihrer Verhinderung oder Aufklärung und Verfolgung die Bedenken gegen die Art der im Bereich des G 10 praktizierten Informationsgewinnung überwiegt. Soweit das BfV an der Vorfeldaufklärung derartiger Straftaten beteiligt ist, ließe sich also an eine analoge Heranziehung des dem § 7 Abs. 3 G 10 zugrundeliegenden Rechtsgedankens denken (vgl. auch schon 1. TB S. 24). Entsprechendes wäre umgekehrt für Übermittlungen des BfV an die Polizei zu erwägen.

Was im Vorstehenden für das BfV ausgeführt wurde, gilt über den Wortlaut von § 3 Abs. 3 Satz 3 BVerfSchG hinaus selbstverständlich auch für MAD und BND (vgl. dazu auch 1. TB S. 25).

Die vom Bundesminister des Innern zur Amtshilfeproblematik gehörten Sachverständigen sind zu recht unterschiedlichen Ergebnissen gelangt. Einigkeit besteht aber wohl bei allen mit der Materie Befaßten darin, daß die Sonderanweisung Grenzkontrolle (SoGK), in der die bisherige Form der Amtshilfe des BGS geregelt ist, in diesem Umfang nicht fortgeführt werden kann. Aufgrund einiger Presseberichte der jüngsten Vergangenheit konnte in der Öffentlichkeit der Eindruck entstehen, als werde die SoGK derzeit kaum mehr angewandt. Ich mußte bei meinen Kontrollen aber feststellen, daß die wesentlichen Teile der SoGK nach wie vor praktiziert werden. Um so mehr ist deshalb darauf zu drängen, daß die SoGK tatsächlich, wie angekündigt, umgehend außer Kraft gesetzt wird. An der Erarbeitung einer Nachfolgeregelung bin ich beteiligt. Für die rechtliche Beurteilung dieser Neufassung wird es zunächst einmal darauf ankommen, den BGS von mehr oder weniger pauschalen Massenmeldungen zu entlasten, die zur Aufgabenerfüllung nicht erforderlich erscheinen und letztlich auf eine Vorratsspeicherung bei den Diensten hinauslaufen könnten.

Ferner muß sichergestellt sein, daß der BGS seine Befugnisse ausschließlich im Rahmen seiner grenzpolizeilichen Aufgaben einsetzt. Kontrollen und Durchsuchungen für die Dienste im Wege der Amtshilfe verstoßen gegen § 3 Abs. 3 Satz 3 BVerfSchG. Lediglich die Erkenntnisse, die anläßlich solcher unter rein grenzpolizeilichen Gesichtspunkten vorgenommenen Kontrollen gewonnen werden, können in dem oben angedeuteten Rahmen an die Dienste weitergeleitet werden. An der Gewährleistung dieses Grundsatzes muß jede Nachfolgeregelung für die SoGK gemessen werden.

Die Nachfolgeregelung der SoGK muß vor allem wesentlich präziser gefaßt werden. Sonst bestünde die Gefahr, daß auslegungsfähige Begriffe noch im Geiste der SoGK ausgelegt und angewandt würden.

Im übrigen ist in diesem Zusammenhang auch für eine ordnungsgemäße Verankerung der Amtshilfe des BGS für die Nachrichtendienste im Bundesgrenzschutzgesetz sowie im BVerfSchG zu sorgen.

Generell ist aus datenschutzrechtlicher Sicht eine möglichst zurückhaltende Zusammenarbeit zum Zwecke der Informationsbeschaffung zu fordern. Es ist dem Verhältnis Bürger/Verwaltung in einem demokratischen Rechtsstaat abträglich, wenn der Bürger damit rechnen muß, daß die einer Behörde in einem ganz bestimmten Zusammenhang gegebenen Informationen im Wege der Amtshilfe in den Unterlagen einer ganz anderen Behörde und in einem ganz anderen sachlichen Zusammenhang auftauchen.

3.11.1.2 Zur Frage meiner Kontrollkompetenz im G 10-Bereich

Sowohl im letzten Jahr als auch in diesem Jahr habe ich beim BND, in diesem Jahr auch beim MAD (im einzelnen s. u. 3.11.4, 3.11.6) Kontrollen im Bereich der Tätigkeit dieser Dienste nach dem G 10 durchgeführt. Beide Dienste haben zwar meine Kontrollkompetenz bestritten, weil der Gesetzgeber eine eigene, quasi-richterliche Funktion ausübende Kontrollinstanz mit der G-10-Kommission geschaffen habe (Art. 10 Abs. 2 Satz 2 GG i. V. m. § 9 Abs. 2—4 G 10), die ausschließlich für die Kontrolle der G-10-Tätigkeit zuständig sei. Dennoch wurde mir die Prüfung zunächst im jeweils gewünschten Umfang gestattet.

Inzwischen hat mich aber der BMI als für das G 10 und das BDSG zuständiger Minister um eine gemeinsame Klärung dieser Rechtsfrage gebeten und unter Anführung der vorstehenden Argumente ebenfalls Zweifel an meiner Kontrollkompetenz im G 10-Bereich geäußert. Erste Konsequenzen zeigten sich bei meinem zweiten Prüfungsbesuch beim BND im vergangenen Jahr: dort wurde mir unter Hinweis auf die noch nicht geklärte Kompetenzfrage die datenschutzrechtliche Prüfung der strategischen Telefonkontrolle nach § 3 G 10 verweigert (s. u. 3.11.4.4). Ich halte diese Zweifel nicht für begründet.

Meine gegenteilige Auffassung begründe ich wie folgt:

Nach § 19 Abs. 1 BDSG kontrolliere ich die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz bei „den in § 7 Abs. 1 genannten Behörden und sonstigen öffentlichen Stellen des Bundes, ausgenommen die Gerichte, soweit sie nicht in Verwaltungsangelegenheiten tätig werden".

Daraus ergibt sich, daß alle Behörden und sonstigen öffentlichen Stellen des Bundes der datenschutzrechtlichen Kontrolle des Bundesbeauftragten unterstellt sind; die Ausnahme in § 19 Abs. 1 betrifft nur die Gerichte, soweit sie Spruchtätigkeit ausüben. Die Ausnahme ist ausschließlich. Dies ergibt sich auch aus § 19 Abs. 3 BDSG, der gerade voraussetzt, daß grundsätzlich auch Sicherheitsbehörden und Nachrichtendienste unter die Kontrolle fallen.

Die Kontrolle bezieht sich auf die Einhaltung des BDSG und „anderer Vorschriften über den Datenschutz". Andere Vorschriften über den Datenschutz sind auch die Bestimmungen des Gesetzes zu Artikel 10 GG, insbesondere §§ 2, 3 und 7.

Nach Artikel 10 Abs. 2 Satz 2 GG tritt „an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane". Andere Nachprüfungsmöglichkeiten als der Rechtsweg werden dadurch nicht ersetzt. Die spezielle Kontrolle durch den Bundesbeauftragten für den Datenschutz wird durch Artikel 10 Abs. 2 GG ebensowenig ausgeschlossen wie die Aufsichtsbefugnisse der Fach- und Dienstaufsichtsbehörden (Bundeskanzleramt für BND, Bundesminister der Verteidigung für MAD). Die Kommission soll die fehlende richterliche Kontrolle ausgleichen; die Ausnahmeregelung des Artikels 10 Abs. 2 Satz 2 GG soll sicherstellen, daß der Betroffene nicht im Rahmen einer gerichtlichen Nachprüfung Kenntnisse erlangt, die ihm um des Schutzes der freiheitlichen demokratischen Grundordnung willen vorenthalten werden müssen. Eine Bekanntgabe an den Betroffenen ist bei meiner Kontrolle — anders als bei gerichtlicher Überprüfung, aber ebenso wie bei der fach- und dienstaufsichtlichen Kontrolle — nicht nur nicht vorgeschrieben, sondern durch die Geheimhaltungspflicht, die mir insofern auferlegt ist, ausgeschlossen.

Wenn das Gesetz zu Artikel 10 GG dem Betroffenen in engem Rahmen den Rechtsweg wieder eröffnet (§ 5 Abs. 5), so ist daraus nicht etwa zu folgern, daß dann andere Kontrollmöglichkeiten entfielen. Vielmehr ist davon auszugehen, daß der Rechtsweg nach Artikel 19 Abs. 4 GG sonst (wenn die Einschränkung nach Artikel 10 Abs. 2 Satz 2 GG nicht gilt) gegen jede Rechtsverletzung eröffnet ist. Neben dem Rechtsweg aber besteht die Kontrollbefugnis des Bundesbeauftragten für den Datenschutz; dies ist in anderen Bereichen noch nie angezweifelt worden.

Meine Nachprüfungsbefugnis ist also weder Ersatz einer gerichtlichen Kontrolle noch durch Ausschluß gerichtlicher Kontrolle mit ausgeschlossen. § 21 BDSG gibt ausdrücklich jedermann das Recht, sich an mich zu wenden, wenn er der Ansicht ist, daß eine Bundesbehörde oder sonstige öffentliche Stelle des Bundes seine schutzwürdigen Belange bei der Verarbeitung personenbezogener Daten verletzt hat. Eine Ausnahme für die Nachrichtendienste ist nicht vorgesehen. Der Betroffene hat daher die Möglichkeit, eine Überprüfung durch mich ohne Rücksicht darauf zu beantragen, ob eine gerichtliche Überprüfung zulässig ist oder nicht. (Eine ganz andere Frage ist es, ob bei der datenschutzrechtlichen Überprüfung durch mich Rücksicht auf ein etwa schwebendes Verfahren zu nehmen wäre).

Eine „Doppelkontrolle" (durch die G 10-Kommission und den Bundesbeauftragten für den Datenschutz) ist auch sinnvoll, weil

— Nachrichtendienste der Eigenkontrolle der Betroffenen entzogen sind (Auskunftsverweigerungsrecht nach § 13 Abs. 2 in Verbindung mit § 12 Abs. 2 Nr. 1 BDSG) und

— die G 10-Kommission wohl nicht die Möglichkeiten und Mittel hat, die technischen Aspekte der Datenverarbeitung bei den Diensten zu prüfen.

§ 19 Abs. 3 Satz 4 BDSG gibt der zuständigen obersten Bundesbehörde die Ermächtigung, meine Prüfungsbefugnisse nach § 19 Abs. 3 einzuschränken. Dazu muß im *Einzelfall* festgestellt werden, daß meine Einsicht in Unterlagen und Akten die Sicherheit des Bundes oder eines Landes gefährdet. Die Kontrollbefugnis kann aber nach dieser Bestimmung nicht generell eingeschränkt werden.

3.11.1.3 Allgemeine Prüfung einiger ausgewählter Fälle bei den Sicherheitsbehörden

Um meine Kenntnisse und meinen Überblick über polizeiliche Fahndungsmethoden sowie den hier stattfindenden Datenaustausch zu erweitern, habe ich im Berichtsjahr einige ausgewählte Fälle aus der *Grenzfahndung* näher untersucht. Die Fälle waren nach dem Zufallsprinzip ausgesucht. Ich habe mir die Ermittlungsakten beim Bundeskriminalamt vorlegen lassen und hiervon ausgehend die Akten bei den Nachrichtendiensten herangezogen, sofern dort welche geführt wurden. Bei den untersuchten Fällen handelte es sich um je fünf Fälle aus dem Spionage- und aus dem Extremismusbereich. Die Fälle gaben keinen Grund zu Beanstandungen.

3.11.2 Bundeskriminalamt

3.11.2.1 INPOL-Neukonzeption

In dem zuständigen Gremium der Innenminister des Bundes und der Länder wurde in diesem Jahr ein neuer Entwurf über Grundlinien für einen sogenannten Kriminalaktennachweis (KAN) beraten. Er soll nunmehr als erstes Teilstück der im letzten Jahr bereits diskutierten Gesamtneukonzeption des INPOL-Systems (s. 2. TB S. 47) verwirklicht werden.

Der KAN soll nach den amtlichen Erläuterungen einen Gesamtnachweis aller Kriminalakten darstellen, die vorhanden sind oder künftig im Rahmen der KpS-Richtlinien (hierzu s. u. 3.11.2.2) angelegt werden. Dabei wird zwar bezüglich des Zugriffs zwischen regional und überregional bedeutsamen Vorgängen differenziert, um zu verhindern, daß nichtberechtigte Stellen Kenntnis von Daten erhalten, die für sie unnötig sind. Doch soll der Gesamtnachweis aller kriminalpolizeilichen Akten des Bundes und der Länder physikalisch voll im BKA geführt werden mit der Folge, daß er für das BKA faktisch jederzeit zugriffsfähig wäre. Aus der beabsichtigten Zielsetzung und der Auskunftsregelung ergibt sich außerdem, daß der KAN entgegen seiner Bezeichnung offenbar weit mehr als ein reiner Aktennachweis sein soll. Er soll es insbesondere von Anfang an

ermöglichen, die Verbrechensbekämpfung zu erleichtern und zu unterstützen. Das ist für die Polizei mit Sicherheit ein legitimes Anliegen. Die Frage ist jedoch, wo die verfassungsmäßigen und datenschutzrechtlichen Grenzen eines Vorhabens wie des KAN liegen.

Bei dem mir im Sommer zugeleiteten Konzept handelt es sich zwar nur um einen Grundriß des beabsichtigten KAN, doch sind hier bereits Tendenzen erkennbar, gegen die ich z. T. erhebliche Bedenken habe. Diese habe ich dem BMI in ausführlichen Stellungnahmen vorgetragen.

Kritisch erscheint in erster Linie die physikalische Verfügbarkeit des gesamten Nachweises beim und für das BKA. Der Vorteil einheitlicher, zentraler Auskunftsmöglichkeit und besserer Datenpflege (insbesondere Korrektursicherheit) wiegt dieses Risiko nicht auf. Die eingebende Stelle muß ohnehin auf jeden Fall für die Datenpflege primär verantwortlich bleiben. Mit der Speicherung an verschiedenen Stellen muß der Bürger auch in anderen Bereichen rechnen. Bei der Polizei wird er in der Regel auch vermuten können, welche Behörde noch Daten über ihn besitzen könnte (z. B. bei direktem Kontakt mit einer bestimmten Polizeibehörde anläßlich einer Durchsuchung usw.). Die Möglichkeit einheitlicher zentraler Auskunft kann nicht die Erforderlichkeit zentraler Speicherung begründen. Die einheitliche Auskunft wäre nur die Folge rechtlich zulässiger und faktisch erforderlicher zentraler Speicherung, nicht umgekehrt. Sonst müßte man alle rechtlichen Schranken für die Zulässigkeit der Speicherung und Übermittlung personenbezogener Daten aufgeben bzw. von der Wünschbarkeit zentraler Auskunftsregelungen abhängig machen. Die „zentralistische" Konzeption ist aber sowohl mit den einfach-rechtlichen Regelungen des BKAG als auch insbesondere mit den verfassungsrechtlichen Prinzipien der Erforderlichkeit und der Verhältnismäßigkeit unvereinbar. Hierauf habe ich bereits letztes Jahr in Übereinstimmung mit der Erklärung der Datenschutzbeauftragten des Bundes und der Länder vom November 1979 hingewiesen (vgl. 2. TB S. 47).

Die physikalische Zentralisierung kann auch nicht als Auftragsdatenverarbeitung nach § 8 BDSG gerechtfertigt werden. Das Verhältnis des BKA zu den Polizeien der Länder und der Umfang der zulässigen Speicherung beim BKA in diesem Zusammenhang werden ausschließlich vom BKAG als bereichsspezifischem Recht geregelt. Es hat dem BKA eigenständige Aufgaben übertragen, mögen diese auch in einem weiteren Sinne die Tätigkeit der Landespolizeibehörden unterstützen.

Daher ist in Übereinstimmung mit den Dateienrichtlinien (s. u. 3.11.2.2) davon auszugehen, daß das BKA für INPOL (ebenso wie das BfV für NADIS) zumindest auch (neben den eingebenden Landesbehörden) selbst *speichernde Stelle* ist. Die primäre Verantwortlichkeit der eingebenden Polizeibehörden für die Richtigkeit und weitere Erforderlichkeit der erhobenen Daten begrenzt lediglich die Prüfungspflichten des BKA und meine korrespondierende Kontrollbefugnis, wie ich bereits im zweiten Tätigkeitsbericht näher dargelegt habe (s. 2 TB S. 43 f.).

Neben diesen grundlegenden Gesichtspunkten ist schon jetzt auf folgende weiteren Probleme hinzuweisen:

— Bei weiteren Planungen zum Aufbau eines (allein unter überregionalen Gesichtspunkten zulässigen) Aktennachweises für die Polizeien des Bundes und der Länder ist klar zu regeln, in welchem Umfang andere Polizeidienststellen, die nicht schwerpunktmäßig mit kriminalpolizeilichen Aufgaben betraut sind, angeschlossen werden dürfen. M. E. kann dies nicht über die aktuellen Personen- und Sachfahndungen hinausgehen. Ein unmittelbarer Zugriff auf kriminalpolizeiliche Erkenntnisse bzw. Fundstellenhinweise steht der Schutzpolizei nicht zu.

— Es müssen für den Sachbearbeiter auch klare Kriterien entwickelt werden, nach denen er zwischen regionaler und überregionaler Bedeutung differenzieren muß. Sollte sich dies als zu schwierig erweisen, wird man die Regel „Im Zweifel nur regionale oder gar nur örtliche Speicherung" zugrunde legen müssen. Eine Abschichtung, die pauschal bei erkennungsdienstlicher Behandlung zentrale Registrierung zuließe (so der mir im Sommer vorgelegte Entwurf), wäre abzulehnen, weil erkennungsdienstliche Maßnahmen zum Beispiel auch gegenüber nicht tatverdächtigen Personen im Strafverfahren möglich sind und weil die Unterlagen nach Feststellung der Identität zu vernichten sind (§§ 163 b, 163 c Abs. 4 StPO).

Solche Unterlagen dürften nicht oder allenfalls in besonderen Ausnahmefällen in einer Zentraldatei gespeichert werden. Das gleiche gilt erst recht für erkennungsdienstliche Maßnahmen im Zusammenhang mit der Aufklärung von Ordnungswidrigkeiten, soweit sie überhaupt für zulässig erachtet werden könnten. Hierauf habe ich den Bundesminister des Innern im Zusammenhang mit den m. E. insoweit ebenfalls klärungsbedürftigen bundeseinheitlichen Richtlinien über erkennungsdienstliche Unterlagen hingewiesen.

In diesem Zusammenhang ist auch festzustellen, daß die gegenwärtig offenbar in großem Umfang vorgenommenen erkennungsdienstlichen Maßnahmen bei Asylbewerbern nach der gegenwärtigen Rechtslage nicht in einem polizeilichen Zentralregister mit Zugriff für alle angeschlossenen Polizeidienststellen zentral aufbewahrt werden dürfen. Auch hierauf habe ich den Bundesminister des Innern aufmerksam gemacht.

Ich halte es nicht für vertretbar, das bisher vorgelegte Konzept ohne deutliche Abstriche zu verwirklichen, und befinde mich mit dieser Auffassung in Übereinstimmung mit den Landesbeauftragten für den Datenschutz.

Auch ist nochmals zu betonen, daß ein Ausbau von INPOL durch Installierung genereller Zugriffsmöglichkeiten auf Dateien anderer Behörden ohne klare Rechtsgrundlage größten Bedenken begegnet (vgl. 2. TB S. 47 und oben 3.9.1.5). Diese Bedenken gelten selbstverständlich nicht nur, wenn ein Online-Anschluß durch Einrichtung von Datensichtstationen

erfolgt. Eine Übermittlung des Gesamtbestandes im jeweils dem Zugriff eröffneten Umfang ist vielmehr auch dann gegeben, wenn durch andere Verfahren (z. B. vermittels entsprechend geschaltetem Fernschreiber) eine ständige Abfrage ohne zwischengeschaltete Prüfungsmöglichkeit der übermittelnden Dienststelle gegeben ist. Auch dies kommt einem Bereithalten zur Einsichtnahme bzw. zum Abruf i. S. von § 2 Abs. 2 Nr. 2 BDSG gleich. Die Schnelligkeit eines solchen Verfahrens (sog. Antwort-Zeit-Verhalten) spielt für diese Beurteilung keine Rolle.

3.11.2.2 Dateienrichtlinien für das BKA und Richtlinien über Kriminalpolizeiliche Sammlungen (KpS)

Für das Bundeskriminalamt und auch die meisten anderen Landeskriminalämter wurden inzwischen die KpS-Richtlinien i. d. F. vom März 1979 in Kraft gesetzt. In meinem 2. Tätigkeitsbericht (S. 45) habe ich diese Richtlinien als einen erheblichen Fortschritt gegenüber den früheren Regelungen bezeichnet. Wie dort ebenfalls berichtet, hat sich der „Arbeitskreis Sicherheit" der Datenschutzbeauftragten des Bundes und der Länder unter meinem Vorsitz in mehreren Sitzungen mit diesen Richtlinien befaßt, um weitere Verbesserungen des bereichsspezifischen Datenschutzes im Bereich der Polizeibehörden des Bundes und der Länder zu erreichen.

Der „Arbeitskreis Sicherheit" hat sich gleichzeitig auch mit dem Entwurf von Richtlinien für die Errichtung und Führung von Dateien über personenbezogene Daten beim Bundeskriminalamt (Dateienrichtlinien) befaßt. Ich habe das Ergebnis dieser Beratungen dem Bundesminister des Innern mitgeteilt und dabei betont, daß ich die Dateienrichtlinien grundsätzlich positiv beurteile.

Die mir zugeleiteten Entwürfe der Dateienrichtlinien sehen wie die KpS-Richtlinien vor, daß dem Betroffenen Auskunft über gespeicherte Daten zu erteilen ist, wenn eine Abwägung der Belange des Betroffenen gegenüber dem Sicherheitsinteresse der Polizeibehörden zugunsten des Betroffenen ausfällt. Auf dem Auskunftsverweigerungsrecht nach § 13 Abs. 2 BDSG wird also nicht mehr generell beharrt. Im übrigen hat das Bundeskriminalamt bisher in den meisten Fällen den Betroffenen auf ihren Antrag hin Auskunft erteilt.

Weiterhin ist zu begrüßen, daß in den Dateienrichtlinien festgelegt wurde, daß das Bundeskriminalamt auch speichernde Stelle bei den Verbunddateien (z. B. INPOL) ist und damit auch für die durch die anderen Teilnehmer des Informationssystems eingestellten Datensätze mitverantwortlich ist (vgl. hierzu auch 2. TB S. 44).

Künftig sind für Dateien des BKA Errichtungsanordnungen zu erstellen, in denen neben dem Umfang der Informationsverarbeitung auch die Rechtsgrundlagen für die Zulässigkeit der Speicherung von Daten anzugeben sind.

In meiner vorgenannten Stellungnahme habe ich aber u. a. folgende Bedenken geltend gemacht:

— Die Übermittlung von Daten an andere Behörden ist in zu weitem Umfang zugelassen, insbesondere soweit es sich um Nachrichtendienste und ausländische Stellen handelt (s. o. 3.11.1.1).

— Bei den Löschungsfristen ist nicht genügend differenziert worden.

— Die in den Dateienrichtlinien vorgesehenen Regelungen über den Abgleich von Daten mit anderen Behörden können selbstverständlich nichts an meiner Auffassung ändern, daß eine gesetzliche Klarstellung für die Rasterfahndung (Näheres s. u. 3.11.2.4) dringend erforderlich ist; diese wird durch die Bestimmung in den Richtlinien nicht ersetzt.

Da die Dateienrichtlinien die KpS-Richtlinien ergänzen sollen, gelten Bedenken gegen zu weitgehende Ermächtigungen für beide Regelwerke. Daher dürfen Verbesserungen bei den Dateienrichtlinien nicht durch weniger datenschutzfreundliche Formulierungen in den KpS-Richtlinien wieder zurückgenommen werden.

Der Bundesminister des Innern hat zugesagt, meine Änderungsvorschläge nochmals in die weiteren Beratungen mit einzubeziehen.

3.11.2.3 BKA-Datei „Bundestagswahlkampf"

Als erster Anwendungsfall der Dateienrichtlinien für das Bundeskriminalamt wurde mir die Errichtungsanordnung für die bis zum 5. Oktober 1980 geführte Datei „Bundestagswahlkampf" übersandt. Eine erste Auswertung dieser Errichtungsanordnung zeigte, daß eine Beurteilung aus datenschutzrechtlicher Sicht über die Art der gespeicherten Daten und über den Datenfluß allein aus dieser Errichtungsanordnung noch nicht möglich war, so daß ich Ergänzungsfragen stellen mußte. Errichtungsanordnungen für andere Dateien sollten deshalb künftig noch genauer abgefaßt werden.

In einem Informationsgespräch mit der Abteilung Sicherungsgruppe des BKA, die die Datei betrieb und alleinigen direkten Zugriff auf diese Datei hatte, habe ich mich vor Ort über die Datei „Bundestagswahlkampf" informiert. Es handelte sich in erster Linie um eine Übersicht der Wahlkampftermine der durch die Sicherungsgruppe zu schützenden Personen. Eingestellt wurden aber auch Personen, die eine mögliche Gefährdung dieses Personenkreises bedeuten konnten. Die Datei „Bundestagswahlkampf" wurde bis zum Wahltermin genutzt. Inzwischen ist eine Auswertung der angefallenen Daten erfolgt mit dem Ziel, über den vergangenen Bundestagswahlkampf hinaus wichtige Informationen in anderen polizeilichen Systemen zu speichern. Die Datei „Bundestagswahlkampf" selbst wurde bis zum 31. Dezember 1980 gelöscht.

3.11.2.4 BKA-Rasterfahndung

Kurz nach Abgabe meines zweiten Tätigkeitsberichtes wurde bekannt, daß das Landeskriminalamt Hamburg mit Unterstützung des Bundeskriminalamtes im Rahmen eines sogenannten „Energieprogrammes" Rasterfahndungen durchgeführt hat. Hierbei wurde eine große Anzahl von Daten der

Hamburgischen Electricitätswerke (HEW) benutzt. Ich habe diese Fahndungsmaßnahme im Rahmen meiner Kontrollzuständigkeit geprüft und folgendes festgestellt:

Aufgrund konkreter Verdachtsgründe vermuteten die Strafverfolgungsbehörden, daß sich der (in Zürich festgenommene) mutmaßliche Terrorist Rolf-Clemens Wagner in Hamburg aufgehalten hatte und daß dort weitere Hinweise für die Terroristenfahndung vorhanden seien. Die Polizei wollte nun versuchen, die von Wagner genutzte Wohnung durch die Auswertung der Stromabrechnungsdaten herauszufinden.

Sie hat die dazu benötigten Daten (und keine weiteren) von den HEW aufgrund eines Beschlagnahmebeschlusses des Ermittlungsrichters beim Bundesgerichtshof erhalten, und zwar in der Form eines Magnetbandes. Die HEW hatten die betreffenden Namen und Anschriften vorher aus ihrem Datenbestand herausgesucht und auf dieses Band überspielt. Das Band wurde dem BKA in Wiesbaden übersandt, wo die Namen und Anschriften in eine andere, für die Ermittlungszwecke besser geeignete Reihenfolge gebracht wurden. Das Ergebnis wurde in einer Liste ausgedruckt. In dieser Liste wurde eine größere Anzahl von Datensätzen gestrichen, weil sie von vornherein nicht für die weitere Ermittlung in Betracht kamen. Die übrigen Datensätze wurden in mehreren Schritten immer weiter gefiltert (gerastert). Insbesondere wurden die Anschriften mit dem Einwohnermelderegister verglichen. Die relevanten Datensätze wurden ausgedruckt. Hinsichtlich der darin bezeichneten Personen wurde mit den üblichen kriminalistischen Methoden ermittelt, d. h. in erster Linie durch Befragung der Zahlungspflichtigen und anderer möglicher Auskunftspersonen. Es wurden aber keine weiteren Datenbestände zum Vergleich herangezogen. Umgekehrt sind die Namen der Stromzahler auch nicht etwa in eine polizeiliche Datei aufgenommen worden — sie waren nicht als Verdächtige von Interesse, sondern allenfalls als Hinweisgeber, die ihrerseits über die Identität der Wohnungsnehmer im unklaren waren.

Da schließlich in keinem Fall Verdachtsmomente auftauchten, wurde das benutzte Band an die HEW zurückgegeben und das zur Umsortierung verwandte BKA-Band gelöscht. Die Listen mit den ausgedruckten Namen und Anschriften wurden vernichtet. Ich habe mich hiervon sowohl an Hand der Akten und durch Befragung des verantwortlichen Personals als auch durch Prüfung der gelöschten Datenträger und Abfragen in den polizeilichen Dateien des BKA überzeugt. In keinem der bisher rund 30 Beschwerdefälle wurde eine Speicherung festgestellt. Selbstverständlich habe ich auch die unter Geheimschutz fallenden Unterlagen eingesehen.

Da es sich bei den Rasterfahndungen um ein länderübergreifendes Problem handelt und ähnliche Maßnahmen in verschiedenen Bundesländern durchgeführt wurden, haben sich auch die jeweils zuständigen Landesbeauftragten für den Datenschutz mit dieser Problematik befaßt. Die Rasterfahndung war auch Gegenstand einer Konferenz der Datenschutzbeauftragten des Bundes und der Länder in München. Die Konferenz kam zu dem Ergebnis, daß die von den Datenschutzbeauftragten geprüften Fahndungsmaßnahmen keine Anlässe für Beanstandungen ergeben haben, daß aber die sehr allgemein gehaltenen Bestimmungen der Datenschutzgesetze sowie die Bestimmungen der Strafprozeßordnung den mit der Rasterfahndung verbundenen Problemen nicht gerecht werden. Die große Zahl der einbezogenen Personen, die Menge der verarbeiteten Daten und die dank der veränderten Informationsmethoden gegebenen Nutzungsmöglichkeiten erfordern vielmehr sehr präzise bereichsspezifische Regelungen.

Insbesondere ist zu regeln,

— zu welchen Zwecken solche Fahndungsmaßnahmen angewandt werden dürfen,

— welche tatsächlichen Voraussetzungen zu fordern sind,

— ob und in welchem Umfang bestimmte Datenarten nicht einbezogen werden dürfen (z. B. Sozialdaten),

— ob die Daten auch zu anderen Zwecken als zu der jeweiligen Fahndung verwendet werden dürfen,

— welche verfahrensmäßigen Sicherungen zu fordern sind (Löschung, Dokumentation, Kontrolle),

— wie eine umfassende datenschutzrechtliche Kontrolle durch die Datenschutzbeauftragten sichergestellt werden kann.

Im Anschluß an die Konferenz der Datenschutzbeauftragten des Bundes und der Länder habe ich mehrmals die unter Beteiligung des Bundeskriminalamtes durchgeführten Rasterfahndungsmaßnahmen daraufhin überprüft, ob die vorhandenen Unterlagen die vorgenannten Anforderungen an die verfahrensmäßigen Sicherungen erfüllen.

Das Ergebnis meine Prüfung habe ich im April dieses Jahres dem Bundesminister des Innern und nachrichtlich dem Bundesminister der Justiz mitgeteilt. In diesem Schreiben habe ich die von den Datenschutzbeauftragten des Bundes und der Länder erarbeiteten Forderungen auf der Grundlage meiner Prüferfahrungen präzisiert. Ich habe deutlich gemacht, daß die bestehenden Rechtsvorschriften auf die bei Rasterfahndung erfolgten Massenverarbeitungen von personenbezogenen Daten nicht passen, da sie vom Einzelfall ausgehen. Es bedarf somit gesetzlicher Klarstellungen, die eindeutig regeln, unter welchen Voraussetzungen und zu welchen Zwekken solche Maßnahmen zulässig sein können. Ich habe besonders darauf hingewiesen, daß eine rein verwaltungsinterne Eingrenzung dieser Fahndungsmaßnahmen, wie sie im Entwurf der Richtlinien für die Errichtung und Führung von Dateien personenbezogener Daten beim Bundeskriminalamt vorgesehen ist, hierfür nicht genügt und daß die Verwertung der bei der Rasterfahndung erlangten Erkenntnisse zu anderen Zwecken nur in besonders schweren Fällen zulässig sein kann. Auch hierfür sollten klare Regelungen geschaffen werden. Die von mir geprüfte verfahrensmäßige Sicherung dieser Fahndungs-

maßnahme hat ergeben, daß die Verfahrensdokumentation noch verbessert werden muß, wenn eine umfassende datenschutzrechtliche Prüfung gewährleistet sein soll. Ich habe deshalb dem Bundesminister des Innern umfangreiche und detaillierte Vorschläge für eine solche Verfahrensdokumentation unterbreitet. Eine abschließende Antwort auf meine Hinweise steht noch aus.

Mit dem Melderechtsrahmengesetz (s. o. 2.3) und den Bestimmungen des Sozialgesetzbuches (X. Buch) zum Schutz der Sozialdaten (s. o. 2.5) sind inzwischen auch erste gesetzliche Vorschriften verabschiedet, die die Nutzung bestimmter Arten von Daten für Rasterfahndungsmaßnahmen einschränken oder (bei Sozialdaten im engeren Sinne, insbesondere medizinischen Daten) ganz ausschließen.

3.11.2.5 Polizeiliche Beobachtung

In meinen bisherigen Tätigkeitsberichten (vgl. 1. TB S. 27 f., 2. TB S. 45) habe ich auf die rechtsgrundsätzlichen Probleme bei der polizeilichen Beobachtung (früher beobachtende Fahndung — Befa — genannt) hingewiesen. Die Speicherung personenbezogener Daten ist nur zur *rechtmäßigen* Aufgabenerfüllung zulässig. Dies setzt für die Polizei voraus, daß bei Eingriffsmaßnahmen wie der Erhebung und Speicherung von Daten im Rahmen der polizeilichen Beobachtung sowohl eine gesetzliche Aufgaben- als auch eine Befugniszuweisung vorliegt. Letztere erscheint jedoch nach wie vor zweifelhaft. Hieran vermag auch die neue Polizeiliche Dienstvorschrift (PDV) 3.84.2 nichts zu ändern, die für die Polizeibehörden des Bundes zum 1. Juli 1980 in Kraft gesetzt wurde.

Ich verkenne nicht, daß die PDV 384.2 gegenüber den früher geltenden Richtlinien erfreuliche Präzisierungen bringt. Doch ist damit keine Klärung der Rechtsgrundlagen erreicht. Die PDV 384.2 enthält leider keinerlei Hinweise auf die Rechtsvorschriften, die die in ihr angesprochenen und „geregelten" Maßnahmen — sei es im Rahmen der Gefahrenabwehr, sei es im Rahmen der Strafverfolgung — tragen sollen. Das Problem wird verschwiegen. Meiner Forderung nach Klärung der Fragen, die ich in einem Schreiben vom Januar 1980 zum Entwurf der PDV 384.2 gegenüber dem Bundesminister des Innern und nachrichtlich dem Bundesminister der Justiz vortrug, wurde nicht Rechnung getragen. Es besteht daher Anlaß, nochmals auf folgendes kurz hinzuweisen:

Für die polizeiliche Beobachtung im Rahmen der *Strafverfolgung* ist keine eindeutige Rechtsgrundlage in der StPO ersichtlich. Die verschiedentlich von BMI oder BMJ in Gesprächen angeführten §§ 161, 163 StPO scheiden m. E. aus. Nach wohl herrschender Meinung sind sie allein als Aufgabenumschreibung zu verstehen. Hierzu sei besonders auf die Ausführungen des Bundesministers der Justiz Dr. Vogel in NJW 1978, S. 1217 ff., 1225 f., verwiesen. Dort wird zu Recht gesagt, daß die Aufgabenzuweisungen an die *Staatsanwaltschaft* in den §§ 152, 160 StPO keine Eingriffsermächtigungen enthalten. Das muß aber in gleicher Weise, ja sogar erst recht für die Umschreibung nach § 163 StPO gelten. Die Anwendung der §§ 161, 163 StPO als Befugnisgrundlagen für polizeiliche Beobachtung zur Strafverfolgung würde darüber hinaus gerade die verkappte Einführung einer Generalklausel in das Strafverfahrensrecht bedeuten, die es nach den Ausführungen des Bundesministers der Justiz a. a. O. und bisher wohl unstreitiger Auffassung nicht gibt. Alles andere stünde auch mit der in Jahrzehnten gewachsenen Systematik der Spezialbefugnisse der StPO im Widerspruch. Danach wird stets zwischen Maßnahmen gegen Zeugen, Tatverdächtige, Nichttatverdächtige und Beschuldigte differenziert, während §§ 161, 163 StPO keine solchen Hinweise enthalten. Das ist auch verständlich, denn die Bedeutung der vorgenannten Bestimmungen liegt neben der Aufgabenumschreibung für die Polizei in § 163 StPO in erster Linie in der Abgrenzung des Verhältnisses der Staatsanwaltschaft zur Polizei und beider Strafverfolgungsorgane zu anderen Behörden.

Auch für die polizeiliche Beobachtung als Maßnahme der *Gefahrenabwehr* bleibt die Rechtslage ungeklärt. Sollte mit der neuen PDV 384.2 beabsichtigt sein, daß die polizeiliche Beobachtung insoweit allein unter den Voraussetzungen der Generalklausel (also bei einer konkreten Gefahr) stattfinden darf, dann hätte dies zumindest deutlich gesagt werden müssen. Abgesehen davon, erscheint es unverständlich, wenn nach wie vor eine so bedeutende und die Öffentlichkeit stark beschäftigende polizeiliche Maßnahme auf der Grundlage der polizeilichen Generalklausel durchgeführt werden soll, während eine Maßnahme wie die Platzverweisung mehr und mehr spezialgesetzlich geregelt wird (vgl. § 12 Musterentwurf Polizeigesetz).

Im Ergebnis muß ich daher feststellen, daß für die Maßnahme der polizeilichen Beobachtung, sei es zur Strafverfolgung, sei es für Zwecke der Gefahrenabwehr, durch die PDV 384.2 in Verbindung mit dem Einführungserlaß die Frage der Rechtsgrundlage nicht befriedigend gelöst ist.

Zumindest verwundern muß darüber hinaus, daß in der Neufassung der PDV 384.2 unter Ziffer 1.5 nach wie vor zu lesen ist, daß Zugang zum Datenbestand „Polizeiliche Beobachtung" unter anderem „die Ämter für Verfassungsschutz" haben. Dieser redaktionelle Fehler sollte zur Vermeidung von Mißverständnissen schleunigst behoben werden. Die früher bestehende Online-Verbindung des BfV zu INPOL sowie zu PIOS wurde zu Recht entsprechend meinen Forderungen im ersten Tätigkeitsbericht (S. 27) aufgehoben (vgl. auch 2. TB S. 45).

3.11.2.6 Arbeitsdatei PIOS-Rauschgift

Seit dem 1. September 1980 ist die Arbeitsdatei PIOS-Rauschgift bundesweit eingeführt. Sie soll als zentrales Informationssystem helfen, Zusammenhänge im Bereich der Rauschgiftkriminalität zu erkennen und durch (nach den unterschiedlichsten Kriterien) mehrdimensionale Auswertung oder Recherchen (d. h. logische Verknüpfung von Erkenntnissen) Schwerpunkte für Ermittlungsansätze oder unterstützende Information für Ermittlungen aufzeigen.

Augenblicklich wird die Arbeitsdatei PIOS-Rauschgift auf der Grundlage vorläufiger Erfassungsrichtlinien betrieben, die bis zum 1. Juli 1981 von endgültigen Richtlinien abgelöst werden sollen. In meiner Stellungnahme vom 16. Juni 1980 zu den vorläufigen Richtlinien habe ich insbesondere bemängelt, daß die Kriterien für die Aufnahme in die Datei zu unbestimmt sind. Darüber hinaus erscheinen mir die datenschutzrechtlichen Hinweise, die den Datei-Anwendern gegeben werden, zu allgemein und der täglichen Praxis nicht angemessen. Ich habe deshalb vorgeschlagen, sie mit demselben Grad an Konkretheit abzufassen, in dem die übrigen Teile der Arbeitsanleitung gehalten sind.

Im Hinblick auf den weit gesteckten Erfassungsbereich halte ich die Festlegung von kürzeren Speicherfristen als in den KpS-Richtlinien für unumgänglich. Die vorläufigen Richtlinien tragen dieser Forderung bereits in einem gewissen Umfang Rechnung, Verbesserungen scheinen mir aber gleichwohl noch nötig und realisierbar zu sein.

3.11.3 Bundesgrenzschutz

Im Berichtsjahr habe ich die Grenzschutzämter Aachen und Braunschweig sowie u. a. die Grenzkontrollstellen Helmstedt-Autobahn und Helmstedt-Bahnhof überprüft. Außerdem haben Informationsgespräche bei der Grenzschutzdirektion stattgefunden. Von gewissen Mängeln bei der Datensicherung abgesehen, wurde vor allem folgendes festgestellt.

— Die *Sonderanweisung Grenzkontrolle (SoGK)* wird in ihren wesentlichen Teilen nach wie vor praktiziert (s. o. 3.11.1.1). Ich habe mich bei meinen Kontrollen in diesem Jahr schwerpunktmäßig mit der Durchführung dieser Sonderanweisung befaßt. Die hierbei festgestellten Fakten sind eine wertvolle Hilfe bei der Diskussion über eine Nachfolgeregelung für die SoGK, wenn diese, wie angekündigt, außer Kraft gesetzt wird.

— Sowohl in Aachen als auch in Helmstedt konnte ich feststellen, daß keine *Bußgeldkartei* geführt wird. Dies scheint auch bei den anderen Grenzschutzämtern nicht der Fall zu sein. Die Notwendigkeit einer zentralen Bußgeldkartei, die zu errichten gelegentlich erwogen wird, vermag ich schon aus diesem Grunde nicht einzusehen. Wenn es bislang den Grenzschutzämtern nicht erforderlich erschien, für ihren relativ überschaubaren Bereich Bußgeldkarteien zu führen, so ist deren Notwendigkeit um so weniger für den gesamten BGS-Bereich ersichtlich.

— Die Überprüfung in Helmstedt hat ergeben, daß die derzeitigen *Abfragemöglichkeiten des BGS beim Ausländerzentralregister* (AZR) einem Online-Anschluß gleichkommen. Die Abfrage erfolgt zwar per Fernschreiber. Jedoch ist das Antwortzeitverhalten derart optimiert, daß eine Abfrage per Datensichtgerät kaum schnellere Ergebnisse brächte. Auch ist beim jetzt praktizierten Verfahren eine Berechtigungsprüfung im Einzelfall nicht mehr möglich. Dies mag im Hinblick auf die Aufgaben des BGS nach § 1 Nr. 4a i. V. m. § 2 BGSG und § 20 Abs. 4 und 5 Ausländergesetz seine Berechtigung haben.

  Aus datenschutzrechtlicher Sicht sind aber für Datenübermittlungen in einem derartigen Umfang ausdrückliche gesetzliche Grundlagen zu fordern. Auch dies habe ich gegenüber dem Bundesminister des Innern deutlich gemacht (vgl. auch 2. TB S. 47).

— Einzelfallprüfung an der Datenstation

  Bei einer von mir vorgenommenen Abfrage einer Personalie mittels Datenstation der Grenzschutzstelle Helmstedt-Autobahn im INPOL-Personenfahndungsbestand wurde als Antwort neben einer datenschutzrechtlich nicht zu beanstandenden aktuellen Fahndungsausschreibung noch eine nicht mehr bestehende Fahndungsausschreibung einer niedersächsischen Polizeidienststelle für diese Person ausgegeben. Wie meine Nachforschungen ergaben, erklärt sich diese Übermittlung damit, daß einige Grenzschutzstellen in Niedersachsen über den Landesrechner des Landeskriminalamtes Niedersachsen in Hannover auch auf das niedersächsische POLAS-System zugreifen können. Da aus meiner Sicht Bedenken gegen eine Zugriffsberechtigung des Bundesgrenzschutzes auf inaktuelle Fahndungsausschreibungen in INPOL bestehen, weil die Kenntnis dieser Daten zur Aufgabenerfüllung des Bundesgrenzschutzes nicht im gleichen Umfang erforderlich ist wie bei der allgemeinen Polizei (vgl. schon 2. TB S. 48), habe ich den Landesbeauftragten für den Datenschutz gebeten, diesen Sachverhalt beim Landeskriminalamt Niedersachsen zu prüfen.

— Projekt einer Grenzdatei

  Seit längerer Zeit wird erwogen, den Beamten des Bundesgrenzschutzes an den Grenzstellen zur Erleichterung der grenzpolizeilichen Entscheidung (insbesondere bei Zurückweisungen) einen größeren Datenbestand als bisher im automatisierten Verfahren zur Verfügung zu stellen. Bisher haben sie nur Zugriff zu den in der Grenzfahndung oder der allgemeinen polizeilichen Fahndung enthaltenen Daten. Für die Erweiterung ist an eine *Grenzdatei* gedacht, die eine Untermenge des Zentralen Personenindex des Bundesgrenzschutzes wäre, auf den zur Zeit nur die Grenzschutzdirektion unmittelbaren Zugriff hat. Erwogen wird auch, in diese Grenzdatei zentral alle Hinweise auf Bußgeldbescheide, die im Zusammenhang mit Grenzübertritten erlassen worden sind, oder auf Einzelfallzurückweisungen sowie auf einzelne Ausnahmesichtvermerke aufzunehmen.

  Für eine Reihe von weiteren Ländern (z. B. Türkei) ist aber inzwischen die Visumpflicht eingeführt worden. Die grenzpolizeiliche Kontrolle konzentriert sich für Bürger aus diesen Ländern nunmehr verstärkt auf die Ordnungsmäßigkeit des Visums. Damit hat sich die Zahl der Fälle reduziert, in denen an der Grenze Nachprüfungen vorgenommen werden, ob ein Ausländer zum

Zwecke der unerlaubten Arbeitsaufnahme einreisen will. Da die Grenzdatei vorwiegend für diese Fälle gedacht wäre, entfällt damit ein wichtiger Grund für ihren Aufbau. Die wenigen noch denkbaren Einzelfälle, die verbleiben, vermögen nach meiner Auffassung die Einrichtung einer neuen, selbständigen Datei nicht zu rechtfertigen (zur zentralen Bußgeldkartei s. o. 3.11.3.1). Soweit im Einzelfall den Grenzschutzstellen Informationen über Ausländer schnell verfügbar sein müssen, kann dies über das AZR geschehen. Die Abfragemöglichkeit beim AZR hat vom Zeitaufwand her inzwischen ein Niveau erreicht, das dem der Abfrage über Datensichtgeräte nur unwesentlich nachsteht (s. o.).

Ich sehe deshalb keine Notwendigkeit für eine besondere Grenzdatei. Mein Gespräche mit Vertretern der Grenzschutzdirektion haben mich in dieser Auffassung bestärkt.

3.11.4 Bundesnachrichtendienst

Die Kontrolle im Bereich des BND wirft spezifische Probleme auf.

3.11.4.1

Daß das weitgehende Fehlen gesetzlicher Regelungen für die Tätigkeit des BND meine Kontrolle nicht gerade erleichtert, habe ich bereits mehrfach erwähnt (vgl. zuletzt 2. TB S. 49). Die Materie ist, wie ich ebenfalls bereits häufig ausgeführt habe, außerordentlich schwierig, und ohne Zweifel gibt es gewichtige Gründe gegen gesetzliche Formulierungen über die Aufgaben und die Handlungsbefugnisse dieses Zweiges der Exekutive. Aus der Grundentscheidung der Verfassung für eine rechtsstaatliche Ordnung folgt aber trotz alledem, daß auch dieser Bereich nicht „gesetzesfrei" agieren darf. Daß es nicht unmöglich ist, Gesetzesbestimmungen auch für diesen zu schaffen, beweist die Existenz des Gesetzes zu Art. 10 GG (G 10); Teilregelungen sind u. a. im Bundeszentralregistergesetz und neuerdings auch im Melderechtsrahmengesetz und im Sozialgesetzbuch (X. Buch) enthalten. Zumindest die Abgrenzung der Aufgabenbereiche der verschiedenen Nachrichtendienste, soweit sie Inlandsbezug aufweisen oder im Inland tätig sein müssen, sowie eine Regelung der für unverzichtbar gehaltenen Informationsströme zwischen inländischen Behörden und den Diensten sollten gesetzlich festgelegt werden. Für benachbarte Bereiche wird dies zunehmend anerkannt (vgl. u. a. das Votum der Ausschußminderheit im Untersuchungsausschuß zum Abhörfall Strauß/Scharnagl, BT-Drucksache 8/3835, S. 71 ff. sowie die Äußerungen des Bundesministers des Innern zur Verrechtlichung der Amtshilfe der Polizei für die Nachrichtendienste sowie zur Novellierungsbedürftigkeit von BGSG und BVerfSchG, u. a. Süddeutsche Zeitung vom 28. August 1980, S. 2, BMI-Nachrichten Nr. 8/1980 S. 9 f.; zur Amtshilfe allgemein s. o. 3.11.1). Ein Grund zur Schaffung gesetzlicher Bestimmungen über Datenübermittlungen an den BND ergibt sich auch daraus, daß bayerische Dienststellen (insbes. die Bayer. Grenzpolizei) an den BND ab 1. Januar 1983 keine personenbezogenen Daten mehr aus Dateien übermitteln dürfen, weil dies nach dem Bayerischen Landesdatenschutzgesetz dann ausdrücklich nur noch zur Erfüllung der *durch Rechtsnorm* zugewiesenen Aufgaben zulässig ist (Artikel 17 Abs. 1, Artikel 37 Abs. 3 Bay. DSG). Ich bin der Auffassung, daß eine gesetzliche Aufgaben- und Befugniszuweisung auch bei Übermittlungen von Bundesbehörden an Behörden der Eingriffsverwaltung, jedenfalls an Sicherheitsbehörden, Voraussetzung rechtmäßiger Aufgabenerfüllung im Sinne von § 10 Abs. 1 BDSG ist.

3.11.4.2

Ich war schon bisher bereit und bin es weiterhin, bei meinen Prüfungen die Besonderheiten der Arbeitsweise des BND zu berücksichtigen. Manche praktischen Schwierigkeiten haben jedoch meine Prüfungstätigkeit erschwert. Es bestand oft erhebliche Zurückhaltung bei der Beantwortung meiner Anfragen. Die Entfernung zwischen Bonn und München läßt häufige Kontrollen „vor Ort" nicht zu. Die Vermittlung von Auskünften durch das Bundeskanzleramt ist daher zumindest in einfachen Fällen unvermeidlich. Das Bundeskanzleramt legt aber auch sonst größten Wert darauf, diese Vermittlungsfunktion wahrzunehmen, und ich gehe auf diesen Wunsch nach Möglichkeit ein. Zusätzlich wünscht das Bundeskanzleramt, daß bei allen Besuchen die vorgesehenen Erörterungsgegenstände schriftlich und möglichst genau vorher angemeldet werden. Hierauf kann ich mich nicht festlegen: § 19 Abs. 3 BDSG gibt mir das Recht zur sofortigen und unangemeldeten Kontrolle.

3.11.4.3

Ich habe in diesem Jahr dreimal Prüfungsgespräche beim BND geführt und zahlreiche Fragen auch mit dem Bundeskanzleramt erörtert. Der Umfang der Prüfungstätigkeit in bezug auf den BND hat in diesem Jahr aus zwei Gründen zugenommen: einmal lag die Zahl der Einzeleingaben etwas höher als im letzten Jahr. Darüber hinaus haben sich aus Prüfungen bei anderen Stellen verschiedene Hinweise ergeben, die mich zu mehreren Anfragen auch beim BND veranlaßten. Einzelne Antworten des BND habe ich bei meinen Besuchen stichprobenartig überprüft und mich von der Richtigkeit der Auskunft überzeugt. Insgesamt kann ich feststellen, daß keine förmlichen Beanstandungen vorzunehmen waren, soweit ich Prüfungen durchgeführt habe. Allerdings setzt diese Wertung voraus, daß man von den rechtsgrundsätzlichen Problemen (s. o. 3.11.4.1) und von dem Umstand absieht, daß die Amtshilfe zwischen Polizei und Nachrichtendiensten nach wie vor unbefriedigend geregelt ist.

Die Einsicht in Unterlagen zu zwei Personen wurde mir unter Berufung auf § 19 Abs. 3 Satz 4 BDSG verweigert. Damit wurde zum erstenmal von dieser Vorschrift Gebrauch gemacht. Über die Berechtigung dieser Auskunftsverweigerung wird noch gestritten.

3.11.4.4

Zur *Telefonkontrolle* des BND nach § 3 G 10: Nachdem im letzten Jahr die Postkontrolle des BND Anlaß zu Befürchtungen in der Bevölkerung gegeben hatte (hierzu 2. TB S. 50), war es in diesem Jahr die Vermutung rechtswidriger Telefonabhörmaßnahmen durch den BND. Das Bundeskanzleramt hat mir dazu Auskünfte gegeben, die zu der Wertung führen, daß sich die Telefonabhörmaßnahmen an den Rahmen des § 3 G 10 halten. Zu einer Prüfung beim BND selbst ist es jedoch noch nicht gekommen, weil mir aufgrund einer Meinungsäußerung der G 10-Kommission (vgl. § 9 Abs. 2 bis 4 G 10) die Kompetenz für den Bereich der Telefonkontrolle abgesprochen wird. Die Kommission vertritt die Ansicht, sie sei in diesem Bereich ausschließlich zuständig (s. o. 3.11.1.2).

Bei meinem ersten BND-Besuch im Berichtsjahr hatte ich erneut Einsicht in die Auflistung der nach § 3 Abs. 2 G 10 anläßlich der Post- und Telefonkontrolle weitergeleiteten personenbezogenen Daten nehmen und mich insoweit von der korrekten Handhabung überzeugen können. Sowohl im Jahr 1979 als auch im Jahr 1980 (Stand: Mai) wurde danach nur eine geringe Zahl von Personen vom BND an andere Nachrichtendienste weitergemeldet, weil die Voraussetzungen des § 3 Abs. 2 G 10 gegeben waren. Ich habe mich auch über den Ablauf der Auswertung bei der Postkontrolle informiert. Hier konnte ich feststellen, daß praktisch ausschließlich Sachangaben interessieren und verwertet werden. Die Prüfung der Telefonkontrolle mußte ich bei meinem ersten Besuch aus Zeitmangel leider aufschieben. Bei meinem zweiten Besuch wurde sie mir wegen der Intervention der G 10-Kommission verweigert. Ich gehe davon aus, daß die Rechtslage in meinem Sinne geklärt wird, und werde diese Kontrolle nachholen.

3.11.4.5

Die nach § 15 BDSG zu führende *Dateienübersicht* des BND habe ich eingesehen. Dabei zeigte sich, daß der BND von einer unzutreffenden restriktiven Auslegung der Pflicht nach § 15 BDSG ausging (zum notwendigen Umfang der Übersicht vgl. 2. TB S. 56). Die Übersicht beschränkte sich auf die Angaben, die für die — für den BND nicht vorgeschriebene — Meldung zum Dateienregister notwendig wären. Ich habe hierauf hingewiesen und gehe davon aus, daß für die Übersicht eine befriedigende Form gefunden wird. Ich werde dies bei meinem nächsten Besuch im BND überprüfen.

3.11.4.6

Endgültige *Löschungsrichtlinien* des BND sind noch nicht erlassen worden, obwohl ich schon im Laufe des Jahres 1979 mehrfach Anregungen hierzu gegeben habe (vgl. 2. TB S. 50) und sich der BND die Überlegungen zu den seit November 1979 in Kraft befindlichen NADIS-Löschungsrichtlinien zunutze machen konnte. Gegenwärtig wendet der BND einen im wesentlichen den Richtlinien des BfV entsprechenden Entwurf an. Hiernach wird im Regelfall eine 15jährige Frist für die Überprüfung auf weitere Erforderlichkeit zugrunde gelegt. Es gibt jedoch auch Fallgruppen, für die erheblich kürzere Fristen angemessen sein dürften. Hierüber stehe ich mit den zuständigen Stellen im Gespräch.

3.11.4.7

Auch in diesem Jahr hat der BND grundsätzlich nicht auf sein *Auskunftsverweigerungsrecht* verzichtet. Lediglich in zwei Fällen war es mir möglich, auf eine Auskunft hinzuwirken. Dabei handelte es sich in dem einen Fall um einen ehemaligen Bewerber beim BND.

3.11.4.8

In einem anderen Fall war befürchtet worden, daß der BND Firmen-Namen oder die Namen von Betriebsräten speichere, um extremistische Bestrebungen zu überwachen. Hier konnte dem Einsender mitgeteilt werden, daß dies nicht geschieht und mit den — bisher allerdings nur in einer Dienstanweisung des Bundeskanzleramtes festgelegten — Aufgaben des BND auch nicht vereinbar wäre. Die Beobachtung sog. verfassungsfeindlicher Bestrebungen ist allein Aufgabe der Ämter für Verfassungsschutz. Aber auch dort findet — jedenfalls durch das meiner Kontrolle unterliegende BfV — keine Speicherung von Personen allein deshalb statt, weil sie Betriebsräte sind (vgl. näher 2. TB S. 51 f.).

3.11.5 Bundesamt für Verfassungsschutz

Einen Schwerpunkt meiner Prüfungstätigkeit bildete im vergangenen Jahr die Kontrolle des Bundesamtes für Verfassungsschutz (BfV). Ich habe dort Querschnittsauswertungen vorgenommen, Einzelfälle überprüft, grundsätzliche Rechtsfragen anhand konkreter Vorgänge angesprochen und insbesondere auch dem Informationsfluß zwischen dem BfV und anderen Sicherheitsbehörden meine Aufmerksamkeit gewidmet. Da meine Recherchen größtenteils noch nicht abgeschlossen sind, können die Ergebnisse erst im nächsten Tätigkeitsbericht dargestellt werden.

Ich habe mich dafür eingesetzt, daß das BfV die *Auskunftsregelung* in Zukunft großzügiger handhabt. In der Vergangenheit war der Eindruck entstanden, daß in einigen Fällen die Auskunftserteilung möglich und sinnvoll gewesen wäre, vom BfV aber aus grundsätzlichen Erwägungen abgelehnt wurde. Das BfV hat mir zugesagt, in Zukunft mehr als bisher meine Anregungen zur Auskunftserteilung und meine Hinweise auf mögliche Ausnahmen zu beachten.

Ein Schwerpunkt meiner Bemühungen ist weiterhin eine sachgerechte *Differenzierung der Speicherfristen* im System NADIS. Ich habe bei meinen Kontrollen im BfV den Eindruck gewonnen, daß nicht jede der dort gesammelten Informationen es wert ist, 15 Jahre lang aufbewahrt zu werden. Gerade bei

der Vorfeldarbeit eines Nachrichtendienstes fällt naturgemäß eine Fülle von Informationen an, die für den Augenblick interessant sein mögen und gegen deren Speicherung zunächst nichts einzuwenden sein wird. Häufig läßt sich dann aber bereits nach wenigen Jahren sagen, insbesondere wenn die Informationen nicht weiter angereichert wurden, daß die weitere Aufbewahrung nicht notwendig ist. Diesem Tatbestand sollte eine flexible Handhabung der NADIS-Fristen entsprechen. Ich bin deshalb der Auffassung, daß die 15-Jahres-Frist bei der Beobachtung des politischen Extremismus (§ 3 Abs. 1 Nr. 1 VerfSchG) keine starre Grenze sein sollte. Das BfV hat mir versichert, daß man das Problem erkannt habe und daß man ihm durch einen Ausbau der Zeitspeicherung zu begegnen suche. Die Gespräche hierüber laufen unter Einbeziehung der Länder.

3.11.6 Militärischer Abschirmdienst (MAD)

Nach wie vor gibt es kein MAD-Gesetz. Daher stellen sich hier im wesentlichen dieselben Fragen wie beim BND (hierzu s. o. 3.11.4.1). Von dieser Grundsatzfrage abgesehen, ergaben sich im Berichtszeitraum vor allem folgende Schwerpunkte:

3.11.6.1 Sicherheitsüberprüfung Wehrpflichtiger unter Mithilfe des BfV

Nachdem im Jahre 1977 alle gemusterten Wehrpflichtigen unter Einschaltung des BfV überprüft worden waren (vgl. hierzu 2. TB S. 54), wurde im Berichtsjahr erneut die Frage diskutiert, ob und in welchem Maße derartige Überprüfungen durchgeführt werden sollen.

Hierbei ist es zunächst interessant, einen Blick auf die Zahlen des Jahres 1977 zu werfen. Seinerzeit waren alle Personen überprüft worden, die als tauglich gemustert waren und bereits den psychologischen Eignungstest abgelegt hatten. In einigen hundert Fällen hatten sich „Erkenntnisse" ergeben; nach näherer Überprüfung blieben noch weniger Fälle übrig. Hinsichtlich dieser verbliebenen Wehrpflichtigen wurden dann „vorbeugende" Maßnahmen bei der Verwendungsplanung getroffen. Dieses Ergebnis steht in keinem angemessenen Verhältnis zu dem Aufwand. Vor allem aber: Das Ziel, einige „Extremisten" (im Sinne von § 3 Abs. 1 Nr. 1 VerfSchG) zu erkennen, rechtfertigt es nicht, über Hunderttausende junger Menschen Erkundigungen beim Verfassungsschutz einzuholen. Vor einer Verwendung im sicherheitsempfindlichen Bereich findet ohnehin eine Sicherheitsüberprüfung statt.

Die Bundesminister des Innern und der Verteidigung haben im Berichtsjahr vereinbart, daß außer der förmlichen Sicherheitsüberprüfung noch eine (weniger aufwendige) „Sicherheitsanfrage" zugelassen wird, und zwar für diejenigen Bereiche, in denen zwar eine Sicherheitsüberprüfung nicht erforderlich erscheint, aber ein Schutzbedürfnis dennoch angenommen wird (etwa Munitions- und Waffenverwalter, Funktionen in Stäben etc.). Davon ist nur ein geringer Teil der Wehrpflichtigen betroffen. Diese werden über die „Sicherheitsanfrage" jeweils vorher unterrichtet. Es ist auch angeordnet, daß die Ämter für Verfassungsschutz nur solche Informationen an die Bundeswehr weitergeben, die für deren Personaleinsatz relevant sind. Es bleibt das Problem, daß für die Übermittlung der Erkenntnisse durch das BfV an die Bundeswehr keine Rechtsgrundlage erkennbar ist (vgl. oben 3.11.1.1 und 3.11.4.1).

3.11.6.2 Sicherheitsüberprüfung von Reservisten

In meinem zweiten Tätigkeitsbericht hatte ich darauf hingewiesen (2. TB S. 43 f.), daß für die Informationserhebung bei Sicherheitsüberprüfungen eine Rechtsgrundlage fehlt. Der Betroffene müsse deshalb auf die Freiwilligkeit seiner Angaben hingewiesen werden.

Diesen Bedenken ist nunmehr für den Verteidigungsbereich Rechnung getragen worden. In § 24 Abs. 6 Wehrpflichtgesetz ist durch das 13. Gesetz zur Änderung des Soldatengesetzes vom 22. Juni 1980 (BGBl. I, S. 58) eine Regelung über die Auskunftspflicht des Betroffenen eingefügt worden.

3.11.6.3 Kriterien für die Speicherung und Löschungsrichtlinien

Der MAD hat Vorschriften über die Löschung gespeicherter Daten in Kraft gesetzt. Im Ergebnis werden weitgehend die NADIS-Fristen übernommen, wenngleich der MAD es für erforderlich ansieht, in einzelnen Fällen hiervon abweichende Fristen vorzusehen. Um nun die NADIS-Fristen in solchen Fällen nicht aufzuweichen, habe ich vorgeschlagen, nach Ablauf der NADIS-Frist im System NADIS in jedem Fall zu löschen. Soweit der MAD in begründeten Einzelfällen die Notwendigkeit sieht, Unterlagen länger aufzubewahren, sollte dies nur in den Dateien des MAD geschehen, zu denen sonstige Stellen keinen Zugriff haben. Die anderen NADIS-Teilnehmer dürfen keinen Hinweis auf noch vorhandene Unterlagen beim MAD erhalten. Nur dann ist sichergestellt, daß die NADIS-Fristen in vollem Umfang wirksam sind. Der MAD hat meinem Vorschlag zugestimmt. Die in innerdienstlichen Vorschriften festgelegten Kriterien für die Speicherung personenbezogener Daten erscheinen mir in mehreren Fällen zu weit gefaßt. Hierüber bin ich mit dem Bundesminister für Verteidigung im Gespräch.

3.11.6.4 Dateienübersicht beim MAD

Die Struktur der Dateienübersicht des MAD ist entsprechend den besonderen Problemen in diesem Bereich und gemäß den Vorgaben des Bundesministeriums der Verteidigung gut geeignet, die Datenverarbeitung dieser Behörden transparent zu machen. Dieses Ziel kann aber nur dann erreicht werden, wenn die Einzelangaben zu den nachgewiesenen Dateien umfassend und präzise erfolgen. In einigen Fällen sind dazu noch Rückfragen und Nacherhebungen erforderlich.

3.11.7 Weitergabe von Unterlagen über Kriegsdienstverweigerer an das BfV

Durch eine parlamentarische Anfrage ist bekanntgeworden, daß im Wege der Amtshilfe Akten über

Wehrdienstverweigerer vom Bundesamt für den Zivildienst an das BfV zur Einsichtnahme übermittelt worden sind. Meine Nachforschungen haben ergeben, daß dies in der Vergangenheit nur in sehr wenigen Fällen geschehen ist. Der BMI hat nunmehr entschieden, daß ihm derartige Aktenanforderungen des BfV vorab zur Prüfung der Erforderlichkeit vorzulegen sind; auf der anderen Seite hat sich der Bundesminister für Arbeit und Sozialordnung die Genehmigung von Aktenübermittlungen durch das Bundesamt für den Zivildienst vorbehalten. Damit ist ein ständiger Informationsaustausch ausgeschlossen. Allerdings bin ich der Auffassung, daß das BfV überhaupt nicht in Akten über Kriegsdienstverweigerer Einsicht nehmen sollte. In diesen Akten befinden sich auch Protokolle über die Prüfungsgespräche. In den Prüfungsgesprächen ist der Kriegsdienstverweigerer gezwungen, seine innersten Gewissensgründe zu offenbaren. Dies geschieht ausschließlich zu dem Zweck der Anerkennung als Kriegsdienstverweigerer. Auch diese wenigen Fälle, in denen dem BfV Akteneinsicht ermöglicht wurde, sind geeignet, das Anerkennungsverfahren für Kriegsdienstverweigerer unnötig zu belasten und damit möglicherweise das Grundrecht des Artikels 4 Abs. 3 GG zu beeinträchtigen.

4 Allgemeine Erfahrungen

4.1 Prüfungskompetenz des BfD

Ein wichtiges Auslegungsproblem ergab sich im Berichtszeitraum zu der Vorschrift des § 19 Abs. 1 Satz 1 BDSG, die meine Zuständigkeit festlegt. Danach kontrolliert der Bundesbeauftragte für den Datenschutz „die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz" bei den Behörden und sonstigen öffentlichen Stellen des Bundes. Die Kompetenzen der Landesbeauftragten für den Datenschutz sind in den Datenschutzgesetzen der Länder in entsprechender Weise beschrieben, ebenso die der Aufsichtsbehörden der Länder für den nicht-öffentlichen Bereich in den §§ 30, 40 BDSG. Fast gleichzeitig kam in den Ländern und in einem von mir behandelten Fall die Frage auf, ob die „anderen Vorschriften" über den Datenschutz nur solche sind, die die Verarbeitung personenbezogener Daten *in Dateien* regeln. Der Bundesminister des Innern vertritt dazu den Standpunkt, das BDSG insgesamt schütze nur personenbezogene Daten, die in Dateien gespeichert, verändert, gelöscht oder aus Dateien übermittelt werden. Es bestehe kein Grund zu der Annahme, daß der Gesetzgeber, wenn er im BDSG von „anderen Vorschriften über den Datenschutz" spreche, diesen Zielbereich des Gesetzes habe verlassen wollen. Ich kann mich dieser Auffassung nicht anschließen und befinde mich damit in Übereinstimmung mit den Landesbeauftragten für den Datenschutz, mit denen ich die Problematik ausführlich erörtert habe. Lediglich ein Landesdatenschutzgesetz hat Formulierungen gewählt, aus denen sich ein Dateibezug auch für die „anderen Vorschriften über den Datenschutz" begründen läßt.

Meine Auffassung stützt sich auf folgende Erwägungen:

Ausgangspunkt der Auslegung muß der Wortlaut der Bestimmungen sein, die diese Formulierung verwenden (§§ 15 Satz 1, 19 Abs. 1 Satz 1, 20 Abs. 1, 29 Satz 1, 30 Abs. 1 und 40 Abs. 1 Satz 1). An keiner der zitierten Stellen findet sich eine Einschränkung etwa der Art, daß die Einhaltung der „anderen Vorschriften über den Datenschutz" nur dann kontrolliert werden dürfe, wenn die Daten „in Dateien gespeichert, verändert, gelöscht oder aus Dateien übermittelt werden". Vielmehr ist im Text gerade die Einhaltung „der Vorschriften dieses Gesetzes" mit der Einhaltung „anderer Vorschriften über den Datenschutz" *konfrontiert*. Gegen eine stillschweigende Ergänzung des § 19 Abs. 1 Satz 1 und der entsprechenden anderen Bestimmungen, für die die folgenden Überlegungen gleichermaßen gelten, um das ungeschriebene Merkmal „Dateibezug" spricht auch der Umstand, daß an anderen Stellen, wo Anlaß für eine solche Ergänzung gesehen wurde, diese ausdrücklich in den Text aufgenommen worden ist, so in § 5 Abs. 1 und § 6 Abs. 1 BDSG, wo auf den „Rahmen des § 1 Abs. 2" verwiesen wird.

Auch eine systematische Interpretation der Struktur des BDSG führt zu keinem anderen Ergebnis. Was „Datenschutz" ist, sagt § 1 Abs. 1. Er enthält keine Bezugnahme auf den Dateibegriff. § 1 Abs. 2 bezeichnet demgegenüber den Schutzbereich „dieses Gesetzes", nicht von „Datenschutz" allgemein. Nur hierauf bezieht sich auch die Definition von „Datei" in § 2 Abs. 3 Nr. 3 mit dem Ausschluß der in Akten gespeicherten Daten aus diesem Begriff.

Wenn demgegenüber gesagt wird, in *allen* Vorschriften des Gesetzes müsse die in § 1 Abs. 2 enthaltene Einschränkung gelten, so wird der unterschiedliche Charakter der verschiedenen Normen verkannt. Das BDSG enthält zumindest zwei Untermengen von Rechtsnormen, zwei (ineinander verwobene und nicht etwa der Abschnittseinteilung entsprechende) Teile, nämlich

— für die Datenverarbeitung in oder aus Dateien Grundsatzregeln, sozusagen die allgemeinen Prinzipien eines Dateien-Datenschutzes, vor allem Zulässigkeitsregeln, die sich an die Datenverarbeiter wenden, und Rechte der Betroffenen;

— darüber hinaus für die Durchführung und Kontrolle des Datenschutzes allgemein *Organisations- und Verfahrensvorschriften*, die nicht nur die Verwirklichung der „eigenen" materiellen Bestimmungen des BDSG zum Ziele haben, sondern Regeln aufstellen, wie die datenschutzrechtlichen Bestimmungen des Bundes insgesamt ausgeführt werden sollen — ein Regelungskomplex, der auch in Form eines selbständigen Gesetzes hätte beschlossen werden können. Dieses Datenschutz-Organisations- und Verfahrensrecht umfaßt zumindest die §§ 15, 17 bis 21, 28 bis 30, 38 bis 40.

§ 45 Satz 3 BDSG läßt darüber hinaus ausdrücklich eine dritte Teilmenge des Datenschutzrechts (über das BDSG hinaus) unberührt, nämlich die Vorschriften über Berufsgeheimnisse.

§ 45 BDSG stellt richtigerweise auf die *Anwendbarkeit* der (anders formulierten) besonderen Rechtsvorschriften „*auf* in Dateien gespeicherte personenbezogene Daten" ab. Wenn der Kontrollbereich des Datenschutzbeauftragten auf die „Dateien-Datenverarbeitung" hätte beschränkt werden sollen, so hätte in § 19 Abs. 1 die gleiche Formulierung wie in dem ersten Halbsatz von § 45 Satz 1, also der „Soweit"-Vorbehalt benutzt werden müssen.

Die Spaltung des Datenschutzes zwischen Datenverarbeitung in Dateien und in anderen Formen ist dem Bürger kaum verständlich zu machen, und wenn bereichsspezifische Datenschutzbestimmungen materielle Regelungen enthalten, die Maßstab der Kontrolle sein können, so wird es kaum noch erklärbar sein, daß die Kontrolle ihrer Einhaltung in dem einen Fall zulässig sei, in dem anderen aber nicht. Eine Stellungnahme zu den jeweiligen Rechts- und Organisationsfragen wird von den Datenschutzbeauftragten ohnehin erwartet, und es wird auch von den Befürwortern einer restriktiven Auslegung nicht bestritten, daß die Datenschutzkontrollinstanzen die speichernden Stellen auch insoweit beraten und Empfehlungen zur Verbesserung des Datenschutzes geben können, als es um Datenverarbeitung außerhalb von Dateien geht. Dann ist wiederum schwer einsichtig, warum dort eine Kontrolle ausgeschlossen sein soll. Daß der Kontrollbereich weit gezogen werden sollte, ergibt auch der Text des § 20 Abs. 1 Satz 1, wonach nicht nur Rechtsverstöße, sondern auch „sonstige Mängel bei der Verarbeitung personenbezogener Daten" beanstandet werden können.

Befürchtungen, in Ausnutzung der Kontrollkompetenz *ohne* den Dateibezug könnten die Datenschutzbeauftragten nunmehr eine Flut von Überprüfungen und Beanstandungen vornehmen, werden durch die Praxis widerlegt. Bei den Kontrollen, die ich bisher vorgenommen habe, hat die Streitfrage übrigens keine Rolle gespielt. Die von mir überprüften Behörden haben sich meiner Kontrolltätigkeit in noch keinem Falle widersetzt, wenn es um die Einhaltung anderer Vorschriften über den Datenschutz bei der Verarbeitung personenbezogener Daten außerhalb von Dateien ging.

Wie der Begriff der „anderen Datenschutzbestimmungen" zu verstehen ist, wenn man den Dateibezug nicht hineinliest, ist hiermit noch nicht entschieden. Datenschutzrecht ist die Summe der rechtlichen Regelungen, die dem Schutz individueller Rechte bei der Datenverarbeitung dienen. Um eine Norm dem Recht des Datenschutzes im engeren Sinne zuzuordnen, muß sie m. E. einen Bezug zur Daten- oder besser Informationsverarbeitung einschließlich der Erhebung und Auswertung von Informationen aufweisen; es darf nicht so sein, daß sie ganz allgemein gefaßt ist und dabei *auch* auf Informationsvorgänge anwendbar ist. Ich meine also, daß die betreffende Regelung den Umgang mit Informationen *unmittelbar* betreffen muß, oder anders ausgedrückt: daß sie den Informationsvorgang von anderen Vorgängen (Entscheidungen, Leistungen) *isoliert* behandeln muß. Hochabstrakte Normen wie die Grundrechte des Grundgesetzes und das Verhältnismäßigkeitsprinzip sind für sich allein keine „Datenschutzbestimmungen" in diesem Sinne. Doch sind z. B. die meisten Bestimmungen des Melderechts, die neuen Vorschriften über den Sozialdatenschutz, Normen über besondere Berufsgeheimnisse und das Amtsgeheimnis, das ungeschriebene Recht der Personalaktenführung, Bestimmungen der Statistikgesetze und Benutzungsordnungen für Archive Teile des Datenschutzrechts.

Ich werde die hier vertretene Auffassung über den Umfang meiner Kontrollzuständigkeit wie bisher auch künftig meinen Überprüfungen zugrunde legen und sehe mich darin auch durch die im politischen Raum erkennbare Tendenz bestärkt, die Stellung des Bundesbeauftragten für den Datenschutz im Rahmen einer Novellierung des BDSG zu verbessern.

4.2 Formulargestaltung

Zahlreiche Eingaben befassen sich mit der datenschutzgerechten Gestaltung von Vordrucken, Fragebögen, Antragsformularen der verschiedensten Art. Viele dieser Hinweise waren Anlaß zu Initiativen für bessere Abfassung der behördlichen Schriftstücke.

So habe ich festgestellt, daß im Steuerrecht, im Sozialversicherungsrecht und im Personalrecht nach Kindschaftsverhältnissen (ehelich, für ehelich erklärt, an Kindes Statt angenommen oder nichtehelich) unterschieden wird, obwohl die Anspruchsvoraussetzungen meist gleich sind. Werden in den entsprechenden Antragsformularen differenzierte Abfragen der Kindschaftsverhältnisse vorgenommen, so sind diese Daten nicht erforderlich. Anderes gilt zum Beispiel lediglich bei Stiefkindern und Enkeln sowie bei Pflegekindern, wenn zusätzliche Anspruchsvoraussetzungen gegeben sind, so bei der Prüfung des Anspruchs eines Kindes auf Maßnahmen zur Früherkennung von Krankheiten, Krankenhilfe und sonstige Hilfen (§ 205 RVO). Nur in solchen Fällen halte ich eine differenzierte Fragestellung für geboten und zulässig. Soweit in Steuervordrucken nicht erforderliche Angaben über Kindschaftsverhältnisse verlangt werden, hat der Bundesminister der Finanzen in Aussicht gestellt, daß die Bundesregierung eine Änderung des § 32 Abs. 4 Einkommensteuergesetz, der solche Angaben fordere, herbeiführen werde. Bis dahin könne auf die Datenerhebung nicht verzichtet werden.

4.3 Grenzen der Automatisierung

Eine Bürgerin hatte sich an mich gewandt, weil ihr Versichertenkonto bei der Bundesversicherungsanstalt für Angestellte fremde Daten enthielt. Eine Nachprüfung ergab folgendes:

Zwei Versicherte gleichen Vor- und Zunamens mit gleichem Geburtsdatum und gleichem Geburtsort hatten zwei verschiedene Versicherungskonten. Bei einem routinemäßigen Durchsuchen des Datenbestandes auf Doppel- und Mehrfachvergabe beim Verband Deutscher Rentenversicherungsträger

wurde aus dieser Gleichheit der Daten maschinell die (falsche) Schlußfolgerung gezogen, es handele sich um *eine* Person mit *zwei* Konten. Eines der Konten wurde kurzerhand aufgelöst, die Daten wurden dem anderen Konto zugeschrieben. Wenn man bedenkt, welche Folgen diese falsche Computerentscheidung hätte haben können, wäre sie nicht entdeckt worden, wird deutlich, weshalb ich mich stets gegen solche rein maschinellen Entscheidungen wende.

Das Verfahren wurde nunmehr so abgeändert, daß dann, wenn der maschinelle Vergleich eine Übereinstimmung ergibt, ein Sachbearbeiter eingeschaltet werden muß. Ich habe darüber hinaus gefordert, daß der oder die betroffenen Versicherten beteiligt werden, wenn auf andere Weise keine eindeutige Klärung erfolgen kann.

4.4 Maßnahmen zur Gewährleistung des Datenschutzes

Die Maßnahmen, die zur organisatorischen und technischen Gewährleistung des Datenschutzes in den einzelnen Behörden angemessen sind, weisen zwangsläufig sehr große Unterschiede auf.

Wesentliche Einflußfaktoren dafür sind

— die Art der zu verarbeitenden Daten,

— die Aufgaben der Behörde und die daraus abgeleiteten Aufgaben der Datenverarbeitung,

— die Größe der Behörde und der Umfang der Datenverarbeitung und

— die bestehende Organisation der Behörde und ihrer Datenverarbeitung.

Weil in diesen Punkten die Bundesbehörden nicht auch nur annähernd übereinstimmen, gibt es kein allgemeingültiges Konzept für angemessene Datensicherungsmaßnahmen, das — und sei es auch mit gewissen Anpassungen — generell als Vorgabe verwendet werden könnte. Die einzelnen Behörden müssen deshalb jeweils an ihren individuellen Verhältnissen orientierte Konzepte für die Gewährleistung des Datenschutzes entwickeln.

4.4.1 Die Bedeutung der Übersicht

Es hat sich wiederholt gezeigt, daß nur eine möglichst vollständige und alle Aspekte der Datenverarbeitung umfassende Bestandsaufnahme der personenbezogenen Daten eine tragfähige Grundlage für die Auswahl, Planung und Realisierung der notwendigen Maßnahmen für den Datenschutz bereitstellen kann. In dieser Bestandsaufnahme sind nicht nur die Art der Daten und die zugehörigen Aufgaben (zur Kontrolle, ob die Speicherung dieser Daten zulässig ist) sowie die regelmäßigen Empfänger (zur Kontrolle, ob die Bekanntgaben zulässig sind), sondern auch die Darstellungsformen und die Aufbewahrungsorte für die einzelnen Darstellungen der Daten zu erfassen. Nur wenn bekannt ist, wo überall Datenträger (z. B. Lochkarten, Bänder einschließlich der Sicherungsbestände, Erfassungsbelege, Listen) gelagert werden, welche Transporte durchgeführt und wie gegebenenfalls Datenträger vernichtet werden (sollen), können die Sicherungsmaßnahmen i. S. von § 6 BDSG geplant, realisiert und (durch Stichproben) kontrolliert werden.

In vielen Bereichen ist eine solche Bestandsaufnahme erfolgt, die entsprechend den Bedürfnissen in einigen Verwaltungen auch deutlich über meine allgemeinen Vorschläge zum Inhalt der Übersicht gemäß § 15 BDSG hinausgeht. Soweit diese umfassende Bestandsaufnahme durchgeführt ist, werden nach meinen Erfahrungen in der Regel auch die Probleme der jeweiligen Behörde gesehen und angemessene Maßnahmen zum Datenschutz und zur Datensicherung durchgeführt, eingeleitet oder zumindest als notwendig erkannt.

Bei meinen Kontrollen habe ich aber auch Fälle angetroffen, in denen die Übersicht gerade dazu ausreichte, die Veröffentlichungen gemäß § 12 BDSG und die Meldungen zu meinem Register mehr schlecht als recht zu ermöglichen. Damit fehlte die Grundlage zur Beurteilung bestehender oder zusätzlich erforderlicher Maßnahmen zur Datensicherung und zur Entwicklung eines Konzepts zur Gewährleistung des Datenschutzes in diesen Behörden. Daß somit verschiedene Schwachstellen unentdeckt bleiben mußten, ist offensichtlich. Beispiele dafür sind:

— Unzureichende Sicherung von Druckerausgaben

  Ein Problem der Datensicherung sind die Druckerausgaben, die üblicherweise den Bereich des Rechenzentrums verlassen und in andere Bereiche gehen, wo sie für die Erfüllung von ständigen und/oder einmaligen Aufgaben benötigt werden.

  Auch hier kann die Übersicht eine Hilfe sein, wenn in ihr erfaßt wird, welche Druckerausgaben erstellt werden, an wen sie gehen, zu welchem Zweck sie verwendet werden und ob und wie diese Druckerausgaben gelöscht, d. h. vernichtet werden bzw. ob sie aufbewahrt werden, und wenn ja, wie lange.

  Erfahrungsgemäß finden sich unentdeckte Sicherheitslücken insbesondere in den folgenden Bereichen:

  — Aufbewahrung der Druckerausgaben am Arbeitsplatz

  — Verfahren bei nicht mehr benötigten Druckerausgaben (z. B. Tausch Alt gegen Neu)

  — Aufbewahrung von nicht oder nicht mehr ständig gebrauchten Druckerausgaben

  — Vernichtung nicht mehr aufzubewahrender Druckerausgaben.

  Ähnliche Sicherungsprobleme bestehen bei Fehldrucken, z. B. den Druckerausgaben bei unvollständig abgelaufenen oder fehlerhaften Programmen. Eine weitere Schwachstelle entsteht gelegentlich durch die wenig gesicherte Lagerung und Vernichtung von Kohlepapier, das für Listenmehrfertigungen verwendet wurde. Da

dieses Kohlepapier üblicherweise nur einmal benutzt wird, sind die durchgeschriebenen Daten ohne besondere Mühe erkennbar.

Für derartige Abfälle könnten zwar auch allgemeine Regelungen greifen, diese sind aber oft lückenhaft, und ihre Revisionsbedürftigkeit wird häufig erst bei einer an den Datenbeständen orientierten Analyse erkannt.

— Unzureichende Sicherung archivierter Eingabebelege

Unterlagen, insbesondere Eingabebelege, die für die Verarbeitung nicht mehr benötigt werden, lagern gelegentlich in kaum gesicherten Abstellräumen. Ein Hinweis auf den Verbleib dieser Unterlagen — aufgabenorientiert bzw. dateibezogen in der Übersicht — würde diese Schwachstelle für den Datenschutzbeauftragten der Behörde leichter kontrollierbar und gegebenenfalls auch behebbar machen.

— Aufbewahren von Eingabedaten

Wer die automatisierte Datenverarbeitung überwiegend oder ausschließlich als technisches Problem sieht, der wird leicht geneigt sein, einmal erfaßte Daten möglichst lange zu speichern. Denn die Aufbewahrung auf Magnetbändern verursacht relativ geringe Kosten, und „es ist ja nie ganz auszuschließen, daß man die Daten noch einmal braucht". Dies gilt auch für regelmäßig anfallende Eingabedaten, die eine Bestandsdatei fortschreiben. Obwohl die inzwischen durch neue Eingaben oder Löschungen veralteten Eingabedaten inhaltlich von den Daten der Bestandsdatei erheblich abweichen können, wird die weitere Behandlung von Eingabemedien gelegentlich in der Übersicht nicht erfaßt.

Dadurch ist es vorgekommen, daß personenbezogene Daten, die auf Grund zwingender Rechtsvorschriften in der Bestandsdatei gelöscht wurden, in den aufbewahrten Eingabebändern noch viele Jahre danach verfügbar waren, ohne daß die Erforderlichkeit dieser fortdauernden Speicherung glaubhaft gemacht werden konnte.

4.4.2 Probleme bei der Durchsetzung von Maßnahmen

Häufig sind technische und organisatorische Maßnahmen zum Datenschutz leicht in den Arbeitsablauf einzufügen, gelegentlich lassen sie sich auch im Zuge von Rationalisierungen verwirklichen oder geben dazu sogar den Anlaß. In anderen Fällen wären die erforderlichen Änderungen jedoch mit baulichen Maßnahmen, erhöhtem Personalaufwand oder anderen Kosten verbunden, denen kein unmittelbar erkennbarer Rationalisierungsvorteil entspricht. In diesen Fällen sind die Bereitschaft, für mehr Datenschutz auch mehr Aufwand in Kauf zu nehmen, und/oder die Durchsetzungskraft oft nicht ausreichend, um gegen das Argument des knappen Geldes die erforderlichen Änderungen zu verwirklichen.

Gelingt es dennoch, das Geld für Datenschutzmaßnahmen bewilligt zu bekommen, so dauert es oft noch längere Zeit, bis die Mittel verfügbar sind und die manchmal schon seit Jahren notwendigen Maßnahmen ergriffen werden können. Dies gilt z. B. für

— Aufenthaltsräume und Garderoben für Rechenzentrumspersonal

Garderoben für das an den Datenverarbeitungsanlagen tätige Personal befinden sich gelegentlich im Maschinensaal, und die Aufenthaltsräume für Mitarbeiter des Rechenzentrums liegen manchmal so, daß Taschen und Mäntel durch den Maschinensaal mitgenommen werden (müssen). Obwohl die in der Anlage zu § 6 BDSG geforderte Abgangskontrolle dann kaum durchführbar ist, können gerade hier Änderungen oft nur sehr langfristig erreicht werden.

— Datenträgerverwaltung

Häufig werden Datenträger, insbesondere Magnetbänder mit personenbezogenen Daten, nicht so verwaltet, daß für alle diese Datenträger nachgewiesen werden kann, wo sie sich jeweils befinden (müßten). Auch dort, wo die Datenträger in einem Archiv verwahrt und nur zur Verarbeitung herausgegeben werden, fehlt gelegentlich eine Kontrolle des vollständigen und rechtzeitigen Rücklaufs. Ferner fehlt in einigen Fällen eine wirksame Trennung zwischen dem Datenträgerarchiv und den DV-Anlagen, wodurch den Maschinenbedienern ausgedehnte Zugriffsmöglichkeiten eröffnet werden.

4.4.3 Reaktion auf Alarmmeldungen

Zum Sichern einzelner Gefahrenpunkte, aber auch zur Sicherung bestimmter Räume, Gebäudeteile oder auch zur Rundum-Sicherung einer Behörde werden häufig besondere Alarmgeber eingesetzt. So ist es z. B. üblich, daß die (wiederholt) falsche Paßworteingabe am Datensichtgerät einen Alarm auslöst, etwa dadurch, daß sofort eine entsprechende Meldung auf dem Konsolbildschirm erscheint. Das damit erreichte Sicherheitsgefühl ist aber trügerisch, wenn — wie bei einer Prüfung in einem größeren Rechenzentrum festgestellt wurde — diesem Alarm keine Sofortmaßnahmen folgen. Ähnliches gilt für Türüberwachungen, bei denen u. a. jedes längere Offenstehen der Tür einen Alarm auslöst, dies aber während der Arbeitszeit ohne jede Folge bleibt — auch das kommt vor.

Diese Beispiele machen deutlich, daß Datenschutz und Datensicherung in erster Linie organisatorische Probleme sind und daß der Einsatz der Technik nur dann erfolgreich ist, wenn sie in einen genau analysierten Ablauf integriert wird. Technische Sicherungsmaßnahmen dürfen nicht nur aufgepropft werden. Vielmehr müssen alle ihre Auswirkungen bekannt sein und Lösungen im organisatorischen Ablauf von vornherein vorgesehen werden.

5 Datenschutz im Ausland, internationale Zusammenarbeit

5.1 Stand der Datenschutzgesetzgebung im Ausland

Spektakuläre Ereignisse hat es in der Datenschutzgesetzgebung des Auslandes im Berichtsjahr nicht gegeben. Es sind keine neuen Datenschutzgesetze verabschiedet worden. In Norwegen und Luxemburg haben die gesetzlich vorgesehenen Kontrollinstitutionen sich konstituiert, die übrigen haben ihre Kontrolltätigkeit inzwischen voll aufgenommen. In den Niederlanden, der Schweiz und England sind die Vorbereitungsarbeiten für eine Datenschutzgesetzgebung in ein konkreteres Stadium übergegangen. Möglicherweise werden schon im Jahre 1981 erste Entwürfe vorgelegt werden können.

5.2 Internationale Übereinkommen

Herausragende Ereignisse auf dem Gebiet des internationalen Datenschutzes waren — wenngleich von der Öffentlichkeit kaum wahrgenommen — die Verabschiedung eines Datenschutz-Übereinkommens durch den Ministerrat des Europarats sowie von Datenschutz-Leitlinien durch den Rat der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD). Damit ist ein beachtlicher Fortschritt erzielt worden. Nicht nur die nationale Datenschutzgesetzgebung wird dadurch Impulse erfahren, ich hoffe und erwarte auch, daß sich schon bald Auswirkungen auf die Datenschutzpraxis in den Ländern zeigen werden, die noch keine eigene Datenschutzgesetzgebung haben. Für die Bundesrepublik Deutschland könnten die internationalen Übereinkommen annähernd die Funktion gewinnen, um deretwillen viele ein Grundrecht auf Datenschutz fordern, nämlich die der Bekräftigung und Verstetigung der Entscheidung für ein ausgeformtes, bürgerfreundliches Datenschutzrecht (vgl. 1. TB S. 65f.).

5.2.1 Europarat

Das am 17. September 1980 vom Ministerrat des Europarats verabschiedete „Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten" ist das Ergebnis mehrjähriger Erörterungen in einem Expertenausschuß des Europarats. Auf den Entwurf und seinen wesentlichen Inhalt habe ich in den vorangegangenen Tätigkeitsberichten (1. TB S. 63f., 2. TB S. 75) hingewiesen. Er war in dem Expertengremium bis zuletzt umstritten. Ich habe davon abgesehen, auch meinerseits auf weitere Verbesserungen und Klarstellungen zu dringen, weil es mir vordringlich erschien, die Konvention möglichst bald zu verabschieden. Da sie auch nach ihrer Ratifizierung in den Mitgliedstaaten nicht unmittelbar geltendes Recht werden wird, kommt es weniger auf den Wortlaut als auf die Gesamtintention an. Diese ist klar genug zum Ausdruck gebracht worden, um die verantwortlichen Stellen in den Unterzeichnerstaaten zu veranlassen, ihr nationales Datenschutzrecht den in der Konvention verankerten Grundsätzen anzupassen.

5.2.2 OECD

Nur wenige Tage nach dem Beschluß des Ministerrats des Europarats hat am 23. September 1980 der Rat der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) die „Leitlinien für den Schutz der Privatsphäre und den grenzüberschreitenden Verkehr personenbezogener Daten" verabschiedet. Die Leitlinien wenden sich, wie ich bereits in meinem 2. Tätigkeitsbericht (S. 75f.) ausgeführt habe, nicht nur an die Regierungen der Unterzeichnerstaaten, sondern auch an nicht-öffentliche Stellen, die personenbezogene Daten verarbeiten. Durch die starke Wirtschaftsbezogenheit der OECD besteht die Chance, daß die Leitlinien sich namentlich auf die Datenschutzpraxis multinationaler Unternehmen auswirken werden. Ich wiederhole hier, was ich schon mehrfach in Gesprächen und Vorträgen zum Ausdruck gebracht habe: Die Anwendung der Datenschutzgrundsätze, wie sie in den Leitlinien und der Europaratskonvention zum Ausdruck gebracht sind, kann dazu beitragen, daß besondere gesetzliche Vorschriften zur Regelung des grenzüberschreitenden Datenverkehrs weitgehend entbehrlich bleiben.

5.2.3 Europäische Gemeinschaft

In der Europäischen Gemeinschaft sind im vergangenen Jahr nennenswerte Fortschritte in Richtung auf ein gemeinschaftseigenes Datenschutzrecht nicht gemacht worden. Dies wurde bisher u. a. damit begründet, zunächst die Ergebnisse einer von der Kommission in Auftrag gegebenen Studie abwarten zu müssen. Diese Studie über Datenschutz und Datensicherung liegt inzwischen vor. Es handelt sich um eine Gemeinschaftsarbeit der Gesellschaft für Mathematik und Datenverarbeitung (GMD) in St. Augustin bei Bonn, des französischen Institut de Recherche d'Informatique et d'Automatique (IRIA) und des englischen National Computing Centre (NCC). Die Studie untersucht qualitative und quantitative Aspekte des grenzüberschreitenden Datenverkehrs, die Organisation und Arbeitsweise der Datenschutzkontrollinstitutionen, internationale ökonomische Aspekte des Datenschutzes sowie Einzelprobleme wie die Frage, ob juristische Personen in den Datenschutz einbezogen werden sollten oder nicht. Mit dieser sehr sorgfältig erarbeiteten Studie besitzt die Kommission eine vorzügliche Grundlage für eigene Datenschutzinitiativen. Die inzwischen vollzogene Entwicklung im Europarat und der OECD könnte indes dazu führen, auf ein gemeinschaftseigenes Datenschutzrecht zu verzichten und sich statt dessen der Europaratskonvention anzuschließen. Welche Lösung auch immer gefunden wird, es sollte möglichst bald etwas geschehen. Das Europäische Parlament hat in seiner vergangenen Legislaturperiode schon einmal eine Datenschutzinitiative der Kommission gefordert und sehr kon-

krete Vorstellungen entwickelt, wie diese beschaffen sein sollte (vgl. 2. TB S. 76). Es wäre sicher sinnvoll, wenn diese Ansätze erneut aufgegriffen, im Lichte der inzwischen eingetretenen Entwicklungen überprüft und bald in parlamentarische Aktionen umgesetzt werden würden.

5.3 Internationale Zusammenarbeit in Fragen des Datenschutzes

Die Zusammenarbeit mit Datenschutzkontrollinstitutionen im Ausland nimmt festere Konturen an. Zwar ist die Zahl der Eingaben, die mich auf diesem Wege erreichten, nach wie vor gering. Vornehmlich handelt es sich dabei um Beschwerden von Personen, die Werbematerial aus der Bundesrepublik erhalten. Sie wollen wissen, wie die werbenden Unternehmen an ihre Anschrift gelangt sind. Ich habe derartige Anfragen — der gesetzlichen Zuständigkeitsverteilung entsprechend — stets an die jeweilige Aufsichtsbehörde weitergeleitet. Der Wert der internationalen Zusammenarbeit kann aber nicht nach der Zahl der Eingaben bemessen werden. Entscheidend ist, daß die Verbindungen tatsächlich hergestellt und ausgebaut werden, damit sie in echten Bedarfsfällen rasch und reibungslos funktionieren.

Der Schwerpunkt der Zusammenarbeit lag im Berichtsjahr im gegenseitigen Meinungs- und Erfahrungsaustausch. Um ihn zu erleichtern, hatte ich mich dazu erboten, daß meine Dienststelle dabei die Funktion eines Sekretariats übernimmt. Davon ist rege Gebrauch gemacht worden. Die Kollegen im Ausland leiteten mir geeignete Informationen zu, die ich sodann gesammelt oder einzeln an die übrigen Datenschutzkontrollinstitutionen weitergeleitet habe.

Den Höhepunkt der Zusammenarbeit bildete die zweite Konferenz der nationalen Datenschutzkontrollinstitutionen, die diesmal in Ottawa/Kanada stattfand. Eingeladen hatte die kanadische Datenschutzbeauftragte (Privacy Commissioner), Frau Inger Hansen; die kanadische Regierung unterstützte die Konferenz in großzügiger Weise. Teilnehmer waren Repräsentanten der Datenschutzkontrollinstitutionen Dänemarks, Frankreichs, Luxemburgs, Norwegens, Schwedens und der Bundesrepublik Deutschland. Ihre endgültige Form hat die Konferenz noch nicht gefunden. War die erste Sitzung in Bonn im Mai 1979 noch ein informelles Treffen gewesen, so war diese zweite Zusammenkunft in Ottawa praktisch ein öffentliches Forum. Anwesend waren Vertreter der Regierungen der Vereinigten Staaten und Kanadas, Repräsentanten multinationaler Unternehmen, am Datenschutz interessierte Wissenschaftler und die Presse. Den Teilnehmern bot sich damit die Gelegenheit, ihre Überlegungen und Perspektiven vor einem breiten, interessierten Publikum darzulegen. Beschlüsse wurden nicht gefaßt. Es läßt sich aber feststellen, daß die Bundesrepublik bei der Verwirklichung des Datenschutzes wohl eine hervorgehobene Stellung einnimmt.

Ob sich diese offene Konferenzform beibehalten lassen wird, wenn der Kreis der teilnehmenden Datenschutzkontrollinstitutionen größer wird, muß der Zukunft überlassen bleiben.

Bonn, den 9. Januar 1981

Prof. Dr. Bull