Deutscher Bundestag
10. Wahlperiode

Drucksache 10/2777

22. 01. 85

Sachgebiet 204

Unterrichtung

durch die Bundesregierung

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

Gliederung

Zugeleitet mit Schreiben des Bundesbeauftragten für den Datenschutz — I — 192 111/9 — vom 22. Januar 1985 gemäß § 19 Abs. 2 des Bundesdatenschutzgesetzes.

1 Einleitung

1.1 Gesamtüberblick

George Orwell's literarische Zukunftsvision eines brutalen, die Menschen auf Schritt und Tritt mit ausgeklügelter Technik beobachtenden Staatsapparats galt nur zufällig dem Jahr 1984, und so konnte es nicht überraschen, daß zwar manche sich des Themas zur Etikettierung ihrer politischen Ambitionen bemächtigten, die Wirklichkeit des Jahres 1984 sich darin aber nicht widerspiegelte. Aus meiner Sicht gibt es nach wie vor keine Anzeichen für eine Entwicklung der Bundesrepublik zu einem Überwachungsstaat, wenngleich die staatliche Datenverarbeitung in vielen Bereichen weiter ausgebaut worden ist.

Auch in diesem Berichtsjahr habe ich bei meinen Kontrollen wieder Fälle unzulässiger oder problematischer Datenverarbeitung vorgefunden; darüber wird im folgenden Näheres berichtet. Doch sei als mein Gesamteindruck vorausgeschickt, daß — entgegen manchen widersprechenden Verlautbarungen — der Datenschutz im Jahre 1984 bemerkenswerte Fortschritte zu verzeichnen und eine deutliche Aufwertung sowohl im Bewußtsein der Betroffenen als auch bei den datenverarbeitenden Stellen erfahren hat. Dies mag einesteils daran liegen, daß Datenschutz im mittlerweile siebenten Jahr der Geltung des Bundesdatenschutzgesetzes den datenverarbeitenden Stellen vertraut geworden ist und sich als selbstverständlich zu beachtendes Element des Verwaltungshandelns weitgehend durchgesetzt hat. Als die eigentliche Ursache für diese verbesserte Akzeptanz aber werte ich das am 15. Dezember 1983 ergangene Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983, das seine über den Verfahrensgegenstand weit hinausreichende Breitenwirkung erst im Berichtsjahr zu entfalten begann. Nach eingehender Berichterstattung und Kommentierung dieser Entscheidung in den Medien, nach Vorlage sorgfältiger und inhaltlich durchaus differierender Analysen von Experten und nach auf vielen Ebenen geführten politischen Diskussionen wich anfängliche Überraschung, zuweilen auch Ratlosigkeit, der Einsicht, daß auf vielen Gebieten öffentlichen Handelns ein Umdenken unvermeidlich und jedenfalls Konsequenzen zu ziehen seien. Die Feststellungen,

— daß die Befugnis des einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen, grundrechtlich gewährleistet ist,

— daß Einschränkungen dieses Rechts nur im überwiegenden Allgemeininteresse zulässig sind und einer gesetzlichen Grundlage, die dem Gebot der Normenklarheit entsprechen muß, bedürfen,

— daß dabei der Grundsatz der Verhältnismäßigkeit zu beachten ist,

— daß zwangsweise erhobene Daten strenger Zweckbindung unterliegen und

— daß bei der Datenverarbeitung der jeweiligen Gefahrenlage angemessene organisatorische und verfahrensrechtliche Vorkehrungen zu treffen sind,

diese Feststellungen haben — wie mir auch viele Eingaben zeigten — den Bürgern mehr als die jahrelange Datenschutzdiskussion und die intensiven Aufklärungsbemühungen in der Vergangenheit deutlich gemacht, daß sie gegenüber staatlicher Datenverarbeitung nicht ohne Rechte sind und daß die datenverarbeitenden Stellen mit personenbezogenen Informationen nicht nach Belieben umgehen dürfen. Die datenverarbeitenden Stellen wiederum hat das Urteil nach meiner Beobachtung zum vertieften Nachdenken darüber gezwungen, ob ihr Handeln jeweils auch gesetzlich hinreichend abgesichert ist, und auch bei den mit Gesetzgebung und Gesetzesvorbereitung befaßten Organen sind mancherlei Zweifel entstanden, ob die bisher zur Rechtfertigung notwendiger Datenverarbeitung dienenden Vorschriften den Grundsätzen des Urteils noch entsprechen. Dazu muß kritisch angemerkt werden, daß derartige Überlegungen schon früher angebracht gewesen wären, denn die Grundgedanken des Urteils des Bundesverfassungsgerichts sind nicht neu, und die Auffassung, daß die Erhebung und Verarbeitung personenbezogener Daten Maßnahmen mit Eingriffscharakter sind, haben nicht nur die Datenschutzbeauftragten immer wieder vertreten. Was letztlich die Wirkung dieses Urteils ausmachte, war wohl die unanfechtbare Autorität, mit der die für manche unbequemen Rechtsgrundsätze verkündet worden sind, und war die Stringenz, mit der das Gericht argumentierte.

Auf Wunsch des Innenausschusses des Deutschen Bundestages habe ich eine umfassende Stellungnahme zu den Auswirkungen des Volkszählungsurteils erarbeitet und am 25. April 1984 dem Ausschuß vorgelegt. Die Stellungnahme ist entsprechend den Vorstellungen des Innenausschusses in drei Teile gegliedert: Im ersten Teil wird eine allgemeine Analyse des Urteils insgesamt gegeben, die auch im Deutschen Verwaltungsblatt 1984, Heft 13, S. 612 ff. veröffentlicht wurde. Der zweite Teil setzt sich mit dem Gesetz über Personalausweise in der Fassung der Bekanntmachung vom 15. März 1983 (BGBl. I S. 289) auseinander; unter Berücksichtigung meiner Stellungnahme wurde inzwischen ein neuer Gesetzentwurf (Drucksache 10/2177) erarbeitet; Näheres hierzu vergleiche unten Nr. 2.1. Insoweit kann hier auf eine Wiederholung meiner gutachtlichen Ausführungen verzichtet werden. Der dritte Teil der Stellungnahme schließlich befaßt sich mit Auswirkungen auf das geltende Bundesdatenschutzgesetz und enthält an den Grundsätzen des Urteils orientierte Novellierungsvorschläge. Darauf wird weiter

unten (Nr. 24) in zusammengefaßter Form näher eingegangen.

Auch der Bundesminister des Innern hat dem Innenausschuß des Deutschen Bundestages eine Stellungnahme zum Volkszählungsurteil des Bundesverfassungsgerichts vorgelegt. Sie weicht in manchen Punkten von meinen Erkenntnissen ab und sieht die Auswirkungen des Urteils insgesamt restriktiver. Beide Stellungnahmen sind bisher im Innenausschuß nicht behandelt worden, sie waren aber Gegenstand von Beratungen in einigen Landtagen oder Landtagsausschüssen, wo man die Frage der Konsequenzen für die Gesetzgebungsarbeit der Länder zum Teil sehr eingehend diskutierte.

Mittelbar, aber nachhaltig hat sich die Entscheidung des Bundesverfassungsgerichts auch auf die Arbeit meiner Dienststelle ausgewirkt. Abgesehen von der erwähnten Stellungnahme, die erheblichen Arbeitsaufwand verursachte, wurde meine Dienststelle in bisher ungewohntem Umfang um Stellungnahmen und Ratschläge zu Gesetzesvorhaben und anderen Maßnahmen gebeten — offenbar in dem Bestreben, den Anforderungen des Volkszählungsurteils an die Datenerhebung und Datenverarbeitung möglichst exakt zu entsprechen, aber auch um vorbeugend und nicht erst aufgrund nachgängiger Kritik der Datenschutzbeauftragten den vom Bundesverfassungsgericht geforderten Datenschutz zu gewährleisten.

Bei meinen Beratungen ging es aber nicht nur um rechtliche Belange. Die Fortentwicklung der Datenverarbeitungstechnik fördert den Trend, von den großen, zentralen Rechenanlagen, die die Verfasser des Bundesdatenschutzgesetzes noch im Blick hatten, überzugehen auf kleinere, aber nicht minder leistungsfähige Systeme, die dezentral eingesetzt werden können, die Datenverarbeitung an den fachlichen Arbeitsplatz verlagern und eine flexiblere Behördenorganisation gestatten. Auch daraus ergeben sich neue Datenschutzprobleme, für die es allgemeingültige Antworten nicht gibt, sondern die im Einzelfall im Beratungsgespräch mit dem jeweiligen Anwender gelöst werden müssen. In diesen Zusammenhang gehört auch meine ständige, teils kontroverse, teils konstruktive Auseinandersetzung mit der Deutschen Bundespost über die Anforderungen des Datenschutzes bei den Neuen Medien.

Die nachfolgende, keineswegs vollständige, sondern nur beispielhafte Aufzählung der Beratungsthemen, mit denen ich mich auf Wunsch von Bundesministerien oder Organen des Bundestages oder aus anderen Gründen zu befassen hatte, mag einen Eindruck davon vermitteln, in welchem Maße mein Amt durch diese mir gesetzlich obliegende Aufgabe in Anspruch genommen war:

Personalausweisgesetz
Bundeszentralregistergesetz
Steuerbereinigungsgesetz 1985
Fahrzeugregistergesetz (ZEVIS)
Änderung des Straßenverkehrsgesetzes (Führerschein auf Probe)
Bundesarchivgesetz
Volkszählungsgesetz 1986
Mikrozensusgesetz
EG-Arbeitskräftestichprobe
Hochschulstatistikgesetz
Außenhandelstatistik
Bildschirmtext-Dienst der DBP
Fernmeldeordnung
Modellversuche nach § 223 RVO
Neuordnung der Hinterbliebenenversorgung
Stiftung „Mutter und Kind"
Unfallverhütungsvorschrift VBG 100
Bewertung einzelner Personalinformationssysteme
Datenschutz bei einzelnen Forschungsvorhaben
Grundsätze für die Einrichtung von Schwarzfahrerdateien
Grundsätze für Bankauskünfte
Neugestaltung des Ausländerzentralregisters
Mitteilungen in Zivilsachen (MiZi) und Mitteilungen in Strafsachen (MiStra)
Richtlinien für die Sicherheitsüberprüfung
Richtlinien über die Zusammenarbeit zwischen Grenzpolizei und Nachrichtendiensten
Neuregelung des polizeilichen Informationsrechts
Errichtungsanordnungen für verschiedene Dateien des BKA.

Manche der dabei behandelten Problemkreise waren wegen ihrer Auswirkungen auf die Landesverwaltung mit den Datenschutzbeauftragten der Länder zu erörtern. Dies gilt u. a. für ZEVIS, MiZi und MiStra, das Volkszählungsgesetz 1986, das Mikrozensusgesetz, die Modellversuche nach § 223 RVO, das Personalausweisgesetz und die Neuregelung des polizeilichen Informationsrechts. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit ihren fachbezogenen Arbeitskreisen bot ein geeignetes Forum für diese Abstimmung, die ich für sachgerecht halte, die jedoch zusätzlich Arbeitskraft meiner Dienststelle bindet.

Es versteht sich, daß infolge dieser umfangreichen und teilweise sehr zeitraubenden Beratungstätigkeit erhebliche Abstriche insbesondere bei den umfassenderen, für das Jahr 1984 eingeplanten Kontrollen notwendig waren. Dabei ist zu bedenken, daß Kontrollen, die durch Bürgerbeschwerden veranlaßt werden, sich nicht zurückstellen lassen, weil jeder Petent Anspruch auf ein Tätigwerden des Datenschutzbeauftragten hat. Trotzdem war es unter erheblichen Anstrengungen möglich, bei folgenden Behörden und öffentlichen Stellen des Bundes die Einhaltung der Datenschutzvorschriften teils systematisch, teils bezüglich einzelner Verfahren oder Vorgänge zu kontrollieren:

Auswärtiges Amt
Bundesminister der Verteidigung
Bundestagsverwaltung
Statistisches Bundesamt
Bundesamt für den Zivildienst
Bundesgesundheitsamt
Kraftfahrt-Bundesamt
Luftfahrt-Bundesamt
Bundeskriminalamt
Bundesamt für Verfassungsschutz
Bundesnachrichtendienst
Militärischer Abschirmdienst
Grenzschutzdirektion

Bundeszentralregister
Hauptzollamt Frankfurt/Main-Flughafen
Oberpostdirektion München
Bildschirmtext-Leitzentrale Ulm
Einzelkontrollen in der Arbeitsverwaltung
Deutsche Angestellten-Krankenkasse
Bau-Berufsgenossenschaft
drei Betriebskrankenkassen.

Die Ergebnisse dieser Überprüfungen werden in den einzelnen Abschnitten dieses Tätigkeitsberichts näher dargestellt, soweit sie nach meinem Dafürhalten für den Deutschen Bundestag von Interesse sind oder anderen Behörden helfen können, vergleichbare Probleme datenschutzgerecht zu lösen.

In einem Jahresarbeitsbericht meiner Dienststelle, der nicht nur über den Stand des Datenschutzes informieren, sondern zugleich auch Tätigkeitsnachweis sein soll, darf die Beratung meiner Tätigkeitsberichte in den zuständigen Gremien des Deutschen Bundestages nicht unerwähnt bleiben. So sehr ich die eingehende Behandlung meiner Berichte in den Parlamentsausschüssen und die mir dadurch eingeräumte Gelegenheit, weitere Erläuterungen dazu zu geben, schätze und als eine erfreuliche und im Interesse der Sache und der Durchsetzung des Datenschutzes auch notwendige Maßnahme empfinde, so muß doch auch gesehen werden, daß durch die zahlreichen Sitzungstermine meine Mitarbeiter und ich in erheblichem Maße in Anspruch genommen werden. Der im Jahr 1984 im Bundestag behandelte und inzwischen mit der am 20. September 1984 verabschiedeten Beschlußempfehlung des Innenausschusses (Drucksache 10/1719) abgeschlossene Fünfte Tätigkeitsbericht ist in acht Ausschüssen, zum Teil jeweils in mehreren Sitzungen, beraten worden. Mein Sechster Bericht für das Jahr 1983 (Drucksache 10/877), dessen Einzelberatung noch aussteht, ist neun Ausschüssen überwiesen worden. Im Interesse einer kontinuierlichen Aufgabenerfüllung meiner Dienststelle, aber auch zur Entlastung der Parlamentsarbeit möchte ich daher den aus der Mitte des Innenausschusses vorgetragenen Gedanken unterstützen, die Tätigkeitsberichte in einem kleineren, möglicherweise auch aus Mitgliedern mitberatender Ausschüsse zusammengesetzten Gremium vorzuberaten, um danach die eigentlichen Ausschußberatungen auf die als besonders bedeutsam erkannten Themen beschränken zu können. Möglicherweise ließe sich so auch eine Beschleunigung der Beratungen erreichen, die bisher regelmäßig erst nach Vorlage des jeweils nächsten Berichts abgeschlossen werden konnten.

Angesichts der Aufwertung, die der Datenschutz durch das Volkszählungsurteil des Bundesverfassungsgerichts erfahren hat, und der vorerwähnten Auswirkungen auf die Arbeit meiner Dienststelle muß ich darauf bestehen, daß mir die Möglichkeit gegeben wird, die mir in § 19 Abs. 1 BDSG übertragenen Aufgaben wieder in einem ausgewogenen Anteilsverhältnis zu erfüllen. Das bedeutet, daß die im Gesetz als primäre Aufgabe genannte Kontrolltätigkeit quantitativ wieder Vorrang, zumindest aber gleiches Gewicht gegenüber der beratenden Funktion erhält. Ich halte es weder mit den Intentionen des Gesetzes noch mit dem Anspruch des Bürgers auf optimalen Schutz seiner personenbezogenen Daten für vereinbar, wenn die zur Durchsetzung des Datenschutzes auch nach meinen Erfahrungen notwendige Kontrolltätigkeit mangels ausreichender personeller Kapazität eingeschränkt werden muß. Die gegenwärtige Personalausstattung meiner Dienststelle ist in den Jahren 1977/1978 festgelegt worden. Sie beruht also auf Prognosen, die noch vor der Berufung des ersten Bundesbeauftragten angestellt worden und durch die zwischenzeitliche Entwicklung überholt sind. Eine Korrektur erscheint mir nunmehr unvermeidlich. Auch der Innenausschuß des Bundestages hat sich dieses Anliegen zu eigen gemacht und in seiner Sitzung am 17. Oktober 1984 im Rahmen der Beratung des Bundeshaushaltsplans 1985 folgendes empfohlen:

> Zu Kapitel 0607 — Der Bundesbeauftragte für den Datenschutz — ist der Innenausschuß einvernehmlich der Auffassung, daß im Rahmen der Planung für den Entwurf eines Bundeshaushaltsplans für das Haushaltsjahr 1986 die Planstellensituation im Amt des Bundesbeauftragten für den Datenschutz dargelegt und geprüft werden sollte, ob aufgrund von Mehrbelastungen, die sich für die Verwaltung und den Bundesbeauftragten für den Datenschutz im Nachgang zum Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz ergeben, die Notwendigkeit zu Planstellenausweitungen besteht und diese gegebenenfalls im Einzelplan 06 auszuweisen (vgl. Bericht des Haushaltsausschusses zum Haushaltsgesetz 1985, zu Nr. 4, Drucksache 10/2329).

Das Bundesverfassungsgericht hat wegen der für den Bürger bestehenden Undurchsichtigkeit der Speicherung und Verwendung von Daten unter den Bedingungen der automatischen Datenverarbeitung und auch im Interesse eines vorgezogenen Rechtschutzes der Beteiligung unabhängiger Datenschutzbeauftragter erhebliche Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung zugemessen. Ich habe die Sorge, daß diesem Postulat nicht hinreichend Rechnung getragen wird, wenn meine Dienststelle die von mir für notwendig gehaltenen und eingeplanten Datenschutzkontrollen infolge anderweitiger Inanspruchnahme nicht durchführen kann. Ich halte mich deshalb für verpflichtet, unter Berufung auf die erwähnte Empfehlung des Innenausschusses in den anstehenden Beratungen zum nächsten Bundeshaushalt auf eine dem Arbeitsanfall entsprechende und zugleich angesichts der angespannten Haushaltslage maßvolle Personalverstärkung meiner Dienststelle zu dringen.

1.2 Kooperation

Nach § 19 Abs. 5 BDSG habe ich auf eine Zusammenarbeit mit den für die Datenschutzkontrolle in den Ländern zuständigen Stellen hinzuwirken. Im Berichtsjahr hat die „Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der

Datenschutzkommission Rheinland-Pfalz" insgesamt viermal getagt. Besondere Schwerpunkte dieser Beratungen waren die Auswirkungen des Volkszählungsurteils (hierzu fand am 9. April 1984 eine Pressekonferenz in Bonn statt), die Neuen Medien insbesondere Bildschirmtext und die geplante Volkszählung. Diese wie aber auch andere Punkte wurden in speziellen Arbeitskreisen z. B. für Statistik, Neue Medien, innere Sicherheit oder Technik und Organisation vorberaten.

Die für die Datenverarbeitung nicht-öffentlicher Stellen zuständigen Aufsichtsbehörden der Länder stimmen ihr Vorgehen im „Düsseldorfer Kreis" ab. An den Sitzungen im Berichtsjahr nahmen stets auch Mitarbeiter meiner Dienststelle teil. Dadurch und weil mehrere Landesbeauftragte für den Datenschutz auch die Aufgaben der Aufsichtsbehörden nach §§ 30, 40 BDSG wahrnehmen und deshalb auch im Düsseldorfer Kreis vertreten sind, wird die Abstimmung zwischen den Kontrollinstanzen für den öffentlichen und denen für den nicht-öffentlichen Bereich erheblich erleichtert. Das herausragende Thema der Beratungen war das Vorgehen der Kreditinstitute bei Bankauskünften (s. Nr. 22.2 dieses Berichts).

Die Zusammenarbeit der Kontrollinstitutionen in den genannten Gremien hat sich bewährt. Sie trägt zur einheitlichen Auslegung und Anwendung des Datenschutzrechts bei und ermöglicht es, für gleiche oder vergleichbare Sachverhalte abgestimmte Lösungen zu finden.

Außer der Beteiligung an den Beratungen der Datenschutz-Kontrollinstanzen habe ich im Berichtsjahr wieder die Möglichkeit wahrgenommen, im Fachausschuß „Datenschutz und Datensicherung" der Arbeitsgemeinschaft für wirtschaftliche Verwaltung e. V. (AWV) und in einigen seiner Projektgruppen mit Vertretern großer DV-Anwender aus der privaten Wirtschaft und Herstellern von DV-Anlagen über Fragen des Datenschutzes zu diskutieren. Auch wenn gerade hier die recht unterschiedliche Interessenlage oft zu Meinungsverschiedenheiten führt, so ist doch das gegenseitige Kennenlernen der Standpunkte nützlich.

1.3 Öffentlichkeitsarbeit

Für die Beantwortung allgemeiner Fragen zum Datenschutz stehen mir drei Broschüren zur Verfügung:

— „Bürgerfibel Datenschutz", eine Einführung zum Datenschutz, die auch den Text des Bundesdatenschutzgesetzes enthält;

— „Der Bürger und seine Daten", eine Übersicht über häufig vorkommende Datenspeicherungen mit Erläuterungen der wesentlichen Zusammenhänge;

— „Der Bürger und seine Daten im Netz der sozialen Sicherung", Informationen zum Sozialdatenschutz mit einer Darstellung der wichtigsten Datenverarbeitungen sowie Erläuterungen und Abdruck der entsprechenden Datenschutzvorschriften.

Von den beiden ersten Broschüren wurden im Berichtsjahr jeweils etwa 30 000 Exemplare und von der dritten, die ich erst gegen Ende des Jahres 1983 fertiggestellt habe, etwas über 60 000 Exemplare versandt. Die Anforderungen dieser Broschüren erfolgen in erheblichem Umfang durch einzelne Interessenten, zum Teil aber auch für interessierte Gruppen gemeinsam, so z. B. für Volkshochschulkurse oder für die bei der Datenverarbeitung beschäftigten Mitarbeiter von Behörden.

Das Interesse der Medien an Fragen des Datenschutzes ist nach wie vor groß und hält erfreulicherweise auch dann an, wenn nicht gerade über Skandale oder andere spektakuläre Ereignisse mit Bezug zum Datenschutz zu berichten ist. Dies gab mir Gelegenheit zu Pressegesprächen sowie zu Interviews. Außerdem habe ich zu verschiedenen Anlässen in Vorträgen und Diskussionen in Fachgremien meine Position dargestellt, u. a. im Eröffnungsvortrag auf der Datenschutz-Fachtagung 1984 (8. DAFTA) zur Frage der Novellierung des BDSG unter Berücksichtigung des Urteils des Bundesverfassungsgerichts zur Volkszählung 1983. Auch einige meiner Mitarbeiter haben mit eigenen Aufsätzen über den Datenschutz informiert.

In größerer Anzahl als im Vorjahr haben Besuchergruppen im Rahmen der vom Bundespresseamt organisierten Besuche der Bundeshauptstadt sich in meiner Dienststelle über Fragen des Datenschutzes und meiner Kontrolltätigkeit informieren lassen und allgemeine oder persönliche Datenschutz-Probleme diskutiert. Ich begrüße dies genauso wie die Mitwirkung meiner Mitarbeiter an Seminaren politischer Bildungseinrichtungen, an Diskussionen mit anderen interessierten Gruppen sowie in den Fortbildungsveranstaltungen der Bundesakademie für öffentliche Verwaltung. Solche Veranstaltungen bieten nicht nur Gelegenheit, um Verständnis für meine Aufgabe zu werben und unbegründete Befürchtungen durch sachliche Darstellungen auszuräumen, sondern sie vermitteln mir nicht selten auch wertvolle Anregungen und konstruktive Kritik zu meiner Tätigkeit. Aus diesen Gründen engagiert sich meine Dienststelle weit stärker in der öffentlichen Auseinandersetzung um die Darstellung ihres Auftrags, als dies sonst für Behörden üblich ist.

2. Innere Verwaltung

2.1 Neue Personalausweise

Wie schon im Vorjahr so zählte auch 1984 die Problematik des fälschungssicheren und maschinenlesbaren Personalausweises zu den Hauptthemen des öffentlichen Interesses in Fragen des Datenschutzes. Die öffentliche Diskussion wie auch meine Arbeit in diesem Bereich wurden wesentlich durch das Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 bestimmt. Neben den aus diesem Urteil unmittelbar für die Volkszäh-

lung und Statistik und die anstehende Novellierung des Bundesdatenschutzgesetzes zu ziehenden Folgerungen hat das Urteil auch Wirkungen für das Personalausweisgesetz. Das Personalausweisgesetz ist dementsprechend ein wesentliches Thema meiner — auf ein entsprechendes Ersuchen — dem Innenausschuß des Deutschen Bundestages vorgelegten Stellungnahme zu den Auswirkungen des Urteils. Zusammenfassend habe ich mich darin zum Personalausweisgesetz wie folgt geäußert:

— Das Gesetz über Personalausweise in der Fassung der Bekanntmachung vom 15. März 1983 entspricht in einer Reihe von Punkten nicht den Anforderungen des Volkszählungsurteils des Bundesverfassungsgerichts und macht insoweit eine erneute Prüfung notwendig.

— Fraglich ist zunächst, ob es im überwiegenden Allgemeininteresse geboten ist, den Personalausweis maschinenlesbar zu gestalten und für bestimmte Zwecke die Nutzung der Maschinenlesbarkeit zuzulassen und ob ein möglicherweise hiermit erreichbarer Sicherheitsgewinn eine solche Ausgestaltung rechtfertigt. In die gebotene Abwägung ist eine zu befürchtende Verunsicherung der Bevölkerung einzubeziehen. Es muß daher nochmals geprüft werden, ob auf die Maschinenlesbarkeit verzichtet werden kann.

— Einige Vorschriften des Personalausweisgesetzes entsprechen nicht den Grundsätzen der Normenklarheit und Verhältnismäßigkeit oder dem Gebot der Zweckbestimmung. Den Maßstäben des Urteils ist durch Änderungen des Personalausweisgesetzes Rechnung zu tragen. Wenn auf die Nutzung der Maschinenlesbarkeit des Personalausweises nicht verzichtet wird, muß der Gesetzgeber schon aus diesem Grund die Voraussetzungen für polizeiliche Personenkontrollen und Identitätsfeststellungen präzise bestimmen und Regelungen für die Informationsverarbeitung der Sicherheitsbehörden des Bundes und der Länder sowie im Strafverfahrensrecht schaffen.

2.1.1 Notwendige Änderungen im Personalausweisgesetz

— Die Begriffe der „Einrichtung" und „Erschließung" von Dateien (§ 3 Abs. 4 und 5, § 4 Personalausweisgesetz) bedürfen aus Gründen der Normenklarheit einer Anpassung an die Terminologie bestehender datenschutzrechtlicher Vorschriften („Speicherung" und „Abruf", § 2 Abs. 2 Nr. 1 und 2 BDSG).

— In § 3 Abs. 4 Personalausweisgesetz ist — sofern in diesem Gesetz die Fälle zulässiger Speicherung der Seriennummer nicht abschließend geregelt werden — festzulegen, daß eine Speicherung der Seriennummer nicht zulässig ist, wenn dies nicht in einer bereichsspezifischen gesetzlichen Regelung ausdrücklich vorgesehen ist.

— Wird an der Maschinenlesbarkeit des Personalausweises festgehalten, dann muß die Nutzung der Maschinenlesbarkeit — wie auch die Einrichtung einer Lesezone und deren Inhalt — gesetzlich bestimmt werden.

— § 3 Abs. 5 Satz 2 Personalausweisgesetz muß aus Gründen der Normenklarheit präzisiert werden. Soll sich die Formulierung „aus Gründen der Strafverfolgung und Gefahrenabwehr" lediglich auf das Wort „Fahndung" beziehen, so ist dies klarer zum Ausdruck zu bringen.

  Auch der Begriff der „Fahndung" muß im Personalausweisgesetz präzisiert werden, solange dies nicht in anderen Gesetzen geschehen ist.

— Im Verhältnis von § 3 Abs. 4 Satz 1 zu Abs. 5 Satz 2 Personalausweisgesetz ist klarzustellen, welche der beiden Vorschriften jeweils vorrangig ist, d. h. ob und unter welchen Voraussetzungen zu den in § 3 Abs. 5 Satz 2 genannten Zwecken auch die Seriennummer gelesen und zum Abruf verwandt werden darf.

— Unter dem Gesichtspunkt der Verhältnismäßigkeit sollte sich die Ausnahme des § 3 Abs. 5 Satz 2 Personalausweisgesetz auf die „Erschließung" aus Dateien beschränken; auf die „Einrichtung" sollte also verzichtet werden. Zur Vermeidung der Entstehung von Bewegungsprofilen muß die Protokollierung von Fahndungsabfragen — gleichgültig ob aus polizeilichen Gründen oder ob aus Gründen der Datensicherheit — im Gesetz ausdrücklich ausgeschlossen werden.

— Die Nutzung der Maschinenlesbarkeit des Ausweises sollte im nicht-öffentlichen Bereich ausgeschlossen werden (§ 4 Personalausweisgesetz).

— Im Bundesgesetz sollte rahmenrechtlich festgelegt werden, daß in die örtlichen Personalausweisregister nur die in diesem Gesetz selbst festgelegten Daten aufgenommen werden dürfen. Rahmenrechtlich sollten auch die Verwendungszwecke des Personalausweisregisters bestimmt und damit sichergestellt werden, daß durch Datenübermittlung aus diesem Register — insbesondere im Falle der Übermittlung von Fotos — das Melderecht und die gesetzlichen Bestimmungen über die Anfertigung und Aufbewahrung erkennungsdienstlicher Unterlagen nicht umgangen werden.

2.1.2 Flankierende Maßnahmen zum Personalausweisgesetz

— Für die zwangsweise Erhebung von Personalausweisdaten durch Polizeibehörden in Form einer Pflicht des Bürgers zum Vorzeigen des Ausweises bedarf es ausdrücklicher gesetzlicher Befugnisnormen; sie existieren für die Polizeibehörden des Bundes und der Länder bislang nur zum Teil (z. B. § 17 BGSG, §§ 111, 163b StPO).

— Für Fahndungsausschreibungen zur polizeilichen Beobachtung und zur zollrechtlichen Überwachung sind die notwendigen gesetzlichen Grundlagen zu schaffen. Eine gesetzliche Regelung ist um so dringender, als diese Maßnahme auch Dritte, insbesondere Kontaktpersonen, betreffen kann.

— Eine gesetzliche Grundlage ist auch für die Amtshilfe des Bundesgrenzschutzes für die

Nachrichtendienste erforderlich, soweit es um die Übermittlung personenbezogener Daten geht. Dies gilt auch für die Ausschreibung von Personen im Grenzfahndungsbestand auf Ersuchen der Nachrichtendienste. Die Übermittlung erhobener Daten an den Bundesnachrichtendienst und/oder an den Militärischen Abschirmdienst setzt voraus, daß deren Befugnis zur Datenverarbeitung geregelt wird; hinsichtlich der Verfassungsschutzbehörden ist eine Neufassung bestehender Vorschriften unter dem Gesichtspunkt der Normenklarheit notwendig.

Zu den notwendigen Änderungen und den flankierenden Maßnahmen haben die Datenschutzbeauftragten des Bundes und der Länder in ihrer Konferenz am 27./28. März 1984 im gleichen Sinne Stellung genommen.

2.1.3 Änderung des Gesetzes über Personalausweise

Der Deutsche Bundestag hat inzwischen durch das Gesetz zur Änderung personalausweisrechtlicher Vorschriften bestimmt, daß der Tag des Inkrafttretens des Vierten Gesetzes zur Änderung des Gesetzes über Personalausweise durch besonderes Gesetz zu bestimmen ist. Der 1. November 1984 als Termin für die Einführung des neuen Ausweises wurde damit aufgehoben, so daß die Möglichkeit besteht, weitere Überlegungen anzustellen und den Grundsätzen des Urteils zum Volkszählungsgesetz Rechnung zu tragen.

Die Fraktionen der CDU/CSU und FDP haben im Oktober 1984 den Entwurf eines Fünften Gesetzes zur Änderung des Gesetzes über Personalausweise im Deutschen Bundestag eingebracht. Mit diesem Gesetz soll der neue Personalausweis voraussichtlich zum 1. Januar 1986 eingeführt werden. Der Entwurf enthält eine Reihe von Vorschriften, durch die der Datenschutz deutlich verbessert und den Anforderungen, die das Bundesverfassungsgericht im Volkszählungsurteil an staatliche Datenverarbeitung gestellt hat, entsprochen wird. Das gilt vor allem für die eindeutige Regelung der Zusammensetzung der Seriennummer, das Verbot der Speicherung der Seriennummer bei den Meldebehörden, die Regelungen über die Verwendung des Ausweises, die Festlegung der dafür zuständigen Behörden, das Verbot maschinellen Lesens des Ausweises im nicht-öffentlichen Bereich und — mit Einschränkungen — auch für die Vorschriften über das örtliche Personalausweisregister.

Meinen seinerzeit gegebenen Anregungen ist damit allerdings noch nicht in jeder Hinsicht Rechnung getragen. Das gilt insbesondere für das maschinelle Lesen des Ausweises. Wohl kann grundsätzlich jedes Ausweisdokument automatisch gelesen werden, und zwar je nach Ausgestaltung mit unterschiedlichem technischen Aufwand. Die Frage aber, ob im Personalausweis eine besondere Lesezone für das maschinelle Lesen vorzusehen und dieses für bestimmte Zwecke zu erlauben ist, wurde auch in diesem Entwurf bejaht, obwohl der ursprünglich dafür angegebene Grund — Verbesserung und Beschleunigung der Grenzkontrollen — wegen deren fortschreitendem Abbau inzwischen weitgehend nicht mehr besteht. Die ausnahmsweise Zulassung des Abrufs und der Speicherung von Daten unter Nutzung der maschinellen Lesbarkeit des Ausweises eröffnet Online-Datenübermittlungen, für die nach allen bisherigen Vorstellungen zur BDSG-Novellierung eine Abwägung der Belange aller Beteiligten erforderlich ist (vgl. 5. TB, S. 113; Entwurf eines Gesetzes zur Änderung des BDSG, Drucksache 10/1180 Artikel 1 Nr. 7 — § 3b —). Die als Ergebnis dieser Abwägung getroffene Entscheidung, daß das Direktabrufverfahren angemessen ist, bedarf daher einer Begründung.

Auch angesichts des gesteigerten Interesses, das diese Problematik in der öffentlichen Diskussion gefunden hat, kann auf eine überzeugende Begründung für die Zulassung des automatischen Lesens nicht verzichtet werden. Staatlicher Zwang, der den Interessen der Bürger widerspricht, kann — wie das Bundesverfassungsgericht im Volkszählungsurteil ausgeführt hat — nur begrenzt wirksam werden, wenn sich der Staat nicht durch Offenlegung der Datenverarbeitungsprozesse um Vertrauen bemüht. Um die Kooperationsbereitschaft der Bürger zu gewährleisten, von der das Gericht spricht, sollte den Bürgern daher mehr Information gegeben werden. Die bei Einbringung des Entwurfs am 25. Oktober 1984 im Deutschen Bundestag gegebene Begründung, daß man sich den technischen Fortschritt zunutze machen müsse und es nicht darauf ankomme, auf welche Weise Daten in ein Computersystem gelangen, wenn nur deren Verwendung geregelt ist, reicht m. E. nicht aus. Denn mit dem in dem Entwurf vorgesehenen Ausweis, seiner speziellen Lesezone und den dafür entwickelten Lesegeräten wird eine gleichförmige Infrastruktur für personenbezogene Datenverarbeitung geschaffen, die ohne nennenswerten zusätzlichen Aufwand auch ganz andere Nutzungen ermöglicht. Die Schwelle für die Zulassung weiterer Datenerfassungen wird dadurch niedriger und neue Gefährdungen der Privatsphäre des Bürgers sind nicht auszuschließen. Derartige Entwicklungen — einmal in Gang gesetzt — sind kaum aufzuhalten.

Vor dem Hintergrund der Forderungen der Datenschutzbeauftragten nach flankierenden Maßnahmen im Sicherheitsbereich sind die Erklärungen der Sprecher der Koalitionsfraktionen in der ersten Beratung des Gesetzentwurfs im Deutschen Bundestag am 25. Oktober 1984 zu begrüßen, das Gesetz solle nicht in Kraft treten, bevor nicht eine Verständigung über die notwendigen bereichsspezifischen Regelungen im Sicherheitsbereich erzielt ist. Besonders dann, wenn auf die Nutzung der maschinellen Lesbarkeit des Personalausweises nicht verzichtet wird, müssen die gesetzlichen Voraussetzungen für polizeiliche Personenkontrollen und Identitätsfeststellungen präzise bestimmt und Regelungen für die Informationsverarbeitung der Sicherheitsbehörden des Bundes und der Länder sowie im Strafverfahrensrecht geschaffen werden. Erst wenn insoweit Entwürfe vorliegen, ist mir eine datenschutzrechtliche Gesamtbewertung des neuen Entwurfs möglich.

2.2 Neukonzeption des Ausländerzentralregisters (AZR)

Die Arbeitsgruppe „Neukonzeption des Ausländerzentralregisters", deren Bildung durch den Bundesminister des Innern ich schon in meinem vorigen Tätigkeitsbericht (6. TB S. 9) erwähnt habe, hat 1984 ihre Arbeit aufgenommen. Sie hat die Aufgabe, eine entscheidungsreife Vorlage zu erarbeiten, die — unbeschadet der Mitarbeit von Vertretern einzelner Bundes- und Landesverwaltungen — in einem späteren Verfahrensschritt Grundlage offizieller Abstimmung mit den Landesregierungen und zwischen den Bundesressorts sein soll.

In den Beratungen habe ich von Anfang an darauf hingewiesen, daß sich die Tätigkeit der Arbeitsgruppe nicht darin erschöpfen darf, Klarheit über die künftige Aufgabenstellung des Registers zu gewinnen, sondern daß auch der Datenschutz angemessen berücksichtigt werden muß. Eine Auflistung von Datenfeldern unter Beschränkung auf das unabweislich Erforderliche sowie eine Darstellung der Kommunikationsstruktur, die — bezogen auf einzelne Datenfelder — die Datenanlieferungspflichtigen und die Zugriffsberechtigten nennt, sind wichtige Arbeitsschritte. Sie sind Voraussetzung für das Vorhaben, den Personenkreis, über den im AZR Daten geführt werden, den Registerinhalt sowie Zugriffsberechtigungen und Beschränkungen der Verwendungszwecke der Daten gesetzlich festzulegen; dies gilt besonders auch für die notwendige Differenzierung zwischen konventionellem und Online-Zugriff. Vor diesem Hintergrund habe ich es begrüßt, daß der Bundesminister des Innern zum Vorgehen der Arbeitsgruppe die Überprüfung der Rechtsgrundlagen des Registers und die Erarbeitung von Vorschlägen zur Schaffung einer ausreichenden gesetzlichen Grundlage als den nächsten wichtigen Schritt bezeichnet hat.

Für die Wirksamkeit dieser Bemühungen, namentlich für die notwendige Prüfung der Erforderlichkeit einzelner Datenfelder, hat sich die Mitwirkung von Vertretern beteiligter Behörden (u. a. Ausländerbehörden, Grenzschutzdirektion) als fruchtbar erwiesen. Die Vorschläge für den Registerinhalt sind im wesentlichen fertiggestellt, wobei verglichen mit dem AZR alter Konzeption eine deutliche Entlastung des Registers und damit auch der übermittelnden Stellen vorgesehen ist. Mit der eingeleiteten Prüfung der Kommunikationsstruktur und der Rechtsgrundlagen stehen weitere wichtige Arbeitsschritte bevor.

2.3 Bundesamt für den Zivildienst

Durch das Kriegsdienstverweigerungs-Neuordnungsgesetz ist mit Wirkung vom 1. Januar 1984 das Anerkennungsverfahren für Kriegsdienstverweigerer neu geregelt worden. Danach entscheidet jetzt das Bundesamt für den Zivildienst über den Antrag eines noch nicht einberufenen Wehrpflichtigen (als Einberufung in diesem Sinne gilt auch die vorsorgliche Benachrichtigung über die mögliche Einberufung als Ersatz). Zur Durchführung der Antragsprüfung bedurfte es einer Umorganisation des Amtes. Im Rahmen einer datenschutzrechtlichen Kontrolle habe ich die Behandlung der Anträge auf Anerkennung als Kriegsdienstverweigerer geprüft.

Ich konnte mich davon überzeugen, daß das Bundesamt für den Zivildienst mit den sensiblen Unterlagen sorgfältig umgeht. Entgegen den Erwartungen hat sich dabei gezeigt, daß die Begründung der Anträge auf Kriegsdienstverweigerung weiterhin häufig ebenso sensible personenbezogene Angaben enthält, wie sie nach dem früheren Antragsverfahren offenbart werden mußten.

Ich bin deshalb mit dem Bundesamt für den Zivildienst und dem Bundesminister für Jugend, Familie und Gesundheit, als dem zuständigen Ressort, im Gespräch darüber, ob und mit welchen Mitteln ein zusätzlicher Schutz des Anerkennungsteils der Kriegsdienstverweigerer-Akte erreicht werden kann. Dies wird dadurch erleichtert, daß nach der Anerkennung die Antragsbegründung und der Lebenslauf nur selten benötigt werden. Ich rechne deshalb in Kürze mit einer sachgerechten Lösung.

2.4 Wahlrecht

Im Rahmen der Vorbereitung von Kommunalwahlen ist mir wiederholt die Frage gestellt worden, ob die in Gemeindewahlordnungen geforderte öffentliche Bekanntgabe des Geburtsdatums des vorgeschlagenen Kandidaten in den Wahlvorschlägen den Grundsätzen des Datenschutzes entspricht. Da die Bundeswahlordnung ebenfalls die Angabe des Geburtsdatums fordert, habe ich den Bundesminister des Innern um Prüfung gebeten, ob die Bekanntgabe des vollständigen Geburtsdatums erforderlich ist. Zugleich habe ich angeregt, lediglich das Geburtsjahr des vorgeschlagenen Kandidaten in den Wahlvorschlägen anzugeben oder jedenfalls die öffentliche Bekanntmachung hierauf zu beschränken.

Nach Auffassung des Bundesministers des Innern kann auf die Angabe der genauen Geburtsdaten zur Identifizierung von Wahlbewerbern in Wahlvorschlägen zur Wahl des Deutschen Bundestages (Kreiswahlvorschlägen und Landeslisten) nicht verzichtet werden. Bei einer nur mangelhaften Bezeichnung eines Bewerbers liege kein gültiger Wahlvorschlag vor, der deshalb zurückgewiesen werden müßte. Für die Identifizierung einer Person sei das Geburtsdatum von entscheidender Bedeutung, insbesondere um bei Namensgleichheit Verwechselungen auszuschließen. Die bloße Angabe des Alters oder des Geburtsjahres der Bewerber in Wahlvorschlägen bietet sich nach Ansicht des Bundesministers des Innern nicht als Alternative an.

In Übereinstimmung mit einer zu dieser Frage vorliegenden Stellungnahme des Niedersächsischen Ministers des Innern bleibe ich bei meiner Auffassung, daß die Kenntnis des genauen Geburtstages für die Willensbildung des Wählers nicht von Bedeutung ist. Sofern Wahlbewerber — aus welchen Gründen auch immer — Tag und Monat der Geburt

der Öffentlichkeit nicht mitteilen möchten, sollte sich die Bekanntmachung künftig auf die Angabe des Geburtsjahres oder des Alters des Bewerbers beschränken. Ich halte eine entsprechende Änderung der Bundeswahlordnung für angezeigt.

2.5 Personenstandswesen

Nach den in meinem Sechsten Tätigkeitsbericht (6. TB S. 12 f.) wiedergegebenen Empfehlungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 6./7. Juni 1983 und der Entscheidung des Bundesverfassungsgerichts zum Volkszählungsgesetz begrüße ich die Mitteilung des Bundesministers des Innern, „eine bereichsspezifische rechtssatzmäßige Regelung der Mitteilungen im Personenstandswesen erscheine angebracht".

Wie von mir schon früher gefordert wurde, (vgl. 6. TB S. 12 f.) ist nunmehr in einer Sechsten Allgemeinen Verwaltungsvorschrift zur Änderung der Allgemeinen Verwaltungsvorschrift zum Personenstandsgesetz (6. DA-ÄndVwV) vorgesehen, daß

- die Pflicht des Standesbeamten, bei Eintragungen über umherziehende Personen ohne festen Wohnsitz die Kriminalpolizei zu unterrichten, künftig entfällt,
- Angaben über empfangene Versorgungsleistungen und deren Mitteilung an die Versorungsämter künftig entfallen,
- bei einer Adoption eine Mitteilung des Standesbeamten an die Meldebehörde der leiblichen Eltern des adoptierten Kindes nicht mehr stattfindet.

Ich habe angeregt, dem Grundsatz der Zweckbestimmung und Zweckbindung der zu übermittelnden Daten besonderes Gewicht zu geben. Nach meiner Auffassung bedarf es nicht nur einer konkreten Ermächtigung zum Erlaß einer Verordnung über Mitteilungspflichten, sondern auch der Prüfung, ob die für die Tätigkeit des Datenempfängers geltenden Gesetze den Anforderungen der Zweckbestimmung und Zweckbindung genügen. Entsprechende Regelungen wären bei Erforderlichkeit der Mitteilungen gesetzlich zu treffen, sei es in den die Empfänger betreffenden flankierenden Regelungen, sei es im Personenstandsgesetz selbst.

Ferner bin ich der Auffassung, daß der Verzicht auf das Aufgebot durch entsprechende Gesetzesänderungen nicht länger aufgeschoben werden sollte, zumal hierüber — wie mir von den Bundesministern des Innern und der Justiz erneut bestätigt wurde — Einvernehmen unter allen Beteiligten besteht.

2.6 Bundesnotaufnahmeverfahren

Ich habe mit dem Bundesminister des Innern bereits in den Jahren 1981/82 den möglichen Inhalt von „Richtlinien über die Weitergabe von Akten durch die Dienststellen des Bundesnotaufnahmeverfahrens an andere Behörden" erörtert. Gleichwohl ist eine abschließende Fassung der Richtlinien vorerst nicht erarbeitet worden.

Inzwischen habe ich Zweifel, ob Richtlinien noch eine geeignete Grundlage für Auskünfte sein können. Es geht dabei um folgende Fragen:

- Welche personenbezogenen Daten werden im Bundesnotaufnahmeverfahren von den zuständigen Dienststellen an andere Behörden weitergegeben (Feststellungen in tatsächlicher Hinsicht)?
- Welche Einschränkungen des Rechts auf informationelle Selbstbestimmung sind im überwiegenden Allgemeininteresse notwendig (Erfordernisprüfung)?
- Welche Rechtsgrundlagen sind hierfür vorhanden oder müssen hierfür (unter Berücksichtigung der Prinzipien der Normenklarheit und Verhältnismäßigkeit) geschaffen werden? Welche Verwertungsbeschränkungen (insbesondere Verbote der Weiterübermittlung dieser so gewonnenen Erkenntnisse) sind eventuell mit der Übermittlung zu verknüpfen?

Diese von mir dem Bundesminister des Innern gestellten Fragen betreffen nicht erst die Weitergabe von Akten nach Abschluß des Verfahrens, sondern schon die Übermittlung personenbezogener Daten vor der Entscheidung über die Notaufnahme. Einer Anwendung des § 4 des Verwaltungsverfahrensgesetzes steht zumindest entgegen, daß ein Amtshilfeersuchen seinem Wesen nach nur ein Ersuchen um Hilfe im Einzelfall bedeutet. Es darf nicht auf Dauer angelegt sein, etwa derart, daß die ersuchte Behörde ständig bestimmte Dienstgeschäfte für die auftraggebende Behörde durchführt.

Was die Datenübermittlung an sogenannte „Leistungsverwaltungen" anbelangt, an Stellen also, von denen der Betroffene die Gewährung von Leistungen, Vergünstigungen, Hilfe etc. zu erwarten hat, so habe ich gebeten zu prüfen, ob solche Übermittlungen nicht ausnahmslos von der Zustimmung des Betroffenen abhängig zu machen sind.

2.7 Waffengesetz

Im Sommer 1984 hat die Bundesregierung einen umfangreichen Gesetzentwurf zur Änderung des Waffengesetzes vorgelegt. Gespräche mit Datenschutzbeauftragten der Länder haben ergeben, daß die Datenerhebung im Zusammenhang mit der Ausstellung von Waffenbesitzkarten und Waffenscheinen sowie die Zuverlässigkeitsprüfung im Genehmigungsverfahren mit den hierbei vorgesehenen Anfragen bei anderen Behörden datenschutzrechtliche Probleme berühren und im Waffengesetz geregelt werden sollten. Dies gilt z. B. für die Frage, ob und in welchem Umfang Auskunft aus polizeilichen Dateien zu erteilen ist. Ich habe Zweifel, ob die dazu in der Allgemeinen Verwaltungsvorschrift zum Waffengesetz enthaltenen Vorschriften ausreichend sind. Ebenso wie einige Datenschutzbeauftragte der Länder sich mit entsprechenden Initiati-

ven an die Innenminister ihrer Länder gewandt haben, habe ich den Bundesminister des Innern um Stellungnahme zu dieser Problematik gebeten. Eine Antwort liegt mir noch nicht vor.

3. Auswärtiger Dienst

Eine von mir im Berichtsjahr durchgeführte Kontrolle des Auswärtigen Amtes hat ein insgesamt hohes Maß an Sorgfalt im Umgang mit personenbezogenen Daten erkennen lassen. Allerdings teile ich nicht die Auffassung des Auswärtigen Amtes, daß die diplomatischen und berufskonsularischen Auslandsvertretungen mit der Zentrale in Bonn eine „ministerielle Einheit" bildeten und daher die Datenweitergabe zwischen diesen Stellen keine Datenübermittlung an Dritte im Sinne des § 2 Abs. 3 Nr. 2 BDSG sei. Im Zusammenhang mit personal- und haushaltsrechtlichen Fragen wird von der „ministeriellen Einheit" der Auslandsvertretungen und der Zentrale in Bonn ausgegangen. Dieses Konzept kann jedoch nicht für den Datenschutz gelten, da anderenfalls § 10 Abs. 1 BDSG (Datenübermittlung zwischen öffentlichen Stellen) im Bereich des Auswärtigen Dienstes wirkungslos würde. Ich halte deshalb daran fest, daß jede Auslandsvertretung und die Zentrale in Bonn jeweils eigene Stellen im Sinne des § 7 Abs. 1 BDSG sind. Die abweichende Auffassung des Auswärtigen Amtes ist jedoch bislang ohne praktische Auswirkungen geblieben, weil bei Übermittlungen zwischen den genannten Stellen die datenschutzrechtlichen Grundsätze, insbesondere das Erforderlichkeitsprinzip, beachtet werden. Die Praxis verdient jedoch weiterhin kritische Aufmerksamkeit.

Weiterer Prüfung bedarf das Verfahren der Mitteilungen von Festnahmen, Verurteilungen und Entlassungen von deutschen Staatsangehörigen in Ostblock-Ländern. Von den Auslandsvertretungen werden solche Daten — wenn die Vertretungen hiervon verläßliche Kenntnis erhalten — an das Auswärtige Amt und von dort an eine Reihe von Behörden übermittelt. Über die Erforderlichkeit dieser Übermittlungen lasse ich mich von den Bundesministern des Innern und der Justiz informieren.

Wird einem Deutschen im Ausland finanzielle Hilfe gewährt, so erhält der Paß des Betroffenen nach einem Erlaß des Auswärtigen Amtes von 1981 einen codierten Eintragungsvermerk. Diese Praxis erscheint mir datenschutzrechtlich problematisch. Im Hinblick auf Überlegungen zum künftigen Paßrecht sollte der Bundesminister des Innern in die weitere Diskussion dieser Problematik einbezogen werden.

In Fällen, in denen Visa-Anträge auf eine private Einladung aus der Bundesrepublik gestützt werden, kann nach § 7 Abs. 4 Ausländergesetz die Aufenthaltserlaubnis mit Bedingungen versehen werden. Ich habe gegenüber dem Auswärtigem Amt angeregt, das Erklärungsformular über eine Bürgschaft für Reisekosten auf die Erforderlichkeit der darin vorgesehenen Angaben zu überprüfen. Das Auswärtige Amt hat diese Anregung aufgegriffen und will auf einige personenbezogene Angaben (z. B. finanzielle Belastungen des bürgenden Gastgebers) künftig verzichten. Derzeit wird ein neues Erklärungsformular in Abstimmung mit mir vorbereitet.

Als verbesserungsbedürftig hat sich auch das Verfahren der Ausgabe, Aufbewahrung und Vernichtung von EDV-Personallisten erwiesen. In dem nunmehr vorgesehenen Prinzip, daß bei Ausgabe einer neuen Liste der Empfänger die überholten Ausdrucke zurückzugeben hat („neu gegen alt"), sehe ich eine deutliche Verbesserung der früheren Regelung. Aus gegebenem Anlaß habe ich besonders darauf hingewiesen, daß es nicht nur auf geeignete technisch-organisatorische Regelungen dieser Art ankommt, sondern ebenso auf deren Einhaltung und eine entsprechende Überwachung.

4. Rechtswesen

4.1 Bundeszentralregister

Beim Bundeszentralregister (BZR) habe ich im Berichtsjahr wiederum eine Kontrolle durchgeführt, die an die Vorjahresprüfung anschloß und schwerpunktmäßig eine Reihe spezifischer Fragen zum Gegenstand hatte. Sie ließ erneut die große Aufgeschlossenheit der Mitarbeiter des BZR für die Anforderungen des Datenschutzes deutlich werden. Sie hat aber zugleich auch gezeigt, daß weiterhin über mögliche Schwachstellen und praktische Möglichkeiten der Verbesserung des Datenschutzes ein intensiver Dialog geführt werden muß.

Zur Veranschaulichung seien einige Problempunkte herausgegriffen:

— Für eine unbeschränkte Auskunft an eine oberste Bundes- oder Landesbehörde reicht „Verwaltungsangelegenheit" als Zweckangabe im Sinne von § 41 Abs. 4 i. V. m. Abs. 1 Nr. 2 BZRG nicht aus. Während ich noch in meinem Sechsten Tätigkeitsbericht über die abweichende Auffassung des Bundesministers der Justiz berichtete (vgl. S. 11 f.), hat dieser nunmehr nach weiterer Erörterung der Angelegenheit durch Erlaß vom April 1984 angeordnet, daß Auskunftsersuchen mit mangelnden oder ungenauen Zweckangaben („Verwaltungsangelegenheit", „Personenkontrolle" o. ä.) zurückzusenden sind. Die Wirksamkeit der Anordnung wird im Jahre 1985 in einem gesonderten Prüfprogramm kontrolliert werden.

— Im Hinblick auf die Ergebnisse meiner Prüfung eines Hauptzollamtes (6. TB S. 16 f.) begrüße ich es, daß nunmehr die Registerführer angewiesen sind, den Finanzbehörden eine Auskunft nach § 41 Abs. 4 i. V. m. Abs. 1 Nr. 4 BZRG nur zu erteilen, wenn als Zweck ein *Straf*verfahren genannt wird („Steuerstrafsache" o. ä.); das Ersuchen ist also zurückzuweisen, wenn als Zweck „Steuersache" oder „Steuerordnungswidrigkeit" angegeben ist. Auch die Wirksamkeit dieser Anordnung wird von mir in einem gesonderten Programm kontrolliert werden.

— Bedenken habe ich dagegen geäußert, einer Justizvollzugsbehörde eine unbeschränkte Aus-

kunft nach § 41 Abs. 1 Nr. 1 BZRG zur Überprüfung eines ehrenamtlichen Mitarbeiters zu erteilen. Nach dieser Vorschrift darf einer Justizvollzugsbehörde Auskunft „für Zwecke des Strafvollzugs" erteilt werden. Ich vertrete die Auffassung, daß sich diese Auskünfte auf Personen beziehen müssen, die von der genannten Aufgabe betroffen sind, nicht aber diese Aufgabe erfüllen. Läßt man hingegen eine Erteilung von Auskünften zu, die der Überprüfung derer dienen, die diese Aufgaben zu erfüllen haben, so wäre dies nicht ohne präjudizielle Wirkung für das Verständnis und die Anwendung der übrigen Auskunftsfälle des § 41 Abs. 1 BZRG. Für den Fall, daß der Bundesminister der Justiz nach weiterer Erörterung die Erteilung einer unbeschränkten Auskunft zur Überprüfung ehrenamtlicher Mitarbeiter für erforderlich hält, sollte eine Änderung der Rechtsvorschrift erwogen werden.

— Nur in einem Einzelfalle gab es bislang Anhaltspunkte dafür, daß die Art der Adressierung einer Auskunft ihre Fehlleitung verursacht haben könnte. Das Problem der Zuverlässigkeit der Adressierung verdient gleichwohl Aufmerksamkeit. Ich habe angeregt, zunächst im Bereich der unbeschränkten Auskunft zu prüfen, inwieweit für die unter den einzelnen Nummern des § 41 Abs. 1 BZRG genannten Auskunftsberechtigten abschließend Behördenkennzeichen vorhanden sind bzw. mit vertretbarem Aufwand beschafft werden können. Zweifel haben sich auch ergeben, ob Datenschutz besser gewährleistet ist, wenn die Behördenadresse durch die Namensangabe präzisiert ist. Nach dem vorläufigen Stand der Diskussion scheint es vielmehr angezeigt, von Namensbezeichnungen abzusehen und Funktionsbezeichnungen den Vorzug zu geben.

— Als ein Problem wurde auch der Inhalt von Auskünften bei Änderungen des Geburtsnamens (durch Namensänderung oder Adoption) und bei Änderung des Vornamens (nach dem Transsexuellengesetz) festgestellt. Dabei handelt es sich um die Erforderlichkeit von Hinweisen auf den vor der Namensänderung geführten Namen im Falle von Eintragungen, die unter diesem früheren Namen entstanden sind. Einen Verzicht auf Hinweise auf den früheren Namen halte ich in den Fällen für geboten, in denen nicht davon auszugehen ist, daß die Bearbeitung beim Empfänger ohnehin zur Offenbarung der früheren Identität des Betroffenen führt. Dies sollte jedenfalls für das Führungszeugnis gelten.

— Verbesserungen des Datenschutzes sind m. E. auch in bezug auf die Authentizität der Mitteilungen an das Bundeszentralregister notwendig und möglich, auch wenn es sich hier nicht spezifisch um die Verantwortung des Bundeszentralregisters handelt. Der Authentizität der Mitteilungen dienen von der Bundesdruckerei erstellte und fortlaufend numerierte Vordrucke. Sofern dies noch nicht geschieht, habe ich empfohlen, daß die Bundesdruckerei Aufschreibungen darüber führt, an welche Stellen welche Nummernserien vergeben sind. Auch wäre mit den Landesjustizbehörden zu klären, ob und welche Verwendungsnachweise geführt werden, um z. B. einen etwaigen Verlust von Blanko-Formularen zu erkennen.

— Auf die Problematik der Suchvermerke habe ich schon 1981 in meinen dem Bundesminister der Justiz zugesandten Vorschlägen zur Novellierung der BZRG hingewiesen. Sie liegt — wie die jetzige Erörterung erneut gezeigt hat — darin, daß die suchende Behörde — auch wenn ihr kein Recht zusteht, eine unbeschränkte Auskunft zu erlangen — durch einen Hinweis auf eine Behörde, die eine Registermitteilung macht, oft zugleich Näheres über Verfahren erfährt, von denen der Betroffene berührt war. Viele Aktenzeichen (Geschäftsnummern) sind zudem „sprechend", d. h. sie geben hierüber einen weiteren Aufschluß. Die Schranken des § 41 BZRG werden damit durchbrochen. Abhilfe wird m. E. nur durch eine Änderung der §§ 27 ff. BZRG erreicht werden können. Als Lösung käme in Betracht, daß nicht unbeschränkt auskunftsberechtigte Behörden nur über vorliegende Adressen des Betroffenen unterrichtet werden, nicht aber Hinweise auf andere Behörden und Geschäftszeichen erhalten.

— Das Bundeszentralregister stellt jährlich für etwa 30 Forschungsvorhaben gemäß § 42 Abs. 2 BZRG personenbezogene Daten zur Verfügung. Ich habe mich davon überzeugt, daß das BZR besonders bei der Prüfung des wissenschaftlichen Anspruchs und der Zuverlässigkeit des Empfängers Sorgfalt walten läßt. Die Übermittlung wird an Auflagen gebunden. Solche sind zur sicheren Verwahrung der empfangenen Daten insbesondere dann angezeigt, wenn es sich um Vorhaben handelt, die sich über lange Zeiträume erstrecken. Ich habe empfohlen, dieser Praxis des BZR auch in § 42 Abs. 2 BZRG Ausdruck zu geben und — wie von mir schon 1981 in Novellierungsvorschlägen gegenüber dem Bundesminister der Justiz angeregt — klarzustellen, daß die Daten nur für den angegebenen Forschungszweck verwendet und die Ergebnisse nur in anonymisierter Form veröffentlicht werden dürfen.

Meine Bemühungen bezwecken nach wie vor nicht nur eine angemessene Datenschutzpraxis, sondern auch eine Verbesserung der Rechtsgrundlagen. Das Zweite Gesetz zur Änderung des Bundeszentralregistergesetzes hat nur einen meiner schon vor Jahren dem Bundesjustizminister vorgelegten Vorschläge berücksichtigt (Entfernung von Hinweisen auf eine frühere Entmündigung im Sinne von § 9 durch Ergänzung des § 25 BZRG). Um so wichtiger ist es, daß — wie in den Beratungen des Entwurfs des Zweiten Änderungsgesetzes unterstrichen wurde — der Bundesminister der Justiz in einem baldmöglichst vorzulegenden Entwurf eines Dritten Gesetzes zur Änderung des Bundeszentralregistergesetzes meine Anregungen berücksichtigt.

4.2 Mitteilungen in Strafsachen

In meinem Sechsten Tätigkeitsbericht (S. 14) habe ich über Vorschläge einer Arbeitsgruppe der Landesjustizverwaltungen für eine Neufassung der Anordnung über Mitteilungen in Strafsachen (MiStra) berichtet. Durch die Entscheidung des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 sieht sich der Bundesminister der Justiz insofern vor eine neue Situation gestellt, als eine Verwaltungsvorschrift als Regelungsform für derartige Mitteilungen nicht mehr ausreicht. Auch ich halte es für sachgerecht, die zunächst vorgesehene weitere Beratung einzelner Regelungsinhalte der MiStra zurückzustellen, bis die Prüfung der Gesetzgebungskompetenz und der gesetzlichen Grundlage sowie der hieraus zu ziehenden Folgerungen abgeschlossen ist. Hierbei kommen dem durch das Volkszählungsurteil bestätigten Grundsatz der Zweckbestimmung und Zweckbindung der Daten besonderes Gewicht zu. Art, Umfang, denkbare Verwendungen der in Betracht kommenden Daten und damit verbundene Mißbrauchsrisiken sind zu berücksichtigen. Eine gesetzliche Ermächtigung, die die Zweckbestimmung dem Verordnungsgeber überläßt, wäre m. E. für die MiStra nicht unproblematisch. Soweit daran gedacht wird, in Verbindung mit einer gesetzlichen Ermächtigung einzelne Mitteilungspflichten zum Inhalt einer Rechtsverordnung zu machen, muß gefordert werden, im Gesetz selbst die Zwecke zu umschreiben, dem Verordnungsgeber also nur ihre Präzisierung zu überlassen. Unter den genannten Gesichtspunkten habe ich erhebliche Bedenken gegen Vorschläge, neben einzelnen Vorschriften generalklauselartige Zusatzregelungen vorzusehen. Um die im Interesse des Datenschutzes sowie einer Minderung der Arbeitslast der Geschäftsstellen der Gerichte erstrebte Reduzierung der Mitteilungspflichten zu erreichen, halte ich es mit den Landesbeauftragten für den Datenschutz für wichtig, besonders die Regelungen über Mitteilungen in bezug auf solche Personen zu überprüfen, die einer Dienst-, Staats- oder Standesaufsicht unterliegen. In allen genannten Punkten sollten die Regelungen derart präzise sein, daß ein Entscheidungsspielraum nicht besteht und daher die Geschäftsstelle die Mitteilung unmittelbar vollziehen kann. Die notwendige Abwägung im Einzelfalle sollte die Ausnahme bilden, dann aber dem Richter oder dem Staatsanwalt selbst vorbehalten bleiben.

Gespräche mit Vertretern des Bundesministers der Justiz und mit dem Leiter des Bundeszentralregisters haben Zusammenhänge zwischen den Bemühungen um eine Überarbeitung der MiStra und den Regelungen des Bundeszentralregistergesetzes deutlich werden lassen. Ich habe den Bundesminister der Justiz zu einer Prüfung der folgenden Fragen angeregt:

— Kann die Übermittlung und Verwendung von Daten, die sich auf Strafverfahren oder Strafverfolgungsmaßnahmen beziehen, in einem einheitlichen Gesetz (unter Einschluß der bisherigen Auskunftsregelungen des Bundeszentralregistergesetzes, der MiStra, der Strafprozeßordnung und der Richtlinien für das Strafverfahren und das Bußgeldverfahren) geregelt werden?

— Wie kann eine zeitliche Beschränkung und Zweckbindung der Verwertung der aufgrund der MiStra erhaltenden Mitteilungen erreicht und mit den Tilgungsvorschriften und Verwertungsverboten nach dem BZRG in Einklang gebracht werden?

— Wie kann generell verhindert werden, daß die Fristen des BZRG durch Parallelspeicherungen bei anderen Behörden (gleichgültig, ob die Auskünfte aus dem BZR, aufgrund der MiStra oder auf andere Weise erlangt wurden) unterlaufen werden?

— Wie kann sichergestellt werden, daß Auskünfte (gleichgültig, ob die Auskünfte aus dem BZR, aufgrund der MiStra oder auf andere Weise erlangt wurden) nicht an Dritte weitergegeben werden, sondern strenger Zweckbindung unterliegen?

4.3 Richtlinien für das Strafverfahren und das Bußgeldverfahren

Ich begrüße es, daß der Bundesminister der Justiz bezüglich der Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV) — namentlich hinsichtlich der in meinen früheren Tätigkeitsberichten (5. TB S. 19f., 6. TB S. 14) erörterten Bestimmungen über Akteneinsicht, Auskünfte und Erteilung von Abschriften — davon ausgeht, daß nach der Entscheidung des Bundesverfassungsgerichts zum Volkszählungsgesetz Regelungen der genannten Art nunmehr einer gesetzlichen Grundlage bedürfen. Die daraufhin eingeleitete umfassende Überprüfung der Richtlinien führte allerdings dazu, daß die ursprüngliche Absicht, das Akteneinsichtsrecht des Beschuldigten (vgl. meine Vorschläge hierzu im 6. TB S. 14) in die Beratungen zum Strafverfahrensänderungsgesetz 1984 einzubringen, wieder aufgegeben wurde. Ich hoffe, daß die vom Bundesminister der Justiz eingeleitete Behandlung der RiStBV in einem Unterausschuß der Justizministerkonferenz bald zu Ergebnissen führt.

4.4 Überprüfung von Urlaubsanschriften und Bezugspersonen von Strafgefangenen

Hinweise von Landesbeauftragten für den Datenschutz haben erkennen lassen, daß Justizvollzugsanstalten bei der Überprüfung von Urlaubsanschriften und Bezugspersonen von Strafgefangenen im Rahmen der Gewährung von Vollzugserleichterungen unterschiedlich verfahren: Teils werden Auskünfte — etwa von der Polizei oder vom Sozialamt — nur mit Einwilligung der jeweiligen Bezugsperson eingeholt, teils auch ohne deren Einwilligung und teils werden solche Auskünfte nicht für erforderlich gehalten. Die in Betracht kommenden Rechtsvorschriften des Strafvollzugsgesetzes (§§ 13 und 14) bieten meines Erachtens keine hinreichende Klarheit darüber, ob und welche Einschränkungen des Rechts auf informationelle Selbstbe-

stimmung Bezugspersonen im überwiegenden Allgemeininteresse hinnehmen müssen und ob sie daher gegebenenfalls auch ohne eine Einwilligung ein solches Auskunftsverfahren dulden müssen.

Ich habe den Bundesminister der Justiz auf diese Problematik aufmerksam gemacht und um Stellungnahme gebeten.

4.5 Mitteilungen in Zivilsachen

Nachdem entsprechende Vorschläge der Datenschutzbeauftragten die Justizverwaltungen bisher nicht zu der geforderten umfassenden Prüfung der Mitteilungspflichten nach der Anordnung über Mitteilungen in Zivilsachen (MiZi) veranlassen konnten, begrüße ich die Feststellung der Bundesregierung, daß auch hier durch das Volkszählungsurteil „eine veränderte rechtliche Lage eingetreten" ist. Der Bundesminister der Justiz hat inzwischen die Landesjustizverwaltungen angeschrieben und ihnen zwecks eingehenderer Prüfung eine erste Bestandsaufnahme darüber zugesandt, welche Mitteilungspflichten auf eine gesetzliche Grundlage zurückgeführt werden können und welche nicht.

Ich hoffe, daß diese Bemühungen durch einen am 6./7. Juni 1984 gefaßten Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder gefördert werden, der folgende Empfehlungen enthält:

— Die MiZi sieht in einer Vielzahl von Verfahren die Übermittlung personenbezogener Daten von den Gerichten der streitigen Zivilgerichtsbarkeit und der freiwilligen Gerichtsbarkeit an Finanzbehörden, Sozialbehörden, Staatsanwaltschaften, Standesämter und andere öffentliche Stellen vor. Mitteilungen dieser Art stellen in aller Regel einen Eingriff in das nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 GG geschützte Recht auf informationelle Selbstbestimmung dar und bedürfen deshalb einer verfassungsgemäßen gesetzlichen Grundlage, die den rechtsstaatlichen Geboten der Normenklarheit und Verhältnismäßigkeit entsprechen muß. Ein Teil der Mitteilungspflichten läßt sich auf Rechtsvorschriften zurückführen. Für andere Mitteilungspflichten ist eine Rechtsgrundlage nicht ersichtlich.

  Eine Überprüfung der Rechtsgrundlagen der Mitteilungspflichten muß mit einer Überprüfung der Erforderlichkeit der Mitteilungen Hand in Hand gehen. Es wird zu prüfen sein, ob nicht manche Mitteilungen angesichts eines veränderten gesellschaftlichen Umfeldes und eines Wandels der Verwaltungsaufgaben ihren Sinn verloren haben. Soweit Mitteilungen für erforderlich gehalten werden, müssen ihre Voraussetzungen und ihr Umfang durch Rechtsvorschrift festgelegt werden.

— Die bestehende Generalklausel, daß Mitteilungen im Einzelfall auch dann zu machen sind, wenn sie zwar nicht ausdrücklich vorgeschrieben, aber durch ein besonderes öffentliches Interesse geboten sind, bedarf der Überprüfung. Eine solche Klausel darf nicht dazu führen, daß die auf den Einzelfall bezogenen Regelungen und die dort vorgesehenen Beschränkungen umgangen werden. Soweit auf eine Generalklausel nicht verzichtet werden kann, muß auch sie den o. g. verfassungsrechtlichen Anforderungen Rechnung tragen.

— Grundsätzlich sollte sich die Übermittlung auf den Tenor der Entscheidung beschränken. Die Übermittlung von Entscheidungsgründen ist nur zuzulassen, wenn deren Kenntnis für die Aufgabenerfüllung der zu benachrichtigenden Behörde erforderlich ist. Insoweit ist zu prüfen, ob nicht die Übermittlung von Entscheidungsgründen — in Umkehrung des bisher praktizierten Regel-Ausnahme-Verhältnisses — auf ausdrücklich geregelte Ausnahmefälle begrenzt werden kann. Wo eine Abwägung im Einzelfall vorgesehen werden muß, sollte sie durch den Richter oder im Rahmen der ihm nach dem Rechtspflegergesetzes übertragenen Aufgaben durch den Rechtspfleger erfolgen.

— Außerdem sollte besonders darauf geachtet werden, daß

  — Datenübermittlungen den betroffenen Bürgern im Hinblick auf Inhalt, Adressat und zugrundeliegende Rechtsgrundlagen transparent zu machen sind,

  — übermittelte Daten nur im Rahmen des Zwecks, zu dem sie übermittelt wurden, genutzt werden dürfen (Zweckbindung),

  — die notwendigen technisch-organisatorischen Maßnahmen der Datensicherung vorzusehen sind und

  — die Aufbewahrungsdauer, unter Berücksichtigung auch der Belange der Betroffenen, auf das erforderliche Maß zu beschränken ist.

Ein Arbeitskreis der Konferenz der Datenschutzbeauftragten ist gegenwärtig damit befaßt, in Ergänzung des vorgenannten Beschlusses Empfehlungen auch zu einzelnen Regelungen der MiZi zu erarbeiten. Die Datenschutzbeauftragten des Bundes und der Länder gehen davon aus, daß sie an den weiteren Überlegungen der Justizverwaltungen rechtzeitig beteiligt werden.

4.6 Schuldnerverzeichnis

Auf die Notwendigkeit, den Datenschutz bei der Übermittlung von Angaben aus dem Schuldnerverzeichnis zu verbessern, insbesondere den Umfang der praktizierten Datenübermittlungen kritisch zu überprüfen und auch die zugrundeliegende gesetzliche Regelung des § 915 ZPO zu überarbeiten, habe ich bereits in früheren Tätigkeitsberichten hingewiesen (vgl. 2. TB S. 18, 3. TB S. 20, 4. TB S. 44 f.). Da der Schuldner häufig von der Eintragung nichts weiß, sollte geprüft werden, wie er besser informiert werden kann. Angesichts der Sensibilität dieser Eintragungen sollte auch der Empfängerkreis von Abschriften aus dem Schuldnerverzeichnis enger

gezogen werden, als dies in der bisherigen Praxis der Fall ist.

Ich habe den Bundesminister der Justiz wiederholt auf diese Problematik hingewiesen und hoffe, daß die von ihm nunmehr angekündigte „Entwicklung einer neuen Konzeption für die Erteilung und die Entnahme von Abschriften aus den Schuldnerverzeichnissen auf der Grundlage der Ausführungen des Bundesverfassungsgerichts in dem Urteil zum Volkszählungsgesetz" bald zu Ergebnissen führt.

4.7 Grundbuchwesen

Aufgrund von Eingaben von Bürgern habe ich bereits in früheren Tätigkeitsberichten (vgl. 5. TB S. 22, 6. TB S. 15) kritisiert, daß schutzwürdige Belange von Miteigentümern gemeinsam genutzter Grundstücke (z. B. Garagenflächen, Zufahrtswege) durch Bekanntgabe des Inhalts von Grundbuchauszügen, die u. a. Darlehensbelastungen der übrigen Miteigentümer enthalten, verletzt werden können.

Auf Nachfragen hat der Bundesminister der Justiz zwar erneut bestätigt, daß eine Novellierung der Grundbuchordnung in Aussicht genommen ist; er konnte jedoch keine Angaben darüber machen, wann ein Referentenentwurf, der eine datenschutzfreundlichere Lösung des genannten Problems bringen sollte, vorgelegt werden kann.

5. Finanzverwaltung

5.1 Steuerbereinigungsgesetz 1985

Die Bundesregierung hat den schon in meinen früheren Tätigkeitsberichten (vgl. 5. TB S. 25 f., 6. TB S. 15 f.) behandelten Entwurf einer Änderung der Abgabenordnung (AO) als Teil des Entwurfes eines Steuerbereinigungsgesetzes 1985 beim Deutschen Bundestag eingebracht. Der Bundestag ist einer Empfehlung seines Finanzausschusses gefolgt, über entscheidungsreife Teile dieses Gesetzentwurfs sofort zu beschließen, die übrigen Teile der Regierungsvorlage — darunter den die Abgabenordnung betreffenden Teil — bis zum Jahre 1985 zurückzustellen. Ich hoffe, daß dadurch keine wesentliche Verzögerung der Klärung der von mir angesprochenen Fragen eintritt.

Der von mir schon wiederholt erhobenen Forderung, bei Kontrollmitteilungen die übermittelnde Stelle *gesetzlich* zur Unterrichtung des Betroffenen zu verpflichten, kommt der Entwurf in § 93 a Abs. 2 AO insoweit entgegen, als er die „Verpflichtung zur Unterrichtung des Betroffenen" zum zwingenden Inhalt einer Rechtsverordnung macht. Die Stellungnahme des Bundesrates (zu § 93 a, dort Absatz 3) sieht demgegenüber lediglich vor, in der Rechtsverordnung „abzugrenzen, in welchen Fällen die mitteilende Stelle verpflichtet ist, den von der Mitteilung Betroffenen zu unterrichten" und wendet sich gegen eine zu umfangreiche kasuistische Aufzählung von Mitteilungspflichten. In meiner Stellungnahme, um die mich der Bundesminister der Finanzen zur Vorbereitung der Antwort der Bundesregierung auf die Stellungnahme des Bundesrates gebeten hat, habe ich an die Forderung der Datenschutzbeauftragten erinnert, Kontrollmitteilungen wegen ihres Eingriffscharakters auf eine eindeutige Rechtsgrundlage zu stellen, und empfohlen, an der „Verpflichtung zur Unterrichtung des Betroffenen" als einem Mindesterfordernis festzuhalten.

Auch ich trete im übrigen dafür ein, gesetzliche Mitteilungspflichten nur im notwendigen Umfang, d. h. lediglich in den Fällen in Anspruch zu nehmen, in denen tatsächlich ein unabweisbares steuerliches Bedürfnis für die Information der Finanzbehörden besteht. In die gleiche Richtung zielen Formulierungen des Bundesministers der Finanzen, in einem neuen Absatz 4 des vorgesehenen § 93 a AO die Möglichkeit zu schaffen, auf die Erfüllung von Mitteilungspflichten zu verzichten.

In der Frage der Kontrollbefugnisse der Datenschutzbeauftragten halte ich an meinen früheren Stellungnahmen (vgl. 5. TB S. 23 f., 6. TB S. 16) fest. Vor dem Hintergrund von Pressemeldungen über Funde von Computerbögen mit den Steuerdaten von über 10 000 Bürgern in den Abfallcontainern eines Finanzamtes halte ich eine gesetzliche Klarstellung, daß den Datenschutzbeauftragten nicht unter Berufung auf das Steuergeheimnis (§ 30 AO) Auskünfte und Einsicht in Akten verweigert werden können, für dringend geboten.

5.2 Automatisiertes Luftfracht-Abwicklungsverfahren (ALFA)

Zur Abwicklung des umfangreichen Luftfrachtverkehrs setzt die Bundeszollverwaltung derzeit auf dem Flughafen Rhein-Main das automatisierte Luftfracht-Abwicklungsverfahren (ALFA) ein. In Vorbereitung ist der Anschluß der Flughäfen Stuttgart und München-Riem. Teilnehmer an diesem System sind neben der Zollverwaltung insbesondere die Luftverkehrsgesellschaften und Speditionsunternehmen.

Im Rahmen eines Kontrollbesuchs beim Hauptzollamt Frankfurt am Main-Flughafen habe ich keine Anhaltspunkte für eine Speicherung von personenbezogenen Daten in diesem System gefunden, die nicht zur rechtmäßigen Erfüllung der in der Zuständigkeit des Hauptzollamts liegenden Aufgaben erforderlich sind. Ich habe jedoch gegenüber dem Bundesminister der Finanzen zu Einzelfragen (z. B. Datensicherung, Eingabe- und Zugriffsberechtigung, Auswertungen) Verbesserungen angeregt. Der Bundesminister der Finanzen hat mir inzwischen mitgeteilt, daß er diese Anregungen aufgegriffen und entsprechende Weisungen zu ihrer Umsetzung beim Hauptzollamt Frankfurt am Main-Flughafen gegeben habe.

6. Verwaltung des Deutschen Bundestages

Die Verwaltung des Deutschen Bundestages betreibt Datenverarbeitung zur Unterstützung der Ab-

geordneten bei ihren parlamentarischen Aufgaben. Aus datenschutzrechtlicher Sicht sind nicht nur die dem Parlament anvertrauten personenbezogenen Daten von Interesse, wie sie z. B. in den Eingaben an den Petitionsausschuß enthalten sind. Auch die Verarbeitung der Personaldaten der rund 1 600 Verwaltungsbediensteten muß dem Datenschutz Rechnung tragen.

Eine erste Kontrolle konnte nur einen noch lückenhaften Überblick über den Stand des Datenschutzes vermitteln. Schon jetzt zeigte sich eine Reihe von Problemen und Schwachstellen insbesondere bei der Organisation des Datenschutzes sowie bezüglich der zur Datensicherung getroffenen Maßnahmen. So fehlt beispielsweise ein geschlossenes System von Regelungen zur Gewährleistung von Datenschutz und -sicherheit, das in das übrige Sicherheitskonzept der Verwaltung des Bundestages eingepaßt ist. Auch bestehen nur unvollkommene Mechanismen, mit denen die Einhaltung der Datenschutzvorschriften kontrolliert werden könnte. So bedarf der wichtige Grundsatz der Funktionentrennung einer wirksameren Regelung und Umsetzung. Die Verantwortlichkeiten — sowohl innerhalb der EDV selbst, als auch die des jeweils fachlich zuständigen Referates — müssen geregelt werden. Die baulich-räumlichen Sicherungsmaßnahmen des Rechenzentrums bedürfen dringend einer Verbesserung.

Automatisiert verarbeitet wird auch die sogenannte Personalhauptdatei, in der nahezu 90 Einzelangaben über jeden Verwaltungsbediensteten gespeichert werden können. Meine Prüfung, ob die Speicherungen im einzelnen und die daraus erstellten Listenauswertungen den datenschutzrechtlichen Zulässigkeitsvoraussetzungen genügen, konnte noch nicht abgeschlossen werden. Zur Datensicherung habe ich jedoch bereits jetzt auf Probleme hingewiesen und Anregungen gegeben.

Auch zu Inhalt und Handhabung einiger manuell geführter Dateien habe ich datenschutzrechtliche Verbesserungen angeregt. Es ist beabsichtigt, die datenschutzrechtliche Prüfung im kommenden Jahr fortzuführen.

7. Personalwesen

7.1 Kontrollen

Im Berichtsjahr habe ich die Einhaltung datenschutzrechtlicher Bestimmungen im Bereich der Personaldatenverarbeitung beim Bundesgesundheitsamt, bei der Bundesversicherungsanstalt für Angestellte, beim Deutschen Bundestag, bei der Deutschen Angestellten Krankenkasse und beim Bundesarchiv kontrolliert.

Bei einer dieser Kontrollen habe ich festgestellt, daß trotz meiner im Fünften Tätigkeitsbericht (S. 28) geäußerten Bedenken eine Reihe von Personalunterlagen doppelt geführt wird. So bleiben z. B. Beurteilungskopien eines Mitarbeiters, der von einer Außenstelle zur Zentrale versetzt wird, in der Außenstelle, die Personalakte (mit der Beurteilung) geht zur Zentrale.

Einer Behörde wurde ein vertrauensärztliches Gutachten übersandt, das anläßlich einer Einstellung gefertigt worden war. Es enthielt umfangreiche Stellungnahmen zu früheren Krankheiten und zum gegenwärtigen Gesundheitszustand unter Angabe sämtlicher Diagnosen. Das Gutachten schließt damit, daß gegen die vorgesehene Einstellung keine ärztlichen Bedenken bestehen. Diese letzte Mitteilung hätte für die Einstellungsbehörde ausgereicht, eine Übersendung der gesamten Gutachten mit der Angabe von Diagnosen war nicht erforderlich. Diese Auffassung habe ich bereits in meinem Zweiten Tätigkeitsbericht (S. 23) vertreten.

Die kontrollierte Stelle hat hinsichtlich der Doppelführung von Personalunterlagen eine Überprüfung zugesagt. Was die Angabe von Diagnosen in Gutachten angeht, werde ich nochmals auf die personalärztlichen Dienste meines Zuständigkeitsbereiches einwirken, die Angaben auf den erforderlichen Umfang zu reduzieren.

Darüber hinaus wurde ich durch zahlreiche Eingaben von Bürgern auf Probleme bei der Verarbeitung von Personaldaten hingewiesen. Es handelte sich sowohl um Einzelfälle als auch um Fragen grundsätzlicher Art. In vielen Fällen war es mir möglich, zu helfen, zum Teil scheiterte eine Lösung an unterschiedlichen Rechtsauffassungen.

Auf Einzelheiten der Kontrollen und auf Probleme, soweit sie exemplarisch erscheinen oder von grundsätzlicher Bedeutung sind, wird an entsprechender Stelle in dem jeweiligen Zusammenhang eingegangen.

7.2 Automatisierte Personaldatenverarbeitung

Im Berichtsjahr ergingen mehrere arbeitsgerichtliche Entscheidungen, die sowohl für den Schutz der Persönlichkeitsrechte des Arbeitnehmers als auch für die Mitbestimmungsrechte der Betriebsräte bzw. der Personalvertretungen von wegweisender Bedeutung sind.

7.2.1 Rechtsprechung zur Mitbestimmung

In seiner Entscheidung vom 14. September 1984 — 1 ABR 23/82 — hatte das Bundesarbeitsgericht zu klären, unter welchen Voraussetzungen ein Mitbestimmungsrecht des Betriebsrats nach § 87 Abs. 1 Nr. 6 BetrVG besteht. Nach dieser Vorschrift hat der Betriebsrat mitzubestimmen bei der Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen. Dem Fall lag folgender Sachverhalt zugrunde:

In zunehmendem Umfang werden automatisierte Verfahren eingesetzt, mit denen z. B. Kundendienstaufträge abgewickelt werden. Sie werden gelegentlich als „International Technical Service System", „Management Informationssystem des Kundendienstes" o. ä. bezeichnet. Überwiegend werden

sie von Firmen der Computer- und Büromaschinenbranche eingesetzt. Muß eines der von den Herstellern vertriebenen Geräte repariert oder gewartet werden, erteilt der Kunde dem Hersteller einen entsprechenden Auftrag. Dieser wird im Auftragskontrollsystem gespeichert und einem Kundendiensttechniker zugewiesen. Nach Erledigung des Auftrags meldet der Kundendiensttechniker eine Reihe von kunden-, tätigkeits- und produktbezogenen Daten sowie seine Personalnummer der Zentrale seines Unternehmens, wo die Daten in das Datenverarbeitungssystem eingegeben werden. Es handelt sich dabei um Angaben über den zeitlichen Aufwand für An- und Abfahrt, die Arbeitszeit, benötigte Ersatzteile usw.; sie dienen u. a. der Abrechnung mit dem Kunden und der Optimierung der Ersatzteilversorgung.

Das BAG hat entschieden, daß derartige Auftragskontrollsysteme nach § 87 Abs. 1 Nr. 6 BetrVG der Mitbestimmung des Betriebsrates unterliegen.

Das BAG hatte bereits früher klargestellt, daß eine technische Einrichtung dann zur Überwachung bestimmt ist, wenn sie aufgrund des verwendeten Programms Verhaltens- oder Leistungsdaten selbst erhebt und aufzeichnet, unabhängig davon, ob der Arbeitgeber die durch die technische Einrichtung erfaßten und festgehaltenen Verhaltens- und Leistungsdaten auch auswerten oder zu Reaktionen auf festgestellte Verhaltens- oder Leistungsweisen verwenden will. Nunmehr war zu klären, ob ein datenverarbeitendes System auch dann eine zur Überwachung von Leistung oder Verhalten der Arbeitnehmer bestimmte technische Einrichtung sein kann, wenn es Verhaltens- oder Leistungsdaten verarbeitet, *die auf nicht-technischem Wege gewonnen* und dem System lediglich zum Zwecke der Speicherung und Verarbeitung eingegeben werden. Das BAG hat diese Frage bejaht und dazu ausgeführt, auch die bloße Auswertung von Verhaltens- und Leistungsdaten mittels einer technischen Einrichtung sei geeignet, die freie Entfaltung der Persönlichkeit des Arbeitnehmers zu behindern, und stelle eine Gefährdung seines Persönlichkeitsrechts dar. Denn die bei „technischer Verarbeitung" notwendige Selektion der Daten, der damit verbundene Kontextverlust sowie die unbegrenzt mögliche Erstreckung der Verarbeitung auf alle Daten einschließlich solcher, die weit zurückliegen und einen gegenwärtigen Aussagewert möglicherweise nicht mehr haben, könnten Einsichten in Leistung und Verhalten von Arbeitnehmern möglich machen, die bei herkömmlicher Überwachung nicht gegeben gewesen seien, und zum anderen — was bedeutsamer erscheine — einer persönlichen, individualisierenden Beurteilung entbehrten, was den Arbeitnehmer zu einem bloßen „Beurteilungsobjekt" machen könne. Das Wissen um eine derartige Verarbeitung von Verhaltens- und Leistungsdaten erzeuge einen Anpassungsdruck, der zu erhöhter Abhängigkeit des Arbeitnehmers führe und damit die freie Entfaltung seiner Persönlichkeit hindern müsse. Gerade die Objektstellung des Arbeitnehmers und dessen Behinderung in der Entfaltung seiner Persönlichkeit stellten sich aber nach der Rechtsprechung des Bundesverfassungsgerichts als Eingriffe in sein Persönlichkeitsrecht dar. Aus dieser Gefahrenlage rechtfertige sich ein Mitbestimmungsrecht des Betriebsrats.

Das BAG hat in diesem Zusammenhang ausgeführt, der Gesetzgeber habe die technische Überwachung von Arbeitnehmern bei Verhalten und Leistung nicht deswegen dem Mitbestimmungsrecht des Betriebsrates unterstellt, weil die Arbeitnehmer vor jeder Form der Überwachung, der Erhebung oder Auswertung von Informationen über Verhalten oder Leistung geschützt werden sollten, sondern weil diese Vorgänge dann zu einer Gefährdung des Persönlichkeitsrechts führten, wenn sie mit Hilfen technischer Einrichtungen vorgenommen würden. Das BAG wendet sich damit gegen die verbreitete Auffassung, die automatisierte Datenverarbeitung sei nur ein technisches Hilfsmittel für Vorgänge, die bislang auch ohne technische Unterstützung zulässigerweise erfolgten und nicht mitbestimmungspflichtig gewesen seien. Es stellt vielmehr klar, daß sich die technische Datenverarbeitung von der herkömmlichen Auswertung durch einen Menschen grundlegend unterscheidet. Die Bedingungen, unter denen die technische Datenverarbeitung zwangsläufig erfolgen müsse, führten zu den aufgezeigten Gefahren für das Persönlichkeitsrecht des Arbeitnehmers, denen zu begegnen dem Betriebsrat ein Mitbestimmungsrecht eingeräumt worden sei.

Das Urteil des BAG hat über den zur Entscheidung stehenden Fall hinaus zu einem seit langem umstrittenen Problem eine Klarstellung gebracht, die Auswirkungen auf Planung und Betrieb von Personaldatensystemen sowohl allgemein wie auch in der Bundesverwaltung haben wird. Die Fortentwicklung der Ausgestaltung des Arbeitnehmerdatenschutzes erscheint mir um so wichtiger, als spezialgesetzliche Bestimmungen auf diesem Gebiet zur Wahrung der schutzwürdigen Belange der Betroffenen im Sinne der §§ 23 ff. BDSG noch weitgehend fehlen.

7.2.2 Einzelne Personalinformationssysteme

Wegen der Vielzahl oft sensibler Informationen über die einzelnen Mitarbeiter und der zahlreichen Auswertungsmöglichkeiten, aber auch wegen der vorstehend unter Nr. 7.2.1 aufgezeigten Gefährdungen des Persönlichkeitsrechts von Arbeitnehmern, bedürfen Personalinformationssysteme aus datenschutzrechtlicher Sicht besonderer Aufmerksamkeit bei der Planung und Entwicklung sowie im Betrieb. (Zur Definition von Personalinformationssystemen vgl. 3. TB S. 27 f.)

— Bei der Kontrolle des Personalinformationssystems der Deutschen Angestellten Krankenkasse waren insbesondere folgende Fragen zu klären:
  — Welche personenbezogenen Daten werden erfaßt?
  — Welche Auswertungen sind im einzelnen vorgesehen?
  — Welche Daten bzw. Programme sollen wem zur Verfügung stehen?

— Wozu dient das Verfahren hinsichtlich jedes einzelnen Datums und jeder einzelnen Auswertung?

— Sind Datenerhebung und -verarbeitung im einzelnen erforderlich?

— Welche Löschungsfristen sind vorgesehen?

— Wurde der Personalrat beteiligt?

Dabei waren Zahl und Verteilung der Mitarbeiter (z. B. auf Zentrale und Außenstellen) und Struktur der Personalverwaltung sowie das vorhandene technische Instrumentarium zu berücksichtigen.

Hinsichtlich der *Speicherung* im Datenbanksystem habe ich mich bei meiner Prüfung auf die Datenbanksegmente „Beurteilungen", „Beihilfen" und „Abwesenheitszeiten" beschränkt.

Die Segmente für Beurteilungen werden gegenwärtig nicht genutzt. Da sie jedoch angelegt sind, könnten sie auch genutzt werden. Falls dies geschieht, habe ich um nähere Informationen gebeten. Dies bedarf dann einer kritischen Prüfung unter Einbeziehung des Personalrates.

Die in den Segmenten für die Bearbeitung der Beihilfen gespeicherten Daten (es handelt sich um Verwaltungsdaten, Diagnosen werden nicht gespeichert) sind für die Aufgabenerfüllung durch die Beihilfestelle erforderlich. Ich habe jedoch festgestellt, daß über die Beihilfestelle hinaus acht weitere Mitarbeiter der Personalabteilung Zugriff hatten. Da Beihilfedaten aus meiner Sicht vom Geheimhaltungsbedürfnis her Sozialdaten entsprechen, halte ich dies für einen Mangel in der Datenverarbeitung. Da er indes noch im Laufe der Kontrolle behoben wurde, konnte von einer Beanstandung abgesehen werden.

Die Segmente für Abwesenheitszeiten werden nur für einen kleinen Teil der Mitarbeiter genutzt. Die Abwesenheitszeiten aller Mitarbeiter werden in einem besonderen Verfahren erfaßt. Dieses Verfahren hat den Zweck, im Zuge einer langfristigen überregionalen Personalplanung einen Überblick über die effektiv zur Verfügung stehende Arbeitskapazität zu geben. Nach meiner Einschätzung ist dieses Ziel ohne eine personenbezogene Erfassung und Auswertung zu erreichen. Ich habe deshalb vorgeschlagen, das bestehende Verfahren durch ein nicht personenbezogenes abzulösen.

Die im System vorhandenen Instrumente zur Benutzerkontrolle, Zugriffskontrolle und Dokumentation sind ausreichend. Diese Verfahren werden jedoch zum Teil gegenwärtig noch nicht genutzt, da sich das System noch im Aufbau befindet.

Mein Eindruck von dem System ist insgesamt positiv. Dazu haben die organisatorische Einbettung des Datenschutzbeauftragten, der unmittelbar der Geschäftsführung unterstellt ist, und seine Beteiligung bei Entwicklung und Betrieb des Systems wesentlich beigetragen.

— Meine bereits in meinem Sechsten Tätigkeitsbericht (S. 18 f.) beschriebene Beteiligung bei der Entwicklung des Personalinformationssystems einer obersten Bundesbehörde konnte in der ersten Hälfte des Berichtsjahres abgeschlossen werden. In den Verhandlungen, an denen auch die Personalvertretung der obersten Bundesbehörde teilnahm, haben sich die beiden folgenden Schwerpunkte herausgebildet:

— Prüfung der Erforderlichkeit jedes Einzeldatums unter Berücksichtigung seiner Sensibilität

— Bewertung der Nutzungsmöglichkeiten des Systems durch die Anwender.

Bei der Prüfung der Erforderlichkeit des Dateinhaltes für die Aufgabenerfüllung wurde die Frage erörtert, ob auf die Speicherung der Beurteilungsnote und der Abwesenheitszeiten nicht verzichtet werden kann. Es wurde Einvernehmen darüber erzielt, daß die Speicherung der Beurteilungsnote nicht erforderlich ist. Dagegen wurde die Aufnahme der Abwesenheitszeiten ins System von der obersten Bundesbehörde für notwendig gehalten, wobei die Nutzung dieser Angaben jedoch insoweit einer Beschränkung unterliegt, als sie jeweils nach einem Jahr gelöscht werden und keine personenbezogene Auswertung nach Krankheitshäufigkeiten erfolgt. Die sonstigen Nutzungsmöglichkeiten des Systems bleiben begrenzt, weil keine freie Dialogsprache eingesetzt wird. Auswertungsprogramme sind durch ein Freigabe- und Prüfverfahren kontrollierbar.

Für die Entwicklung von Datensicherungsverfahren (z. B. Zugriffskontrolle, Speicherkontrolle) habe ich meine weitere Beratung angeboten.

7.2.3 Telefondatenverarbeitung

Mit den Fragen der automatischen Telefondatenverarbeitung habe ich mich schon in mehreren Tätigkeitsberichten befaßt (3. TB, S. 28 f., 4. TB S. 39 f., 5. TB S. 29 ff.). Die Aktualität dieser Fragen zeigt sich auch darin, daß an mich zunehmend Anfragen zur datenschutzrechtlichen Beurteilung derartiger Systeme gerichtet wurden. Außerdem haben in letzter Zeit mehrere Argbeitsgerichte zur Zulässigkeit der Telefondatenverarbeitung mit unterschiedlichen Ergebnissen entschieden. Diese Entscheidungen sind noch nicht rechtskräftig, so daß eine Grundsatzentscheidung des Bundesarbeitsgerichts (BAG) zu erwarten ist.

In einem anderen Zusammenhang hat das BAG festgestellt, daß schon das Sammeln oder Verarbeiten von Verhaltens- und Leistungsdaten als Überwachung zu verstehen sei, und daß eine solche Überwachung dann das Persönlichkeitsrecht gefährde, wenn sie mit Hilfe technischer Einrichtungen erfolge (s. auch Nr. 7.2.1). Auch bei der automatischen Telefondatenverarbeitung werden zu Abrechnungzwecken personenbezogene Daten gespeichert, die für eine Verhaltenskontrolle verwendet werden können. Insofern liegt auch hier eine Gefährdung des Persönlichkeitsrechts. Bei einer auto-

matisierten Telefondatenverarbeitung sollte deshalb wie folgt verfahren werden:

1. Bei *dienstlichen* Gesprächen können zu Zwecken der Wirtschaftlichkeitskontrolle und der Dienstaufsicht für jede Nebenstelle die Nebenstellennummer, die Zielnummer und die Gebühreneinheiten sowie der Zeitpunkt des Gesprächs gespeichert und Ausdrucke gefertigt werden, wenn diese Kontrollen auch tatsächlich stattfinden. Im allgemeinen werden für Kontrollzwecke Stichproben genügen, so daß insoweit die Ausdrucke nur für einen begrenzten Zeitraum erforderlich sind. Ausdrucke dürfen nur dem jeweiligen Vorgesetzten zugehen. Ein Listenumlauf ist unzulässig. Eine Verknüpfung mit anderen Daten darf nicht erfolgen.

2. Bei *privaten* Gesprächen dürfen zu Zwecken der Abrechnung die gleichen Daten wie bei dienstlichen Gesprächen gespeichert werden, die Zielnummer jedoch nur, soweit der Benutzer dies wünscht oder es technisch nicht möglich ist, sie zu unterdrücken oder zu verkürzen. Soweit danach Zielnummern gespeichert sind, dürfen sie nur auf ausdrücklichen Wunsch des Benutzers — und nur für diesen — ausgedruckt werden. Gleiches gilt für mehrere regelmäßige Benutzer desselben Telefonapparates, sofern keine andere Möglichkeit der Gebührenaufteilung besteht.

   Im übrigen ist ein Ausdruck zulässig, wenn und soweit dies im Einzelfall zur Klärung von Streitigkeiten bei der Gebührenabrechnung erforderlich ist. Der Ausdruck ist nur dem Betroffenen und der Abrechnungsstelle zur Verfügung zu stellen. Dort darf er nur zu Abrechnungszwekken verwendet werden.

   Bei Verdacht einer übermäßigen Inanspruchnahme kann ein Ausdruck ohne Zielnummern für einen bestimmten Zeitraum zur Durchführung der Dienstaufsicht gefertigt werden.

3. Die Zielnummer *dienstlicher* Gespräche von Personalräten und Stellen mit vergleichbarer Funktion (besondere Vertrauensstellung, Schweigepflichten), z. B. Ärztlicher Dienst, Vertrauensleute für Schwerbehinderte, werden *nicht* aufgezeichnet, wenn dies technisch möglich ist. Erfolgt die Aufzeichnung zwangsläufig durch technische Einrichtungen, ist organisatorisch sicherzustellen, daß *in keinem Fall* ein *Ausdruck* erfolgt.

4. Die Telefondaten werden gelöscht, sobald ihre Speicherung nicht mehr erforderlich ist:
   - — Die gespeicherten Zielnummern dienstlicher Gespräche sind drei Monate nach ihrer Entstehung zu löschen.
   - — Ausdrucke sind unmittelbar nach erfolgter Kontrolle zu vernichten, sofern nicht aus Gründen der Rechnungsprüfung eine längere Aufbewahrung geboten ist.
   - — Die Daten privater Gespräche sind sofort nach erfolgter Abrechnung zu löschen.
   - — Ausgedruckte Zielnummern bei der Abrechnungsstelle sind sofort nach Klärung der Streitigkeiten zu vernichten.

5. An Regelungen über die Telefondatenerfassung ist die Personalvertretung zu beteiligen. Sie sind allen davon betroffenen Bediensteten bekanntzugeben.

7.3 Personalaktenführung

7.3.1 Neuregelung des Personalaktenrechts

In meinem Sechsten Tätigkeitsbericht (S. 18) habe ich über den Stand der Neufassung des § 90 BBG berichtet. Die in der Stellungnahme der Bundesregierung angekündigte interministerielle Arbeitsgruppe zur Entwicklung einheitlicher Richtlinien über das Führen und Verwalten von Personalakten ist inzwischen gebildet worden. Ich bin an dieser Arbeitsgruppe beteiligt. Sie beschäftigt sich schwerpunktmäßig auch mit den Problemen, deren Regelung ich bereits seit mehreren Jahren gefordert habe.

Besonders hervorheben möchte ich dabei:

- — Abschottung der Beihilfeakten
- — Inhalt und Behandlung personalärztlicher Unterlagen
- — Behandlung von Prüfungsakten
- — Inhalt und Verwendung von Personalbögen
- — Behandlung von Bewerbungsunterlagen und Vorakten (z. B. Referendarakten)
- — Aufbewahrungsfristen für Personalakten bzw. für Teile der Personalakten
- — Anspruch auf Entfernung von Unterlagen aus Personalakten
- — gesetzliche Verankerung des Personalaktengeheimnisses
- — Einsichtsrechte der Betroffenen oder Hinterbliebenen
- — Einsichtsrechte von Fachvorgesetzten
- — Einsichtsrechte der Personalvertretung
- — Auskunft aus der Personalakte
- — Weitergabe der Personalakte

Viele der hier aufgezeigten Einzelprobleme waren auch Gegenstand zahlreicher Eingaben. Die umfassende Regelung des Personalaktenrechts einschließlich eindeutiger Datenschutzvorschriften ist daher dringlich.

7.3.2 Personalärztliche Gutachten

Bereits in meinem Zweiten Tätigkeitsbericht (S. 23) habe ich die Problematik des Inhalts und der Behandlung ärztlicher Gutachten beim Eingehen oder

im Rahmen eines Beschäftigungsverhältnisses dargestellt. Ich habe damals berichtet, daß Einvernehmen mit dem Leitenden Arzt des Ärztlichen und Sozialen Dienstes der obersten Bundesbehörden im Bundesministerium des Innern dahin gehend erzielt wurde, daß

- an die personalbearbeitende Stelle keine Diagnosedaten, sondern das Ergebnis der ärztlichen Untersuchung nur insoweit übermittelt wird, als es für die konkrete Personalentscheidung relevant ist (d. h. die Mitteilung besagt z. B. lediglich, daß der Bewerber für eine Übernahme in das Beamtenverhältnis uneingeschränkt oder nur eingeschränkt geeignet ist und gegebenenfalls, welche Einschränkungen vorliegen),
- bei der Aufnahme ärztlicher Unterlagen in die Personalakte unter Beachtung des Verhältnismäßigkeitsgrundsatzes restriktiv zu verfahren ist,
- die Übersendung ärztlicher Unterlagen von einer Dienststelle an eine andere regelmäßig der Zustimmung des Betroffenen bedarf,
- der untersuchte Bedienstete ein Recht auf Einsicht in die ihn betreffenden ärztlichen Gutachten hat, gleichviel ob sie sich in der Personalakte oder beim Ärztlichen und Sozialen Dienst befinden.

Im Berichtsjahr wurde ich mit einem Fall konfrontiert, in dem die Übermittlung von Diagnose- und Prognosedaten in einem personalärztlichen Gutachten dazu führte, daß eine Bewerberin die bereits zugesagte Stelle in einer obersten Bundesbehörde nicht erhielt. Der gutachtende Arzt hatte sich dabei von der guten Absicht leiten lassen, durch die Aufnahme dieser Daten die Aussichten der Petentin auf Einstellung zu fördern, da er meinte, sonst möglicherweise ihre fehlende gesundheitliche Eignung für die vorgesehene Beschäftigung feststellen zu müssen. Dies erschien ihm jedoch ohne erläuternden und relativierenden Kontext nicht vertretbar. Die Folge war jedoch, daß nun die Einstellungsbehörde aufgrund der Diagnose- und Prognosedaten die an sich vom Arzt zu beantwortende Frage der gesundheitlichen Eignung der Petentin selbst negativ entschied. Im weiteren Verlauf wurde der Petentin erst aufgrund nachdrücklicher Intervention meinerseits und selbst dann noch ohne Anerkennung einer Rechtspflicht Einblick in das Gutachten gewährt. In einem Gespräch mit dem Ärztlichen und Sozialen Dienst konnte ich die Vernichtung des Gutachtens und eine Neubegutachtung der Petentin erreichen. Das neue Gutachten stellte fest, daß sie für die vorgesehene Beschäftigung gesundheitlich geeignet sei. Die betreffende Stelle allerdings war zwischenzeitlich anderweitig besetzt worden und eine andere Stelle nicht frei.

Dieser Einzelfall macht deutlich, welche einschneidenden negativen Folgen es für den einzelnen haben kann, wenn meine eingangs dargestellten einvernehmlich erarbeiteten Grundsätze nicht beachtet werden.

7.4 Sonstiges

7.4.1 Gehaltsscheckverfahren

Die Bundesbehörden räumen nicht selten ihren Mitarbeitern die Möglichkeit ein, über die behördeneigenen Zahlstellen Geld vom Gehaltskonto abzuheben. Die Bediensteten sind dafür verantwortlich, daß die anschließend von der Bundeskasse dem Geldinstitut vorgelegten Schecks gedeckt sind. Bei Verstößen können die Bediensteten vom Gehaltsscheckverfahren ausgeschlossen werden.

Bei einer obersten Bundesbehörde habe ich festgestellt, daß alle Fälle der Nichteinlösung eines Schecks ohne Ansehen des Grundes oder des Betrages routinemäßig schriftlich dem Personalreferat gemeldet werden. Dieses klärt sodann mit dem Betroffenen den Sachverhalt.

Lagen die Gründe für die Nichteinlösung außerhalb des Einflußbereiches des Bediensteten (z. B. Bankversehen), wird die Mitteilung ein Jahr aufbewahrt und dann vernichtet. In allen anderen Fällen wird die Mitteilung mit der schriftlich festgehaltenen Erklärung des Bediensteten zur Personalakte genommen. Die Behörde hält dieses Verfahren für erforderlich, um eventuell später zum Ausschluß aus dem Gehaltsscheckverfahren führende Wiederholungsfälle erkennen zu können. Ich habe die Verhältnismäßigkeit dieses Vorgehens bezweifelt.

Die Behörde hat sich inzwischen bereit erklärt, in Bagatellfällen die Meldungen ohne weitere Aufbewahrung sofort zu vernichten. Meiner weitergehenden Anregung, eine Vorklärung des Sachverhaltes durch den Zahlstellenaufsichtsbeamten vornehmen zu lassen und nur noch solche Fälle dem Personalreferat zu melden, die disziplinarrechtlich relevant sein könnten, hat sich die Behörde nicht angeschlossen. Sie hat allerdings ihre Bereitschaft erklärt zu prüfen, ob die Mitteilungen in eine Beiakte zur Personalakte genommen werden können, in der sie Vernichtungsfristen unterliegen. Ich halte dies für einen Fortschritt, bin gleichwohl weiterhin der Ansicht, daß das Personalreferat grundsätzlich nur von disziplinarrechtlich relevanten Vorfällen Kenntnis erhalten sollte. Ich vermute, daß dieses Problem nicht auf eine Behörde beschränkt ist, sondern ressortübergreifend besteht. Ich werde es daher in der interministeriellen Arbeitsgruppe zur Neuregelung des Personalaktenrechts mit dem Ziel einer einheitlichen Regelung ansprechen.

7.4.2 Wählerverzeichnis für Personalratswahlen

Von Behörden und Gewerkschaften sind anläßlich der Vorbereitung von Personalratswahlen Fragen zu den Wählerverzeichnissen an mich herangetragen worden. Dabei wurde es für rechtlich zweifelhaft gehalten, ob in die Wählerverzeichnisse Angaben über Dienststellen- oder Betriebszugehörigkeit, Geburtsdatum und Privatanschrift aufgenommen sowie die Verzeichnisse in öffentlich zugänglichen Bereichen ausgehängt werden dürfen. Nach meiner Einschätzung sind diese Bedenken teilweise berechtigt.

Für die Wahlen zu den Personalvertretungen bei Bundesbehörden und -einrichtungen nach dem Bundespersonalvertretungsgesetz haben die Wahlvorstände Verzeichnisse der wahlberechtigten Beschäftigten (Wählerverzeichnisse) aufzustellen und auszulegen. Die Aufnahme in das Wählerverzeichnis ist formelle Voraussetzung für das aktive Wahlrecht. Über den Inhalt des Wählerverzeichnisses enthält die Wahlordnung keine nähere Bestimmung.

Bei der Wahl von Stufenvertretungen oder bei räumlich getrennten Behörden habe ich gegen die Aufnahme der Dienststellen- oder Betriebszugehörigkeit keine datenschutzrechtlichen Bedenken. Für nicht erforderlich halte ich hingegen die Angabe des Geburtsdatums in den auszulegenden Wählerverzeichnissen. Für die Feststellung der Wahlberechtigung ist die allgemeine Bekanntgabe des Alters nicht nötig. Hinzukommt, daß bei Bediensteten im öffentlichen Dienst Personaldaten, zu denen auch das Geburtsdatum zählt, durch das Amts- und Personalaktengeheimnis zusätzlich geschützt sind. Im übrigen bietet sich hier eine Parallele zu dem Verfahren nach der Bundeswahlordnung an. In diesem Zusammenhang habe ich schon im Jahre 1979 anläßlich der Novellierung der Bundeswahlordnung (BWO) angeregt, das Geburtsdatum im Wählerverzeichnis gemäß § 14 Abs. 1 BWO zu streichen. Der Bundesminister des Innern ist dem insoweit gefolgt, als auf Verlangen des Wahlberechtigten im Wählerverzeichnis während der Auslegungsfrist das Geburtsdatum unkenntlich zu machen ist (vgl. § 21 Abs. 3 BWO). Ich würde es begrüßen, wenn auch bei Personalratswahlen in dieser Weise verfahren würde und bereits in der Ankündigung der Personalratswahlen ein Hinweis darauf erfolgte, daß Bedienstete der Aufnahme ihres Geburtsdatums innerhalb einer angemessenen Frist vorab widersprechen können und dieses Datum dann nicht im Wählerverzeichnis erscheint.

Bei der Durchführung der Wahl des Hauptpersonalrates beim Bundesministerium des Innern wird 1985 meinem Anliegen bereits Rechnung getragen werden. Darüber hinaus wird grundsätzlich auf die Veröffentlichung der Geburtsdaten im Wählerverzeichnis verzichtet, so daß es keines Widerspruchs der Betroffenen bedarf.

Die Angabe der Privatanschrift halte ich für datenschutzrechtlich unzulässig, da sie bei der Beurteilung der Wahlberechtigung keine Rolle spielt.

Die Wahl des Ortes, an dem die Verzeichnisse auszuhängen sind, kann problematisch sein. Nach § 2 Abs. 3 der Wahlordnung ist das Wählerverzeichnis „an geeigneter Stelle" zur Einsicht auszulegen. Sinn und Zweck dieser Regelung zielen darauf ab, daß jeder Wahlberechtigte jederzeit ungehindert Zugang zum Wählerverzeichnis haben muß. Jeder Wahlberechtigte muß es also ohne besondere Umstände innerhalb seines normalen dienstlichen Bewegungsfeldes erreichen können. Dabei sind allerdings bei Behörden mit Publikumsverkehr Kollisionen mit Datenschutzansprüchen möglich, weil oft die geeignetsten Stellen für Auslage bzw. Aushang des Wählerverzeichnisses auch diejenigen sind, zu denen Außenstehende Zugang haben. Dies ist nach den jeweiligen örtlichen Umständen zu entscheiden.

7.4.3 Krankenkontrolle

Im Mai 1983 führte ein Postbediensteter Beschwerde darüber, daß gemäß einer bei der Dienststelle üblichen Praxis während seiner Erkrankung der Postbetriebsarzt auf Bitten der Amtsleitung vom behandelnden Hausarzt Erkundigungen über Art, Ursache und Dauer der Erkrankung eingeholt habe. Die zuständige Oberpostdirektion hatte diesen Sachverhalt gegenüber dem Bediensteten bestätigt mit dem Hinweis, daß festgestellt werden sollte, ob die Erkrankung in ursächlichem Zusammenhang mit einer überdurchschnittlichen psychischen Inanspruchnahme bei der Fertigung einer Verhandlungsniederschrift aufgetreten sei.

Ein derartiges Verfahren zur Kontrolle von arbeitsunfähig erkrankten Bediensteten ist nach meiner Auffassung unzulässig, weil es einen Bruch der ärztlichen Schweigepflicht voraussetzt und damit das für eine erfolgreiche ärztliche Betreuung unbedingt notwendige Vertrauensverhältnis zwischen Arzt und Patient beeinträchtigt. Aus diesen Gründen ist seit langem allgemein anerkannt und auch allgemeine Praxis, daß die für den Arbeitgeber bestimmte Arbeitsunfähigkeitsbescheinigung des behandelnden Arztes keine Angaben über Art und Ursache der Erkrankung und über den Zustand des Patienten enthalten darf. Die logische Konsequenz ist, daß die Dienstbehörde eines Beamten niemals von dem behandelnden Arzt Auskunft über Umstände erbitten oder einholen darf, die der ärztlichen Schweigepflicht unterliegen. Der Arzt darf keine Auskunft geben, wenn eine Dienstbehörde sich über die Krankheit oder die Behandlung eines ihrer Beamten erkundigt.

Auf meine Bitte um Stellungnahme hat der Bundesminister für das Post- und Fernmeldewesen lediglich den Sachverhalt bestätigt und darauf hingewiesen, daß die Vorschriften des BDSG keine Anwendung fänden, da im Zusammenhang mit der Erkrankung des Bediensteten keine Speicherung ihn betreffender Daten in Dateien erfolgt sei. Weitere Anfragen blieben bislang unbeantwortet, so daß ich nicht beurteilen kann, ob es sich um ein bei der Deutschen Bundespost übliches Verfahren oder um einen Einzelfall handelt.

8. Deutsche Bundespost

Die Deutsche Bundespost (DBP) setzt in großem Umfang neue elektronische Technik zur Durchführung ihrer Aufgaben ein. Dadurch sollen nicht nur bestehende Dienstleistungen modernisiert, sondern dem Postkunden auch neue zur Verfügung gestellt werden. Aus der Sicht des Datenschutzes ergeben sich daraus nicht nur Fragen nach Art und Umfang der getroffenen technischen und organisatorischen Maßnahmen, sondern auch solche nach Erforderlichkeit und somit Zulässigkeit der eingesetzten

Verfahren zur Verarbeitung personenbezogener Daten.

8.1 Organisation des Datenschutzes bei der Deutschen Bundespost

Ich habe bei meinen Kontrollen bei Dienststellen der Deutschen Bundespost wiederholt feststellen können, daß sich Datenschutz- und Datensicherheitsprobleme speziell aufgrund der besonderen *örtlichen* — technischen, organisatorischen oder aber personellen — Bedingungen ergeben. Von der zuständigen übergeordneten Stelle sind diese Probleme oft nicht vorhersehbar. Aus diesem Grunde erscheint es problematisch, daß bei neuen Fachaufgaben oder aber Modifikationen bestehender Aufgaben die Gewährleistung des Datenschutzes entsprechend der „Datenschutz-Anweisung" ausschließlich im Ministerium geprüft wird. Eine Prüfung durch das Datenschutzreferat erfolgt auch nur dann, wenn es vom Fachreferat beteiligt wird. Der mit dem Datenschutz beauftragte Beamte im nachgeordneten Bereich wird im Regelfall nicht eingeschaltet. Dieses System birgt die Gefahr, daß eine Fachaufgabe, bei der personenbezogene Daten verarbeitet werden, ohne vorherige datenschutzrechtliche Prüfung zur Ausführung gelangt. Dadurch kann es zu Beeinträchtigungen schutzwürdiger Belange der Betroffenen kommen. Ich habe daher empfohlen, die bestehende „Datenschutz-Anweisung" unter diesen Gesichtspunkten zu überarbeiten und darüber hinaus im Rahmen der Fortbildung den mittleren Führungskräften Basiswissen über den Datenschutz zu vermitteln.

8.2 Erhebungen bei Fernsprechteilnehmern

Zur Gewinnung statistischer Daten, die eine Verbesserung der Prognosemodelle und somit eine verbesserte Planung im Fernsprechwesen ermöglichen sollen, hat die Deutsche Bundespost bei zahlreichen Fernsprechteilnehmern Erhebungen sowohl durch Fragebögen als auch durch automatische Einrichtungen durchgeführt. Mit Hilfe der Fragebögen wurden neben Angaben über das Telefonierverhalten solche über den sozialen Status erhoben. Im automatisierten Verfahren wurden sowohl — anonymisierte — Verkehrsmessungen als auch detaillierte (personenbezogene) Aufzeichnungen über Zeitpunkt, Dauer und Ziel der gewählten Fernsprechverbindung vorgenommen.

Konzeption und Durchführung dieses Vorhabens boten in einigen Punkten Anlaß zur Kritik. Da die Erhebung und Verarbeitung der genannten Daten für die Durchführung des Fernsprechdienstes nicht erforderlich und somit auch nicht zulässig waren, durften sie nur mit Einwilligung der Betroffenen vorgenommen werden. Auf die Freiwilligkeit ihrer Mitwirkung sind sie in den untersuchten Aktionen jedoch nicht bzw. nicht ausreichend deutlich hingewiesen worden. So mußte der Fernsprechteilnehmer den Eindruck gewinnen, er sei sowohl zur Beantwortung des Fragebogens als auch zur Duldung der automatischen Gesprächsdatenerfassung verpflichtet. Auch die Aufklärung über das Verfahren selbst war unzureichend.

Darüber hinaus war die Sicherung der entstandenen und verarbeiteten Daten in einigen Punkten nicht ausreichend.

Ich habe den Bundesminister für das Post- und Fernmeldewesen aufgefordert, für künftige Aktionen gleicher oder ähnlicher Art die Möglichkeit der *anonymisierten* Erhebung der Daten zu prüfen. In Fällen, in denen diese nicht möglich ist, muß der Betroffene ausdrücklich auf die Freiwilligkeit seiner Mitwirkung hingewiesen und ihm das Verfahren erläutert werden. Insbesondere muß er auch über eventuell vorgesehene automatische Gesprächsdatenregistrierungen unterrichtet werden (s. unter Nr. 8.3). Angesichts der Sensibilität der Daten bedarf die Datensicherung besonderer Aufmerksamkeit.

Wohl als Folge der lückenhaften Datenschutzorganisation (s. o. Nr. 8.1) sind in diesen Fällen auch die gesetzlichen Meldepflichten (§ 19 Abs. 4 BDSG) für die Dateien nicht erfüllt worden.

8.3 Registrierung und Bekanntgabe von Telefonverbindungsdaten

Sowohl im Rahmen der Bearbeitung von Einwendungen gegen die Höhe von Telefonrechnungen als auch auf besonderen Antrag von Fernsprechkunden — z. B. in Fällen von telefonischer Belästigung — registriert die Deutsche Bundespost Daten über den äußeren Ablauf der Telefonverbindungen. Mit Hilfe einer Zählervergleichseinrichtung werden dabei Zeitpunkt und Dauer des Gesprächs sowie die angewählte Telefonnummer (Zielnummer) automatisch aufgezeichnet. Die Zielnummer wurde auch dem antragstellenden Teilnehmer grundsätzlich nur auf richterliche Anordnung bekanntgegeben. Da dieses Verfahren sich in der Praxis als unbefriedigend herausgestellt hat, habe ich auf Wunsch des Ausschusses für das Post- und Fernmeldewesen des Deutschen Bundestages diesem den Entwurf einer Beschlußempfehlung zur Änderung des Verfahrens vorgelegt. In seiner Sitzung am 28. März 1984 hat der Ausschuß den Entwurf zustimmend zur Kenntnis genommen. Der Beschluß zur „Aufzeichnung und Bekanntgabe von Einzelgesprächsdaten" hält an dem Grundsatz fest, eine Aufzeichnung von Einzelgesprächen nur auf Antrag des Teilnehmers vorzunehmen. Erfordern betriebliche Anlässe eine solche Aufzeichnung, kann eine Information des Teilnehmers dann unterbleiben, wenn dies den Zweck der Aufzeichnung beeinträchtigen würde. Bezüglich der Bekanntgabe der Zielnummer an den Teilnehmer sieht der Beschluß ein *Antragsverfahren* vor, das auch dem Schutzbedürfnis der Mitbenutzer des Telefonanschlusses Rechnung trägt. Die Zielnummern werden nur mitgeteilt, wenn der Teilnehmer die zu seinem Haushalt gehörenden Mitbenutzer benennt und deren schriftliche Einwilligung beibringt. Eine richterliche Anordnung ist demnach im Regelfall nicht erforderlich.

8.4 Kontrolle einer Oberpostdirektion

Bei der Datenschutzkontrolle einer Oberpostdirektion wurden einige grundsätzliche Probleme der Organisation des Datenschutzes bei der Deutschen Bundespost besonders deutlich. Ich verweise hierzu auf meine Ausführungen unter Nr. 8.1 sowie die dort gegebenen Empfehlungen.

Breiten Raum nahm die Kontrolle der beim Rechenzentrum der Oberpostdirektion getroffenen technischen und organisatorischen Maßnahmen des Datenschutzes ein. Dabei zeigten sich einige Schwachstellen und Problempunkte. So erscheint eine Verbesserung der Kontrolle und Dokumentation von Produktionsaufträgen zumindest für solche Bereiche erforderlich, in denen Daten hoher Sensibilität verarbeitet werden (z. B. PERSIS).

Im Rahmen seiner Aufgabenstellung für das Personalinformationssystem PERSIS der Deutschen Bundespost generiert das Rechenzentrum der geprüften Oberpostdirektion eine Datei, die zahlreiche personenbezogene Daten *aller* Bediensteten der Deutschen Bundespost enthält. Kopien dieser Datei werden mehreren Stellen der Deutschen Bundespost zugeleitet. Angesichts der hohen Sensibilität solcher Personaldaten ist eine weite Streuung bedenklich. Ich habe den Bundesminister für das Post- und Fernmeldewesen gebeten, mir die Erforderlichkeit der Kenntnisnahme der Daten durch die verschiedenen Empfangsstellen darzulegen.

Die Stellungnahme des Ministeriums hierzu wie auch zu weiteren von mir gegebenen Empfehlungen und Anregungen wird derzeit von mir ausgewertet.

Zum Testen eines neuen EDV-Programmes waren listenmäßige Auswertungen aus — allerdings veralteten — Personaldaten der Bediensteten der Oberpostdirektion vorgenommen worden. Hier sollte im Einzelfall von der Deutschen Bundespost kritisch geprüft werden, ob Testläufe mit solchen Echtdaten unerläßlich sind und durch welche Maßnahmen der Datensicherung eine Beeinträchtigung schutzwürdiger Belange der Betroffenen ausgeschlossen werden kann.

8.5 Bildschirmtext (Btx)

Nachdem die Entwicklung des neuen Bildschirmtext-Verfahrens, das die in den Feldversuchen verwendete Technik ablösen sollte, sich verzögert hatte, nahm in der Mitte des Berichtsjahres die Btx-Leitzentrale in Ulm den Regelbetrieb für das neue System auf.

In mehreren intensiven Gesprächen, aus den mir zur Verfügung gestellten Unterlagen sowie auch anläßlich der Datenschutzkontrolle bei der Leitzentrale (s. u.) konnte ich mich ausführlich über die angebotenen und für den weiteren Ausbau geplanten Leistungen sowie über die damit zusammenhängende Verarbeitung personenbezogener Daten informieren.

Dabei zeigte sich, daß das zur Zeit eingesetzte Verfahren noch einige Fragen offenläßt, die für ein sicheres und datenschutzgerechtes System gelöst werden müssen.

8.5.1 Offene Probleme bei Bildschirmtext

In der Fernmeldeordnung sind zwar verschiedene Rechtsfragen des Btx-Systems geregelt. Diese Vorschriften sind aber hinsichtlich des Datenschutzes unvollständig. So ist z. B. nicht festgelegt, wann die Verbindungsdaten zu löschen sind, die einerseits zum Erbringen der gewünschten Leistungen verarbeitet und kurzfristig gespeichert werden müssen, andererseits aber auch geeignet sind, ein genaues Profil der Systembenutzung zu zeichnen (vgl. dazu 5. TB S. 36 ff.). Zwar werden diese Daten im jetzt eingesetzten System so schnell wie vertretbar gelöscht, das Fehlen einer entsprechenden Rechtsvorschrift begründet hier aber Mißverständnisse und Besorgnis. Die einschlägigen Regelungen sind in der Fernmeldeordnung weit verstreut und dadurch für den Bürger auch zu unübersichtlich. Deshalb habe ich den Bundesminister für das Post- und Fernmeldewesen gebeten zu prüfen, in welcher Form eine vollständige, zusammenhängende und klare Regelung für diesen neuen Dienst geschaffen werden kann, die auch dem Benutzer die notwendige Übersichtlichkeit über die Rechtslage vermittelt.

Bei der Abrechnung der von verschiedenen Anbietern im Btx-System angebotenen vergütungspflichtigen Seiten — d. h. bei dem Verfahren, in dem aus den einzelnen vergütungspflichtigen Abrufen die Belastungen für den Benutzer und die Gutschrift für den Anbieter errechnet werden — werden zur Zeit mehr und detailliertere Daten gespeichert, als vom Zweck her gesehen erforderlich und datenschutzrechtlich vertretbar ist. Auch sonst erscheint das Verfahren der Abrechnung unzweckmäßig und zu aufwendig. Ich begrüße es daher, daß die Bundespost meiner Anregung gefolgt ist und eine Überarbeitung des Abrechnungskonzepts eingeleitet hat.

Die Sicherung des Zugangs zum Btx-Dienst hat noch nicht das Niveau erreicht, das dem erhofften Massenbetrieb angemessen ist. Dies liegt u. a. auch daran, daß es bisher unterlassen wurde, die Benutzer eindringlich auf das hinzuweisen, was sie selbst tun können und müssen, um zu verhindern, daß andere in ihrem Namen und auf ihre Rechnung Btx benutzen können. Die Post hat inzwischen angekündigt, daß sie über entsprechende Hinweise im System Abhilfe schaffen wird.

Ein weiteres Problem ist die noch unzureichende Verfolgung von Versuchen, durch Ausprobieren das persönliche Kennwort eines fremden Benutzers herauszufinden. Für die Sicherheit ist aber entscheidend, daß das persönliche Kennwort geheim gehalten werden kann. Die Reaktion des Systems auf solche Versuche besteht zur Zeit lediglich darin, daß die Verbindung aufgelöst wird, wenn hintereinander drei Fehlversuche unternommen werden. Geschieht dies von einem Btx-Anschluß dreimal am

selben Tag, so wird dieser Anschluß gesperrt. Werden aber immer nur zwei Fehlversuche in Folge unternommen oder täglich nur zwei Verbindungsauflösungen verursacht, so bleibt dies ohne weitere Wirkung. Insbesondere fehlen Aufzeichnungen darüber, wie häufig und mit welcher Hartnäckigkeit Kennwort-Versuche durchgeführt werden, von wem bzw. von welchem Anschluß oder aus welchen Regionen diese Versuche kommen und gegen wen sie gerichtet sind. So kann weder der gefährdete Benutzer gewarnt noch eine andere gezielte Schutzmaßnahme getroffen werden. Aufgrund meiner Anregungen prüft die Post, welche Aufzeichnungen und Auswertungen hier zweckmäßig sind.

Durch die Erhöhung der Vergütungsgrenze für vergütungspflichtige Abrufe auf jetzt 9,99 DM ist das finanzielle Risiko für jeden Btx-Teilnehmer erheblich gestiegen. So konnte in einem Experiment mit einem erschlichenen persönlichen Kennwort und durch geschickten Einsatz eines Kleinrechners gezeigt werden, daß innerhalb eines Tages weit über 100 000 DM durch Aufrufe vergütungspflichtiger Leistungen zu Lasten eines ahnungslosen Btx-Teilnehmers gebucht werden können. Auch wenn der Betrag schließlich nicht eingefordert wurde, die Rechtslage noch offen ist und der Ausgang eines Rechtsstreits auch von der schwierigen Beweislage beeinflußt werden dürfte, zeigt dieses Experiment doch deutlich, daß eine Begrenzung des Risikos notwendig ist. Das kann mit den eingesetzten modernen Computern durchaus sachgerecht gelöst werden, indem eine sowohl aus der Sicht des Betreibers als auch den individuellen Bedürfnissen des Benutzers angemessene Summenbegrenzung vorgesehen wird. Die Post hat aber bisher nicht die Absicht erkennen lassen, diese Risikominderung zu ermöglichen (zu den hier angesprochenen sowie zu anderen Fragen der Datensicherheit bei Btx vgl. auch die Problemskizze im Anhang zu diesem Bericht).

8.5.2 Kontrolle der Btx-Leitzentrale

Das Bildschirmtextnetz kann technisch als zweistufige Rechnerhierarchie gesehen werden: Schaltet sich ein Btx-Teilnehmer vom häuslichen Fernseher aus in den Bildschirmtextdienst ein, so wird zunächst eine Verbindung zur regionalen Bildschirmtext-Vermittlungsstelle aufgebaut. Nachdem der Teilnehmer sich an das System angeschaltet hat, stellt die Vermittlungsstelle automatisch eine Verbindung zur Btx-Leitzentrale in Ulm her. Dort wird — wiederum automatisch — nicht nur die Zugangsberechtigung geprüft, sondern dort werden auch alle bezüglich einer Bildschirmtextbenutzung entstehenden Daten gespeichert und zur weiteren Verarbeitung aufbereitet. Wegen der großen Datenmenge einerseits und der Sensibilität der Daten andererseits müssen hohe Anforderungen an die technischen und organisatorischen Maßnahmen zur Sicherstellung des Datenschutzes gestellt werden. Eine erste Datenschutzkontrolle der Btx-Leitzentrale ergab, daß nicht nur der technische, sondern auch der organisatorische Aufbau der Dienststelle noch nicht abgeschlossen ist. Insbesondere sind die bestehenden Regelungen bezüglich Aufbau- und Ablauforganisation unvollständig. Ich halte es daher für dringend erforderlich, in einem geschlossenen Organisationskonzept nicht nur Aufbau und Arbeitsabläufe der Leitzentrale selbst zu regeln, sondern auch die sich aus der Eigenart der Aufgabe ergebenden besonderen Beziehungen zu anderen organisatorischen Gliederungen der Deutschen Bundespost, wie z. B. dem Fernmeldeamt, dem Fernmeldetechnischen Zentralamt und dem Bundesminister für das Post- und Fernmeldewesen. Wohl ist der Rahmen für die Durchführung des Datenschutzes auch in der Btx-Leitzentrale durch die „Datenschutz-Anweisung" des Ministeriums gegeben, er bedarf jedoch der Ausfüllung durch spezielle und hinreichend detaillierte Regelungen, die den besonderen Belangen der Dienststelle Rechnung tragen. Solche dienststelleninternen Regelungen müssen mit definierten Schnittstellen in das gesamte Sicherheitskonzept des Fernmeldeamtes eingepaßt sein. Wichtig sind hierbei insbesondere die Aufgabenbereiche des mit der Wahrnehmung des Datenschutzes beauftragten Beamten sowie der Betriebssicherung Fernmeldewesen.

Wer Daten verarbeitet, muß die Wirkung der dafür eingesetzten Programme genau kennen. Deshalb hat es überrascht, daß der Deutschen Bundespost als Betreiber des Bildschirmtext-Systems keine umfassende Dokumentation aller eingesetzten Programme vorliegt. Zur Begründung dafür hat sie auf ihre vertraglichen Regelungen mit der Lieferfirma IBM hingewiesen. Dadurch ist es der Deutschen Bundespost verwehrt, sich genaue Kenntnis der Programme in allen Details ohne Hilfe Dritter zu verschaffen. Vor diesem Hintergrund erscheint schwer vorstellbar, wie die Deutsche Bundespost ihrer Verantwortung für die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme (§ 15 Nr. 2 BDSG) gerecht werden kann.

Meine Datenschutzkontrolle in Ulm hat gezeigt, daß die Probleme von den Verantwortlichen erkannt sind; ich hoffe, daß bald entsprechende Lösungen gefunden werden. Wichtig erscheint mir zunächst, daß für die Btx-Leitzentrale die Funktion eines Sicherheitsbeauftragten vorgesehen ist, der schwerpunktmäßig auch Aufgaben des Datenschutzes wahrnehmen soll. Ich verweise hierzu auf meine Ausführungen zur Organisation des Datenschutzes bei der Deutschen Bundespost (s. oben Nr. 8.1).

8.6 Funkfernsprechdienst (Autotelefon)

Mit Hilfe von Überleiteinrichtungen, die bei Fernmeldeämtern installiert sind, wird die Funkverbindung zwischen dem normalen (drahtgebundenen) Telefonnetz und dem Autotelefon hergestellt. Dabei entstehen für jedes Funkferngespräch automatisch (personenbezogene) Datensätze, die den äußeren Ablauf der Verbindung beschreiben. Insbesondere bei vom Auto aus aufgebauten Gesprächen werden nicht nur genaue Zeitangaben, sondern — neben der eigenen — auch die vollständige Rufnummer des angerufenen Teilnehmers registriert. Diese Angaben werden für die Durchführung des Funkfernsprechdienstes nicht benötigt. Sie stellen im übrigen Einzelgesprächsdaten im Sinne des Beschlus-

ses des Ausschusses für das Post- und Fernmeldewesen des Deutschen Bundestages dar (s. oben Nr. 8.3). Ich halte an meiner Ansicht fest — die auch in dem von mir entworfenen Beschluß zum Ausdruck kommt —, daß aus Gründen des Datenschutzes die Aufzeichnung solcher Einzelgesprächsdaten die Einwilligung des betroffenen Teilnehmers (in der Regel in Form eines Antrages) voraussetzt. Diese fehlt hier; vielmehr muß angenommen werden, daß den meisten Autotelefonbenutzern solche Registrierungen nicht bekannt sind.

Ich habe mich davon überzeugen lassen, daß die verwendete Technik des heute betriebenen Funkfernsprechnetzes B2 eine Änderung des Verfahrens mit vertretbarem Aufwand nicht gestattet. Bei der Konzipierung und dem Betrieb künftiger Funkfernsprechnetze muß zur Sicherstellung des Datenschutzes der Betroffenen jedoch den angesprochenen Problemen Rechnung getragen werden.

Allerdings begründet die Deutsche Bundespost bestimmte Speicherungen und listenmäßige Auswertungen der Gesprächsdatensätze zum Teil mit der Notwendigkeit der Aufklärung und Verfolgung von Fällen mißbräuchlicher Nutzung des Funkfernsprechdienstes. Dabei handelt es sich um zuweilen vorkommende Mißbräuche, bei denen nach (technisch einfachen, wenngleich rechtswidrigen) Eingriffen in die verwendeten Geräte Funkferngespräche geführt werden, die eine Gebührenbelastung unbeteiligter Dritter zur Folge haben. Das geplante neue System muß diese Mißbrauchsmöglichkeiten auch aus Gründen des Datenschutzes entscheidend mindern. Dadurch würde die Notwendigkeit der genannten Speicherungen bzw. Auswertungen durch die Deutsche Bundespost entfallen.

Bislang werden im Rechenzentrum des Fernmeldeamtes Mannheim die Gesprächsdaten aus den Überleiteinrichtungen zusammengefaßt, zur Erstellung der Fernmelderechnung aufbereitet und wie erwähnt listenmäßig ausgewertet. Angesichts der hohen Sensibilität der Daten halte ich es für notwendig, daß das Verfahren der Erstellung, der Verteilung und des Verbleibs der Listen sowie ihre Vernichtung lückenlos dokumentiert wird. Auch sollte überprüft werden, ob alle Stellen, die derzeit Empfänger solcher Listen sind, diese für ihre Tätigkeit benötigen.

Eine besondere Problematik sehe ich in der Auflistung aller solcher Funkferngespräche, die von Bediensteten der Deutschen Bundespost über dienstliche Funkfernsprechanschlüsse geführt werden. Wohl wird der angegebene Zweck — Mißbrauchskontrolle des Anschlusses — von mir dann anerkannt, wenn tatsächlich eine Auswertung dieser Listen zu dem genannten Zweck erfolgt. In jedem Fall halte ich es aber für unerläßlich, daß alle betroffenen Bediensteten über dieses Verfahren informiert werden (vgl. oben Nr. 7.2.3).

8.7 Telefon-Fernwirkdienst TEMEX

Unter „Fernwirken" wird die Übertragung von Meßwerten — Zählerständen, Temperaturangaben usw. — über größere Entfernungen mit Hilfe elektronischer Übertragungsmedien verstanden. Hierbei ist z. B. an die automatisierte Übertragung etwa des Zählerstandes der „Stromzähler" in den privaten Haushalten an das Elektrizitätsversorgungsunternehmen zu denken. Auch kann beispielsweise in Notfällen die automatische Alarmierung eines privaten Hilfsdienstes mit Hilfe von Fernwirkeinrichtungen erfolgen. Das Eindringen von außen in den geschützten Bereich der Wohnung mittels solcher automatisch ablaufender und für den Bürger nicht überschaubarer Vorgänge hat Besorgnisse aufkommen lassen, das Elektrizitätsversorgungsunternehmen z. B. könnte — vom Bürger unbemerkt — Aufzeichnungen über seine Lebensgewohnheiten durch punktuelle Registrierung und zweckwidrige Auswertung der Meßdaten gewinnen oder unbefugte Dritte könnten in mißbräuchlicher Weise auf Daten zugreifen („mitlesen") und/oder sie zuungunsten des Betroffenen verändern. Solche und weitere Bedenken hatten die Datenschutzbeauftragten in Bund und Ländern schon frühzeitig geltend gemacht. Ich habe es daher begrüßt, daß der Verwaltungsrat der Deutschen Bundespost die Beschlußfassung über die vom Bundesministerium für das Post- und Fernmeldewesen vorgesehene Einführung des TEMEX-Dienstes mit Rücksicht auf die noch offenen Fragen des Datenschutzes zurückgestellt hat. Inzwischen habe ich dem Bundesminister für das Post- und Fernmeldewesen eine erste Stellungnahme zur datenschutzrechtlichen Problematik des TEMEX-Dienstes zugeleitet. Darüber hinaus habe ich die Schaffung eines Beratungsgremiums — z. B. in Form eines Beirates — befürwortet, das während der Dauer der vorgesehenen Systemversuche auch Datenschutzprobleme erkennen und lösen helfen könnte. Im Rahmen dieser Systemversuche sollen vorerst ausschließlich datenschutzrechtlich weniger sensible Anwendungen, wie z. B. die Übertragung von Alarmen und Notfallmeldungen erprobt werden.

8.8 Telebox-Dienst

Mit dem Telebox-Dienst will die Deutsche Bundespost ein „elektronisches Postfach" anbieten, in das zwar jedermann Nachrichten ablegen, das aber nur vom berechtigten Inhaber „geleert" werden kann. Im Juni dieses Jahres hat die Deutsche Bundespost ein Testsystem mit 100 Boxen in Betrieb genommen, das bis Ende 1986 auf 2 000 Boxen ausgebaut werden soll.

Der Telebox-Dienst soll es ermöglichen, kurze Textmitteilungen anderen Personen oder Personengruppen schnell zu übermitteln. Voraussetzung ist dabei, daß sowohl der Absender als auch der/die Empfänger geeignete Terminals — z. B. Personalcomputer — besitzen und für sie im Telebox-Rechner der Deutschen Bundespost eine Box eingerichtet wurde. Dann kann z. B. der Vertreter eines überregional operierenden Versicherungsunternehmens — unabhängig von Aufenthaltsort und Tageszeit — seinem Unternehmen die wichtigsten Daten der jeweils getätigten Vertragsabschlüsse übermitteln. Unbefugten soll das Lesen des Box-Inhaltes durch

die Verwendung persönlicher Paßworte verwehrt werden. Aus der Sicht des Datenschutzes liegen die Probleme im wesentlichen im Bereich der technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit. Dabei ist sicherzustellen, daß nur Berechtigte den Inhalt der Boxen lesen und löschen können. Darüber hinaus darf ein unbemerktes Verändern abgelegter Nachrichten wie auch das Absenden „anonymer Briefe" nicht möglich sein.

Beim Telebox-Dienst ist das Risiko des unbefugten Zugangs deshalb besonders hoch, weil geeignete Terminals — Geräte, die an jedes Telefon angeschlossen werden können — bereits jetzt in großer Anzahl in Betrieb sind und ihre Anzahl ständig wächst. Der Zugang zur einzelnen Telebox ist nur durch ein Paßwort geschützt. In der Öffentlichkeit sind bislang zwei Fälle unbefugten und mißbräuchlichen Systemzugangs bekanntgeworden; von einer hohen Dunkelziffer ist auszugehen. Ich habe daher erhebliche Zweifel, ob die derzeitigen Regelungen den Forderungen des § 6 BDSG gerecht werden. Insbesondere sollte sorgfältig geprüft werden, ob der realisierte Paßwortschutz ausreichende Datensicherheit bietet.

8.9 Automatisierung im Fernsprechdienst (KONTES)

Die Deutsche Bundespost beabsichtigt, die Fernsprechteilnehmerverwaltung, insbesondere den Anmelde- und den Auskunftsdienst sowie die Erstellung der Fernsprechbücher zu automatisieren. Zu diesem Zweck sollen alle Informationen, die der Deutschen Bundespost über einen Teilnehmer und seinen Anschluß bekannt sind, in Rechnersystemen erfaßt und verarbeitet werden.

Im Rahmen des Projektes KONTES werden im Bereich der Oberpostdirektion München die Teilprojekte AUDI (Auskunftsdienst) und BUDI (Fernsprechbuchdienst), im Bereich Düsseldorf das Teilprojekt ANDI (Anmeldedienst) erprobt. Ich habe mir von der Deutschen Bundespost das technische Konzept sowie den vorgesehenen Terminplan darlegen und die wichtigsten Aspekte der Teilprojekte AUDI und BUDI vor Ort erläutern lassen. Dies ermöglicht noch keine eingehende datenschutzrechtliche Beurteilung, läßt aber bereits jetzt einige Problempunkte erkennen. So wird besonders im automatisierten Verfahren sichergestellt werden müssen, daß nicht entgegen dem Willen des Fernsprechteilnehmers Angaben zu seiner Person der Deutschen Postreklame übermittelt werden (vgl. 5. TB S. 34). Auch muß gewährleistet sein, daß über solche Fernsprechanschlüsse, die auf Antrag oder von Amts wegen nicht ins Fernsprechbuch eingetragen werden (sogenannte „Geheimnummern"), auch vom Auskunftsdienst keine Auskunft erteilt wird.

8.10 Automatisierung am Postschalter

Über einen Praxistest, bei dem die Deutsche Bundespost einige automatisierte Postschalter betreibt, habe ich in meinem Sechsten Tätigkeitsbericht berichtet (vgl. S. 23). Der Bundesminister für das Post- und Fernmeldewesen hat mich davon unterrichtet, daß der bisherige Betriebsversuch im Sommer 1984 eingestellt worden ist. In der Zwischenzeit wurde ein neues Betriebskonzept erarbeitet. Ein wesentlicher Unterschied zum bisherigen Konzept ist — neben der Abkehr vom Online-Betrieb — der zu begrüßende geringere Umfang der Speicherung personenbezogener Daten. Es ist vorgesehen, bis Ende 1989, beginnend ab April 1987, alle ca. 20 000 Schalter der Postämter und Poststellen I mit dem neuen System auszurüsten. Mit dem Bundesminister für das Post- und Fernmeldewesen wurde eine fortlaufende Unterrichtung über den Fortgang des Projekts vereinbart.

8.11 Weitergabe von Urteilsabschriften durch die Deutsche Bundespost

Durch die Eingabe eines Bürgers bin ich darauf hingewiesen worden, daß die Deutsche Bundespost ein gegen einen Postbediensteten ergangenes Urteil wegen seiner grundsätzlichen Bedeutung einer Vielzahl von Stellen ihres Geschäftsbereichs zur Kenntnis gebracht hat, ohne den Namen des Betroffenen vorher unkenntlich gemacht zu haben. Darüber hinaus ist das Urteil dem Bundesminister des Innern und von hier an die für den Problemkreis zuständigen obersten Bundes- und Landesbehörden ebenfalls unter Namensnennung übermittelt worden. Der Bundesminister für das Post- und Fernmeldewesen hat die unterbliebene Anonymisierung als ein Versehen bedauert. Er und der Bundesminister des Innern haben die Empfänger des Urteils um nachträgliche Schwärzung der personenbezogenen Daten gebeten.

Es ist zu hoffen, daß dieser Vorgang und seine Erörterung zur weiteren datenschutzrechtlichen Sensibilisierung der Behörden und ihrer Bediensteten in vergleichbaren Fällen beigetragen hat.

9. Verkehrswesen

9.1 Fahrzeugregistergesetz (ZEVIS)

Ein Schwerpunkt meiner Beratungstätigkeit auf dem Gebiet des Verkehrswesens bezog sich auf den Gesetzentwurf zur Änderung des Straßenverkehrsgesetzes, der vom Bundesminister für Verkehr zur Zeit erarbeitet wird, und der in einem neuen Abschnitt Regelungen über die Fahrzeugregister bei den örtlichen Kfz-Zulassungsstellen sowie beim Kraftfahrt-Bundesamt (KBA) in Flensburg vorsieht. Mit diesem Gesetzentwurf soll vor allem die Einführung des „Zentralen Verkehrsinformationssystems (ZEVIS)" beim KBA auf eine gesetzliche Grundlage gestellt werden. Dies entspricht dem aufgrund der Empfehlung des Innenausschusses vom Deutschen Bundestag in seiner Sitzung am 20. September 1984 gefaßten Beschluß, ihm so bald wie möglich einen entsprechenden Gesetzesvorschlag zuzuleiten und bis zu dessen Inkrafttreten

vom geplanten weiteren Ausbau von ZEVIS abzusehen.

Über die Entwicklungs- und Aufbauphase von ZEVIS und meine Bedenken, diese ohne Rechtsgrundlage fortzusetzen, habe ich in meinen beiden letzten Tätigkeitsberichten (5. TB S. 41 ff., 6. TB S. 25/26) ausführlich berichtet.

Zu dem vom Bundesminister für Verkehr vorgelegten Gesetzentwurf, der als Ergebnis intensiver bilateraler Beratung und mehrerer Ressortbesprechungen inzwischen einen über weite Strecken erfreulich hohen datenschutzrechtlichen Stand erhalten hat, erscheinen folgende grundsätzliche Bemerkungen angebracht:

a) Der Entwurf enthält keine Regelung des rechtssystematischen Verhältnisses zwischen den registerrechtlichen Regelungen der Datenübermittlung einerseits und den Befugnissen der Strafverfolgungsorgane und der Behörden der polizeilichen Gefahrenabwehr zur Erhebung, Speicherung und weiteren Verarbeitung der erfragten personenbezogenen Daten andererseits.

   Ich gehe davon aus, daß die Regelungen des Entwurfs nur den registerrechtlichen Aspekt berücksichtigen, im übrigen aber jeweils zusätzlich eine (gesetzlich begründete) Befugnis für Maßnahmen der Strafverfolgung bzw. der Gefahrenabwehr voraussetzen. Aus Gründen der Normenklarheit und um unbegründete Befürchtungen auszuräumen, sollte das Verhältnis der Normenbereiche zueinander in diesem Sinne klargestellt werden.

b) Die Einrichtung von Online-Anschlüssen zur Übermittlung personenbezogener Daten an Strafverfolgungsorgane und Behörden der Gefahrenabwehr gibt diesen die Möglichkeit, von ihren Befugnissen zum Sammeln personenbezogener Daten in einer sehr viel nachhaltigeren Weise Gebrauch zu machen. Der Ausbau der automatisierten Datenverarbeitung sollte deshalb den Gesetzgeber veranlassen, diese Befugnisse gesetzlich genauer zu umschreiben und im Sinne des Datenschutzes deutlicher zu begrenzen. Insbesondere muß gesetzlich klargestellt werden, daß Datenübermittlungen bzw. -abrufe aus dem Fahrzeugregister nicht beliebig und routinemäßig (etwa zu präventiven Sicherheitszwecken) erfolgen dürfen, sondern nur dann, wenn fallbezogene Umstände vorliegen, die ein derartiges Vorgehen rechtfertigen.

   Auch die Dringlichkeit gesetzlicher Regelungen für die Komplexe der polizeilichen Beobachtung und der Amtshilfe zwischen Polizei und Verfassungsschutz sowie Bundesnachrichtendienst wird durch das Projekt ZEVIS erneut unterstrichen.

c) Ich habe bereits in meinen früheren Tätigkeitsberichten (2. TB S. 42, 4. TB S. 21, 5. TB S. 42, 6. TB S. 25) darauf hingewiesen, daß die im Rahmen von ZEVIS vorgesehene Online-Konzeption nur durch gesetzliche Regelungen zugelassen werden kann. Nach dem Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 hat der Gesetzgeber, wenn er die Verarbeitung zwangsweise erhobener Daten regelt, organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken. Diese Pflicht wird insbesondere bei der Regelung von Verfahren der Online-Übermittlung aktuell. Sie erfordert in diesem Fall eine genaue Auseinandersetzung mit Inhalt, Art und Struktur des Informationsbedarfs der jeweiligen Übermittlungsempfänger. Ferner muß der Bedarf der Strafverfolgungsorgane und der Behörden der polizeilichen Gefahrenabwehr bezüglich des Online-Verfahrens im einzelnen dargelegt werden.

   Zur Frage der Zulässigkeit der sogenannten P-Anfrage (Anfrage nach der Anschrift, dem Geburtsdatum oder den Fahrzeugen einer namentlich benannten Person) im Online-Verfahren hat der Bundesminister des Innern mit Schreiben vom 26. Januar 1984 Stellung bezogen und an Einzelfällen dargestellt, daß die Verfügbarkeit der P-Anfrage im Online-Verkehr für den Erfolg bestimmter polizeilicher Maßnahmen wesentlich ist; meiner Bitte, das polizeiliche Informationsbedürfnis auch quantifizierend darzulegen, konnte der Bundesminister des Innern jedoch mangels Unterlagen hierzu nicht entsprechen.

   Da somit keine ausreichende Beurteilungsgrundlage besteht, kann ich meine Bedenken allenfalls vorläufig zurückstellen, wenn eine Regelung getroffen wird, die geeignet ist, zunächst praktische Erfahrungen mit diesem Übermittlungsverfahren zu sammeln. Auf dieser Grundlage wäre dann eine endgültige Entscheidung zu einem späteren Zeitpunkt zu treffen.

d) Grundsätzlich ist davon auszugehen, daß die Rechtmäßigkeit der Übermittlung von personenbezogenen Daten im Rahmen der Datenschutzkontrolle überprüfbar sein muß. Dies bedingt, daß nachträglich feststellbar sein muß, wann welche Angaben an wen übermittelt wurden und welches die rechtfertigenden Gründe hierfür waren. Dies gilt unabhängig von der Form der Übermittlung. Durch entsprechende gesetzliche Regelungen ist sicherzustellen, daß im Falle der Übermittlung von Daten aus den Fahrzeugregistern (und von Fahrerlaubnisdaten aus dem Verkehrszentralregister) durch geeignete organisatorische und technische Maßnahmen eine objektive Kontrolle der Zulässigkeit der Abrufe möglich ist. Insbesondere ist eine Protokollierung der einzelnen Abrufe geboten. Die Protokolle dürfen ausschließlich für Kontrollzwecke verwendet werden. Die Möglichkeit einer zweckfremden Verwendung kann durch eine flexibel gehandhabte Auswahlprotokollierung und gestaffelte Löschungsfristen weitestgehend ausgeschlossen werden.

   Die am Übermittlungsverfahren beteiligten Behörden sind gesetzlich zu verpflichten, von sich aus die Rechtmäßigkeit der Datenverarbeitung effektiv zu kontrollieren. Aufgabe der Datenschutzbeauftragten des Bundes und der Länder

wird es sein, das Verfahren der Selbstkontrolle und seine praktische Anwendung zu überprüfen und darüber hinaus eigene Stichproben sowie Überprüfungen aus gegebenem Anlaß vorzunehmen.

Da Erfahrungen mit dem Betrieb und der Zulässigkeitskontrolle von Datenverarbeitungssystemen, die unterschiedlichen Fachbehörden den direkten Zugriff eröffnen, bisher nicht vorliegen, sollte die gesetzliche Regelung so flexibel gestaltet werden, daß gezielt Erfahrungen mit unterschiedlichen Varianten gewonnen und daraus praktische Konsequenzen im Sinne einer Optimierung von Effektivität und Wirtschaftlichkeit der Kontrollverfahren gezogen werden können.

Wenn die bestehenden technischen und organisatorischen Möglichkeiten der Zulässigkeitskontrolle genutzt werden, kann der Datenschutz beim Verfahren des Online-Zugriffs genauso gut — und teilweise besser — verwirklicht werden wie bei den herkömmlichen Formen der Übermittlung. Mitunter wird allerdings behauptet, die Übermittlung durch Online-Zugriff sei prinzipiell risikoreicher, weil hier die Möglichkeit der vorherigen Zulässigkeitsprüfung durch die übermittelnde Stelle wegfalle. Dies trifft aber nicht zu. Denn auch beim herkömmlichen Übermittlungsverfahren kann die übermittelnde Stelle nur prüfen, ob die anfragende Stelle diejenige ist, als die sie sich ausgibt (Identitätskontrolle), ob die Stelle für Anfragen der betreffenden Art grundsätzlich zuständig ist und ob sie einen zulässigen Anfragegrund angibt. Alle diese Prüfungen können beim Online-Übermittlungsverfahren in die automatisierte Berechtigungsprüfung übernommen werden. Dabei kann in mancher Beziehung eine höhere Präzision erreicht werden.

Eine weitergehende Zulässigkeitsprüfung, etwa bezüglich der Frage, ob die von der anfragenden Stelle behaupteten Voraussetzungen tatsächlich vorliegen, wird auch im herkömmlichen Übermittlungsverfahren nicht vorgenommen. Eine solche Prüfung durch die übermittelnde Stelle wäre — ganz abgesehen von den erheblichen praktischen Problemen — auch aus der Sicht des Datenschutzes gar nicht zu wünschen, weil sie die Offenlegung umfassender und oft sensibler personenbezogener Informationen nötig machen würde. So müßten beispielsweise Polizei und Staatsanwaltschaft Ermittlungsakten an das Kraftfahrt-Bundesamt senden und damit die Verstrickung bestimmter Personen in strafbare Handlungen offenlegen, um Namen und Anschrift der Halter von möglicherweise beteiligten Fahrzeugen zu erhalten. Dies würde der verfassungsrechtlichen Verpflichtung widersprechen, Organisation und Verfahren so einzurichten, daß die Grundrechte der Betroffenen möglichst geschont werden. Die Konsequenz daraus ist bei der herkömmlichen und bei der Online-Übermittlung gleich: Übermittlungsersuchen werden nur formal geprüft, wobei die (gleichen) Prüfmerkmale entweder in Arbeitsanweisungen für die Registerbediensteten oder im DV-Programm niedergelegt sein können. Eine umfassende, auch inhaltliche Überprüfung der Zulässigkeit der Übermittlung kann in beiden Fällen nur nachträglich durchgeführt werden und muß — gestützt auf entsprechende Aufzeichnungen — bei der anfragenden Stelle ansetzen.

e) Von grundlegender konzeptioneller Bedeutung für die Ausgestaltung der Nutzungs- und Übermittlungsregelungen ist der vom Bundesverfassungsgericht besonders hervorgehobene Grundsatz der Zweckbestimmung und Zweckbindung. Die Diskussion hat sich bisher leider allzusehr auf die Frage konzentriert, ob und wie die Zweckbindung aufrechterhalten werden kann, wenn die Daten anderen Stellen zum Online-Zugriff bereitgestellt werden. Vor allem bei der (geplanten) Online-P-Anfrage wurden Zweifel geäußert, ob sie mit der Zweckbindung im Einklang steht.

   Im Grunde genommen handelt es sich jedoch um zwei getrennte Fragen. Der Grundsatz der Zweckbindung beantwortet die Frage, für welche anderen Zwecke als den ursprünglichen Verarbeitungszweck personenbezogene Daten verwendet werden dürfen. Er gilt ganz unabhängig von dem technisch-organisatorischen Verfahren, in dem Daten für andere Zwecke bereitgestellt werden. Die Übermittlung in der Form des Online-Zugriffs ist eines von mehreren denkbaren Übermittlungsverfahren. Mit der Auswahl eines bestimmten Verfahrens wird nur die Frage beantwortet, *wie* übermittelt wird, nicht aber was und zu welchem Zweck.

   Ein mittelbarer politischer und auch verfassungsrechtlicher Zusammenhang ist allerdings nicht zu leugnen. Wie das Bundesverfassungsgericht festgestellt hat, darf der fortgeschrittene technologische Entwicklungsstand bei der Verfassungsinterpretation nicht unberücksichtigt bleiben. Dies bedeutet konkret: Je schneller, leichter und besser auswertbar personenbezogene Daten für alle möglichen Zwecke der Verwaltung zur Verfügung stehen, um so akuter wird die Verpflichtung des Gesetzgebers, im einzelnen festzulegen und abzugrenzen, für welche anderen Zwecke die Daten im Hinblick auf ein von ihm anerkanntes überwiegendes Allgemeininteresse zur Verfügung stehen dürfen. P-Anfragen, also Anfragen nach der Anschrift, dem Geburtsdatum oder den Fahrzeugen einer namentlich benannten Person, konnte das Kraftfahrt-Bundesamt schon bisher beantworten, allerdings nur mit erheblichem technischen und zeitlichen Aufwand und deshalb in sehr beschränktem Umfang. Mit der Verwirklichung der Online-P-Anfrage im Rahmen des ZEVIS würden diese Beschränkungen, die auf die Häufigkeit von Anfragen regulierend wirken, wegfallen. Deshalb ist der Gesetzgeber aufgerufen, die obsolet gewordene technische und organisatorische Schranke durch ein rechtliches Regulativ zu ersetzen.

Zu Einzelregelungen des Gesetzentwurfs mit datenschutzrechtlichem Bezug werde ich mich im Hin-

blick auf die laufenden Abstimmungsgespräche innerhalb der Bundesregierung und der Koalitionsfraktionen im weiteren Gesetzgebungsverfahren äußern.

9.2 Übermittlung von Zulassungsdaten durch das KBA an die Automobilwirtschaft

Das Kraftfahrt-Bundesamt (KBA) speichert die Daten der An-, Um- und Abmeldungen aller in der Bundesrepublik zugelassenen Kraftfahrzeuge zentral und stellt sie für die Aufgabenerfüllung der Verkehrsverwaltung zur Verfügung.

Jahrelang war es Praxis des KBA, auch der Automobilindustrie Daten aus dem Kfz-Zulassungswesen zu überlassen. Die Automobilindustrie ebenso wie die Importeure ausländischer Fahrzeuge begründeten ihr „berechtigtes Interesse" an einigen dieser Daten damit, daß dadurch Sicherheitsmängel an Fahrzeugen beseitigt, Produktionsmängel frühzeitig erkannt, eine optimale Versorgung der Autofahrer mit Ersatzteilen und anderem Service erreicht und Vertragsabsprachen beim Vertrieb von Fahrzeugen überwacht werden könnten. Alles dies diene — zumindest mittelbar — der Verkehrssicherheit. Das KBA hielt daher eine Weitergabe der Daten auf der Grundlage des § 11 Satz 1 2. Alternative BDSG für zulässig, nicht zuletzt auch deswegen, weil — außer bei Rückrufaktionen — weder Namen noch Anschriften von Haltern mitgeteilt wurden.

Ich habe gegen einen erheblichen Teil der Übermittlungen datenschutzrechtliche Bedenken erhoben. Die Datenempfänger können durch Verknüpfung mit eigenen Datenbeständen die Händler und unter besonderen Umständen auch die Fahrzeughalter identifizieren. Somit handelt es sich um personenbezogene Daten.

Für die datenschutzrechtliche Beurteilung ist es wesentlich, daß die Angaben zwangsweise vom Betroffenen erhoben werden. Für solche Daten gilt der Grundsatz der Zweckbestimmung und Zweckbindung. Soweit die Verwendung der Daten nicht dem Zweck dient, zu dem sie dem Bürger abgefordert wurden, liegt eine Zweckentfremdung vor, die nur durch Gesetz im überwiegenden Allgemeininteresse gestattet werden kann.

Auskünfte des KBA für Rückrufaktionen sind demnach unbedenklich, wenn sichergestellt ist, daß die Daten ausschließlich zu diesem, der Verkehrssicherheit dienenden, Zweck benutzt werden. Die Durchführung der Rückrufaktion darf daher nicht mit Werbemaßnahmen verbunden werden.

Mit der Zweckbindung vereinbar ist auch die Übermittlung einiger Zulassungsdaten zur fortlaufenden Produktbeobachtung, um sicherheitsrelevante Serienfehler rechtzeitig als solche erkennen, sie korrigieren und die Fehlerquelle beseitigen zu können. Bedingung ist, daß die Angaben ausschließlich zahlenmäßig, nämlich zur Bildung mathematisch-statistischer Vergleichsgrößen, verwendet werden und eine anderweitige Auswertung durch technische und organisatorische Maßnahmen ausgeschlossen wird. Die Datenempfänger müssen sich zur Kontrolle der Zweckbindung mit einer jederzeitigen Überprüfung durch die Datenschutzaufsicht einverstanden erklären. Der Bundesminister für Verkehr beabsichtigt eine entsprechende Änderung des Straßenverkehrsgesetzes.

Für nicht mit der Zweckbestimmung vereinbar halte ich die Übermittlung personenbezogener Daten für unternehmensstrategische und absatzpolitische Zwecke der Automobilwirtschaft. So sehr eine leistungsstarke Kundendienst- und Vertriebsorganisation auch im Interesse des Autofahrers liegen mag, so sehr fehlt ihr doch der direkte Bezug zu dem Zweck der Datenerhebung. Dasselbe gilt für den Wunsch der Fahrzeugindustrie, mit Hilfe von Zulassungsdaten die Einhaltung ihrer mit Großabnehmern getroffenen vertraglichen Abmachungen überprüfen und sogenannte graue (Re-)Importe aufdecken zu können. Das Interesse der Unternehmen ist zwar durchaus legitim, stellt aber kein überwiegendes Allgemeininteresse dar, hinter dem das informationelle Selbstbestimmungsrecht der Betroffenen zurückzustehen hat.

9.3 KBA-Daten an Funkkontrollmeßstellen der Deutschen Bundespost

Anläßlich eines Kontrollbesuchs beim Kraftfahrt-Bundesamt wurde ich gebeten, das KBA dahin gehend zu beraten, ob eine Übermittlung von Fahrzeug-/Halterdaten aus dem zentral geführten Kraftfahrzeugbestand an den Funkkontrollmeßdienst der Deutschen Bundespost datenschutzrechtlich unbedenklich ist.

Der Funkkontrollmeßdienst der Deutschen Bundespost führt nach fachlicher Weisung des Fernmeldetechnischen Zentralamtes u. a. Ermittlungen zur Feststellung nicht genehmigter Sendefunkstellen durch, um Störungen des Fernmeldeverkehrs, insbesondere auch von Funkdiensten, feststellen und beheben zu können. Außerdem hat die Deutsche Bundespost Gebührenausfälle durch mißbräuchliche Benutzung von Funkanlagen, insbesondere im Funkfernsprechverkehr (Autotelefon); zu deren Verfolgung benötigen die Funkkontrollmeßstellen nach Auffassung der Deutschen Bundespost Fahrzeug-/Halterdaten, um im öffentlichen Interesse weitere Maßnahmen einleiten zu können. Der Bundesminister für das Post- und Fernmeldewesen verweist dabei auf die sonderordnungsbehördliche Zuständigkeit der Deutschen Bundespost zur Beseitigung von Störungen aufgrund der §§ 1 und 2 des Gesetzes über Fernmeldeanlagen (FAG).

Meine Prüfung hatte folgendes Ergebnis:

Die Übermittlung von Fahrzeug-/Halterdaten an die Funkkontrollmeßstellen der Deutschen Bundespost zur Ermittlung nichtgenehmigter Sendefunkstellen (Autotelefone) ist nach §§ 3, 10 BDSG zu beurteilen, da bereichsspezifische Übermittlungsvorschriften nicht bestehen. Die Errichtung und der Betrieb von Funksprechanlagen ist gemäß § 15

Abs. 1 FAG strafbar. Die Funkkontrollmeßstellen sind mit ihren technischen Möglichkeiten in der Lage, den Kreis der Tatverdächtigen so einzugrenzen, daß die Polizei — gegebenenfalls im Wege eines Auskunftsersuchens an das KBA — in der Lage ist, den Tatverdächtigen festzustellen und weitere Maßnahmen der Strafverfolgung einzuleiten. Diese polizeiliche Ermittlungstätigkeit kann die Deutsche Bundespost für sich nicht in Anspruch nehmen. Ein Erfordernis der Datenübermittlung ist jedenfalls solange nicht ersichtlich, als sie lediglich die Strafverfolgung durch Anzeige bei einer Staatsanwaltschaft bezweckt. Der Bundesminister für das Post- und Fernmeldewesen hat auch nicht geltend gemacht, daß er zur hinreichenden Konkretisierung der Verdachtsmomente, die eine Anzeige überhaupt erst sinnvoll und aussichtsreich erscheinen läßt, nur mit Hilfe der Auskunft aus dem KBA in der Lage ist. Die Datenübermittlung an die Funkkontrollmeßstellen ist daher weder zur rechtmäßigen Aufgabenerfüllung des KBA noch des Funkkontrollmeßdienstes der Deutschen Bundespost erforderlich.

Ich habe den Bundesminister für das Post- und Fernmeldewesen und das KBA entsprechend unterrichtet.

9.4 Verkehrszentralregister

Das beim Kraftfahrt-Bundesamt (KBA) in Flensburg geführte Verkehrszentralregister (VZR) enthält rechtskräftige Entscheidungen wegen Ordnungswidrigkeiten, Entziehungen und Versagungen von Fahrerlaubnissen, Fahrverbote sowie strafrechtliche Verurteilungen im Zusammenhang mit der Teilnahme am Straßenverkehr (§ 28 des Straßenverkehrsgesetzes — StVG —).

9.4.1 Auskunftserteilung nach § 30 StVG (Vollauskunft)

Das Kraftfahrt-Bundesamt erteilt Auskünfte aus dem Verkehrszentralregister stets als „Vollauskunft", d. h. *alle* über eine Person vorhandenen Eintragungen werden *in vollem Umfang* mitgeteilt. Eine Prüfung, ob der Zweck des Auskunftsbegehrens die Übermittlung sämtlicher Eintragungen erforderlich macht oder ob eine Teilauskunft ausreicht, wird nicht vorgenommen. Als Rechtsgrundlage für diese Art der Auskunftserteilung wird § 30 StVG angegeben.

Ich hatte den Bundesminister für Verkehr mehrfach auf meine Rechtsauffassung hingewiesen (s. u. a. 5. TB S. 40), daß § 30 Abs. 2 Satz 1 StVG umfassend und abschließend nur regelt, welche Stellen auskunftsberechtigt sind. Satz 2 regelt darüber hinaus, wie die Auskünfte zu erteilen sind, und zwar so, „daß die anfragende Stelle die Akten über die den Eintragungen zugrundeliegenden Entscheidungen beiziehen kann". Über den Umfang der Auskunft trifft § 30 StVG keine Regelung. Insoweit sind daher die Vorschriften der §§ 3, 10 und 11 BDSG zu beachten. Dies bedeutet, daß in jedem Einzelfall zu prüfen ist, in welchem Umfang eine Auskunft zur rechtmäßigen Erfüllung der Aufgaben des Empfängers erforderlich ist bzw. inwieweit der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden.

Im Hinblick auf die vom Bundesminister für Verkehr angekündigte bereichsspezifische Regelung hatte ich bisher von einer Beanstandung abgesehen. Da es jedoch zu einer solchen Regelung nicht gekommen und diese in absehbarer Zukunft auch nicht zu erwarten ist, mußte ich die vom KBA praktizierte Vollauskunft gemäß § 20 Abs. 1 BDSG beanstanden.

Der Bundesminister für Verkehr teilte mir daraufhin mit, daß das Auskunftsverfahren so umgestellt werden solle, daß ab 1. Januar 1985 auch Teilauskünfte gegeben werden können. Dieses soll in der Weise geschehen, daß für die Verfolgung von Ordnungswidrigkeiten, bei der Erst-/Neuerteilung einer Fahrerlaubnis sowie bei der Erteilung einer Sonderfahrerlaubnis auf die Übermittlung etwaiger Eintragungen bezüglich einer Fahrlehrerlaubnis sowie einer Fahrerlaubnis zur Fahrgastbeförderung verzichtet werden soll. Hinzu kommt noch eine Auskunftseinschränkung im Falle der Ersatzausfertigung eines Führerscheins.

Ich habe mit Befriedigung zur Kenntnis genommen, daß der Bundesminister für Verkehr eine am Informationsbedarf orientierte Auskunftsregelung nicht länger generell ablehnt. Zu bedauern ist aber, daß er aus der Vielzahl der Eintragungen lediglich einige wenige herausgreifen und deren Übermittlung auch nur bei der Auskunft für einige wenige Zwecke ausschließen will. Damit würden nur einzelne, eklatante Fälle korrigiert. Ich habe dem Bundesminister für Verkehr daher mitgeteilt, daß meine Beanstandung im wesentlichen bestehenbleibt.

9.4.2 Eintragungsregelung des § 13 Abs. 1 Nr. 1 Buchstaben m bis o StVZO

§ 28 des Straßenverkehrsgesetzes (StVG) ermächtigt den Bundesminister für Verkehr zum Erlaß von Vorschriften „über die Erfassung ... von Versagungen (und) ... Entziehungen einer Fahrerlaubnis". Der Bundesminister für Verkehr hat jedoch mit der Verordnung zur Änderung der Straßenverkehrszulassungsordnung (StVZO) vom 20. Juni 1973 folgende Eintragungstatbestände in § 13 Abs. 1 Nr. 1 StVZO zusätzlich aufgenommen:

m) die Erteilung der Fahrerlaubnis nach vorangegangener Versagung oder Entziehung,

n) die Erteilung der Fahrerlaubnis nach vorangegangener Versagung oder Rücknahme oder nach vorangegangenem Widerruf,

o) die Erlaubnis, von einem ausländischen Fahrausweis wieder Gebrauch zu machen, nachdem die Aberkennung nach § 11 Abs. 1 der Verordnung über internationalen Kraftfahrzeugverkehr ausgesprochen war.

Der Unterausschuß des Rechtsausschusses des Bundesrates hatte bei der Prüfung der Rechtsgrundlage zwar erkannt, daß § 28 Nr. 4 und 5 StVG nicht die Eintragung der *Erteilung* von Erlaubnissen, sondern nur die Eintragung der *Versagung* und *Entziehung* regelt, meinte aber unter dem Gesichtspunkt der Praktikabilität, die vorgesehene Regelung sei nicht zu beanstanden. Daraufhin hat der Bundesrat der entsprechenden Änderung der StVZO in seiner Sitzung am 4. Mai 1973 nicht widersprochen. Ich habe den Bundesminister für Verkehr darauf hingewiesen, daß § 28 StVG die Eintragungstatbestände abschließend festlegt. Den oben erwähnten Eintragungstatbeständen fehlt somit die gesetzliche Ermächtigungsgrundlage; die aufgrund dieser Vorschrift durchgeführte Verarbeitung personenbezogener Daten verletzt § 3 BDSG. Ich habe die vom Kraftfahrt-Bundesamt praktizierte Speicherung und Auskunftserteilung daher gemäß § 20 Abs. 1 BDSG beanstandet.

Der Bundesminister für Verkehr beruft sich dagegen auf den Unterausschuß des Rechtsausschusses des Bundesrates und lehnt es ab, dem Kraftfahrt-Bundesamt die Anwendung der obigen Vorschrift zu untersagen. Auch mein Hinweis, daß die vom Bundesrat im Jahre 1973 gezogene Schlußfolgerung vor Inkrafttreten des Bundesdatenschutzgesetzes und vor dem Volkszählungsurteil des Bundesverfassungsgerichts vielleicht verständlich war, einer Prüfung unter dem Gesichtspunkt der Normenklarheit nach den heutigen Maßstäben aber nicht standhalte, vermochte den Bundesminister für Verkehr nicht zur Änderung seines Standpunktes zu bewegen. Er ist vielmehr der Auffassung, daß eine Regelung in diesem Bereich dem vorgesehenen Verkehrszentralregistergesetz vorbehalten bleibe. Da ein entsprechender Gesetzentwurf noch nicht vorliegt (s. Nr. 9.4.6), die Herstellung eines gesetzmäßigen Zustandes jedoch geboten ist, sollte meiner Meinung nach § 13 Abs. 1 Nr. 1 Buchst. m bis o bei der nächsten Änderung der StVZO gestrichen und das KBA bereits jetzt angewiesen werden, bei Wiedererteilung von Fahrerlaubnissen die bisherigen Eintragungen zu löschen sowie die vorhandenen Bestände in diesem Sinne zu berichtigen.

9.4.3 Eintragung von Versagungsentscheidungen

Im Hinblick auf die Entscheidung des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 hatte ich den Bundesminister für Verkehr um Prüfung gebeten, ob es sachlich erforderlich und angemessen ist, Versagungen von Fahrerlaubnissen in *allen* Fällen in das Register einzutragen. Ich kann z. B. nicht erkennen, daß die Tatsache einer oder mehrerer nicht bestandener Prüfungen für spätere Verwaltungsentscheidungen relevant sein soll. Ich halte die Auffassung des Bundesministers für Verkehr, daß in der Tatsache mehrfach nicht bestandener Prüfungen die Ungeeignetheit des Bewerbers zum Führen von Kraftfahrzeugen zum Ausdruck komme, in dieser allgemeinen Aussage nicht für haltbar. Meiner Meinung nach muß einem Bewerber — ohne Rücksicht auf bisher ergangene Entscheidungen — die Möglichkeit eingeräumt werden, eine positive Entscheidung zu erreichen. Dieses wird aber durch die Eintragung nicht bestandener Prüfungen zumindest erschwert. Eine Eintragung ist meiner Meinung nach nur dann gerechtfertigt, wenn eine Versagung auf körperlichen oder geistigen Mängeln beruht. § 28 StVG ermächtigt zum Erlaß von Vorschriften über die Erfassung „*von* Versagungen (und) ... Entziehungen" und verlangt nicht die Erfassung *aller* diesbezüglichen Entscheidungen.

Der Bundesminister für Verkehr ist nur bereit, diese Frage im Rahmen des vorgesehenen Verkehrszentralregistergesetzes (s. Nr. 9.4.6) aufzugreifen. Ich halte dagegen eine entsprechende Klarstellung bei der nächsten Änderung der StVZO für geboten. Meiner Meinung nach muß der Verordnungsgeber handeln, sobald Schwachstellen erkannt sind, die die Grundsätze der Erforderlichkeit und Angemessenheit zu Lasten des Bürgers tangieren.

9.4.4 Entziehung von Sonderfahrerlaubnissen

Die Praxis der Sonderfahrerlaubnisbehörden bei der Mitteilung von Entscheidungen über die Entziehung von Sonderfahrerlaubnissen an das Verkehrszentralregister und die örtlichen Straßenverkehrsbehörden (5. TB S. 41) ist mit dem Bundesminister für Verkehr und den fachlich zuständigen Bundesministerien erörtert worden. Im allgemeinen werden Sonderfahrerlaubnisse nur entzogen, wenn allgemeine verkehrsrechtliche Gründe (z. B. mangelhafte körperliche oder geistige Eignung — § 4 StVG, § 15 b StVZO —) dies erfordern. Lediglich die Behörden der Bundeswehr entziehen Sonderfahrerlaubnisse auch dann, wenn charakterliche Mängel aufgrund dienstlicher Verfehlungen vorliegen. Sie teilen die Entziehung auch in diesen Fällen dem Kraftfahrt-Bundesamt und den örtlichen Straßenverkehrsbehörden mit. Der Bundesminister der Verteidigung hat Prüfung zugesagt, inwieweit sich die Bundeswehr an die Praxis der übrigen Sonderverwaltungen anschließen kann, in diesen Fällen die Sonderfahrerlaubnisse lediglich nach § 14 Abs. 2 StVZO einzuziehen. Über diese Entscheidung wird anderen Stellen nichts mitgeteilt.

Der Bundesminister für Verkehr hat mich inzwischen wissen lassen, daß er entsprechend meiner Forderung beabsichtigt, die Datenübermittlung zwischen Sonder- und allgemeinen Fahrerlaubnisbehörden durch Änderung der StVZO zu regeln. Ein entsprechender Entwurf liegt mir jedoch noch nicht vor.

9.4.5 Vorlage eines Auszugs aus dem Verkehrszentralregister bei Anrechnung der Schadensfreiheit aus Verträgen Dritter

Nach Nr. 28 des Tarifs in der Kraftfahrtversicherung (Stand: 1. Januar 1984) können Versicherungsunternehmen für die Anrechnung der Schadensfreiheit aus Verträgen Dritter den Nachweis verlangen, daß weder ein Fahrverbot noch ein Stand von mehr als neun Punkten im Verkehrszentralregister eingetragen sind.

Aufgrund einer Eingabe bin ich darauf aufmerksam geworden, daß ein Versicherungsunternehmen zur Übertragung des Anspruchs des bisherigen Versicherungsnehmers dem neuen Versicherungsnehmer auf dem Antragsvordruck die Erklärung abverlangt, daß nach Aufforderung des Versicherungsunternehmens ein Auszug aus dem Verkehrszentralregister nachgereicht wird.

Der Inhalt dieser Erklärung geht nach meiner Auffassung über das hinaus, was tariflich als Nachweis erforderlich ist. Während die entsprechende Regelung des Tarifs lediglich eine Bestätigung des Vorliegens der beiden Bedingungen vorsieht, versteht man unter Zusendung eines „Auszugs aus dem Register" die Bekanntgabe des gesamten Registerinhalts. Die Übergabe dieser Unterlagen an den Versicherer ist datenschutzrechtlich außerordentlich bedenklich, weil damit Registerauszüge (indirekt) an Stellen übermittelt werden, die nach der abschließenden Verwertungsregelung für Eintragungen in das Verkehrszentralregister nicht empfangsberechtigt sind (§ 30 StVG). Eine Rückfrage beim Bundesaufsichtsamt für das Versicherungswesen ergab, daß dieses Verfahren von sämtlichen Versicherungsunternehmen praktiziert wird, dieses dort bekannt war und kein Anlaß gesehen wurde, hiergegen einzuschreiten.

In Verhandlungen mit dem Bundesminister für Verkehr habe ich erreicht, daß das Kraftfahrt-Bundesamt in Zukunft keine Registerauszüge mehr erteilt, sondern lediglich Negativatteste des Inhalts, daß weder ein Fahrverbot eingetragen noch ein Stand von mehr als neun Punkten erreicht ist. Der Bundesminister für Wirtschaft hat sich meiner Rechtsauffassung angeschlossen. Das Bundesaufsichtsamt für das Versicherungswesen teilte die Änderung des Verfahrens allen Versicherungsunternehmen und den Aufsichtsbehörden der Länder mit; daraufhin änderten die Versicherungsunternehmen ihre Vordrucke und verlangen vom Versicherungsnehmer nur noch ein Negativattest des obigen Inhalts.

9.4.6 Stand der Planungen zu einem VZR-Gesetz

Der Bundesminister für Verkehr hat mir mitgeteilt, daß entsprechend dem vorgelegten Verkehrssicherheitsprogramm der Bundesregierung derzeit ein Verkehrszentralregistergesetz (VZRG) vorbereitet wird. Dieses Gesetz soll alle das VZR betreffenden Vorschriften auf eine gemeinsame gesetzliche Grundlage stellen.

Die bestehenden Vorschriften sind zum Teil unklar, unvollständig und widersprüchlich, einigen fehlt die notwendige gesetzliche Grundlage. Vor allem nach dem Volkszählungsurteil des Bundesverfassungsgerichts muß ein bereichsspezifisches Gesetz geschaffen werden, das die Erhebung, Speicherung und Übermittlung unter dem Gesichtspunkt der Einschränkung des Rechts auf informationelle Selbstbestimmung zweckgebunden regelt und Verwertungsverbote für andere, nicht dem Gesetzeszweck dienende Aufgaben ausspricht. Wie notwendig dies auch aus praktischer Sicht der Betroffenen ist, zeigen die in den Abschnitten 9.4.2 und 9.4.3 dargestellten Vorgänge.

Ein weiteres Problem, das eine bereichsspezifische Regelung erfordert, stellt sich im Zusammenhang mit der Verwertung strafrechtlicher Verurteilungen, die sowohl im Bundeszentralregister als auch im Verkehrszentralregister gelöscht sind. § 50 Abs. 2 des Bundeszentralregistergesetzes (BZRG) bestimmt, daß für Verurteilungen, die auch in das Verkehrszentralregister einzutragen waren (§ 13 StVZO), das Verwertungsverbot des § 49 Abs. 1 BZRG dann nicht gilt, wenn es sich um ein Verfahren handelt, das die Erteilung oder Entziehung der Fahrerlaubnis zum Gegenstand hat. Das Bundesverwaltungsgericht hat in einem Urteil vom 17. Dezember 1976 — Az. VII C 28.74 — (BVerwGE 51, 359) u. a. festgestellt, daß die Tilgung einer Eintragung im Verkehrszentralregister ein Verwertungsverbot für den der getilgten Eintragung zugrundeliegenden Sachverhalt bewirkt. Danach dürfen Entscheidungen, die im Verkehrszentralregister eingetragen sind und der Tilgung unterliegen, dem Betroffenen nicht mehr vorgehalten und nicht mehr zu seinem Nachteil verwertet werden. In der Praxis wird jedoch — wie eine Umfrage bei den Landesbeauftragten für den Datenschutz ergab — nicht immer so verfahren. Einige Länder halten in Verfahren über die Erteilung oder Entziehung einer Fahrerlaubnis den Betroffenen strafrechtliche Verurteilungen ohne Rücksicht auf deren Tilgung vor, andere nur solche, die nicht älter als zehn Jahre sind; einige Länder haben ihre nachgeordneten Behörden angewiesen, Entscheidungen nicht mehr gegenüber den Betroffenen zu verwerten, wenn sie der Tilgung unterliegen.

Ich habe den Bundesminister für Verkehr auf diese fortdauernde Ungleichbehandlung der betroffenen Bürger hingewiesen, und für den Fall, daß ein Zeitpunkt für die Beendigung dieses Zustandes durch neue gesetzliche Regelungen nicht absehbar ist, gefordert, daß der Bund die Initiative ergreifen sollte, um vorab eine einheitliche Regelung zu erreichen, die dem heutigen Datenschutzverständnis entspricht.

Der Bundesminister für Verkehr teilte mir nunmehr mit, daß die Mehrzahl der Bundesländer nicht bereit sei, auf eine solche, durch das Gesetz ausdrücklich für zulässig erklärte Verwertung grundsätzlich zu verzichten, auch wenn die Fälle mengenmäßig keine Rolle spielten. Ich habe schließlich den Bundesminister für Verkehr dazu bewegen können, mit dem Bundesminister der Justiz die Möglichkeit einer Übergangsregelung zu prüfen.

Inwieweit die vom Bundesrat und vom Deutschen Bundestag geforderte Prüfung einer Verknüpfung von BZR und VZR dazu führt, daß die Arbeiten an dem Entwurf eines Verkehrszentralregistergesetzes verzögert werden, vermag ich nicht zu übersehen; eine baldige Vorlage des Gesetzes halte ich aus datenschutzrechtlicher Sicht für unabdingbar.

9.5 Angabe von Beruf und Gewerbe des Halters bei der Kfz-Zulassung

In früheren Tätigkeitsberichten (3. TB S. 35, 4. TB S. 21, 5. TB S. 39) habe ich auf die Problematik der Erhebung der Berufs- und Gewerbeangaben bei der Kfz-Zulassung hingewiesen. Diese Angaben dienen zwar nicht der Kfz-Zulassung, werden nach Mitteilung des Bundesministers für Verkehr jedoch benötigt, um bei der Inanspruchnahme von Bürgern und Unternehmen zu Sach- und Dienstleistungen nach dem Bundesleistungsgesetz (BLG) sowie dem Verkehrssicherstellungsgesetz (VSG) den Grundsätzen der Gleichbehandlung und der Verhältnismäßigkeit Rechnung tragen und Rückschlüsse auf die für Dienstleistungen erforderliche Sachkunde des Halters oder seiner Mitarbeiter ziehen zu können.

Die zwangsweise Erhebung dieser Angaben ist durch die Verordnungsermächtigung des § 6 Abs. 1 Nr. 3 des StVG, die auch Regelungen „für Zwecke der Verteidigung" zuläßt, zwar grundsätzlich gedeckt. Jedoch habe ich den Bundesminister für Verkehr bereits im Jahre 1980 darauf hingewiesen, daß eine solche Nutzung aufgrund der weiteren Bearbeitung der obigen Angaben durch das KBA überhaupt nicht möglich ist. Die Berufsangaben von Nichtselbständigen werden nämlich nur nach den vier Gruppen Beamte, Angestellte, Arbeiter, Nichterwerbspersonen/Unbekannt verschlüsselt und haben daher für die genannten Aufgaben keinerlei Informationswert. Das gleiche gilt im Grundsatz für die Verschlüsselung der Gewerbeangaben von Selbständigen, da sich der verwendete Schlüssel allein an volkswirtschaftlichen Gesichtspunkten orientiert.

Diese Art der Verarbeitung der Angaben zu Beruf und Gewerbe durch das KBA hatte ich im Jahr 1981 beanstandet, da sie für Zwecke nach dem Bundesleistungsgesetz und dem Verkehrssicherstellungsgesetz ungeeignet, damit nicht erforderlich und somit datenschutzrechtlich unzulässig ist.

Daraufhin hatte der Bundesminister für Verkehr noch im Jahre 1981 angekündigt, die Gliederung und Verschlüsselung der Berufs- und Gewerbeangaben unter Berücksichtigung der Nutzung für die obigen Zwecke zu überprüfen und gegebenenfalls zu verfeinern.

Trotz wiederholter Erinnerungen liegt mir noch immer kein Vorschlag vor, der meinen Bedenken Rechnung trägt. Unter Bezug auf das Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 habe ich dem Bundesminister für Verkehr mitgeteilt, daß es für eine Weiterführung der bisherigen Praxis, auch übergangsweise, keinerlei Rechtfertigung mehr gibt. Insbesondere ist mir das vom Bundesminister für Verkehr im Juni 1984 vorgetragene Argument unverständlich, der Informationsfluß dürfe „bis zu einer in Kürze eventuell schon bevorstehenden Neuregelung" nicht unterbrochen werden, weil sonst die Erfüllung der Aufgaben nach dem BLG und dem VSG Schaden leiden könne. Denn ein Informationsfluß zur Erfüllung dieser gesetzlichen Aufgaben hat — jedenfalls soweit es um Personenkraftwagen geht — noch nie stattgefunden, und es ist auch heute noch nicht absehbar, ob und wann er zustandekommen wird.

9.6 Deutsche Bundesbahn

Eine Kontrolle der technischen und organisatorischen Maßnahmen bei der Bundesbahndirektion Köln im Jahre 1982 hatte ergeben, daß die innerbehördliche Organisation den Anforderungen des Datenschutzes nicht gerecht wurde. Aufgrund meiner Beanstandung gemäß § 20 BDSG wurde im Jahre 1983 sowohl die Datenschutzorganisation der Deutschen Bundesbahn geändert (Allgemeine Verwaltungsvorschrift des Vorstandes der Deutschen Bundesbahn gemäß § 16 BDSG), als auch die innerbetriebliche Organisation der automatischen Verarbeitung personenbezogener Daten durch eine entsprechende Dienstanweisung neu geregelt, so daß meine Beanstandung insoweit ausgeräumt ist. Das Ergebnis dieser Prüfung hat mich darin bestärkt, bei der Deutschen Bundesbahn auch die Einhaltung der materiell-rechtlichen Datenschutzvorschriften zu kontrollieren. Eine bereits für 1983 vorgesehene Prüfung war aus Kapazitätsgründen jedoch auch im Jahre 1984 nicht möglich.

9.6.1 Einsatz von Bildschirmgeräten bei der Fahrkartenausgabe

Aufgrund mehrerer Eingaben wurde ich darauf aufmerksam gemacht, daß beim Einsatz von Bildschirmgeräten bei der Ausgabe bestimmter Fahrausweise, z. B. Bezirkskarten und Seniorenpässe, eingegebene personenbezogene Daten (Name und Anschrift) von anderen Kunden mitgelesen werden können; dadurch wurden personenbezogene Daten Unbefugten gegenüber offenbart. Ich habe die Deutsche Bundesbahn auf diesen Mißstand erstmals im Jahre 1982 hingewiesen. Daraufhin hatte die Deutsche Bundesbahn ihr Personal angewiesen, den Bildschirm *auf Wunsch* des Kunden so zu drehen, daß Unbefugte Namen und Anschrift nicht lesen können. Inzwischen habe ich erreichen können, daß der Bildschirm bei der Eingabe personenbezogener Daten *stets* abgedreht oder das Bild mit Hilfe der Kontraststeuerung so abgedunkelt wird, daß ein Mitlesen nicht mehr möglich ist.

9.6.2 Einzug von Forderungen

Durch eine Eingabe habe ich erfahren, daß die Deutsche Bundesbahn Forderungen, die rechtskräftig feststehen, durch Inkassobüros einziehen läßt. Gegen eine solche Abwicklung bestehen vom Grundsatz her keine datenschutzrechtlichen Bedenken. Die Art und Weise der Informationsverarbeitung durch ein bestimmtes Inkassobüro verletzte jedoch schutzwürdige Belange. Die beauftrage Firma verwertet die ihr übergebenen Informationen nicht nur für den Forderungseinzug, sondern auch für die Erteilung von Wirtschaftsauskünften. Mit dem Hinweis auf diese Auskunftstätigkeit setzt sie den Schuldner gezielt unter Druck. In ihrem Anschreiben an den Schuldner heißt es: „Wir

sind die bedeutendste Kreditschutz-Organisation in Europa und ein ungewöhnlich erfolgreiches Inkassoinstitut. Unter anderem erteilen wir auch täglich mehrere tausend Kreditauskünfte über Firmen und Personen. Wie Sie diese alte Schuld jetzt erledigen, wird sich auch auf Ihre Beurteilung bei der Erteilung von Auskünften auswirken." Andere Firmen verfahren ähnlich und werben sogar in Anzeigen mit der Wirksamkeit dieses Druckmittels.

Die Praxis, die erhaltenen Informationen für ganz andere Zwecke zu verwerten, ist mit dem Datenschutz nicht vereinbar. Auch die Drohung mit einer zweckfremden, in dieser Form unzulässigen Datenverwertung, verletzt den Datenschutz.

Ich habe daher die Deutsche Bundesbahn aufgefordert, ihren Auftragnehmer zur ausschließlich zweckgebundenen Verarbeitung der Daten anzuhalten. Die Deutsche Bundesbahn trifft eine datenschutzrechtliche Mitverantwortung für den ordnungsgemäßen Datenumgang, denn sie hat es in der Hand, durch Auswahl eines geeigneten Inkassobüros eine zweckwidrige Datennutzung zu unterbinden. Die Deutsche Bundesbahn hat inzwischen von der Firma die Zusicherung erhalten, die für das Inkasso erhaltenen Daten ausschließlich in diesem Zusammenhang zu nutzen; auch der Text des Anschreibens wird korrigiert.

Der Fall weist im übrigen auf eine grundsätzliche Schwäche der Datenschutzbestimmungen hin: Das Bundesdatenschutzgesetz sieht zwar für jede Speicherung oder Übermittlung von Daten eine Zulässigkeitsprüfung vor; die zweckfremde Nutzung und die Zweckänderung sind dagegen im Gesetz nicht erwähnt, obwohl sie sich für den Betroffenen regelmäßig genauso wie eine unzulässige Übermittlung auswirken. Solange es an einer entsprechenden Regelung fehlt, dürften die Aufsichtsbehörden der Länder auf erhebliche Widerstände stoßen, wenn sie eine Zweckbindung bei der Datenverarbeitung erreichen wollen.

Der Vorgang zeigt weiterhin, daß die Verantwortung für den Datenschutz nicht am Dateibezug enden sollte. Im vorliegenden Fall findet bei der Deutschen Bundesbahn keine Datenverarbeitung nach § 1 Abs. 2 BDSG statt, weil die persönlichen Angaben über die Schuldverhältnisse in Akten aufbewahrt werden. Eine dateimäßige Datenverarbeitung erfolgt erst beim Inkasso-Unternehmen. Die Regelung des § 8 Abs. 1 BDSG, nach der die Datenverarbeitung eines Beauftragten dem Auftraggeber zuzurechnen ist, greift hier nicht ein, weil sich das Auftragsverhältnis nicht auf die technische Abwicklung beschränkt. Diese Auffassung des Begriffs der Auftragsdatenverarbeitung ist zwar nach Wortlaut und Zweck der gesetzlichen Regelung nicht zwingend, wird aber von den Aufsichtsbehörden der Länder überwiegend zugrundegelegt.

Eine BDSG-Novelle, die die Erhebung einbezieht und sich von der Beschränkung auf die dateimäßige Verarbeitung löst, könnte der datenschutzrechtlichen Mitverantwortung beider Beteiligten besser Rechnung tragen.

9.6.3 Schwarzfahrerdatei

Die Deutsche Bundesbahn erfaßt im Verbundverkehr bei den sogenannten „S-Bahn-Gruppen" oder „Verbundgruppen" die Daten von solchen Schwarzfahrern, die das erhöhte Beförderungsentgelt nicht unmittelbar beim Fahrausweisprüfer bezahlt haben. Die erhobenen Daten werden manuell erfaßt; zentrale Dateien der Verbünde existieren nach Auskunft der Deutschen Bundesbahn noch nicht.

Der Schwerpunkt meiner Prüfung auf diesem Gebiet betraf bisher die Zulässigkeit der Erhebung personenbezogener Daten (s. auch 3. TB S. 38). In letzter Zeit bin ich jedoch verstärkt um Beratung dahin gehend gebeten worden, ob die Errichtung zentraler Schwarzfahrerdateien, ferner ob und in welchem Umfang ein Datenaustausch über Schwarzfahrer zwischen einzelnen Verkehrsunternehmen bzw. zwischen Verkehrsunternehmen und Verkehrsverbünden aus der Sicht des Datenschutzes unbedenklich seien. Derartige Überlegungen wurden nach Angaben der Deutschen Bundesbahn bisher in den Verkehrs- und Tarifverbünden Frankfurt, Hamburg, München, Stuttgart und beim Verkehrsverbund Rhein-Ruhr angestellt.

Die Erhebung, Speicherung und Übermittlung von personenbezogenen Daten im Rahmen der Errichtung dieser Dateien berühren vornehmlich die Zuständigkeiten der Landesbeauftragten für den Datenschutz als zuständige Kontrollbehörde für die kommunalen Eigenbetriebe und die obersten Datenschutzaufsichtsbehörden bezüglich der nichtöffentlichen Unternehmen. Wegen der grundsätzlichen Bedeutung habe ich die Angelegenheit am Beispiel der vom Verkehrsverbund Rhein-Ruhr GmbH in Erwägung gezogenen Zentralisierung der bei den einzelnen Verbundunternehmen bestehenden Dateien mit Vertretern der nordrhein-westfälischen Datenschutzstellen erörtert. Dabei sind u. a. folgende Grundsätze erarbeitet worden, die ich der Deutschen Bundesbahn zur Kenntnis gegeben habe:

— Nach § 24 Abs. 1 BDSG — 2. Alternative — ist die Datenübermittlung zulässig, soweit sie zur Wahrung berechtigter Interessen der übermittelnden Stelle oder eines Dritten oder der Allgemeinheit erforderlich ist und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden.

  Ein solches Interesse sowohl der einzelnen Verbundunternehmen als auch des Verkehrsverbundes kann angenommen werden, da der Schwarzfahrer durch sein Verhalten die Gesamteinnahmen des Verkehrsverbundes schmälert, wodurch auch der Einnahmen-Anteil, der auf das einzelne Verbundunternehmen entfällt, verringert wird.

  Durch die Datenübermittlung werden Belange des Betroffenen (hier des Schwarzfahrers) beeinträchtigt, weil dadurch die Tatsache der Schwarzfahrt nicht nur dem feststellenden Unternehmen, sondern auch dem Verbund und eventuell den weiteren angeschlossenen Unternehmen bekannt wird. Die in § 24 Abs. 1 BDSG

vorgegebene Abwägung zwischen den berechtigten Interessen einerseits und den schutzwürdigen Belangen des Betroffenen andererseits führt zu der Entscheidung, daß das berechtigte Interesse höherrangig zu bewerten ist, da das Erschleichen einer Beförderung mit einem Verkehrsmittel, das eine Straftat gemäß § 265a StGB darstellen kann, als vertragswidriges bzw. treuwidriges Verhalten anzusehen ist.

— Eine Übermittlung der Daten von Schwarzfahrern sowohl zwischen den einzelnen Verbundunternehmen als auch von den Verbundunternehmen zu dem Verkehrsverbund kann demnach grundsätzlich als zulässig angesehen werden. Bei der Prüfung der Frage, ob sie im Einzelfall unbedenklich ist, kommt es wesentlich darauf an, welcher Personenkreis und welche Daten erfaßt und wie die Zugriffs- und Übermittlungsverfahren geregelt sind. Dabei ist das vom Bundesverfassungsgericht in seinem Urteil zum Volkszählungsgesetz 1983 bekräftigte Verbot der Datenerhebung auf Vorrat zu beachten.

— Eine Übermittlung personenbezogener Daten ist nur im Einzelfall auf Anfrage zulässig. Dies gilt sowohl für die Übermittlung durch den Verkehrsverbund an ein Verbundunternehmen als auch für die Datenübermittlung zwischen Verbundunternehmen. Eine Übermittlung von Gesamtübersichten in bestimmten Zeitabständen an sämtliche Verbundunternehmen ist unzulässig.

— Das Verfahren ist dem Fahrgast transparent zu machen, z. B. durch einen entsprechenden Hinweis in den Beförderungsbedingungen.

— Die Dauer der Speicherung ist auf 18 bis höchstens 24 Monate zu beschränken, wenn nicht vor Ablauf dieses Zeitraums ein Wiederholungsfall eingetreten ist.

9.7 Luftverkehrsverwaltung

Bei der Kontrolle des Luftfahrt-Bundesamtes (LBA) in Braunschweig haben sich zahlreiche Schwachstellen, Mängel und Datenschutzverstöße gezeigt, so daß ich mehrere Beanstandungen aussprechen mußte, eine auch unmittelbar gegen den Bundesminister für Verkehr im Hinblick auf die ihm obliegende Verpflichtung nach §§ 15, 16 BDSG, den Datenschutz in seinem Geschäftsbereich sicherzustellen.

a) Fehlende Rechtsgrundlage

Für eine Reihe von Datenverarbeitungsvorgängen fehlt es an der erforderlichen Rechtsgrundlage, beispielsweise für die Datensammlungen über Luftfahrer, für die Erhebung und Übermittlung im Bereich der Flugunfalluntersuchung und für die Veröffentlichung der Luftfahrzeugrolle.

Die Angaben für diese Datenbestände werden zum Teil vom Betroffenen mit Auskunftsverpflichtung erhoben. Nach den vom Bundesverfassungsgericht im Volkszählungsurteil aufgestellten Maßstäben für Einschränkungen des Rechts auf informationelle Selbstbestimmung setzt ein Zwang zur Angabe personenbezogener Daten voraus, daß der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt. Eine pauschale gesetzliche Aufgabenzuweisung genügt dazu nicht, ebensowenig Dienstanweisungen. Der Bundesminister für Verkehr hat den gesetzlichen Regelungsbedarf anerkannt und um meine Beratung bei der Erarbeitung der erforderlichen Rechtsgrundlagen gebeten.

Der gravierendste Verstoß gegen den Datenschutz lag beim Umgang mit Daten aus Flugunfalluntersuchungen. Die vollständigen Unterlagen wurden bisher jedem, der ein berechtigtes Interesse glaubhaft machen konnte, zur Verfügung gestellt, z. B. Unfallbeteiligten, Rechtsanwälten, Versicherungen sowie Justiz- und Verwaltungsbehörden.

Die Sensibilität der Unterlagen ergibt sich daraus, daß der Vorgang je nach Ursachen und Folgen des Unfallgeschehens neben den technischen Angaben zum Fluggerät und zur Flugbewegung Berichte von Polizei und Fachinstituten, medizinische Gutachten, Tonbandaufzeichnungen aus dem Cockpit, Vernehmungsprotokolle, Aussagen von Beteiligten, Photos (mit teilweise sehr sensiblen Detaildarstellungen), Gutachten, Stellungnahmen etc. enthält.

Gegen die Verbreitung dieser Unterlagen bestehen vielfältige datenschutzrechtliche Bedenken:

— Angaben aus ärztlichen Befunden gelangen in unbefugte Hände.

— Dritte erhalten unbefugt Einblick in die persönlichen Verhältnisse der verschiedenen Betroffenen.

— Im Regelfall ist es nicht erforderlich, die gesamte Unterlage zu versenden.

— Es besteht die Gefahr des unbefugten Kopierens, Verfälschens oder Vernichtens der Original-Unterlagen.

Obwohl dem Luftfahrt-Bundesamt wie auch dem Bundesverkehrsministerium die datenschutzrechtlichen Bedenken bekannt waren, wurden keine Konsequenzen daraus gezogen. Erst mein Prüfungsbericht veranlaßte das Ministerium, die Versendung der Unterlagen grundsätzlich zu stoppen.

b) Technische und organisatorische Mängel

Beim Luftfahrt-Bundesamt bestanden fast keine Maßnahmen zum Datenschutz gemäß §§ 6, 15 Satz 2 Nr. 1 und Nr. 2 BDSG. Soweit Vorkehrungen getroffen waren, verliefen sie unkoordiniert und waren deshalb praktisch wirkungslos. Dabei hatte das Bundeskriminalamt das Luftfahrt-Bundesamt als sicherheitsempfindlichen Bereich eingestuft und zu besonderen Sicherheitsvorkehrungen aufgefordert.

Weitere Versäumnisse zeigten sich bei der Überprüfung von Vordrucken: Es wurden Daten erhoben, ohne daß es dafür eine Rechtsgrundlage gab; der nach § 9 Abs. 2 BDSG erforderliche Hinweis auf die

Rechtsgrundlage in Erhebungsformularen fehlte; Angaben, für die die gesetzliche Auskunftspflicht entfallen war, wurden gleichwohl weiter erhoben, und zwar ohne den dann gebotenen Hinweis auf die Freiwilligkeit der Beantwortung (§ 9 Abs. 2 BDSG).

Außerdem habe ich kritisiert, daß Daten, die für die Aufgabenerfüllung nicht mehr benötigt werden, weder gesperrt noch gelöscht wurden, obwohl vergleichbare Angaben beim Verkehrszentralregister und beim Bundeszentralregister Tilgungsfristen unterliegen.

Ich habe die verantwortlichen Stellen darauf hingewiesen, daß ein Großteil der Mängel hätte erkannt und behoben werden können, wenn der Datenschutz in den Verwaltungsablauf organisatorisch eingebunden gewesen wäre (Nr. 10 der Anlage zu § 6 BDSG).

10. Archivwesen

Bei der Vorbereitung des Entwurfes für ein Bundesarchivgesetz habe ich den Bundesminister des Innern intensiv beraten (vgl. 5. TB Nr. 2.9). Meine Vorschläge wurden weitgehend berücksichtigt.

Der jetzt vorliegende Regierungsentwurf (BR-Drucksache 371/84) stellt im wesentlichen sicher, daß Unterlagen von Stellen des Bundes nur unter Wahrung des Datenschutzes archiviert und im Bundesarchiv genutzt werden. Die Grundidee der Regelung besteht darin, daß archivwürdige Unterlagen auch unter Abweichung von allgemeinen Datenschutzregelungen weiter aufbewahrt werden, ihre Nutzung aber erst nach Ablauf von Sperrfristen zugelassen wird, deren Dauer sich nach der Art und Empfindlichkeit der Informationen richtet.

Einige meiner Hinweise wurden allerdings nicht berücksichtigt:

— Ich hatte vorgeschlagen, alle speziellen Geheimhaltungspflichten, die durch die Pflicht zur Übergabe an das Bundesarchiv durchbrochen werden sollen, im Gesetz aufzuzählen und die Notwendigkeit der Durchbrechung im einzelnen zu begründen, insbesondere soweit Vertrauensverhältnisse (z. B. zwischen Arzt und Patient) tangiert werden. Die Bundesregierung hält es aber für wichtiger, das Gesetz so offen zu gestalten, daß auch künftig neu begründete Geheimhaltungspflichten zugunsten der Archivierung durchbrochen werden können. Auch dies ist aber hinnehmbar, weil die Übergabe an das Archiv nur unter der Bedingung zugelassen wird, daß schutzwürdige Belange Betroffener nicht beeinträchtigt werden. Der zur Geheimhaltung Verpflichtete hat also in jedem Einzelfall eine Interessenabwägung vorzunehmen.

  Allerdings ist die genannte Bedingung im Entwurf unglücklich formuliert, nämlich dahin gehend (§ 2 Abs. 3 Satz 1 letzter Halbsatz des Gesetzentwurfes), daß schutzwürdige Belange Betroffener „angemessen berücksichtigt" werden. Ich habe darauf hingewiesen, daß diese — im Gesetzentwurf mehrfach verwandte — Formulierung irreführend ist, da die Belange Betroffener ohnehin nur berücksichtigt werden, wenn sie „schutzwürdig" sind, was bereits eine abwägende Bewertung impliziert. Eine weitere Relativierung durch das Merkmal „angemessen" wäre sachlich verfehlt und ist von den Verfassern des Entwurfs wohl auch gar nicht gewollt.

— Unterblieben ist eine Klarstellung, daß die Pflicht der abgebenden Stellen, die Sicherheit der Bundesrepublik Deutschland und der Länder zu wahren, der Übergabe von Unterlagen an das Bundesarchiv dann nicht entgegensteht, wenn zu ihrer Erfüllung die Kenntnis der in den Unterlagen enthaltenen Informationen nicht mehr erforderlich ist, und daß Sicherheit und Geheimhaltung dann gegebenenfalls durch das Bundesarchiv zu gewährleisten sind. Ohne eine solche Klarstellung besteht die Gefahr, daß eine datenschutzrechtlich gebotene Löschung unter Berufung auf die Anbietungspflicht nach dem Bundesarchivgesetz unterlassen und gleichzeitig die Übergabe der Unterlagen an das Bundesarchiv unter Hinweis auf Sicherheitsbelange verweigert wird.

Die Stellungnahme des Bundesrates zu dem Gesetzentwurf (BR-Drucksache 371/84 — Beschluß —) enthält Vorschläge, die eine Einschränkung der Rechte des Betroffenen zur Folge haben. Dagegen habe ich Bedenken erhoben und die Bundesregierung insbesondere gebeten, an dem Grundsatz festzuhalten, daß der Betroffene immer dann ein Auskunftsrecht haben muß, wenn ihn betreffende Unterlagen der Benutzung durch Dritte offenstehen.

11. Statistik

11.1 Mikrozensus 1984 und EG-Arbeitskräftestichprobe 1984

Auf Wunsch des Innenausschusses des Deutschen Bundestages hatte ich zu der Frage Stellung zu nehmen, ob der Mikrozensus und die EG-Arbeitskräftestichprobe auf der Grundlage der bestehenden Rechtsvorschriften durchgeführt werden können oder ob nicht zunächst neue Bestimmungen geschaffen werden müssen, die den Anforderungen aus dem Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 vollständig entsprechen.

Für den Mikrozensus habe ich daraufhin u. a. vorgeschlagen, vor Durchführung der Zählung die vom Bundesverfassungsgericht geforderten organisatorischen Regelungen zum Schutze der Betroffenen in das Mikrozensusgesetz aufzunehmen und die vorgesehenen Erhebungsmerkmale im Gesetz zu präzisieren.

Auf Empfehlung des Innenausschusses des Deutschen Bundestages hat die Bundesregierung daraufhin den Vollzug des Mikrozensusgesetzes für das Jahr 1984 ausgesetzt und eine Neufassung des Mikrozensusgesetzes in Angriff genommen (vgl. dazu unten Nr. 11.2.2).

Für die EG-Arbeitskräftestichprobe hatte ich empfohlen, vor der Erhebung die zugrundeliegende EG-Verordnung durch deutsche Rechtsvorschriften zu ergänzen, um auch für diese Statistik rechtzeitig die notwendigen gesetzlichen Schutzvorkehrungen zu treffen. Der Innenausschuß des Deutschen Bundestages konnte sich jedoch nicht dazu entschließen, eine Hinausschiebung auch dieser statistischen Erhebung zu empfehlen. Sie wurde durchgeführt, obwohl die zugrundeliegenden Rechtsvorschriften den Anforderungen des Bundesverfassungsgerichtsurteils zum Volkszählungsgesetz 1983 nicht entsprachen. Zur Begründung hatte die Bundesregierung angegeben, ein Verschieben gerade dieser Erhebung verletze überwiegende Allgemeininteressen; verfassungsrechtliche Mängel eines Gesetzes schlössen seinen Vollzug nicht generell aus; das Bundesverfassungsgericht habe sogar — befristet — den weiteren Vollzug von Gesetzen zugelassen, die es ausdrücklich für verfassungswidrig erklärt hat.

Ganz unabhängig von diesen Überlegungen hätte die Erhebung aber nur auf freiwilliger Grundlage, d. h. ohne Auskunftspflicht für die Betroffenen, durchgeführt werden müssen. Eine gesetzliche Grundlage für eine zwangsweise Inanspruchnahme des Bürgers fehlt. Die EG-Verordnung sieht eine Auskunftspflicht nicht vor. Sie ergibt sich auch nicht aus deutschem Recht. Denn das Bundesstatistikgesetz kann sie nicht begründen, da die spezielle Erhebung dem Gesetzgeber seinerzeit gar nicht bekannt war und auch ein deutsches Einzelstatistikgesetz nicht erlassen wurde. Diese Feststellungen gelten übrigens auch für andere durch EG-Recht angeordnete Statistiken. Auf diese Bedenken habe ich die Bundesregierung vor Beginn der Erhebung hingewiesen.

In der Zwischenzeit hat die Bundesregierung eine ergänzende Vorschrift für künftige EG-Arbeitskräftestichproben vorbereitet (vgl. Nr. 11.2.2).

11.2 Beratung der Bundesregierung bei einzelnen Gesetzesvorhaben im Bereich der Statistik

11.2.1 Entwurf eines neuen Volkszählungsgesetzes 1986

Der Bundesminister des Innern hat meine Empfehlungen, die teilweise auch auf Vorschlägen der Landesbeauftragten für den Datenschutz beruhen, weitgehend berücksichtigt.

In der Begründung zum Gesetzentwurf wurde die Notwendigkeit einer Totalerhebung mit Auskunftspflicht verdeutlicht. Zwar wäre dieser Nachweis für jedes einzelne Erhebungsmerkmal wünschenswert gewesen, doch ist auch zu berücksichtigen, daß das Bundesverfassungsgericht bei der Überprüfung des Volkszählungsgesetzes 1983 die Erhebung in dieser Form für zulässig erklärt hat und in der Zwischenzeit ein relevanter Fortschritt in der Methodenentwicklung nicht zu verzeichnen war. Im Gesetzestext wurde die Transparenz für die Betroffenen durch die genaue Beschreibung aller Erhebungsmerkmale entscheidend verbessert. Außerdem hat die Bundesregierung den Vorschlag der Datenschutzbeauftragten aufgenommen, den gesetzgebenden Körperschaften die vorgesehenen Erhebungsbögen zusammen mit dem Gesetzentwurf vorzulegen. Das Parlament kann dadurch die konkreten Auswirkungen für die Betroffenen sehr genau abschätzen und in seine Entscheidung einbeziehen.

Weiterhin wurden folgende Punkte in den Entwurf aufgenommen:

— Anforderungen an die Erhebungsstellen (mit dem Ziel der Abschottung von anderen Aufgaben der Gemeinden);

— das Verbot, als Zähler Personen einzusetzen, die in unmittelbarer Nähe der Betroffenen wohnen oder bei denen zu befürchten ist, daß sie die Erkenntnisse zu Lasten der Betroffenen nutzen könnten;

— die Konkretisierung der Rechte und Pflichten der Zähler, z. B. die Pflicht, das Statistikgeheimnis zu beachten und auch über alle anderen bei der Zählung bekanntgewordenen Angelegenheiten der Betroffenen Verschwiegenheit zu wahren, ferner das Verbot für die Zähler, fremde Wohnungen ohne Einwilligung der Bewohner zu betreten;

— die Möglichkeit für die Betroffenen, ihre Angaben statt gegenüber dem Zähler gegenüber den Erhebungsstellen zu machen (nur wenige Angaben, die der Durchführung der Zählung dienen sollen, sind gegenüber dem Zähler zu machen; ich gehe davon aus, daß diese begrenzte Auskunftspflicht gegenüber dem Zähler im Gesetzgebungsverfahren noch ebenso auf das erforderliche Maß reduziert wird, wie das in dem neuen Entwurf für ein Mikrozensusgesetz geschehen ist);

— die ausdrückliche Begrenzung von Funktion und Inhalt der Ordnungsnummern;

— die Einschränkung der Übermittlung von personenbezogenen Einzelangaben an Gemeinden (die Datenübermittlung ist nicht gestattet, wenn das statistische Landesamt die Auswertung vornehmen kann oder wenn nicht gewährleistet ist, daß die Angaben nur für statistische Zwecke in einem gesonderten statistischen Amt der Gemeinde genutzt werden);

— die Konkretisierung der Löschungsvorschriften.

Der Gesetzentwurf verzichtet außerdem

— auf die Befugnis, Straße und Hausnummer als Erhebungsmerkmale für die statistische Auswertung zu verwenden und sie im Rahmen der gesetzlichen Bestimmungen zu übermitteln und

— auf die Befugnis, personenbezogene Einzelangaben an oberste Bundes- und Landesbehörden zu übermitteln.

Bis auf ganz wenige Punkte von geringerer Bedeutung, die ich im weiteren Gesetzgebungsverfahren

noch vorbringen werde, und vorbehaltlich der erwähnten Reduzierung der Auskunftspflicht des Betroffenen gegenüber dem Zähler, schafft das Gesetz damit einen geeigneten Rahmen, um den Datenschutz bei der Volkszählung zu gewährleisten.

Es wird jetzt entscheidend darauf ankommen,

— daß der Datenschutz im Gesetzgebungsverfahren nicht wieder abgebaut wird,

— daß die Öffentlichkeit gut aufgeklärt wird,

— daß das Verfahren in den Ländern datenschutzgerecht ausgestaltet wird und

— daß Länder und Gemeinden das Projekt nicht mit Zusatzbefragungen befrachten.

11.2.2 Entwurf eines neuen Mikrozensusgesetzes

Für den (kürzlich sowohl interfraktionell als auch durch die Bundesregierung eingebrachten) Mikrozensusgesetzentwurf habe ich ähnliche Vorschläge gemacht wie für das Volkszählungsgesetz. Sie sind ebenfalls weitgehend berücksichtigt worden, so daß ich den Entwurf nunmehr als eine tragfähige Grundlage für die Gewährleistung des Datenschutzes bezeichnen kann.

Notwendig bleibt allerdings, die Bürger davon zu überzeugen, daß die Erhebungsmerkmale in der vorgesehenen Ausprägung im überwiegenden Allgemeininteresse notwendig sind und daß auf eine Auskunftspflicht vorerst nicht verzichtet werden kann; in diesem Zusammenhang ist auch eine Aufklärung darüber notwendig, wie die Auskunftspflichtigen ausgewählt werden. Zur Unterrichtung aller Beteiligten sollte auch die mir erst kürzlich zugegangene Gesetzesbegründung beitragen. Zumindest in einem Punkt erfüllt sie diesen Zweck jedoch nicht: Es wird nicht deutlich, warum es im überwiegenden Allgemeininteresse notwendig sein soll, die Höhe des Einkommens so detailliert zu erfragen, wie es im Gesetzestext vorgesehen ist.

Der Gesetzentwurf enthält auch Regelungen für künftige EG-Arbeitskräftestichproben (§ 14) und berücksichtigt damit meine Bedenken, die ich gegen die Durchführung der EG-Arbeitskräftestichprobe 1984 erhoben habe (vgl. oben Nr. 11.1).

11.2.3 Entwurf eines Hochschulstatistikgesetzes

Nach dem Hochschulstatistikgesetz vom 7. September 1971 (BGBl. I S. 1473, Neufassung vom 21. April 1980, BGBl. I S. 453) ist die Erhebung der Daten, die die Hochschulen für ihre Verwaltungszwecke benötigen, mit der statistischen Datenerhebung zu einem einheitlichen Vorgang (Verbunderhebung) zusammengefaßt. Die vom Gesetzgeber seinerzeit gewählte rechtliche Konstruktion ist allerdings ungewöhnlich. Die Hochschulangehörigen (Studenten, Prüfungskandidaten, Personal) werden ausdrücklich aufgrund ihrer statistischen Auskunftspflicht in Anspruch genommen; die Hochschulen haben lediglich ein abgeleitetes, im Hochschulstatistikgesetz verankertes Recht, die zu statistischen Zwecken erhobenen Daten für ihre Verwaltungszwecke zu benutzen.

Aus dieser Konstruktion resultieren Schwierigkeiten, auf die ich bereits in meinem Ersten Tätigkeitsbericht unter Nr. 3.3.3 (S. 17 f.) aufmerksam gemacht habe. Ich habe darauf hingewiesen, daß eine solche Durchbrechung des Grundsatzes, daß statistische Angaben nicht zu personenbezogenen Vollzugsmaßnahmen verwendet werden dürfen, das Vertrauen in die Integrität der statistischen Geheimhaltung gefährdet. Das Volkszählungsurteil des Bundesverfassungsgerichts hat diese Beurteilung bestätigt.

Ich begrüße es daher, daß der Bundesminister für Bildung und Wissenschaft eine grundlegende Änderung der Konzeption der Hochschulstatistiken beabsichtigt, durch die die bisherigen Schwierigkeiten ausgeräumt werden können. Eine Verwendung statistischer Angaben für Verwaltungszwecke ist danach nicht mehr vorgesehen. Außerdem sollen die Statistiken nur noch als Sekundärstatistik, d. h. aufgrund vorhandener Verwaltungsunterlagen und ohne zusätzliche Befragung der Betroffenen, durchgeführt werden. Lediglich für die Prüfungskandidatenstatistik ist dieser Punkt noch nicht abschließend geklärt. Schließlich soll die Studentenstatistik nicht mehr als Verlaufsstatistik angeordnet werden; gegen diese Änderung wendet sich allerdings der Wissenschaftsrat.

Während bei einer periodischen Bestandsstatistik lediglich die verschiedenen Gesamtzustände zu verschiedenen Zeitpunkten festgestellt werden, wird bei einer Verlaufsstatistik die zeitliche Entwicklung jedes betroffenen Individuums verfolgt. Die individuelle Verknüpfbarkeit mit den jeweils hinzukommenden neuen Daten bedingt eine dauerhafte personenbezogene Speicherung der Angaben, schließt also die sonst übliche frühzeitige Anonymisierung aus.

Die Verlaufsstatistik greift damit stärker in die Rechte der Auskunftspflichtigen ein. Ob allerdings insoweit ein überwiegendes Allgemeininteresse besteht, erscheint zweifelhaft. Die Notwendigkeit und auch die Eignung der Verlaufsstatistik für im überwiegenden Allgemeininteresse liegende Zwecke wurden bisher nicht überzeugend dargetan. Bedenken resultieren nicht zuletzt daraus, daß die Studentenstatistik seit Erlaß des Hochschulstatistikgesetzes im Jahre 1971 als Verlaufsstatistik vorgesehen ist, eine verlaufsstatistische Auswertung bis heute jedoch nicht stattgefunden hat.

11.2.4 Zweites Gesetz zur Änderung des Gesetzes über die Lohnstatistik

In dem Novellierungsentwurf, der die Vorschriften über die Lohnstatistiken im Bereich der Landwirtschaft betrifft, wurde auf meine Empfehlung hin

— das Erhebungsverfahren im Gesetz geregelt,

— die Normenklarheit durch eine präzisere Fassung von Erhebungsmerkmalen verbessert und

— die Dauer der Auskunftspflicht des Einzelbetriebs begrenzt.

11.3 Statistisches Bundesamt

Im Sommer dieses Jahres hat das Statistische Bundesamt an die Universität Frankfurt ein Magnetband übermittelt, das außer den angeforderten anonymen Angaben über Bundestagswahlen auch noch Daten aus früheren Verarbeitungen enthielt, die zwar wenig sensibel, aber personenbezogen waren.

Meine Untersuchung hat ergeben, daß infolge mangelhafter technischer und organisatorischer Maßnahmen weder die Weisung, Bänder mit nicht mehr benötigten personenbezogenen Daten zu löschen, noch die Weisung, für den Versand an Dritte nur gelöschte Bänder zu verwenden, befolgt worden waren.

Ich habe den Datenschutzverstoß beanstandet und an die von mir schon früher für dringlich erklärte Überarbeitung des Sicherheitskonzepts erinnert. Im Rahmen der vorgesehenen erneuten Kontrolle des Statistischen Bundesamtes werde ich überprüfen, in welcher Weise meinen Empfehlungen entsprochen worden ist.

12. Sozialwesen — Allgemeines

12.1 Sozialversicherungsnummer

In meinem Fünften Tätigkeitsbericht (S. 68) hatte ich meine Auffassung dargelegt, daß über eine Ausdehnung des Anwendungsbereichs der Rentenversicherungsnummer — über den Bereich der Rentenversicherung hinaus — allein der Gesetzgeber entscheiden dürfe. Im Verlauf der parlamentarischen Behandlung des Tätigkeitsberichts hat die Bundesregierung angekündigt, daß der Bundesminister für Arbeit und Sozialordnung eine gesetzliche Regelung beabsichtige, durch die die Anwendung der Rentenversicherungsnummer gesetzlich geregelt und zugleich auf den Bereich der sozialen Sicherung begrenzt werden solle. Die Vorschläge im einzelnen sollten mit mir abgestimmt werden (vgl. Bericht des Innenausschusses, BT-Drucksache 10/1719, S. 16, zu II. 14).

Ein erstes Gespräch über die Konzeption des Bundesministers für Arbeit und Sozialordnung zur Einführung einer allgemeinen Versichertennummer (Sozialversicherungsnummer) hat im März 1984 stattgefunden. Ich habe dabei erneut auf die Risiken einer allgemeinen, für alle Zweige der Sozialversicherung und die Arbeitslosenversicherung zu verwendenden Versichertennummer hingewiesen. Meine im Fünften Tätigkeitsbericht ausführlich begründete Ablehnung einer erweiterten Verwendung der Rentenversicherungsnummer wird auch durch das Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz gestützt. Das Gericht sieht in einer etwaigen Einführung eines einheitlichen Personenkennzeichens oder eines sonstigen Ordnungsmerkmals einen entscheidenden Schritt, den einzelnen Bürger in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren. Da in der Sozialversicherung etwa 90 Prozent der Gesamtbevölkerung mit wesentlichen Daten über ihren sozialen Status, ihr Berufsleben und ihre Gesundheit erfaßt sind, gelten diese Bedenken entsprechend für eine einheitliche Versichertennummer für die Sozialversicherung.

Vor diesem Hintergrund habe ich gegenüber dem Bundesminister für Arbeit und Sozialordnung die Auffassung vertreten, daß die verschiedenen Versicherungszweige weiterhin grundsätzlich ihr jeweiliges Ordnungsmerkmal beibehalten, die Verwendung der Rentenversicherungsnummer als Kommunikationsmittel auf die DEVO/DÜVO-Datenflüsse beschränkt und darüber hinaus nur zugelassen werden sollte, soweit es der Sache nach erforderlich ist. Die Verwendung der Rentenversicherungsnummer bzw. die Einführung der einheitlichen Versichertennummer als Ordnungsmerkmal im Bereich der gesetzlichen Unfallversicherung, namentlich beim Arbeitsmedizinischen Dienst der Bau-Berufsgenossenschaften und im Rahmen anderer arbeitsmedizinischer Untersuchungen (s. unten Nr. 16.2), sowie in der Arbeitslosenversicherung und insbesondere außerhalb der Sozialversicherung (z. B. durch den Arbeitgeber), muß aber weiterhin ausgeschlossen sein.

12.2 Ausweiskarte für Bauarbeitnehmer

Anfang des Jahres ist mir vom Bundesminister für Arbeit und Sozialordnung der Referentenentwurf eines Gesetzes zur Förderung der Beschäftigung zugegangen. Als Artikel 2 war ein Gesetz über die Ausweiskarte für Arbeitnehmer im Baugewerbe vorgesehen.

Nach der Zielsetzung dieses Gesetzes sollten durch verstärkte und mit Hilfe einer besonderen Ausweiskarte erleichterte Kontrollen der illegalen Beschäftigung von Arbeitnehmern im Baugewerbe entgegengewirkt, die Beschäftigungschancen von Arbeitssuchenden verbessert und einer Gefährdung der sozialen Sicherung der Arbeitnehmer vorgebeugt werden. Die Ausweiskarte sollte von den Krankenkassen ausgegeben und vom Arbeitgeber mit Angaben über den einzelnen Beschäftigten ausgefüllt werden. Der Arbeitnehmer sollte verpflichtet werden, bei einer Beschäftigung an einer nicht ortsfesten Arbeitsstätte den Ausweis mitzuführen und den Vertretern der zur Kontrolle ermächtigten Behörden vorzulegen. Für Kontrollzwecke sollten die persönlichen und sachlichen Angaben über die betroffenen Arbeitnehmer zusammen mit einer Seriennummer des Ausweises beim jeweiligen Arbeitgeber und bei den zuständigen Krankenkassen in besonderen Dateien gespeichert werden.

Ich habe gegen dieses Vorhaben insbesondere Bedenken im Hinblick auf die Verhältnismäßigkeit des Mittels sowie seiner Eignung zur Erreichung des erstrebten Zweckes geltend gemacht.

Im Hinblick auf meine datenschutzrechtlichen und verfassungsrechtlichen Einwände ist es zu begrüßen, daß die Bundesregierung inzwischen von diesem Vorhaben Abstand genommen hat. Der Gesetzentwurf der Bundesregierung (Beschäftigungsförderungsgesetz 1985, Bundestags-Drucks. 393/84) enthält den Vorschlag einer Ausweiskarte für Bauarbeitnehmer nicht mehr.

12.3 Stiftung „Mutter und Kind — Schutz des ungeborenen Lebens"

Im Mai dieses Jahres ist mir der Entwurf der Bundesregierung für ein Gesetz zur Errichtung einer Stiftung „Mutter und Kind — Schutz des ungeborenen Lebens" bekannt geworden. Die Stiftung ist inzwischen mit dem Inkrafttreten des Gesetzes am 14. Juli 1984 entstanden. Zweck der Stiftung ist es, bestimmten Einrichtungen in den Ländern Mittel zur Verfügung zu stellen, mit denen werdenden Müttern im Einzelfall und unter bestimmten Voraussetzungen finanzielle Hilfen gewährt werden können.

Die Gewährung solcher Hilfen setzt nach den Regelungen des Gesetzes die Angabe und Verwendung personenbezogener Daten über die persönlichen und sachlichen Verhältnisse der werdenden Mutter voraus. Diese Angaben betreffen zum Teil sehr intime und deshalb sehr sensible Bereiche. Ich hätte es deshalb für sachgerecht gehalten, wenn die Geheimhaltung der personenbezogenen Daten und der notwendige Schutz gegen unbefugte Offenbarung durch Bezugnahme auf die Vorschriften über das Sozialgeheimnis und den Schutz der Sozialdaten in diesem Gesetz verankert worden wäre. Da ich jedoch an dem Gesetzgebungsvorhaben nicht beteiligt worden bin, konnten wegen des fortgeschrittenen Stadiums des Gesetzgebungsverfahrens meine dahin gehenden Anregungen zur Gewährleistung des Datenschutzes nicht mehr berücksichtigt werden. Ein im Deutschen Bundestag eingebrachter Änderungsantrag, der diese Anregungen aufgriff, wurde mehrheitlich abgelehnt.

Ich habe deshalb anschließend darauf hingewirkt, daß die aus meiner Sicht unbedingt notwendigen Datenschutzregelungen wenigstens in die vom Stiftungsrat zu erlassenden Richtlinien über die Vergabe und Verwendung der Stiftungsmittel übernommen werden. Dies hat im Ergebnis zu akzeptablen Lösungen geführt. Leider konnte ich mich mit der mir besonders wichtig erscheinenden Forderung, für die Antragstellung und die dabei zu erhebenden Angaben die Verwendung eines einheitlichen Vordrucks vorzusehen, nicht durchsetzen. Doch nur so läßt sich nach meiner Einschätzung sicherstellen, daß von der werdenden Mutter nur die für die Hilfegewährung objektiv erforderlichen Angaben erhoben werden. Ich habe deshalb vorgeschlagen und wiederhole dies nachdrücklich, daß der Stiftungsrat sich dieser Problematik noch einmal annehmen und meinen Bedenken durch eine Änderung der Richtlinien Rechnung tragen sollte.

13. Arbeitsverwaltung

13.1 Kontrollen

Im Berichtsjahr habe ich aufgrund von Beschwerden gemäß § 21 BDSG mehrere Einzelfallkontrollen bei den Arbeitsämtern Göttingen und Berlin sowie bei der Zentralen Bühnen-, Fernsehen- und Filmvermittlung der Bundesanstalt für Arbeit in Berlin durchgeführt. Es ging dabei im wesentlichen um die Befürchtung der Betroffenen, daß ihnen wegen unzutreffender oder unzulässig gespeicherter Daten und Informationen in den Vermittlungsunterlagen kein oder kein ihren Fähigkeiten entsprechender Arbeitsplatz vermittelt werde. Bei meinen Prüfungen stellten sich diese Befürchtungen teilweise als gegenstandslos heraus. In anderen Fällen konnte ich erreichen, daß von den Betroffenen beanstandete Daten und Unterlagen berichtigt oder gelöscht bzw. entfernt wurden.

13.2 Psychologische und psychiatrische Gutachten

Die Arbeitsverwaltung bedient sich zur Feststellung der gesundheitlichen Eignung von Arbeitssuchenden für eine Vermittlung auf dem Arbeitsmarkt eines eigenen Ärztlichen Dienstes. In besonderen Fällen kann die Arbeitsverwaltung den Arbeitssuchenden mit seinem Einverständnis auch psychologisch untersuchen und begutachten (§ 14 Abs. 2 AFG). Der Ärztliche Dienst stellt darüber der Arbeitsvermittlung ein entsprechendes, mehr oder weniger ausführliches Gutachten zur Verfügung.

Mehrere Petenten wandten sich hilfesuchend an mich, weil sie sich durch die Art der Erstellung psychologischer oder psychiatrischer Gutachten durch den Ärztlichen Dienst der Arbeitsämter, sowie durch die Aufbewahrung und Verwendung dieser Gutachten in ihren Rechten beeinträchtigt sahen. Zur Verdeutlichung der Problematik möchte ich an dieser Stelle einen Fall exemplarisch darstellen.

Eine Petentin hatte sich bereits 1982 an mich gewandt, um gegenüber einem Arbeitsamt und dem Ärztlichen Dienst des zuständigen Landesarbeitsamtes Einsicht in die über sie vorliegenden Gutachten des Ärztlichen Dienstes zu erreichen. Diese wurde ihr aufgrund meines Tätigwerdens schließlich gewährt. Sie stellte fest, daß eine Reihe von Gutachten existierten, die ihr „Abartigkeit" bzw. „abartiges Verhalten" attestierten. In diesen Gutachten sah sie den hauptsächlichen Grund dafür, daß sie seit mehreren Jahren keinen Arbeitsplatz erhalten hat. Außerdem fühlte sie sich durch diese Bezeichnungen diskriminiert und forderte die Vernichtung der Gutachten, wenigstens aber eine textliche Änderung und bat mich auch insoweit um Hilfe. Die Eingabe veranlaßte mich zu einer örtlichen Prüfung bei dem betroffenen Arbeitsamt.

Die Prüfung ergab, daß bei der Vermittlungsstelle des Arbeitsamts bzw. beim Ärztlichen Dienst mehrere Gutachten vorhanden waren, die aus der Zeit von 1967 bis 1982 stammten. Ein Gutachten aus dem Jahre 1977 war ursprünglich für die Krankenkasse

der Petentin während einer akuten Erkrankung erstellt und mit ihrer Einwilligung dem Ärztlichen Dienst übermittelt worden. Die jüngeren Gutachten waren — ohne erneute Untersuchung — nach Aktenlage unter Bezugnahme auf die alten Gutachten, insbesondere auf das Gutachten von 1977, erstellt worden. Sie enthielten teilweise die von der Petentin kritisierten Formulierungen sowie die Aussage, ihr sei „eine Tätigkeit als Arbeitnehmer unter den üblichen Bedingungen des allgemeinen Arbeitsmarktes nicht möglich". Im Verlauf der Auseinandersetzungen über das Einsichtsbegehren der Betroffenen in die vorliegenden Gutachten hatte der frühere Leiter des Ärztlichen Dienstes die „teilweise über zehn Jahre alten Gutachten . . . als durch die neueren Gutachten überholt" bezeichnet, „so daß die darin enthaltenen Befunde und Stellungnahmen keinerlei Bedeutung mehr haben". Gleichwohl lehnte das Arbeitsamt die Arbeitsvermittlung der Petentin auf der Grundlage dieser Gutachten weiterhin ab. Obwohl die Petentin 1978 ein rechtskräftiges Urteil des Sozialgerichts erstritt, in dem u. a. das der Ablehnung zugrundeliegende Gutachten als „unbeachtlich, da ohne jede medizinische Begründung" bezeichnet wurde, blieben sämtliche Gutachten ohne Änderung in den Akten. Sie dienten — trotz Vorlage anderslautender privatärztlicher, im Auftrag des Gesundheitsamtes erstellter Gutachten — im Jahre 1982 als Grundlage für ein erneutes negatives Gutachten nach Aktenlage. Dies hatte die Ablehnung der Zahlung von Arbeitslosengeld zur Folge, weil danach die Betroffene angeblich aus gesundheitlichen Gründen für eine Arbeitsvermittlung nicht zur Verfügung stand. Obwohl auch diese Entscheidung durch das Sozialgericht aufgehoben wurde, haben mit der gleichen Begründung weitere Vermittlungsversuche durch das Arbeitsamt nicht stattgefunden.

Dieses Vorgehen verstößt nicht nur gegen interne datenschutzrechtlich relevante Dienstanweisungen der Bundesanstalt für Arbeit, nach denen ärztliche Gutachten nach Ablauf von drei Jahren in die Altaktei abzugeben und nach weiteren sieben Jahren zu vernichten sind, sondern auch gegen § 84 SGB X. Die teilweise über zehn Jahre alten Gutachten sind insbesondere nach den Feststellungen des Sozialgerichts als Grundlage für die Frage der Vermittlungsfähigkeit nach meiner Auffassung nicht mehr geeignet; somit ist ihre Kenntnis zur rechtmäßigen Erfüllung der Aufgaben des Arbeitsamtes nicht erforderlich. Dies betrifft nicht nur die Aufbewahrung beim Ärztlichen Dienst, sondern erst recht die Aufbewahrung und Verwendung in der Vermittlungs- bzw. Leistungsabteilung des Arbeitsamtes. Das gleiche gilt auch für die späteren Gutachten, die ohne Untersuchung nach Aktenlage erstellt wurden und deren Grundlage ausschließlich die Altgutachten waren.

Ich habe dies als Verstoß gegen Datenschutzbestimmungen nach § 20 Abs. 1 BDSG beanstandet. Die Bundesanstalt für Arbeit hat mir in ihrer Stellungnahme entgegengehalten, daß die Altgutachten nicht unter die Aufbewahrungs- und Vernichtungsfristen der internen Dienstanweisung fielen, weil sie durch die Bezugnahme jeweils Bestandteil der neuen Gutachten geworden seien. Genau diese Wirkung soll jedoch m. E. durch richtig verstandene Tilgungsfristen vermieden werden.

Die Bundesanstalt für Arbeit hat schließlich in diesem Einzelfall — ohne Anerkennung einer Rechtspflicht — den Ärztlichen Dienst angewiesen, die umstrittenen Gutachten aus den Unterlagen zu entfernen.

Auch in anderen Einzelfällen konnte im Benehmen mit der Arbeitsverwaltung eine angemessene Lösung gefunden werden. Nach Auffassung aller Beteiligten ist jedoch eine generelle Klärung notwendig. Die Bundesanstalt für Arbeit hat deshalb eine allgemeine, verbindliche Regelung bezüglich der Erstellung, Verwendung, Aufbewahrung und Vernichtung ärztlicher, insbesondere psychologischer und psychiatrischer Gutachten in Aussicht gestellt. Dabei wird es insbesondere darauf ankommen, daß die Arbeitsämter vom Ärztlichen Dienst nur die Angaben erhalten, die sie zur Erfüllung ihrer Aufgaben unverzichtbar benötigen. Deshalb sollte in allen arbeitsamtsärztlichen Gutachten künftig die Angabe von Diagnosen und Befunden unterbleiben. Statt dessen sollte ausführlicher als bisher das Leistungsbild des Betroffenen hinsichtlich der zumutbaren bzw. der zu vermeidenden Tätigkeiten beschrieben werden.

13.3 Arbeitslosenhilfe

Auch in diesem Berichtsjahr haben mir zahlreiche Bürger ihre datenschutzrechtlichen Bedenken im Zusammenhang mit dem Arbeitslosenhilfeverfahren der Arbeitsämter vorgetragen.

Der überwiegende Teil der Petenten wendet sich dagegen, daß arbeitslosen Angehörigen ihr Einkommen bekannt wird, weil der Arbeitslose ihre Verdienstbescheinigung dem Arbeitsamt vorlegen muß.

Andere Bürger befürchten Benachteiligungen, wenn ihrem Arbeitgeber bekannt wird, daß ein Angehöriger arbeitslos ist. Die vom Arbeitgeber auszufüllende Bescheinigung enthält nämlich neben dem Kopf „Bundesanstalt für Arbeit" die Überschrift „Verdienstbescheinigung (Arbeitslosenhilfe) für Angehörige des Antragstellers — vom Arbeitgeber auszufüllen".

Bereits in meinem Fünften Tätigkeitsbericht (S. 58) hatte ich das Verfahren, Einkommensbescheinigungen unterhaltspflichtiger Angehöriger über den Arbeitslosen vorzulegen, als unbefriedigend bezeichnet. In meinem Sechsten Tätigkeitsbericht (S. 31) hatte ich ausgeführt, die Bundesanstalt für Arbeit habe sich meiner eindringlichen Bitte, das Verfahren zu ändern, in ihrer Stellungnahme zu meinem Fünften Tätigkeitsbericht nach wie vor verschlossen.

Anfang April des Berichtsjahres habe ich den Präsidenten der Bundesanstalt für Arbeit in dieser Sache erneut angeschrieben. Ich habe darauf hingewiesen, daß bei der Gewährung von Ausbildungs-

hilfe nach dem Bundesausbildungsförderungsgesetz (BAFöG) ein vergleichbarer Sachverhalt vorliegt. Nach § 50 Abs. 2 BAFöG entfallen im Bewilligungsbescheid auf begründetes Verlangen eines Elternteils oder des Ehegatten die Angaben über dessen Einkommen. Die Hinweise zum Ausfüllen des Antrages enthalten dementsprechend den ausdrücklichen Hinweis, daß die Erklärung über das Einkommen auch getrennt vom Antrag des Auszubildenden dem Amt für Ausbildungsförderung unmittelbar übersandt werden kann. Nach Abstimmung mit dem Bundesministerium für Arbeit und Sozialordnung hat mir der Präsident der Bundesanstalt für Arbeit mitgeteilt, eine sinngemäße Anwendung des § 50 (2) BAFöG sei „aus Rechtsgründen nicht möglich". Um eine breitere empirische Basis für die Beurteilung künftiger Regelungen (einschließlich gesetzlicher Änderungen) zu gewinnen, sollten jedoch Erhebungen darüber angestellt werden, in welchem Umfang die Sachbearbeitung in den Leistungsabteilungen der Arbeitsämter zusätzlich belastet würde, wenn die Unterhaltsverpflichteten auf Voraussetzungen und mögliche Folgen einer unmittelbaren Übersendung hingewiesen würden. Die Arbeitsverwaltung beabsichtigt, einen entsprechenden Versuch bei 5 bis 10% der Arbeitslosenhilfe-Fälle durchzuführen.

Interessant ist in diesem Zusammenhang, daß mir ein Arbeitsamt auf meine Bitte um Stellungnahme geantwortet hat, ein Angehöriger, der seine Einkommensverhältnisse dem Arbeitslosen nicht offenbaren will, könne die Verdienstbescheinigung selbstverständlich dem Arbeitsamt direkt zuleiten. Nach dieser Einschätzung von Praktikern bin ich zuversichtlich, daß eine Änderung des Verfahrens in absehbarer Zeit möglich sein wird.

Hinsichtlich der Vorlage des Vordruckes „Verdienstbescheinigung" der Arbeitsverwaltung durch den Angehörigen bei seinem Arbeitgeber habe ich der Bundesanstalt meine Zweifel an der Erforderlichkeit der damit verbundenen Offenbarung des Sozialdatums „Arbeitslosigkeit" mitgeteilt. Die Bundesanstalt hat mir geantwortet, grundsätzlich müsse der Vordruck verwendet werden, eine Ausnahme könne nur dann gemacht werden, wenn „normale Verdienstbescheinigungen" nach Inhalt und Form dem Vordruck entsprechen.

Nach meiner Auffassung kann es hier auf die Form nicht entscheidend ankommen. Soweit Verdienstbescheinigungen vorgelegt werden, die alle für die Arbeitsverwaltung erforderlichen Angaben enthalten, sollten künftig derartige formlose Bescheinigungen akzeptiert werden.

13.4 Kindergeld

In meinem Sechsten Tätigkeitsbericht (S. 31/32) habe ich über Probleme bei der Einkommensermittlung zur Durchführung des Bundeskindergeldgesetzes berichtet.

Zum Nachweis des Einkommens im Kalenderjahr 1983 (für das Kindergeld im Jahre 1985) wurde ein neuer Fragebogen entwickelt. Dieser Fragebogen enthält nicht mehr den von verschiedenen Seiten kritisierten Hinweis gemäß § 9 Abs. 2 BDSG auf die Freiwilligkeit der Angaben. Statt dessen wurde — an auffälliger Stelle — folgender Hinweis aufgenommen:

> „Ohne Angaben und Nachweise über das Einkommen kann ab Januar 1985 kein höheres Kindergeld als der Sockelbetrag bezahlt werden. Ihre Mitwirkungspflicht ergibt sich aus § 60 SGB I. Vergleichen Sie auch Nr. 3 und Nr. 39 Abs. 1 des Merkblattes".

Zusammen mit dem Merkblatt „Kindergeld" der Bundesanstalt für Arbeit, das der Antragsteller in der Regel bei der ersten Antragstellung erhält, klärt dieser Hinweis den Betroffenen ausreichend über die Anrechnungsvorschriften und über die Bedeutung seiner Mitwirkungspflicht auf. Allerdings ist dieser Hinweis insofern mißverständlich bzw. unvollständig, als in dem Fragebogen auch Angaben über das Einkommen des Ehegatten des Kindergeldberechtigten verlangt werden; die Mitwirkungspflicht gemäß § 60 SGB I erstreckt sich jedoch nicht auf den Ehegatten.

Der Fragebogen enthält weiter die Erklärung „ich bin — wir sind — damit einverstanden, daß künftig die für das Kindergeldverfahren erforderlichen Angaben unmittelbar bei der Finanzverwaltung eingeholt werden: Ja/Nein". Auf der Rückseite des Fragebogens ist das Verfahren der „Einkommensermittlung im Wege des Datenaustausches zwischen Finanzbehörden und Kindergeldkasse" ausführlich erläutert. Aus diesen Erläuterungen ergibt sich mit der notwendigen Klarheit, daß ein maschinelles Verfahren stattfindet, daß die Einwilligung jederzeit widerruflich ist und welche Daten im einzelnen von der Finanzverwaltung mitgeteilt werden.

Diese Einwilligungserklärung ist die Grundlage für die Anwendung der zwischen den Steuerverwaltungen der Länder und der Bundesanstalt für Arbeit geschlossenen „Rahmenvereinbarung über einen Datenaustausch für die Berechnung des einkommensabhängigen Kindergeldes", die mit den Datenschutzbeauftragten des Bundes und der Länder weitgehend abgestimmt worden ist. Die Rahmenvereinbarung enthält die notwendigen Verfahrensregelungen einschließlich der Festlegung der zu verwendenden Datensätze, die Bestimmung einer strengen Zweckbindung der ausgetauschten Daten, und — entsprechend den Forderungen der Datenschutzbeauftragten — die Feststellung, daß es für die Prüfung der kindergeldrechtlichen Einkommensgrenze auf die Summe der positiven Einkünfte ankommt und daß deshalb eine Aufteilung nach einzelnen Einkunftsarten nicht vorzunehmen ist. Diese Regelung soll allerdings im Verlaufe des Jahres 1985 anhand der gewonnenen Erfahrungen im Benehmen mit den Datenschutzbeauftragten darauf überprüft werden, ob eine Erweiterung hinsichtlich der mitzuteilenden Einkünfte für solche Fälle erforderlich ist, in denen in der Summe der Einkünfte auch negative Einkünfte enthalten sind.

Das Verfahren, regelmäßig nur die Summe der positiven Einkünfte zu erheben und eine Aufteilung

nach einzelnen Einkunftsarten nicht vorzunehmen, muß grundsätzlich auch für die Fälle des manuellen Einzelnachweises außerhalb des automatisierten Datenaustausches gelten. Das Verlangen, hier stets alle Einzeleinkünfte anzugeben bzw. im Steuerbescheid lesbar zu belassen, kann aus § 60 SGB I nicht abgeleitet werden, da es insoweit an der Erforderlichkeit bzw. der „Erheblichkeit" für die Leistung mangelt. Insoweit kann es sich daher nur um freiwillige Angaben handeln; auf die Freiwilligkeit ist der Betroffene hinzuweisen, was jedoch nicht geschieht.

Die Vorschriften des § 60 SGB I i. V. m. § 11 BKGG können nicht über ihren tatsächlichen Gehalt hinaus ausgelegt werden mit der — vom BMA gegebenen — Begründung, „daß der einfache Bürger nicht fähig und nicht bereit ist, sich in die Zusammenhänge abstrakt und selbstrechnend einzuarbeiten". Dieses Argument ist zudem nicht einleuchtend. Es könnte den Anschein erwecken, daß „einfache Bürger" alle diejenigen seien, die mit dem automatisierten Datenaustausch nicht einverstanden sind; ebenso könnte das Gegenteil richtig sein. Zum anderen spricht die Wahrscheinlichkeit eher dafür, daß derjenige, der in seiner Einkommensteuererklärung negative Einkünfte geltend gemacht hat, die Zusammenhänge auch kennt. Ein erklärender Satz und ein Hinweis, daß bei Unklarheiten das Arbeitsamt *bereit* ist, aus dem vollständig vorgelegten Steuerbescheid die maßgeblichen Daten selbst zu ermitteln, wäre bürgerfreundlich und würde m. E. die Bereitschaft der Betroffenen zur entsprechenden Mitwirkung auf freiwilliger Basis fördern.

14. Rentenversicherung

14.1 Amtshilfe

Sicherheitsbehörden im Sinne des § 72 SGB X benötigen in Einzelfällen zur Erfüllung ihrer Aufgaben Angaben über frühere Arbeitgeber eines Betroffenen. Entsprechende Angaben liegen im allgemeinen den Sozialversicherungsträgern (Rentenversicherungsträger, Krankenkasse) vor. Auf entsprechende Offenbarungsersuchen können diese Angaben im Rahmen des § 72 SGB X mitgeteilt werden.

Wenn der zuständige Sozialversicherungsträger von der Sicherheitsbehörde nicht auf andere Weise ermittelt werden kann, wird in der Regel der Verband Deutscher Rentenversicherungsträger (VDR) um Mitteilung des zuständigen Rentenversicherungsträgers aus der bei der Datenstelle der deutschen Rentenversicherung (DSRV) geführten Stammsatzdatei aller Versicherten oder um Weiterleitung der Anfrage an den zuständigen Versicherungsträger gebeten, von wo die benötigten Angaben über frühere Arbeitgeber des Betroffenen dann unmittelbar der Sicherheitsbehörde mitgeteilt werden können.

Über die Zulässigkeit dieses Verfahrens ist es zwischen dem VDR und den Sicherheitsbehörden zu Meinungsverschiedenheiten gekommen.

Die Sicherheitsbehörden stützen ihre Auskunftsersuchen in der Regel auf § 72 SGB X. Der VDR vertrat die Auffassung, daß auf ein solches Auskunftsersuchen der Sicherheitsbehörden lediglich die Postleitzahl des Wohnortes des betreffenden Versicherten mitgeteilt werden könne, weil dies das einzige Datum aus dem nach § 72 Abs. 1 Satz 2 SGB X zu offenbarenden Datenkatalog sei, das in der Stammsatzdatei der DSRV enthalten ist. Aufgrund dieser Angabe könne der Kreis der in Betracht kommenden Rentenversicherungsträger eingegrenzt werden; an diese seien dann entsprechende Auskunftsersuchen zu richten. Zwar könnte der ersuchenden Stelle vom VDR theoretisch auch der kontoführende Versicherungsträger bekanntgegeben werden, da diese Angabe aus dem Stammsatzbestand der DSRV zu ersehen sei, jedoch sei die Offenlegung dieses Datums nach § 72 Abs. 1 Satz 2 SGB X nicht zulässig. Die Weitergabe von Auskunftsersuchen an den zuständigen Versicherungsträger sei als (unzulässige) Umgehung des Offenbarungsverbots nach § 72 Abs. 1 SGB X anzusehen und widerspreche dem Sinn und Zweck der Regelung des 2. Kapitels SGB X.

Ich habe dazu folgende Rechtsauffassung vertreten:

Die Angabe „zuständiger Rentenversicherungsträger" stellt zweifellos ein Sozialdatum dar, das vom VDR als Sozialgeheimnis zu wahren ist (§ 35 Abs. 1 SGB I). Eine Offenbarung ist nur unter den Voraussetzungen der §§ 67 bis 77 SGB X zulässig (§ 35 Abs. 2 SGB I).

Als Offenbarungsbefugnis kommen in den hier vorliegenden Fällen — neben der Einwilligung des Betroffenen — die Vorschriften der §§ 68 und 72 SGB X in Betracht. In beiden Vorschriften sind die zu offenbarenden Daten abschließend aufgezählt; in beiden Vorschriften ist das Datum „zuständiger Rentenversicherungsträger" nicht genannt. Daraus ergibt sich, daß die Offenbarung dieser Information nicht zulässig ist. Es kann deshalb dahinstehen, welche dieser beiden Vorschriften als Grundlage für das Ersuchen der Sicherheitsbehörden herangezogen wird.

Die möglichen Alternativen wären: Anfrage an alle in Betracht kommenden Rentenversicherungsträger („Streuung") oder Weiterleitung der Anfrage durch den VDR an den zuständigen Träger. Beide Möglichkeiten halte ich für zulässig. Aus allgemeinen Datenschutzgründen ist jedoch die Weiterleitung der Streuung vorzuziehen. Sie ist datenschutzgerechter, da vermieden wird, daß zuviele Rentenversicherungsträger von einem Auskunftsersuchen einer Sicherheitsbehörde erfahren.

Datenschutzvorschriften — insbesondere § 72 SGB X — werden durch die Weiterleitung der Anfragen an den zuständigen Rentenversicherungsträger nicht verletzt. Gegenüber dem VDR handelt es sich insofern nicht um ein Offenbarungsersuchen nach § 72 (oder § 68) SGB X, sondern um ein Ersuchen um Hilfeleistung im Rahmen der allgemeinen Amtshilfe. Die Tatsache, daß als Ergebnis dieser Amtshilfe der ersuchenden Stelle der zustän-

dige Rentenversicherungsträger bekannt wird, steht m. E. der Amtshilfe nicht entgegen; diese zusätzliche Information ist ebenso bei allen anderen denkbaren Verfahrensweisen unvermeidlich, z. B. wenn die ersuchende Stelle aus der vom VDR offenbarten Postleitzahl den Versicherungsträger selbst feststellt oder bei Anfragen an alle oder an den möglicherweise zuständigen Träger „auf Verdacht".

Der VDR hat mir daraufhin mitgeteilt, daß er seine Bedenken gegen das Verfahren der Weiterleitung von Auskunftsersuchen zurückstellt. Er gehe künftig davon aus, daß jedes Auskunftsersuchen der in § 72 SGB X genannten Stellen die Bitte um Weiterleitung an die zuständige Versicherungsanstalt einschließt, soweit die erbetenen Auskünfte vom VDR aus rechtlichen oder tatsächlichen Gründen nicht unmittelbar erteilt werden können.

14.2 Sozialbericht bei Abhängigkeitskranken

Bereits in meinem Dritten und Vierten Tätigkeitsbericht habe ich über die datenschutzrechtlichen Probleme im Zusammenhang mit der Erstellung des Sozialberichts im Rehabilitationsverfahren Abhängigkeitskranker informiert (vgl. 3. TB S. 39, 4. TB S. 14).

Die von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder in dem Beschluß vom 28./29. September 1981 (vgl. 4. TB) gemachten Vorschläge zur Neugestaltung des Berichts-Formulars wurden in dem derzeit verwendeten Sozialbericht nur zum Teil berücksichtigt. Ich habe deshalb bereits am 5. November 1982 — im Auftrag der Konferenz — den Verband Deutscher Rentenversicherungsträger (VDR), der in dieser Angelegenheit die Federführung für die Rehabilitationsträger übernommen hat, auf die noch offenen Fragen hingewiesen. Neben einigen Klarstellungen in der Formulierung und einer umfassenderen Aufklärung des Betroffenen über seine Rechte und Pflichten in diesem Verfahren sind insbesondere zwei inhaltliche Fragen, die den Persönlichkeitsschutz des Kranken berühren, von erheblicher Bedeutung.

Dabei geht es einmal um den Umfang der für die Erstellung des Sozialberichts zu erhebenden und im Sozialbericht darzustellenden persönlichen, wirtschaftlichen und (psycho)sozialen Verhältnisse des Betroffenen, und zum andern darum, ob und gegebenenfalls in welcher Form und in welcher Tiefe Angaben über die gesundheitlichen Verhältnisse, das Krankheitsbild und sonstige medizinische Fragen in den Sozialbericht aufzunehmen sind.

Zum Umfang des Sozialberichts hatten die Datenschutzbeauftragten darauf hingewiesen, daß die Erheblichkeit und Erforderlichkeit der Angaben für die zu treffenden Entscheidungen im Einzelfall zu prüfen seien; daraus folge, daß das Formular nicht in allen Fällen vollständig ausgefüllt werden müsse. Dies sollte durch einen Hinweis in der „Ergänzenden Information" (für den Sozialarbeiter) klargestellt werden.

Demgegenüber vertritt der VDR nachhaltig die Auffassung, daß der Sozialbericht kein Rahmenformular in dem Sinne sei, daß es dem Sozialarbeiter freistehe, zu entscheiden, welche Fragen er beantworten will und welche nicht. Der Sozialarbeiter solle vielmehr zu allen Fragen Stellung nehmen, soweit es ihm möglich ist.

Diese Auffassung übersieht m. E., daß das Ausfüllen des Formulars eine entsprechende Befragung des Betroffenen und eine mehr oder weniger weitgehende „Ausforschung" seines Intimbereichs voraussetzt. Die Frage berührt also sehr eng die Persönlichkeitsrechte des Betroffenen und letzten Endes den Umfang und die Grenzen seiner Mitwirkungspflicht gemäß § 60 ff. SGB I. Die Angaben eines Abhängigkeitskranken über seine soziale Situation zählen zu den sensitivsten persönlichen Daten überhaupt. Das Verhältnismäßigkeitsgebot führt daher zu engen Grenzen der Mitwirkungspflicht. Diese Grenze hat auch der Sozialarbeiter zu beachten, der den Sozialbericht erstellt.

Die Datenschutzbeauftragten halten daher ihre Auffassung aufrecht, daß in vielen Fällen eine vollständige Beantwortung der im Sozialbericht gestellten Fragen den Rahmen der Erforderlichkeit und damit der Mitwirkungspflicht des Betroffenen sprengt. Wegen der besonderen Sensitivität der im Sozialbericht erhobenen Daten ist eine Prüfung der Erforderlichkeit in jedem Einzelfall unerläßlich. Die aus dem verfassungsrechtlich gebotenen Schutz der Persönlichkeit abgeleiteten Grenzen der Mitwirkungspflicht dürfen nicht etwa dadurch umgangen werden, daß der Rentenversicherungsträger die vollständige Ausfüllung des Sozialberichts verlangt und andernfalls den Antrag auf Rehabilitationsmaßnahmen ohne nähere Prüfung zurückweist.

In der Frage der Erhebung „medizinischer Daten" hatten die Datenschutzbeauftragten in dem o. a. Beschluß gefordert, den Sozialarbeiter darauf hinzuweisen, daß Daten, die nur für die Behandlung des Betroffenen relevant sind, nicht erhoben werden dürfen; sie könnten jedoch auf freiwilliger Grundlage vom Betroffenen erhoben und den Behandlungseinrichtungen direkt zugeleitet werden.

Der VDR hat dem entgegengehalten, daß es bei den im Sozialbericht verlangten medizinischen Angaben nicht um Befunde gehe, sondern nur um Angaben zur allgemeinen Anamnese.

Schon ein solcher klärender Hinweis im Sozialbericht wäre für den Sozialarbeiter hilfreich. Allerdings widerspricht die vorliegende Fassung des Sozialberichts m. E. dieser Feststellung. So enthält der Sozialbericht unter der Rubrik „4. Vorgeschichte und derzeitiger Gesundheitszustand" Fragen nach dem Verhalten unter Einfluß von Suchtmitteln, dem Grad der Abhängigkeit, nach seelisch-geistigen Veränderungen, Delirium oder ähnlichen Komplikationen und nach dem körperlichen Zustand. Die dazu zu machenden Angaben gehen jedoch weit über eine „allgemeine Anamnese" hinaus. Die „Ergänzende Information" (für den Sozialarbeiter) be-

zeichnet folgerichtig diese Angaben als im Grenzbereich zum medizinischen Gutachten liegend.

Es ist unbestritten, daß die Rehabilitationsträger sowohl für die Herbeiführung der Entscheidung über die Maßnahme als auch für deren Durchführung Kenntnis von allen erheblichen Daten erhalten müssen. Für die Entscheidung und Durchführung der Rehabilitationsmaßnahmen erheblich, d. h. berücksichtigungsfähig, sind jedoch nur solche Angaben, die einen Aussagewert für den bestimmten Zweck besitzen. Diesen Aussagewert besitzen aber Angaben „im Grenzbereich zum medizinischen Gutachten" nicht, zumal dem die Beratung in den Betreuungsstellen zunächst abschließenden Sozialbericht in aller Regel bei der Krankenkasse die Einholung der erforderlichen ärztlichen Gutachten folgt. Dies zeigt, daß die Aufnahme solcher medizinischer Daten in den Sozialbericht nicht erforderlich ist.

Ich halte eine Änderung des Sozialberichts-Formulars insoweit nach wie vor für erforderlich. Eine einvernehmliche Lösung erscheint jedoch auf Bundesebene nicht möglich.

14.3 Einzelfälle

In einer Reihe von Einzelfällen habe ich Einsichts- bzw. Löschungsrechte von Versicherten gegenüber Versicherungsträgern durchsetzen können.

Derartige Einzelfälle mögen zuweilen auf den ersten Blick von geringerer Bedeutung sein, sie zeigen jedoch, daß das Datenschutzbewußtsein der Betroffenen weiter gewachsen ist. Zahlreiche Versicherte haben sich auch gegen Offenbarungen von Sozialdaten gewandt. Meine Überprüfungen haben jedoch fast ausnahmslos ergeben, daß es sich um befugte Offenbarungen handelte. Die vielfältigen Informationsbeziehungen zwischen den Sozialleistungsträgern sind für Außenstehende meist nur schwer zu durchschauen. Hier sind die Versicherungsträger aufgerufen, über das bisherige Maß hinaus durch Veröffentlichungen in Mitgliederzeitschriften etc. zur Transparenz für den Betroffenen beizutragen. Allein die starke Nachfrage nach der von mir herausgegebenen Broschüre „Der Bürger und seine Daten im Netz der sozialen Sicherung" zeigt, daß hier noch erheblicher Bedarf besteht.

Ein nicht unerheblicher Teil der Bürgereingaben konnte übrigens durch Versenden dieser Broschüre und Hinweis auf einschlägige Textstellen arbeitssparend beantwortet werden.

15. Krankenversicherung

15.1 Kontrollen

Im Berichtsjahr wurden datenschutzrechtliche Kontrollen unterschiedlichen Umfanges bei den Betriebskrankenkassen der Firmen Deinhard & Co, Volkswagenwerk AG und Klöckner-Humboldt-Deutz-AG, Zweigniederlassung Fahr, durchgeführt. Zwei der dabei getroffenen Feststellungen erscheinen von allgemeinem Interesse:

— Die abgerechneten Krankenscheine werden bei einer Kasse sechs Jahre aufbewahrt. Nach § 33 Abs. 2 der Allgemeinen Verwaltungsvorschrift über das Rechnungswesen in der Sozialversicherung (SRVWV) brauchen Krankenscheine und sonstige Berechtigungsscheine für die Inanspruchnahme von Leistungen einschließlich der Verordnungsblätter für Arzneien, Verband-, Heil- und Hilfsmittel nur solange aufbewahrt zu werden, wie dies für Prüfzwecke der *Krankenkassen* erforderlich ist.

  Auf meine Bitte um Erläuterung dieser Prüfzwecke und der deswegen erforderlichen Aufbewahrungsdauer hat mir die Kasse mitgeteilt, daß nach ihrer Auffassung der Rahmen der maßgeblichen Prüfzwecke weit zu ziehen sei; er erstrecke sich von den internen Prüfungen durch die Innenrevision der Kasse über die Prüfverfahren bei den Prüfungs- und Beschwerdeausschüssen der Kassenärztlichen- und der Kassenzahnärztlichen Vereinigungen bis hin zu den Ermittlungen durch Polizei und Staatsanwaltschaften. Beispiele aus der jüngsten Vergangenheit hätten gezeigt, daß Polizei und Staatsanwaltschaften oftmals bei ihren Ermittlungen auf Krankenscheine zurückgreifen müßten, die schon älter als fünf Jahre seien.

  Diese Auffassung widerspricht der Rechtslage.

  Personenbezogene Angaben in Krankenscheinen und anderen Berechtigungsscheinen unterliegen dem Sozialgeheimnis gemäß § 35 SGB I. Die Herausgabe (Offenbarung) solcher Unterlagen an Polizei und Staatsanwaltschaften im Rahmen von Ermittlungsverfahren ist nach § 35 Abs. 3 SGB I nur unter den Beschränkungen und Voraussetzungen der §§ 72, 73 und 76 Abs. 1 SGB X zulässig. Mit Ausnahme der Offenbarung zur Aufklärung eines Verbrechens (§ 73 Nr. 1 SGB X) ist die Offenbarung auf Daten beschränkt, die regelmäßig auch in anderen Unterlagen bzw. Dateien enthalten sind. Im übrigen ist ein Offenbarungsanspruch Dritter grundsätzlich auf Daten beschränkt, die dem Leistungsträger für die Erfüllung seiner eigenen Aufgaben (noch) zur Verfügung stehen. Keinesfalls wäre es zulässig, wenn Leistungsträger personenbezogene Daten sammelten und generell länger als für ihre eigene Aufgabenerfüllung erforderlich aufbewahrten nur im Hinblick darauf, daß die Daten in Einzelfällen zur Aufklärung eines Verbrechens oder für andere kassenfremde Zwecke nützlich sein könnten. Dies käme einer Sammlung personenbezogener Daten auf Vorrat gleich, die auch das Bundesverfassungsgericht in seinem Urteil zum Volkszählungsgesetz als unzulässig bezeichnet hat.

  Aus diesen Gründen halte ich es für erforderlich, daß jeder Leistungsträger für personenbezogene Daten und Unterlagen, für die nicht anderweitige Aufbewahrungsfristen gelten, die seinen Bedürfnissen entsprechenden Aufbewahrungsfristen festsetzt und dabei in den in § 33 Abs. 2

SRVWV genannten Fällen die Prüfzwecke und deren mögliche Dauer konkret definiert. Ich werde bei künftigen Kontrollen darauf besonders achten.

— In einer Krankenakte einer Krankenkasse befand sich der Entlassungsbericht einer Rehabilitations-Fachklinik eines Rentenversicherungsträgers mit außergewöhnlich umfangreichen und detaillierten ärztlichen Angaben zu Epikrise, Anamnese, Befund und Behandlung des Betroffenen. Kostenträger der Rehabilitationsmaßnahme war der Rentenversicherungsträger.

Die Übermittlung des Entlassungsberichts und die damit verbundene Offenbarung von Sozialdaten durch den Rentenversicherungsträger an die Krankenkasse — ohne Einwilligung des Betroffenen — ist nach § 69 Abs. 1 Nr. 1 SGB X zulässig, soweit sie für die Erfüllung der Aufgaben des Leistungsträgers erforderlich ist. Die Beschränkung der Offenbarungsbefugnis schließt die Beschränkung der Verwendung der offenbarten Daten auf das für die Aufgabenerfüllung Erforderliche durch den Empfänger ein. Dies folgt auch aus § 78 SGB X, wonach der Empfänger die Daten nur zu dem Zweck verwenden darf, zu dem sie ihm befugt offenbart worden sind, d. h. unbefugt offenbarte Daten dürfen nicht verwendet werden und sind zu löschen.

Zwar kann im allgemeinen, insbesondere bei Verwendung von vorgeschriebenen oder üblichen Vordrucken, der Empfänger zunächst von einer befugten Offenbarung durch die übermittelnde Stelle ausgehen. Bei außergewöhnlich umfangreichen Darstellungen insbesondere der gesundheitlichen Verhältnisse des Betroffenen ist jedoch die empfangende Stelle nach meiner Auffassung nicht von der Pflicht entbunden, die Erforderlichkeit der Angaben für ihre Aufgabenerfüllung zu prüfen und gegebenenfalls nicht erforderliche Angaben zu vernichten bzw. zu löschen oder unkenntlich zu machen.

Das Bundesversicherungsamt hat sich in diesem Fall meiner Auffassung angeschlossen und die betreffende Krankenkasse gebeten, unter dem Blickwinkel der Erforderlichkeit zu überprüfen, welche Teile des Entlassungsberichts für ihre Aufgabenerfüllung nicht benötigt werden und vernichtet werden können.

15.1.1 Betriebskrankenkasse Volkswagenwerk AG

In meinem Sechsten Tätigkeitsbericht (S. 34) habe ich über einen ersten Besuch bei der Betriebskrankenkasse Volkswagenwerk AG (BKK VW AG) und über die dort auftretenden spezifischen Datenschutzprobleme berichtet. Im März 1984 habe ich eine weitere, abschließende Kontrolle der BKK durchgeführt, die schwerpunktmäßig der Untersuchung und Beurteilung des Systems PEDATIS und insoweit des Auftragsverhältnisses zwischen Kasse und Werk insbesondere unter dem Gesichtspunkt der Vorschrift des § 80 Abs. 5 SGB X galt.

PEDATIS ist das *P*ersonal-*Da*ten-*I*nformations-*S*ystem der Volkswagenwerk AG. In diesem komplexen Datenbanksystem werden die Daten aller Betriebsangehörigen im Rahmen der Personalverwaltung automatisiert gespeichert und in vielfältigen Verwendungszusammenhängen verarbeitet. Insoweit unterliegt PEDATIS als Datenverarbeitungssystem eines privaten Unternehmens nicht meiner Kontrolle.

In PEDATIS werden jedoch auch Versicherungs- und Leistungsdaten der Mitglieder der BKK verarbeitet. Hinsichtlich dieser Daten ist die BKK als Auftraggeber speichernde Stelle und „Herr der Daten", während das Unternehmen als Auftragnehmer über die Hard- und Software und somit auch über die Schutz- und Kontrollmechanismen verfügt.

Die BKK VW AG unterliegt meiner Kontrolle. Wenn, wie im vorliegenden Fall, Datenverarbeitung im Auftrag stattfindet, kann die Einhaltung datenschutzrechtlicher Vorschriften bei der Verarbeitung der Krankendaten nur dann wirksam und vollständig kontrolliert werden, wenn auch die Datenverarbeitung seitens des Auftragnehmers in die Kontrolle einbezogen wird. Dies ist — im Einvernehmen mit der VW AG und der zuständigen Datenschutz-Aufsichtsbehörde — geschehen.

Die enge Verbindung der Datenverarbeitung der Kasse mit der Arbeitnehmerdatenverarbeitung des Werks kommt einerseits den Interessen der Versicherten in hohem Maße entgegen, was insbesondere bei der Abwicklung der Leistungen im Falle von Arbeitsunfähigkeit deutlich wird. Andererseits ist aber nicht zu verkennen, daß eine solch enge Verbindung Risiken für den Schutz der Sozialdaten in sich birgt. Der Gesetzgeber hat deshalb für die Verarbeitung personenbezogener Sozialdaten im Auftrag durch nicht-öffentliche Stellen besondere Bedingungen aufgestellt: Nach § 80 Abs. 5 SGB X ist eine solche Auftragsdatenverarbeitung nur zulässig, wenn Teilvorgänge der automatischen Datenverarbeitung hierdurch erheblich kostengünstiger besorgt werden können (oder wenn anders Störungen im Betriebsablauf nicht vermieden werden können).

Daraus, sowie aus der Gesetzesbegründung zum SGB X und dem BDSG ergeben sich insbesondere für die Verarbeitung von Daten der Betriebskrankenkassen durch den Arbeitgeber folgende Beurteilungskriterien:

— Es dürfen nur Teilvorgänge der Datenverarbeitung in einem Auftragsverhältnis erledigt werden.

— Die Teilvorgänge müssen erheblich kostengünstiger besorgt werden.

— Wegen der besonderen abstrakten Gefährdung in solchen Fällen sind an den Datenschutz höchste Anforderungen zu stellen, die der Auftraggeber in einer für die Datenschutzkontroll- und Aufsichtsbehörden verständlichen Form zu dokumentieren hat.

Die Kontrolle hat ergeben, daß von den Teilvorgängen der Datenverarbeitung lediglich die Datenerfassung und ein Teil der Datenpflege durch die Kasse erfolgen. Den größeren Teil der Datenverarbeitung erledigt das Werk.

Durch die gemeinsame Nutzung von PEDATIS werden Teilvorgänge, die bei getrennter Verarbeitung sowohl von der Kasse als auch vom Werk durchzuführen wären, nur einmal — und zwar vom Werk — erledigt. Daraus ergeben sich offensichtlich entsprechende Einsparungen für die Kasse. Darüber hinaus trägt das Werk für die Kasse die vom Rechenzentrum in Rechnung gestellten Kosten, so daß hierfür Beitragsmittel nicht aufzuwenden sind. Deshalb kann davon ausgegangen werden, daß die Datenverarbeitung durch das Werk für die Kasse insgesamt erheblich kostengünstiger ist als eine eigene Datenverarbeitung durch die Kasse oder eine Auftragserteilung an den Landesverband der Betriebskrankenkassen.

Die Sicherheit der Datenverarbeitung ist nach den getroffenen Feststellungen auch den besonderen Umständen angemessen. Gleichwohl waren zur Gewährleistung des Sozialdatenschutzes in einigen Teilbereichen noch Verbesserungen zu fordern. Die Erfüllung dieser Forderungen in angemessener Zeit wurde zugesagt und zum Teil bereits realisiert.

Abgesehen von hohen Anforderungen an die Sicherung erfordert diese besondere Auftragssituation eine über das übliche Maß hinausgehende Transparenz. Die Nutzung der Datenfelder in PEDATIS muß deshalb besonders sorgfältig dokumentiert werden. Nur so kann nachgewiesen und sichergestellt werden, daß das Werk auf Sozialdaten keinen Zugriff hat. In einer solchen Dokumentation ist zu belegen, welches Datenfeld von wem (Person oder Personenkreis) benutzt werden darf, wer also Daten eingeben, lesen, auf sie zugreifen darf und wer sie zu pflegen hat.

Insgesamt hat die Kontrolle ergeben, daß die vom Gesetzgeber aufgestellten Voraussetzungen für die Datenverarbeitung im Auftrag einer Betriebskrankenkasse durch den Arbeitgeber hier erfüllt sind.

15.1.2 Betriebskrankenkasse Klöckner-Humboldt-Deutz AG

Die Kontrolle bei der Betriebskrankenkasse Klöckner-Humboldt-Deutz AG, Zweigniederlassung Fahr, war ausgelöst worden durch den Brief eines niedergelassenen Arztes, der darauf hingewiesen hatte, daß der Leiter (Geschäftsführer) der Betriebskrankenkasse in Personalunion auch eine höhere Funktion in der Personalabteilung des Unternehmens innehabe. Bei dieser Konstellation sei zu befürchten, daß Informationen aus dem gesundheitsspezifischen Bereich der Betriebsangehörigen an die Firma weitergereicht und dort für Personalentscheidungen Verwendung finden könnten. Es häufe sich die Zahl der Patienten, die aus Angst vor betrieblichen Konsequenzen sich nicht dazu entschließen könnten, sich in eine aus fachärztlicher Sicht dringend angezeigte ärztlichen Behandlung zu begeben.

Nachdem zunächst schriftliche Erörterungen mit dem Vorstand der Kasse nicht zu konkreten Ergebnissen geführt hatten, habe ich eine datenschutzrechtliche Kontrolle in der Betriebskrankenkasse durchgeführt. Dabei wurden folgende Feststellungen getroffen:

Die Tätigkeiten des Geschäftsführers in der Krankenkasse und in der Personalabteilung des Unternehmens sind zeitlich und räumlich voneinander getrennt. In der Personalabteilung ist er für die Gehälter und für Einstellung und Versetzung von Tarifangestellten des Werkes Gottmadingen zuständig. Bei der Wahrnehmung seiner Aufgaben für die Kasse kommen ihm aufgrund der faktischen Aufgabenverteilung innerhalb der Kasse personenbezogene Versichertendaten, die für seine Tätigkeit in der Personalabteilung Verwendung finden könnten, regelmäßig nicht zur Kenntnis.

Mit der Pflicht zur Wahrung des Sozialgeheimnisses, die der Krankenkasse als Leistungsträger durch § 35 Abs. 1 SGB I auferlegt ist, ist eine Tätigkeit des Geschäftsführers der Kasse in der Personalabteilung des Unternehmens gleichwohl nicht vereinbar: Die Wahrung des Sozialgeheimnisses schließt die Verpflichtung der Kasse ein, die Sozialdaten durch positive Vorkehrungen zu schützen, d. h. alle personellen, organisatorischen und technischen Manahmen zu treffen, die geeignet und erforderlich sind, um zu verhindern, daß Sozialdaten unbefugt oder zweckwidrig verwendet werden können. Dies bedeutet auch, daß personelle Inkompatibilitäten zu vermeiden sind und hat zur Folge, daß Personen als Mitarbeiter einer Betriebskrankenkasse nicht nach § 362 Abs. 1 RVO bestellt werden dürfen, die betriebliche Personalentscheidungen zu treffen berechtigt sind, an solchen Personalentscheidungen mitwirken oder diese vorbereiten. Dies gilt in besonderem Maße für die Person des Geschäftsführers der Betriebskrankenkasse.

Die Betriebskrankenkasse Klöckner-Humboldt-Deutz AG, Zweigniederlassung Fahr, hat diese mit der Wahrung des Sozialgeheimnisses verbundenen Pflichten nicht beachtet; die Doppelfunktion ihres Geschäftsführers in der Kasse und in der Personalabteilung des Unternehmens stellt einen Verstoß gegen datenschutzrechtliche Bestimmungen dar. Ich habe diesen Verstoß gemäß § 20 BDSG beanstandet.

Weitergehende Befugnisse, etwa ein Weisungs- oder Anordnungsrecht, stehen mir nicht zur Verfügung. Eine Änderung der nach meiner Auffassung gesetzwidrigen Situation ist kurzfristig nicht zu erwarten, zumal das Bundesversicherungsamt „im Hinblick auf die beabsichtigte Trennung der beanstandeten Doppelfunktion, die in zwei bis drei Jahren verwirklicht werden soll, von der aufsichtsrechtlichen Weiterverfolgung der Angelegenheit abgesehen" hat.

Um die offensichtlich bestehenden Besorgnisse von Versicherten im Rahmen des Möglichen wenigstens etwas zu mildern, habe ich eine entsprechende allgemeine Aufklärung der Versicherten über die tatsächlichen Aufgaben des Geschäftsführers in seinen beiden Funktionen angeregt.

15.2 Modellversuche zur Erhöhung der Leistungs- und Kostentransparenz in der gesetzlichen Krankenversicherung

15.2.1 Modellversuche gemäß § 223 RVO

Die Vorschrift des § 223 wurde im Jahre 1977 in die RVO eingefügt. Danach kann die Krankenkasse in geeigneten Fällen im Zusammenwirken mit den Kassenärztlichen (und Kassenzahnärztlichen) Vereinigungen, den Krankenhausträgern für den jeweiligen Bereich sowie den Vertrauensärzten die Krankheitsfälle vor allem im Hinblick auf die in Anspruch genommenen Leistungen überprüfen; die Krankenkasse kann den Versicherten und den behandelnden Arzt über die in Anspruch genommenen Leistungen und ihre Kosten unterrichten.

Diese Vorschrift sollte von der Zielsetzung her über eine bessere Transparenz des Leistungs- und Kostengeschehens in der gesetzlichen Krankenversicherung Möglichkeiten der Kostendämpfung aufzeigen. Überprüfungen im Zusammenwirken mit den Leistungserbringern sollen dazu beitragen, übermäßigen und unwirtschaftlichen Leistungsaufwand zu vermeiden.

Die Vorschrift ist in der Vergangenheit weitgehend unbeachtet geblieben, vermutlich vor allem deshalb, weil der Regelungsinhalt nicht klar war und geeignete Verfahren zur Feststellung „geeigneter Fälle" und zu Art und Umfang der vorgesehenen Überprüfung und Unterrichtung nicht zur Verfügung standen.

Der Bundesminister für Arbeit und Sozialordnung hat deshalb am 14. Oktober 1980 in einer öffentlichen „Bekanntmachung über die Förderung von wissenschaftlich begleiteten Modellversuchen zur Erhöhung der Leistungs- und Kostentransparenz in der gesetzlichen Krankenversicherung gemäß § 223 RVO" interessierte Krankenkassen zur Mitwirkung bei der Durchführung solcher Modellversuche aufgerufen.

In meinem Zuständigkeitsbereich werden bei drei Kassen Modellversuche gemäß § 223 RVO durchgeführt. Ich habe von diesen Modellversuchen erst relativ spät, nämlich im April 1983, anläßlich einer routinemäßigen Datenschutzkontrolle bei einer der beteiligten Krankenkassen Kenntnis erlangt. Seit etwa einem Jahr haben die Modellversuche auch in der Öffentlichkeit ein breites und zunehmend kritisches Echo gefunden.

Eine Realisierung der in § 223 RVO genannten Handlungsmöglichkeiten setzt offensichtlich — in „geeigneten Fällen" — die auf den einzelnen Krankheitsfall bezogene, für eine individuelle Unterrichtung auch auf den einzelnen Versicherten und den einzelnen Arzt bezogene Erfassung und Zusammenführung der jeweiligen Leistungs- und Kostendaten voraus. Diese Daten stehen den Krankenkassen auf Einzelbelegen (z. B. Krankenscheine, Arzneimittelverordnungsblätter, Heil- und Kostenpläne, Krankenhausrechnungen u. ä.) zu Abrechnungszwecken zur Verfügung. Die Abrechnung der erbrachten Leistungen erfolgt überwiegend pauschal. Eine versichertenbezogene Erfassung solcher und anderer Kassenleistungen (z. B. Krankengeld) auf der nach § 369a RVO für jeden Erkrankten anzulegenden Krankenkarte erfolgt nur in sehr beschränktem Umfang. Nach den Allgemeinen Verwaltungsvorschriften der Bundesregierung über das Rechnungswesen bei den Trägern der sozialen Krankenversicherung vom 31. August 1956 (mit nachfolgenden Änderungen) sind dies im wesentlichen Leistungen im Zusammenhang mit Arbeitsunfähigkeit und Krankenhausbehandlung sowie größere Heil- und Hilfsmittel einschließlich Zahnersatz.

Daneben führt die Krankenkasse nach § 319a RVO ein — dateimäßiges — Mitgliederverzeichnis, das — ebenfalls nach den Allgemeinen Verwaltungsvorschriften — Daten zur Mitgliedschaft sowie „Angaben, die satzungsgemäß für die Gewährung der Versicherungsleistungen erforderlich sind", enthält. Über die seinerzeitige Absicht des Bundesministers für Arbeit und Sozialordnung, die in § 319a RVO vorgesehene Rechtsverordnung über Inhalt und Form des Mitgliederverzeichnisses zu erlassen, und über die dabei aufgetretenen datenschutzrechtlichen Bedenken — auch in bezug auf § 223 RVO — habe ich in meinem Fünften Tätigkeitsbericht (S. 63) berichtet.

Für die Durchführung des § 223 RVO erscheint es naheliegend und möglicherweise auch notwendig, jedenfalls in den „geeigneten Fällen" alle erbrachten Leistungen und ihre Kosten jeweils bezogen auf den Krankheitsfall, den Versicherten und den Arzt zu erfassen und zusammenzuführen. Diese Erfassung und Zusammenführung der in unterschiedlicher Form und aus anderen Zusammenhängen sowie für andere Zwecke bei den Krankenkassen vorhandenen sogenannten Routinedaten stellt nach meiner Auffassung einen Vorgang des (Neu-)Speicherns oder auch des Veränderns personenbezogener Daten dar. Nach geltendem Datenschutzrecht (§ 9 Abs. 1 BDSG) ist dies zulässig, wenn es zur rechtmäßigen Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben erforderlich ist.

Nach dem Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz ist die Verwendung zwangsweise oder unter faktischem Zwang erhobener Daten eine Einschränkung des Rechts auf informationelle Selbstbestimmung. Erst wenn Klarheit besteht, welche Verknüpfungs- und Verwendungsmöglichkeiten bestehen, läßt sich die Frage einer zulässigen Beschränkung dieses Rechts beantworten. Solche Einschränkungen bedürfen auf jeden Fall einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muß, d. h. aus der gesetzlichen Grundlage müssen sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben. Das bedeutet wiederum, daß der Gesetzgeber den Verwendungszweck präzise bestimmt und daß die Daten für diesen Zweck geeignet und erforderlich sind. Alle Stellen müssen sich deshalb auf das zur Erfüllung ihrer Aufgaben und auf das zum Erreichen des

angegebenen Ziels erforderliche Minimum von Daten beschränken.

Daraus ergibt sich nach meiner Auffassung die Notwendigkeit, die Vorschrift des § 223 RVO, bevor die Krankenkassen sie in der Praxis vollziehen, hinsichtlich der Zwecke, der den Kassen dabei zufallenden Aufgaben und der dafür zu verwendenden personenbezogenen Daten zu präzisieren. Soweit hinsichtlich der zu verwendenden Daten § 319a und/oder § 369a RVO in Bezug genommen wird, halte ich auch eine Präzisierung dieser Vorschriften für erforderlich; die Allgemeinen Verwaltungsvorschriften, die die Art der zu erfassenden Daten regeln und im übrigen nur einen geringen Teil der für § 223 RVO „notwendigen" Daten umfassen, sind dafür keine ausreichende Rechtsgrundlage.

Anhaltspunkte für Inhalt und Umfang der notwendigen Präzisierungen können und sollen die Ergebnisse der Modellversuche liefern. Insofern ist eine Beschränkung der Datenverarbeitung auf „geeignete Fälle" und auf die dafür „erforderlichen" Daten im Rahmen der Modellversuche (noch) nicht möglich. Für die entsprechenden wissenschaftlichen Untersuchungen kann die Erfassung, Speicherung und Verwendung der jeweils für notwendig erachteten Leistungs- und Kostendaten der Versicherten auch aus datenschutzrechtlicher Sicht hingenommen werden, wenn dadurch die Persönlichkeitsrechte bzw. die schutzwürdigen Belange der Betroffenen nicht verletzt werden. Durch intensive Prüfung der einzelnen Modellvorhaben, die von den jeweiligen Krankenkassen unterschiedlich angelegt sind, und durch detaillierte datenschutzrechtliche Beratung der Kassen konnten jeweils Verfahren gefunden werden, die jedenfalls in den Phasen der Datenerfassung und -speicherung sowie der wissenschaftlichen Auswertung solche Verletzungen vermeiden. Nach Abschluß dieser Arbeiten wird zu prüfen und zu beurteilen sein, auf welcher Rechtsgrundlage, in welcher Form und mit welchen Daten die Modellversuche zum Abschluß gebracht werden können, und welches endgültige Verfahren aufgrund der Ergebnisse der Modellversuche in Betracht kommt.

Ich verhehle nicht, daß aus meiner gegenwärtigen Sicht gegen die in § 223 RVO angelegte totale oder zumindest sehr weitgehende Erfassung und Verwendung von Krankheits-, Leistungs- und Kostendaten der Versicherten grundsätzliche und übergreifende Bedenken bestehen. In die gleiche Richtung gegen Äußerungen des Verbandes der Angestellten-Krankenkassen (vgl. 5. TB S. 64), daß hier ein Instrument geschaffen wird, das eine umfassende Durchleuchtung der persönlichen (krankheitsbedingten) Verhältnisse der Versicherten ermögliche und eine Gefährdung des Anspruchs auf Schutz des allgemeinen Persönlichkeitsrechts mit sich brächte.

Um nicht mißverstanden zu werden: Maßnahmen gegen die Kostenexplosion im Gesundheitswesen sind unbestreitbar dringend notwendig. Aber sie müssen geeignet sein, dieses Ziel zu erreichen, und sie dürfen den Schutz des einzelnen vor übermäßiger Erfassung und Registrierung seiner persönlichen und sachlichen Verhältnisse nicht gefährden und sein informationelles Selbstbestimmungsrecht nicht unverhältnismäßig beschränken. Alle bisherigen Versuche, die Kosten im Gesundheitswesen auf dem Wege der Kostentransparenz oder durch „Vorrechnung" der Kosten gegenüber dem einzelnen Versicherten zu reduzieren, sind fehlgeschlagen. Deshalb scheinen mir Zweifel angebracht, ob der jetzt eingeschlagene Weg zum Ziel führt und ob die Eignung als Voraussetzung für grundrechtsbeschränkende Maßnahmen bejaht werden kann. Zum anderen bedarf eine nicht nur für einige Versicherte versuchsweise, sondern für alle Versicherten auf Dauer und mit dem Ziel der Außenwirkung erfolgende Kontrolle ihrer Krankheitskosten einer präzisen gesetzlichen Grundlage. Dabei wird es darauf ankommen, die Risiken solcher Systeme so gering wie möglich zu halten. Dazu gehört nicht nur abstrakt, daß die Entstehung von Teilabbildern der Persönlichkeit des einzelnen (in dem sehr sensitiven Bereich seiner Krankheiten), die mit der Würde des Menschen nicht vereinbar wären (BVerfGE 65, 1), ausgeschlossen wird. Vielmehr ist darüber hinaus — gegebenenfalls in Abweichung von den Offenbarungsbefugnissen des SGB X — sicherzustellen, daß derartige umfassende Darstellungen aller Krankheiten eines Versicherten innerhalb der jeweiligen Krankenkasse verbleiben. In § 223 RVO ist dies nicht gewährleistet, sondern im Gegenteil: diese Daten sollen im Rahmen des Zusammenwirkens mit den Kassenärztlichen und Kassenzahnärztlichen Vereinigungen, den Krankenhausträgern sowie den Vertrauensärzten anderen Personen und Stellen zur Kenntnis gelangen. Auch das Sozialgeheimnis bietet dagegen keinen absoluten Schutz. Im Rahmen des § 69 SGB X sind sehr weitgehende Datenübermittlungen zulässig, wenn dies zur Erfüllung der Aufgaben anderer Stellen im Sozialbereich erforderlich ist. Die Erfahrung zeigt, daß der Maßstab der Erforderlichkeit in der Praxis sehr großzügig gehandhabt wird. Als Beispiel mag genügen, daß die Träger der gesetzlichen Unfallversicherung für die Prüfung von ursächlichen Zusammenhängen bei Berufskrankheiten in der Regel die Kenntnis *aller* Vorerkrankungen für erforderlich halten und deshalb bei den Krankenkassen alle dort gespeicherten Krankheitsdaten erfragen und zumeist auch erhalten. Meine Bedenken gegen die beabsichtigte Einführung einer allgemeinen Versicherungsnummer in der Sozialversicherung (vgl. Nr. 12.1) erhalten in diesem Zusammenhang zusätzliches Gewicht.

Mir liegt daran, diese nach der gegenwärtigen Rechtslage bestehenden Gefährdungen deutlich zu machen, um zu erreichen, daß sie bei der gesetzlichen Regelung, die ich wegen der Einschränkung des informationellen Selbstbestimmungsrechts der Betroffenen für zwingend erforderlich halte, bedacht und ausgeräumt werden.

15.2.2 Modellversuch „Arzneimitteltransparenz und -beratung am Beispiel der Region Dortmund"

Ein weiterer Versuch zur Erhöhung der Leistungs- und Kostentransparenz im Gesundheitswesen wird

in Dortmund durchgeführt. Dieser Modellversuch ist im Vergleich zu den unter Nr. 15.2.1 beschriebenen Modellversuchen dadurch gekennzeichnet, daß er gemeinsam von mehreren Krankenkassen einer Region zusammen mit der zuständigen Kassenärztlichen Vereinigung und dem zuständigen Apothekerverein durchgeführt wird, und daß die wissenschaftliche Evaluation auf eine Abschätzung der globalen Wirkungen der in einer zweijährigen praktischen Erprobung gewonnenen Erkenntnisse zielt. Die wissenschaftlichen Untersuchungen sind hier also der praktischen Erprobung nicht vor- sondern nachgeschaltet.

Der Modellversuch ist auf Transparenz und Beratung bei den Arzneimitteln begrenzt. Die Erfassung von Daten aus den den Krankenkassen zur Verfügung stehenden Leistungsbelegen beschränkt sich daher auf die Arzneimittelverordnungsblätter der Dortmunder Ärzte.

Die erfaßten Daten werden in ausreichend anonymisierter Form (hinsichtlich der Versicherten) der Kassenärztlichen Vereinigung zur Verfügung gestellt. Basierend auf diesem sogenannten Transparenzdatenbestand wird zunächst eine arzt- und protuktgruppenorientierte Grundauswertung nach Verordnungshäufigkeit, Mengen und Kosten sowie nach feineren, auf der mittleren Tagesdosis basierenden Indikatoren durchgeführt. Von den Ergebnissen wird der einzelne Arzt in allgemeiner Form informiert. Darüber hinaus erfolgt eine Auswahl solcher Ärzte, die aufgrund bestimmter Indikatoren für eine vertiefende Information und/oder Beratung in Betracht kommen. Für den Fall, daß eine Beratung auf der Grundlage anonymisierter Daten nicht ausreicht, ist beabsichtigt, auf personenbezogene Behandlungsunterlagen zurückzugreifen, d. h. fall- und versichertenbezogene Behandlungsscheine und Arzneimittelverordnungsblätter hinzuzuziehen. Gegen die Verwendung personenbezogener Versichertendaten in diesem Zusammenhang wurden von den Datenschutzbeauftragten Bedenken geltend gemacht; für die damit verbundene Offenbarung von Sozialdaten besteht keine zweifelsfreie Rechtsgrundlage. Vor einer endgültigen Entscheidung muß eine datenschutzrechtlich unbedenkliche Lösung erst noch gefunden werden.

Die meiner Zuständigkeit unterliegenden beteiligten Ersatzkassen nehmen eine versichertenbezogene Zuordnung der erfaßten Verordnungsblätter nicht vor. Die Versichertenberatung bei den Ersatzkassen wird sich auf solche Fälle beschränken, in denen der Versicherte sich auf Veranlassung seines behandelnden Arztes mit der Bitte um Beratung an seine Kasse wendet. Diese Beratung wird sich im wesentlichen auf Möglichkeiten therapieunterstützender Maßnahmen beziehen. Hiergegen bestehen keine Bedenken.

Die für die Durchführung des Modellversuchs festgelegten Datenschutz- und Datensicherungsmaßnahmen sind ausreichend. Insbesondere findet eine Verknüpfung der „Transparenzdatenbestände" mit anderen, bei den beteiligten Institutionen zur Wahrnehmung ihrer Routineaufgaben gespeicherten Daten nicht statt. Die Transparenzdatenbestände werden nach Ablauf des Modellversuchs (zwei Jahre nach Beginn) irreversibel anonymisiert, in dieser Form zu Zwecken der Evaluation und der statistischen Auswertung ein weiteres Jahr aufbewahrt und dann endgültig gelöscht.

15.3 Angabe des Arbeitgebers auf Krankenscheinen und Verordnungsblättern

Mehrfach haben Bürger kritisiert, daß auf Krankenscheinen, Überweisungsscheinen, Arzneimittelverordnungsblättern, und anderen Vordrucken im Bereich der gesetzlichen Krankenversicherung die Angabe ihres Arbeitgebers vorgesehen ist. Insbesondere arbeitslose Bürger fühlen sich dadurch diskriminiert, weil in diesen Fällen als „Arbeitgeber" vermerkt wird: „Arbeitsamt", „arbeitslos" o. ä.

Die verwendeten Vordrucke beruhen auf Vordruckvereinbarungen zwischen den Kassenärztlichen und Kassenzahnärztlichen Bundesvereinigungen und den Bundesverbänden der Krankenkassen auf der Grundlage der Bundesmantelverträge bzw. der Ersatzkassenverträge. Form und Inhalt der Vordrucke sind dabei in der Regel verbindlich festgelegt.

Eine Umfrage unter einigen großen Ersatzkassen und Betriebskrankenkassen meines Zuständigkeitsbereichs zur Notwendigkeit bzw. zum Zweck der Angabe des Arbeitgebers auf den Vordrucken sowie zur jeweiligen Praxis hat ein unterschiedliches Bild ergeben:

1. Krankenschein

Die Krankenscheinformulare werden von den Kassen selbst hergestellt. Die entsprechende Vordruckvereinbarung läßt den Kassen einen gewissen Gestaltungsspielraum. Die Angabe des Arbeitgebers ist nicht zwingend vorgeschrieben.

Bei zwei Ersatzkassen und einer Betriebskrankenkasse enthält der Krankenschein keine Rubrik „Arbeitgeber", weil dafür keine Notwendigkeit gesehen wird.

Eine Betriebskrankenkasse verwendet Krankenscheinvordrucke mit der Rubrik „Arbeitgeber", legt jedoch auf diese Angabe keinen besonderen Wert; sie überläßt es dem Mitglied, den Arbeitgeber einzutragen oder auch nicht.

Lediglich eine Ersatzkasse besteht auf der Angabe des Arbeitgebers wegen der arbeitgeberorientierten Zuordnung der Mitglieder in den Bezirksgeschäftsstellen.

2. Überweisungsschein

Die Form ist durch die entsprechende Vordruckvereinbarung verbindlich festgelegt, und zwar mit der Rubrik „Arbeitgeber". Zur Erforderlichkeit dieser Angabe gelten die unter 1. genannten Ausführungen.

3. Arzneimittelverordnungsblatt

Der Vordruck ist ebenfalls — mit der Rubrik „Arbeitgeber" — verbindlich festgelegt.

Eine zwingende Notwendigkeit für diese Angabe wird von keiner Kasse — einschließlich der Ersatzkasse, die auf der Angabe im Krankenschein besteht — gesehen; im Einzelfall könne sie als zusätzliches Kriterium die Prüfung der Mitgliedschaft oder der Kassenzuständigkeit erleichtern. Nach den mitgeteilten Erfahrungen wird die Rubrik überwiegend ausgefüllt. Der Arzt sei im übrigen lediglich verpflichtet, die Angaben aus dem Krankenschein zu übernehmen. Sofern vom Arzt bei dem Versicherten der Arbeitgeber erfragt werde, liege dies außerhalb des Einflußbereichs der Krankenkasse.

Das Ergebnis der Umfragen — es ist nach meiner Einschätzung prinzipiell auf alle Kassen übertragbar — zeigt, daß die Angabe des Arbeitgebers auf den Vordrucken für die Aufgabenerfüllung der Krankenkassen in Einzelfällen zwar nützlich sein kann, grundsätzlich aber nicht erforderlich ist. Auch nach den Grundsätzen des Volkszählungsurteils des Bundesverfassungsgerichts dürfen nicht erforderliche Angaben nicht zwangsweise abverlangt werden. Die Partner der Vordruckvereinbarungen sind daher aufgefordert, diese Vordrucke insoweit zu ändern.

15.4 Krankenversicherung der Mitarbeiter

Bereits in früheren Jahren hatte ich mich mehrfach mit Datenschutzproblemen zu befassen, die sich daraus ergeben, daß die Mitarbeiter in den Krankenkassen in der Regel auch bei derselben Krankenkasse krankenversichert sind und daß dabei Gesundheits- und Leistungsdaten häufig einem Vorgesetzten zur Kenntnis gelangen, der gleichzeitig mit Personalführungsaufgaben hinsichtlich dieser Mitarbeiter betraut ist (vgl. 5. TB S. 63).

Gemeinsam mit den Kassen konnten in zwei Fällen organisatorische Lösungen gefunden werden, die solche Unverträglichkeiten weitgehend vermeiden.

Eine große Ersatzkasse hat ihren Mitarbeitern eine Wahlmöglichkeit eingeräumt, bei welcher Geschäftsstelle außerhalb ihrer Beschäftigungsstelle ihre Krankenversicherung abgewickelt werden soll.

Bei einer Betriebskrankenkasse oblag die Führung der Leistungskarten der Mitarbeiter dem Leiter der Leistungsabteilung. Diese Aufgabe wurde einem Mitarbeiter außerhalb der Leistungsabteilung und ohne Vorgesetztenfunktion übertragen.

15.5 Einzelfälle

Die Mitarbeiter der Krankenkassen zeigen im allgemeinen viel Verständnis für Datenschutzfragen. Daß es noch immer Ausnahmen gibt, zeigen drei Beispiele, die mir aus Eingaben Versicherter bekannt geworden sind:

— Da zur Beitragsbemessung von den Kassen die Höhe des Einkommens ermittelt werden muß, lassen sich die Kassen im Bedarfsfall Einkommensteuerbescheide vorlegen. Diese Bescheide werden offenbar in einer ganzen Reihe von Fällen fotokopiert und zu den Akten des Versicherten genommen. Da Einkommensteuerbescheide jedoch eine Reihe von Angaben enthalten, die zur Aufgabenerfüllung der Krankenkassen nicht erforderlich sind, halte ich diese Verfahrensweise für unzulässig. Andere Nachweise, wie etwa eine Bescheinigung des Finanzamtes über das Gesamteinkommen sollten hier ausreichen.

— In einem Fall wurde dem arbeitslosen Sohn eines Versicherten, der Krankengeld bezog, zur Prüfung des Anspruchs auf Arbeitslosenhilfe eine Bescheinigung über die Höhe des Krankengeldes ausgestellt. Der Sohn lebte mit dem Vater nicht in einem Haushalt. Der Vater sah in der Offenbarung der Höhe des Krankengeldes gegenüber dem Sohn einen Verstoß gegen das Sozialgeheimnis.

  Die Kasse war nach ihrer Stellungnahme davon ausgegangen, daß das Einverständnis des Versicherten vorausgesetzt werden könne, da es sich um seinen Sohn gehandelt habe und die häuslichen Verhältnisse nicht bekannt gewesen seien. Sie hat inzwischen eingeräumt, daß dies eine Fehleinschätzung war und sich bei dem Vater entschuldigt.

— In einem anderen Fall hatte sich ein Versicherter an seine Kasse gewandt mit der Bitte um Auskunft gemäß § 13 BDSG über die zu seiner Person gespeicherten Daten. Als Antwort erhielt er ein Exemplar des Bundesanzeigers, in dem die Kasse veröffentlicht hatte, welche Datenarten sie speichert. Der Inhalt des Datensatzes wurde dem Betroffenen nicht mitgeteilt, wie es § 13 BDSG verlangt. Daß die Kasse ein Auskunftsbegehren so mißverstanden hat zeigt, daß die nach § 79 Abs. 1 SGB X i. V. mit § 29 Satz 3 Nr. 3 BDSG notwendige Schulung des Personals offenbar unzulänglich war.

16. Unfallversicherung

16.1 Kontrollen

— Zu der in meinem Vierten Tätigkeitsbericht (S. 16f.) beschriebene Kontrolle der *Bau-Berufsgenossenschaft Hamburg* habe ich die dort angekündigte Nachkontrolle durchgeführt.

  Die Übersicht gemäß § 15 Abs. 1 BDSG war immer noch nicht vorhanden. Die Berufsgenossenschaft beabsichtigt, die Übersicht mit einem automatischen Verfahren zu erstellen und zu führen.

  Das zur Kontrolle der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme (§ 15 Satz 2 Nr. 2 BDSG) erforderliche Verfahren der Auftragsvergabe wurde stichprobenweise

kontrolliert. Es ergab sich kein Anlaß zur Beanstandung.

Die im Bereich Datensicherung angesprochenen Mängel sind durch den inzwischen erstellten Neubau behoben worden.

Die Bau-BG hat eine moderne Anlage zur Zugangskontrolle eingesetzt. Jedes Betreten des Gebäudes und der einzelnen Sicherheitszonen wird erfaßt und ausgedruckt. Der Drucker steht in der Personalabteilung. Ich habe datenschutzrechtliche Bedenken geltend gemacht zum einen wegen des so entstehenden und nahezu perfekten Bewegungsbildes für einen Teil der Beschäftigten, und zum anderen gegen den Standort des Druckers. Eine durch ein solches Verfahren mögliche Verhaltenskontrolle ist mit dem Recht auf freie Entfaltung der Persönlichkeit nicht vereinbar.

Die nach Nr. 1 der Anlage zu § 6 Abs. 1 Satz 1 BDSG erforderliche Zugangskontrolle ist auch mit Maßnahmen, die den einzelnen Mitarbeiter weniger belasten, zu erreichen. So könnte z. B. jedes Betreten eines gesicherten Bereichs gespeichert, jedoch nur die unberechtigten Zugangsversuche ausgedruckt werden. Berechtigte Zutritte sollten nur aus besonderem Anlaß ausgedruckt werden.

Ich habe gemeinsam mit der Berufsgenossenschaft eine Regelung gefunden, die für eine Übergangszeit akzeptabel ist. Im kommenden Jahr werde ich jedoch — gegebenenfalls auch zusammen mit der Herstellerfirma der Anlage — eine endgültige Lösung anstreben.

— Die von mir bereits 1978 kontrollierte *See-Berufsgenossenschaft* hat sich im Berichtsjahr von mir hinsichtlich der Sicherheitsmaßnahmen für ihr neues Rechenzentrum beraten lassen. Dabei ergab sich, daß die geplanten Maßnahmen insgesamt ausreichend sind. Hinsichtlich der Paßwort-Vergabe und der Magnetbandverwaltung habe ich Verbesserungen empfohlen; ihre Einführung wurde von der See-Berufsgenossenschaft zugesagt.

Im Bereich Aktenverwaltung habe ich festgestellt, daß es der See-Berufsgenossenschaft aus organisatorischen und aus Platzgründen nicht möglich ist, die in laufender Bearbeitung befindlichen Akten nach Dienstschluß in verschließbaren Schränken zu verwahren. Dies wäre aber wegen der besonderen Schutzbedürftigkeit von Sozialdaten erforderlich. Da die Räume jedoch verschlossen werden, sobald sie der jeweilige Sachbearbeiter verläßt und die Berufsgenossenschaft zugesagt hat, stichprobenweise Kontrollen durchzuführen, habe ich meine Bedenken zurückgestellt.

Die See-Berufsgenossenschaft hat außerdem anhand eines Einzelfalles folgende Frage zu § 76 Abs. 2 SGB X angesprochen:

Ein Betroffener hatte unter Berufung auf § 84 SGB X die Entfernung bestimmter ärztlicher Angaben und Unterlagen aus seinen Unfallakten verlangt. Diesem Verlangen ist die See-Berufsgenossenschaft insbesondere deswegen nicht nachgekommen, weil sich eine Löschungspflicht nur auf Daten in Dateien bezieht. Die See-Berufsgenossenschaft hat das Löschungsverlangen dagegen als (vorsorglichen) Widerspruch gegen eine zukünftige Offenbarung gemäß § 76 Abs. 2 Satz 2 SGB X gewertet und entsprechend vorgemerkt, daß diese Angaben nicht offenbart werden dürfen. Dies halte ich für eine datenschutzgerechte Lösung und empfehle sie auch anderen Stellen.

16.2 Unfallverhütungsvorschriften

In meinem Fünften Tätigkeitsbericht (S. 69) habe ich über Probleme bei der Durchführung von Unfallverhütungsvorschriften (dort: VBG 119) berichtet. Im Sommer dieses Jahres ist mir der Entwurf einer Unfallverhütungsvorschrift „Arbeitsmedizinische Vorsorge" (VBG 100) bekanntgeworden.

Die VBG 100 soll die Überwachung des Gesundheitszustandes von Arbeitnehmern in zahlreichen Bereichen regeln, in denen Vorsorgeuntersuchungen bereits in der Arbeitsstoffverordnung vorgeschrieben sind. Im Anhang 6 der Durchführungsanweisungen zur VBG 100 wird deshalb die Arbeitsstoffverordnung unter den „insbesondere zu beachtenden einschlägigen Vorschriften" genannt.

Entgegen § 19 Abs. 3 Arbeitsstoffverordnung soll jedoch nach § 9 Abs. 4 Satz 3, Abs. 5 VBG 100 eine Kopie der Gesundheitskarte auch nach dem Ausscheiden des Arbeitnehmers beim Unternehmer aufbewahrt bzw. der Berufsgenossenschaft zur Aufbewahrung übergeben werden. Dies erscheint nicht nur wegen des nach meiner Auffassung bestehenden Vorrangs der Arbeitsstoffverordnung, sondern auch im Hinblick auf das vom Bundesverfassungsgericht in seinem Urteil zum Volkszählungsgesetz festgestellte Recht auf informationelle Selbstbestimmung bedenklich.

Außerdem ist die vorgesehene Verwendung der Rentenversicherungsnummer als Ordnungsmerkmal im Zusammenhang mit arbeitsmedizinischen Vorsorgeuntersuchungen nach meiner Auffassung ohne gesetzliche Grundlage nicht zulässig (vgl. dazu Nr. 12.1).

Im Verlaufe des darüber mit der Zentralstelle für Unfallverhütung und Arbeitsmedizin beim Hauptverband der gewerblichen Berufsgenossenschaften geführten Schriftwechsels hat mir diese unter anderem mitgeteilt, daß der Bundesminister für Arbeit und Sozialordnung die notwendigen Bestimmungen über die Behandlung der Gesundheitskarte in den Entwurf der neuen Gefahrstoffverordnung aufgenommen habe.

Dieser Entwurf ist mir nicht bekannt. Ich gehe jedoch davon aus, daß er mir rechtzeitig zugehen wird, nachdem der Bundesminister für Arbeit bereits im Rahmen der parlamentarischen Behandlung meines Fünften Tätigkeitsberichts zugesagt hat, sich insoweit mit mir abzustimmen (vgl. BT-Drucksache 10/1719 S. 25/26). Dabei sollte es gelin-

gen, auch über weitere datenschutzrechtliche Fragen im Zusammenhang mit der Durchführung arbeitsmedizinischer Vorsorgeuntersuchungen zu einvernehmlichen Lösungen zu kommen.

16.3 Arztberichte

Ein Bürger hatte sich bei mir beschwert, daß nach einem Arbeitsunfall seinem Arbeitgeber von dem zuständigen Träger der Unfallversicherung die Kopie des Durchgangsarztberichts (Bericht des Unfallarztes für den Versicherungsträger) mit detaillierten Krankheitsbefunden „zugespielt" worden sei.

Meine Feststellungen bei der betreffenden Berufsgenossenschaft ergaben, daß im Rahmen der Untersuchung von Unfallursachen durch den technischen Aufsichtsdienst personenbezogene Unfallmeldungen an den Unternehmer mit einem Fragebogen versandt werden, mit dessen Hilfe technische Unfallschwerpunkte ermittelt werden sollen. Je nachdem, in welcher Form der Berufsgenossenschaft der betreffende Unfall zuerst bekannt wird, kann diese Unfallmeldung die Unfallanzeige des Unternehmers oder der Durchgangsarztbericht sein.

Personenbezogene Daten, die der Berufsgenossenschaft von einem Arzt zugänglich gemacht worden sind, dürfen — auch im Rahmen des § 69 Abs. 1 Nr. 1 SGB X — nur unter den einschränkenden Voraussetzungen des § 76 SGB X offenbart werden. Danach ist die Offenbarung des Durchgangsarztberichtes an den Arbeitgeber des Betroffenen nicht zulässig. Ich habe diesen Verstoß gegen datenschutzrechtliche Bestimmungen gemäß § 20 BDSG beanstandet und darauf hingewiesen, daß entsprechende Maßnahmen zu treffen sind, die sicherstellen, daß künftig nur noch nach dem festgelegten Arbeitsablauf — der die Übersendung des Durchgangsarztberichtes nicht vorsieht — verfahren wird und Durchgangsarztberichte in keinem Fall mehr an den Unternehmer gelangen.

Die Berufsgenossenschaft hat daraufhin alle Beteiligten nochmals darauf hingewiesen, daß Unfallmeldungen oder Durchgangsarztberichte keinesfalls dem Anschreiben an den Unternehmer beigefügt werden dürfen.

17. Gesundheitswesen

17.1 Bundesgesundheitsamt

Nach mehreren Teilkontrollen in den Jahren 1980, 1981 und 1982 (vgl. 3. TB S. 45, 4. TB S. 19 und 5. TB S. 71) wurde in diesem Jahr eine weitere Kontrolle beim Bundesgesundheitsamt durchgeführt. Schwerpunkte waren diesmal allgemein die Organisation und Durchführung des Datenschutzes, die Datenverarbeitung bei der Wahrnehmung eigener Verwaltungsaufgaben sowie die Überprüfung der in der Risiko- und Schwachstellenanalyse vom 1. August 1982 in Aussicht gestellten Maßnahmen. Insgesamt hat sich dabei der Eindruck einer positiven Entwicklung des Datenschutzes im Bundesgesundheitsamt bestätigt. Gleichwohl sind einige weitere Verbesserungen notwendig.

Wie bereits früher festgestellt wurde, läßt die besondere Aufgabenstellung des Bundesgesundheitsamtes mit einem hohem Anteil wissenschaftlicher Forschung Standardlösungen zur Sicherstellung des Datenschutzes nicht zu. So können z. B. von den berechtigten Benutzern des DV-Systems Dateien eingerichtet und mit bestehenden oder besonders dafür erstellten Programmen verarbeitet werden, ohne daß der Inhalt dieser Arbeit erkennbar oder kontrollierbar wäre. Zur Minderung der darin begründeten besonderen Risiken habe ich verschiedene Maßnahmen vorgeschlagen, z. B. hinsichtlich der Passwort-Vergabe und der Protokollierung von Versuchen, das Passwort zu einer Benutzerkennung durch Probieren herauszufinden oder ohne Eingabe des richtigen Passworts auf Dateien zuzugreifen. Gegenwärtig ist es nicht möglich, solche Versuche gezielt zu verfolgen, weil sie durch das System nicht erkannt werden. Hinsichtlich der Sicherung der zentralen Datenverarbeitungsanlage und der dort verwendeten Datenträger ist der augenblickliche Zustand nur deswegen hinnehmbar, weil der Umzug in die neuen Räume kurz bevorsteht. Während die äußeren Sicherungsmaßnahmen augenfällig verbessert worden sind, fehlt nach wie vor eine angemessene Regelung für den Datenträgerverkehr zwischen Archiv und Maschinenraum. Die Planungen für das neue Rechenzentrum lassen erwarten, daß diese Probleme mit dem Umzug gelöst werden.

Bei der Kontrolle der Verschreibungspraxis für Betäubungsmittel beschränkt sich die Opiumstelle des Bundesgesundheitsamtes auf die Abgabe der Sonderrezepte und das Registrieren der Empfänger sowie der jeweils abgegebenen Rezeptformulare. Bei auffälligem Anforderungsverhalten von Ärzten informiert die Opiumstelle die zuständige Landesbehörde; einigen Ländern werden auf Anforderung regelmäßig Gesamtübersichten übermittelt. Aus der Sicht des Datenschutzes begegnet dies keinen Bedenken.

Das Bundesgesundheitsamt hat in diesem Zusammenhang die Möglichkeit, von den Apotheken die dort aufbewahrten Rezeptdurchschriften zur Auswertung anzufordern. Solche Auswertungen dienen der Überprüfung des Verschreibungs- und Abgabeverhaltens, aber nicht der Überprüfung der Patienten. Deswegen ist die Angabe des Patienten auf der Apothekerkopie nicht erforderlich. Von der Möglichkeit, Kopien bei den Apotheken anzufordern, hat das Bundesgesundheitsamt in den letzten zwei Jahren allerdings keinen Gebrauch gemacht.

Im Rahmen der Überwachung nach dem Bundesseuchengesetz erstellt das Institut für Sozialmedizin und Epidemiologie Meldungen an die Weltgesundheitsorganisation sowie Fachstatistiken und Berichte für die Bundes- und Landesregierungen. Für die Erfüllung dieser Aufgaben reichen die bestehenden Rechtsgrundlagen nicht aus. In diesem Zusammenhang muß auch der Inhalt der Meldebö-

gen auf sachliche Erforderlichkeit der einzelnen Angaben überprüft werden. Zweifel bestehen z. B. bezüglich der Angaben zur Person und zum Umfeld der Ansteckung im Malaria- und im Lepra-Erhebungsbogen.

Noch gravierender als bei der Überwachung nach dem Bundesseuchengesetz ist das Fehlen einer ausreichenden Rechtsgrundlage bei der Führung des Impfschadenregisters. Hier haben einige Bundesländer die der Sache nach erforderlichen Meldungen der einzelnen Schadensfälle bereits eingestellt.

Ich habe ferner die Datenverarbeitung im Personalbereich kontrolliert, und zwar sowohl die automatisierte Verarbeitung der Mitarbeiterdaten als auch die manuelle Verarbeitung in Personalakten und anderen Personalunterlagen.

Bei der Kontrolle der jeweils automatisiert geführten Stellendatei und Personaldatei wurden keine wesentlichen Mängel festgestellt. Einige noch mögliche Verbesserungen wurden zugesagt. Unter Datenschutzaspekten ist zu begrüßen, daß im Personalverwaltungssystem keine sensiblen Daten wie z. B. zur Arbeitsunfähigkeit, dienstliche Beurteilungen oder medizinische Daten gespeichert werden.

Organisation, Führung und Verwaltung der Personalakten des Bundesgesundheitsamtes sind Gegenstand einer „Anweisung zur Führung und Verwaltung der Personalakten des Bundesgesundheitsamtes" (Registraturanweisung P) vom 25. April 1979. Diese internen Richtlinien entsprechen nicht bzw. nicht mehr in allen Einzelregelungen datenschutzrechtlichen Erfordernissen. So fehlen z. B. Regelungen, die eine Abschottung der personalärztlichen Unterlagen und medizinischen Daten in Beihilfevorgängen sicherstellen. Die Kontrolle hat indessen ergeben, daß die Personalaktenführung und -verwaltung sich nicht ausschließlich an den internen Richtlinien ausrichtet, sondern unabhängig hiervon zeitgemäße Gesichtspunkte des Datenschutzes berücksichtigt.

Die festgestellten Einzelheiten der Führung und Verwaltung der Beihilfeunterlagen zeigen eine unter datenschutzrechtlichen Aspekten beispielhafte Praxis der Abschottung sensibler Mitarbeiterdaten.

Anhand von Stichproben wurde die Praxis der Aufbewahrung ärztlicher Gutachten in den Personalakten überprüft. In einem Fall trug der mit Sonderstreifen verschlossene Umschlag die Aufschrift: „Vertraulich — verschlossen — Arztsache: Amtsärztliches Gutachten vom 6. 1. 1984." In einem anderen Fall lautete die Aufschrift: „Attest des Hausarztes, Befund des Vertrauensarztes, geöffnet und verschlossen" nebst Datum und Unterschrift des Personalsachbearbeiters.

Der Leiter des Personalreferats hat in Erwägung gezogen, alle ärztlichen bzw. medizinisch relevanten Unterlagen künftig nur noch beim Betriebsärztlichen Dienst zu führen. Sollte sich dies nicht realisieren lassen, habe ich empfohlen, alle Verschlußumschläge, die ärztliche Gutachten oder Zeugnisse mit medizinischen Daten enthalten, mit folgendem Aufdruck zu versehen: „Vertrauliche Arztsache — nur vom Betriebsarzt zu öffnen."

Die Führung und Verwaltung der personalärztlichen Unterlagen im Betriebsärztlichen Dienst entspricht den datenschutzrechtlichen Erfordernissen, wie sie zwischen dem Leitenden Arzt des Ärztlichen und Sozialen Dienstes der obersten Bundesbehörden im Bundesministerium des Innern und mir vereinbart worden sind. Ich habe darüber in meinem Zweiten Tätigkeitsbericht (S. 23) berichtet. Dies gilt insbesondere für die ärztlichen Untersuchungsunterlagen. Während der Befundbogen beim Ärztlichen Dienst verbleibt, soll das ärztliche Zeugnis über die Einstellungsuntersuchung, das an die Personalabteilung gesandt wird, ausschließlich formularmäßige Angaben über das Bestehen bzw. Nichtbestehen gesundheitlicher Bedenken enthalten, jedoch keine Angaben diagnostischer Art.

Weitere Kontrollen beim Bundesgesundheitsamt, die datenschutzrechtliche Fragen bei der medizinischen Forschung betreffen werden, sind vorgesehen.

17.2 Datenschutz im Krankenhaus

Die Fragen des Datenschutzes im Krankenhaus sind von großer Komplexität. Sie betreffen die Zulässigkeit der Erhebung, Speicherung, Verwendung und Übermittlung/Offenbarung personenbezogener Daten für die unterschiedlichsten Verwendungszwecke innerhalb (der verschiedenen Bereiche) und außerhalb des Krankenhauses, z. B. die verwaltungsmäßige Abwicklung des Behandlungsvertrages (Kostenerstattung), die Behandlung und etwaige Nach- und Weiterbehandlungen, die wissenschaftliche Forschung oder auch gesetzliche Mitteilungspflichten z. B. an den Standesbeamten.

Der gesamte Fragenkomplex ist seit mehreren Jahren Gegenstand von Erörterungen und Verhandlungen in den zuständigen Gremien der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzaufsichtsbehörden der Länder unter Beteiligung der Deutschen Krankenhaus Gesellschaft. Ziel dieser Gespräche ist die Erstellung einer möglichst umfassenden und abschließenden Empfehlung zur Gewährleistung des Datenschutzes bei der Verarbeitung und Verwendung personenbezogener Daten des Patienten im Zusammenhang mit einem Aufenthalt im Krankenhaus, die den Anforderungen des Datenschutzes und der Praxis in gleicher Weise gerecht wird. Eine derartige generelle Gesamtlösung erweist sich wegen der unterschiedlichen Organisationsformen und Aufgabenstellung der verschiedenen Krankenhäuser (allgemeines Krankenhaus, Spezial- und Fachklinik, Universitäts-Klinik) und wegen der Vielfalt der Informationsbeziehungen als zunehmend schwieriger.

Ein unter den Datenschutzbeauftragten des Bundes und der Länder abgestimmtes Zwischenergebnis, basierend auf dem Stand der Erörterungen der Datenschutzaufsichtsbehörden, liegt inzwischen vor.

Abweichend von der ursprünglichen Vorstellung, einen abschließenden Datenkatalog für die Speicherung sowie eine detaillierte Darstellung der zulässigen Informationsbeziehungen zu erstellen, beschränkt sich dieses Zwischenergebnis notgedrungen auf bestimmte Grundaussagen.

Grundlage der Speicherung personenbezogener Daten des Patienten ist der Behandlungsvertrag. Maßstab für die Zulässigkeit der Speicherung personenbezogener Daten ist deren Erforderlichkeit für die ordnungsgemäße Abwicklung des Behandlungsvertrages. Soweit diese Erforderlichkeit gegeben ist, bedarf es keiner Einwilligung des Patienten. Zweifelhaft erscheint in diesem Zusammenhang die (generelle) Speicherung des Geburtsortes und der Staatsangehörigkeit des Patienten, seines Familienstandes und Berufs, sowie der Anzahl der Kinder und des Arbeitgebers. Die Religionszugehörigkeit darf nur gespeichert werden, wenn der Betroffene diese Angaben freiwillig gemacht hat.

Medizinische Angaben sind für die verwaltungsmäßige Abwicklung des Behandlungsvertrages grundsätzlich nicht erforderlich und dürfen deshalb für diesen Zweck nicht gespeichert werden. Soweit einzelne medizinische Daten (z. B. Diagnose) für Verwaltungszwecke (z. B. Abrechnung) benötigt werden, muß der Zugriff der Verwaltung auf die unbedingt erforderlichen Informationen beschränkt werden. Dies führt zu der Frage, inwieweit eine klare Trennung zwischen den Daten, deren Speicherung für die verwaltungsmäßige Abwicklung des Behandlungsvertrages erforderlich ist, und den Daten, deren Speicherung die medizinische Behandlung erfordert, geboten ist. Insoweit kommt einer entsprechenden Zugriffsregelung entscheidende Bedeutung zu.

Für Übermittlungen/Offenbarungen im Rahmen des Behandlungsvertrages bedarf es keiner gesonderten Einwilligung des Patienten. Dies gilt auch für Mitteilungen an Krankentransport-Unternehmen, Diagnostikeinrichtungen, Labors, Apotheken, Orthopädie-Werkstätten u. ä. ärztliche Hilfseinrichtungen, wenn diese Mitteilungen zur Behandlung des Patienten erforderlich sind. Bei einer Weitergabe von Patientenunterlagen an ein nachbehandelndes Krankenhaus bzw. einen niedergelassenen Arzt können aber Zweifel entstehen, ob die Weitergabe dem Willen des Patienten entspricht. Zur Klarstellung sollte hier auf eine entsprechende Äußerung des Patienten nicht verzichtet werden.

Zu Verwaltungszwecken gespeicherte Patientendaten dürfen nur an den Kostenträger und nur im erforderlichen Umfang übermittelt werden. Eine Übermittlung von medizinischen Daten ist nur aufgrund von Rechtsvorschriften oder mit Einwilligung des Betroffenen zulässig. Im Sozialleistungsbereich hat der Betroffene eine Mitwirkungsverpflichtung, der eine Beratungs- und Aufklärungspflicht des Sozialleistungsträgers entspricht. Die Übersendung des vollständigen ärztlichen Entlassungsberichts an den Leistungsträger ist unzulässig. Dem Leistungsträger dürfen nur die zur Prüfung seiner Leistungsverpflichtung erforderlichen Daten, wie Aufnahme- und Entlassungsdiagnosen, Behandlungszeiten, ärztlicher und technischer Leistungsaufwand mitgeteilt werden.

Weitere Einzelheiten, insbesondere zur Weitergabe von Patiendaten an Dritte, bedürfen noch der Untersuchung und Erörterung.

18. Verteidigung

18.1 Wehrersatzwesen

In vielen Eingaben im Berichtsjahr wurden Fragen zum Datenschutz bei den Kreiswehrersatzämtern oder der Bundeswehr gestellt. Die Wehrüberwachung und die Datenverarbeitung im Zusammenhang mit der Kriegsdienstverweigerung interessierten hier besonders. Einige dieser Fälle zeigten, daß die Bindung an den Dateibegriff — also die Gewährung von Rechten des Betroffenen nur bei den Datenverarbeitungen, die mit Dateien erfolgen — häufig zu unbefriedigenden Antworten und Ergebnissen führt. Zum Beispiel richtet sich die Weitergabe von Akten von Wehrpflichtigen innerhalb des Geschäftsbereichs des Bundesministers der Verteidigung ausschließlich nach eigenen Verwaltungsvorschriften des Bundesministers der Verteidigung. Somit greift hier auch mein Kontrollrecht nicht. Gleichwohl ist der Bundesminister der Verteidigung bereit, zu solchen Eingaben zumindest soweit Stellung zu nehmen, daß es mir möglich ist, dem Betroffenen eine weiterführende Antwort zu geben.

Ferner weisen die Fragen in den Eingaben oft auf noch bestehende Probleme des Verfahrens WEWIS (Wehrersatzwesen-Informationssystem) und der dazu gehörigen Organisation in den Wehrbereichen und beim Bundesminister der Verteidigung selbst hin. In den vergangenen Jahren habe ich in diesem Zusammenhang bereits Kontrollen bei Kreiswehrersatzämtern und in einer Wehrbereichsverwaltung vorgenommen. Die dabei gewonnenen Erkenntnisse führen zusammen mit den Hinweisen aus den Eingaben oft zu Empfehlungen zur datenschutzgerechten Organisation im Aufgabenbereich Wehrpflicht. Dies geschieht in enger Zusammenarbeit mit dem Datenschutzbeauftragten des Bundesministers der Verteidigung. So wurde aufgrund meiner Anregung veranlaßt, daß auf alle Listen, die von WEWIS erstellt werden, ein Vernichtungsdatum gedruckt wird. Damit wird jeder Empfänger daran erinnert, daß die Liste nur begrenzt aufbewahrt werden darf, und die Vorgesetzten bzw. die Fachaufsicht können bei Kontrollen leichter feststellen, ob Weisungen beachtet werden.

Ich erwähne die Eingaben zur Wehrpflicht, weil sie verdeutlichen, daß umfangreiche, tratitionell geprägte Aufgaben nur in einem langdauernden Prozeß den Anforderungen eines zeitgemäßen Datenschutzes angepaßt werden können. Dies gilt besonders für einen so großen und komplexen, zentral organisierten Geschäftsbereich wie den des Bundesministers der Verteidigung. Ich gehe jedoch davon aus, daß durch meine ständige Beschäftigung

mit diesem Bereich und die konstruktive Zusammenarbeit mit dem BMVg datenschutzgerechte Weisungen, Erlasse oder Richtlinien geschaffen werden.

18.2 WEWIS

Nach vorangegangenen Kontrollen in mehreren Kreiswehrersatzämtern habe ich im Berichtsjahr das weitgehend zentralisierte und automatisierte Wehrersatzwesen-Informationssystem (WEWIS) geprüft. Dazu habe ich die aktuelle Version des Verfahrens, die WEWIS-Dateien, Datensätze, Regelungen für Online-Zugriffe und die password-Organisationen kontrolliert.

WEWIS unterstützt die Aufgaben nach dem Wehrpflichtgesetz. Dazu gehören u. a. die Wehrerfassung, die Vorbereitung der Musterung und des Eignungs- und Verwendungstests, die Einberufung zum Grundwehrdienst, die personelle Vorbereitung der Mobilmachung und die Wehrüberwachung. WEWIS dient der Arbeit von 97 Kreiswehrersatzämtern und 6 Wehrbereichsverwaltungen, des Bundeswehrverwaltungsamtes und des Bundesministers der Verteidigung; die jeweiligen Daten-Bestände werden bei 6 Rechenzentren geführt. Es gibt einen verkürzten zentralen Bestand (u. a. ohne Namen und Anschrift). Die Wehrbereichsverwaltungen verfügen lediglich über die Daten der Wehrpflichtigen, für die sie zuständig sind. In WEWIS werden zur Zeit rd. 5 Millionen Datensätze von Reservisten und Ersatzreservisten, die in Wehrüberwachung stehen, verwaltet. Auf die jeweiligen Datenbestände kann im Rahmen der Zuständigkeit online zugegriffen werden.

Die Kontrolle der Erforderlichkeit von Datenfeldern in den WEWIS-Dateien und in allen verarbeiteten Datensätzen ist noch nicht abgeschlossen. Der Schwerpunkt der bisherigen Kontrollen lag vielmehr bei technischen und organisatorischen Maßnahmen zur Sicherheit. Diese gingen zum Teil über WEWIS hinaus, weil hier ein enger Zusammenhang mit der Sicherheit der sonstigen Datenverarbeitung beim Bundesminister der Verteidigung besteht. Dabei ging es u. a. um die richtig organisierte Anwendung eines eingekauften Software-Produktes und dessen Verträglichkeit mit einer Sicherheits-Software desselben großen Computer-Herstellers. Ferner wurde empfohlen, die password-Organisation und die Dokumentation von Online-Zugriffen auf WEWIS zu verbessern und eine neue Konzeption der internen Anwendungskontrolle von WEWIS zu entwickeln. Die Verbesserung der password-Organisation und der Dokumentation von Online-Zugriffen wurden bereits veranlaßt. In diesem Zusammenhang sind auch die nachfolgenden Ausführungen zu sehen. Die Kontrolle von WEWIS wird fortgesetzt.

18.3 Nutzung von WEWIS in einem Disziplinarverfahren

Aufgrund der Ermittlungen des Militärischen Abschirmdienstes waren gegen einen General der Bundeswehr schwerwiegende Sicherheitsbedenken erhoben worden. Um diese zu entkräften, hat der General ein Disziplinarverfahren gegen sich beantragt. Im Zuge der Vorermittlungen in dieser Disziplinarsache wurde von einem Schweizer Journalisten ein Tonband-Protokoll übergeben, auf dem ein Reservist der Bundeswehr namens „Achim Müller" vermeintlich sachdienliche Aussagen zu diesem Fall gemacht hatte. Um „Achim Müller" als Zeugen vernehmen zu können, sollte versucht werden, seinen Aufenthaltsort zu ermitteln. Aus den vorliegenden Unterlagen konnte der mögliche Aufenthaltsort auf zwei Wehrbereiche eingegrenzt werden. Zur Feststellung des Aufenthaltsorts wurde eine entsprechende WEWIS-Auswertung vorgenommen.

Sie ergab eine Liste von mehreren tausend Datensätzen von Personen aus vier Wehrbereichen, die in einem bestimmten Zeitraum, der ebenfalls aus dem Tonbandprotokoll zu entnehmen war, in der Bundeswehr gedient hatten. In der dem Wehrdisziplinaranwalt überlassenen Liste hat dieser dann 22 Personen aus den zwei Wehrbereichen festgestellt, in denen „Achim Müller" nach den von Anfang an vorliegenden Unterlagen möglicherweise seinen Wohnsitz haben konnte. Zu diesen 22 Personen wurden bei den zuständigen Kreiswehrersatzämtern die Personalakten angefordert. Deren Durchsicht ergab keinerlei Hinweis darauf, daß ein Reservist „Achim Müller" tatsächlich existierte.

Im Rahmen der Ermittlungen wurden außerdem die Besucherzettel des Bundesministeriums der Verteidigung aus dem Zeitraum überprüft, in dem der General im Ministerium Dienst geleistet hatte. Die Daten derjenigen Besucher, die ihn in dieser Zeit besucht hatten, wurden beim Bundeszentralregister in Berlin abgefragt. Dies sollte ebenfalls dazu führen, mögliche Zeugen in der Disziplinarsache feststellen und vernehmen zu können. Als Grundlage der Anfrage war angegeben: „Besucherüberprüfung".

In meinem Prüfbericht habe ich gegenüber dem Bundesminister der Verteidigung die geschilderte Auswertung in WEWIS beanstandet, weil

- nach meiner Ansicht die bestehenden Rechtsvorschriften keine hinreichende Rechtsgrundlage für eine Maßnahme dieser Art bieten,
- nach meiner Auffassung der Verhältnismäßigkeitsgrundsatz nicht eingehalten war,
- bei der Durchführung der Maßnahme an den Wehrdisziplinaranwalt mehr Daten übermittelt wurden als erforderlich, da bereits vor der WEWIS-Bestandsauswertung eine Eingrenzung auf die Datensätze von zwei Wehrbereichen möglich gewesen wäre.
- das gesamte Verfahren nicht schriftlich dokumentiert und damit für mich nur schwer nachprüfbar war.

Die Anfrage an das Bundeszentralregister habe ich bemängelt, da der Grund der Anfrage nicht korrekt angegeben war.

In seiner Stellungnahme hat der Bundesminister der Verteidigung im wesentlichen Rechtsansichten vertreten, die mit meiner Auffassung nicht übereinstimmen.

Auf Anforderung des Innenausschusses des Deutschen Bundestages habe ich aufgrund meiner Unterrichtungspflicht gemäß § 19 Abs. 2 BDSG dem Vorsitzenden u. a. meinen Prüfbericht und die Stellungnahme des Bundesministers der Verteidigung (mit dessen Einverständnis) hierzu übersandt.

18.4 Institut für Wehrmedizinalstatistik und ärztliches Berichtswesen

In meinem Sechsten Tätigkeitsbericht (S. 53) hatte ich berichtet, daß die Unterlagen im Institut für Wehrmedizinalstatistik und ärztliches Berichtswesen in Remagen sowohl solche Gesundheitsdaten, die während ärztlicher Behandlungen entstanden sind, als auch ärztliche Gutachten enthalten, die über die Verwendungsfähigkeit des Soldaten Auskunft geben. Ich hatte beim Bundesminister der Verteidigung angeregt zu prüfen, ob beide Datenarten voneinander getrennt werden können.

Der Bundesminister der Verteidigung hat jetzt zwar eingeräumt, daß eine solche Trennung die Entscheidung der Ärzte darüber erleichtern könne, welche Unterlagen den um Überlassung ersuchenden Stellen im Rahmen der Einwilligung des Betroffenen zur Verfügung gestellt werden können. Im Geschäftsbereich des Bundesministeriums der Verteidigung sprächen jedoch gewichtige Gründe gegen eine solche Maßnahme. Die im Bereich der Streitkräfte eingesetzten Ärzte seien fast ausschließlich als behandelnde Ärzte *und* Gutachter tätig. Diese beiden Tätigkeiten vermischten sich derart, daß eine Trennung der ärztlichen Unterlagen unter dem Gesichtspunkt, ob es sich um therapeutische Aufzeichnungen oder um gutachterliche Aussagen handele, nicht möglich sei.

Diese Stellungnahme widerspricht Äußerungen von Angehörigen des Instituts, die in Gesprächen während meiner damaligen Kontrolle die Trennung für durchführbar hielten.

19. Öffentliche Sicherheit — Allgemeines

19.1 Tätigkeitsüberblick

19.1.1 Kontrolltätigkeit im Sicherheitsbereich

Meine Kontrolltätigkeit im Sicherheitsbereich bezog sich in den letzten Jahren jeweils auf bestimmte Ausschnitte der Datenverarbeitung bei den einzelnen Behörden, nämlich

- 1981 auf die Prüfung der Datei PIOS beim Bundeskriminalamt (vgl. 4. TB 22 f.);
- 1982 auf die Prüfung der Abteilung II des Amtes für Sicherheit der Bundeswehr — jetzt Amt des MAD — (verfassungsfeindliche Bestrebungen mit Bundeswehrbezug; sog. Zersetzungsabwehr), der Abteilung Staatsschutz und des Interpolverkehrs des Bundeskriminalamtes sowie des Bundesnachrichtendienstes (vgl. 5. TB S. 89 f., 91 f., 95 ff.);
- 1983 schließlich auf die bisher umfangreichste Einzelprüfung bei den Sicherheitsbehörden (Abteilung III — Linksextremismus — des Bundesamtes für Verfassungsschutz).

Demgegenüber war die Kontrolltätigkeit 1984 bewußt durch eine Reihe kürzerer Prüfungen einzelner Problembereiche bei den Sicherheitsbehörden gekennzeichnet. Der Grund hierfür lag vor allem darin, daß Schwerpunktprüfungen, die zum Teil mehrere Monate in Anspruch nahmen, aufgrund der vorhandenen Arbeitskapazität des zuständigen Referates nur begrenzt möglich sind, zumal wichtige andere Bereiche nicht völlig ausgespart werden können. Dennoch war es möglich, eine Reihe von kürzeren Kontrollen durchzuführen. Zu nennen sind vor allem

- beim Bundeskriminalamt: die Prüfung der Datei „Lage I", die aus Anlaß der Demonstrationen gegen den NATO-Doppelbeschluß im Herbst 1983 eingerichtet worden war;
- beim Bundesamt für Verfassungsschutz: die Prüfung der Übermittlung von Daten an ausländische Dienststellen;
- beim Bundesnachrichtendienst: zwei Querschnittsprüfungen mit den Schwerpunkten Auskunftstätigkeit allgemein sowie Speicherung in bestimmten Bereichen;
- beim Militärischen Abschirmdienst: eine intensive Erfolgskontrolle im Nachgang zu meinem Prüfbericht von 1982; ferner die bei Drucklegung noch nicht ausgewertete Prüfung der MAD-Gruppe VI in München sowie Kontrollen im Bereich Militärischer Abschirmdienst und beim Bundesminister der Verteidigung betreffend bestimmte Maßnahmen der Datenverarbeitung aus Anlaß der Ermittlungen in einem Disziplinarverfahren.

Daneben wurde eine Vielzahl von Prüfungen aufgrund von Einzeleingaben oder Einzelereignissen vor Ort durchgeführt. Zu nennen ist hierbei vor allem die Prüfung der Mitarbeit des Bundeskriminalamtes im Zusammenhang mit der Aktion „Gitternetz" des Landes Rheinland-Pfalz (vgl. hierzu Nr. 20.1.1).

19.1.2 Mitarbeit an neuen Regelungen

Neben der Kontrolltätigkeit wurden in vielen Tätigkeitsbereichen Stellungnahmen für die Neugestaltung bestehender Vorschriften, die erstmalige Erarbeitung von Grundregelungen und die Umgestaltung bestimmter Maßnahmen der Datenverarbeitung im Sicherheitsbereich abgegeben:

Zu nennen sind u. a.:

- Richtlinien über die Sicherheitsüberprüfung;

— Richtlinien über die Zusammenarbeit zwischen Grenzpolizei und Nachrichtendiensten;

— Richtlinien für den Aufbau eines Grenzaktennachweises als Grundlage für die Datenverarbeitung des Grenzschutzeinzeldienstes;

— Neugestaltung der Datenverarbeitung beim Militärischen Abschirmdienst unter jeweiliger Einbeziehung meiner Vorschläge aus früheren Prüfungen;

— Neuregelung des Ausländerzentralregisters, soweit es die Sicherheitsbehörden anbelangt (hierzu s. oben Nr. 2.2);

19.1.3 Erreichte Verbesserungen

Die im Zusammenhang mit meiner Kontroll- und Beratungstätigkeit bisher erreichten Verbesserungen lassen sich dabei im wesentlichen wie folgt zusammenfassen:

— Bei der Zulässigkeit der Speicherung wird die Erforderlichkeit zum Teil strenger geprüft als bisher. In Zweifelsfällen werden zunehmend kürzere Überprüfungsfristen vorgesehen.

— Bei der Übermittlung an andere Stellen wird prinzipiell eine größere Restriktion angestrebt, insbesondere soweit es den nachrichtendienstlichen Bereich betrifft.

— Generell wird mehr auf Relevanz und Richtigkeit eigener Unterlagen vor Auskunftserteilung an andere Stellen geachtet, insbesondere dann, wenn die Unterlagen nicht auf eigenen Erkenntnissen beruhen.

— Bei der Löschung wird der Abbau der sogenannten Altfälle verstärkt vorangetrieben (das sind Fälle, deren letzte Erkenntnis nach dem Stand der gegenwärtigen innerdienstlichen Richtlinien mehr als 10 Jahre im polizeilichen Bereich bzw. 15 Jahre im nachrichtendienstlichen Bereich zurückliegt).

  Die Einhaltung von Überprüfungsfristen wird für die Zukunft technisch-organisatorisch verbessert.

— Speziell für die Übermittlung an ausländische Behörden wurde eine Reihe von datenschutzrechtlichen Verbesserungen seitens des Bundeskriminalamtes für den polizeilichen Bereich und seitens des Bundesamtes für Verfassungsschutz für den nachrichtendienstlichen Bereich zugesagt, die ich aufgrund meiner einschlägigen Kontrolltätigkeit angeregt hatte. Die Auswirkungen und Einhaltung dieser Zusagen werde ich im nächsten Jahr überprüfen.

All dies darf jedoch nicht darüber hinwegtäuschen, daß es noch eine Vielzahl offener Fragen gibt, deren Lösung seit Jahren angemahnt, aber bisher nicht erreicht wurde. Darüber hinaus gibt es zunehmend neue Probleme, die aufgrund neuer technischer Verfahrensweisen zu bedenken und nach Möglichkeit vor Einsatz der Techniken zufriedenstellend zu lösen sind (hierzu näher Nr. 19.2 und 20.1).

19.1.4

Schließlich ist meine Mitarbeit in nationalen und internationalen Gremien der Datenschutzbeauftragten zu erwähnen (Arbeitskreise Sicherheit und Polizeirecht der Datenschutzbeauftragten des Bundes und der Länder; Internationale Konferenz der Datenschutzkontrollinstitutionen; Arbeitsgruppe „Datenschutz im Polizeibereich" beim Europarat), die einen erheblichen Arbeitsaufwand erforderte.

19.2 Übergreifende Probleme

Im folgenden soll auf die wichtigsten Probleme aufmerksam gemacht werden, die sich bei allen Sicherheitsbehörden — allerdings mit zum Teil unterschiedlichen Gewichtungen — stellen. Dabei ist vorab darauf hinzuweisen, daß diese Auflistung nicht den Eindruck erwecken soll, die gesamte Datenverarbeitung bei den Sicherheitsbehörden des Bundes sei gekennzeichnet von diesen Problemschwerpunkten. Vieles ist aus der Sicht des Datenschutzes besser geworden, vieles wird inhaltlich bereits in einer Weise abgewickelt, wie es die noch fehlende gesetzliche Grundlage vorsehen sollte. Gerade die Darstellung zu Nr. 19.1.3 soll dies belegen. Ein großer Teil der Praxis der Datenverarbeitung ist jedoch aus datenschutzrechtlicher Sicht noch unbefriedigend, obwohl seit Jahren auf Abhilfe gedrängt wurde. Andere Fragen haben sich erst in letzter Zeit anhand neuer Datenverarbeitungsvorhaben oder im Zusammenhang mit Prüfungen der jüngsten Zeit gestellt.

In allen Fällen ergibt sich die Notwendigkeit, hierauf gesondert einzugehen, vor allem vor dem Hintergrund des Urteils des Bundesverfassungsgerichts zum Volkszählungsgesetz. Die dort aufgestellten Grundsätze für die Datenverarbeitung durch den Staat sind gerade für den Sicherheitsbereich besonders wichtig, da es hier ganz überwiegend um informationelle Tätigkeit geht, die entweder aufgrund von Maßnahmen erfolgt, die gegebenenfalls zwangsweise durchgesetzt werden können (so z. B. der gesamte Bereich der offenen polizeilichen Personenkontrolle) oder die heimlich geschehen (so zum Teil durch die Polizeibehörden und die überwiegende Tätigkeit der Nachrichtendienste). Für die Zulässigkeit dieser Maßnahmen bedarf es daher jeweils „bereichsspezifischer, präziser und amtshilfefester" Regelungen, wie sie von den Datenschutzbeauftragten des Bundes und der Länder seit Jahren gefordert, aber bisher nicht oder nur unzureichend erlassen wurden. Dies gilt für alle Phasen sicherheitsbehördlicher Datenverarbeitung und — allerdings in unterschiedlichen Abstufungen — für alle Sicherheitsbehörden des Bundes, und nicht nur etwa für BND und MAD, bei denen allerdings bisher die größten Regelungslücken bestehen.

Hierbei handelt es sich um

— offene Fragen beim Umfang der Erhebung und Speicherung von Daten sowohl hinsichtlich des betroffenen Personenkreises als auch des Inhalts der Speicherung;

— ungelöste Probleme bei der Übermittlung, Verwertung und Zweckbindung der Daten,

— Pflichten zum und beim Löschen von Daten,

— die Verbesserung der Transparenz und

— die Notwendigkeit gesetzlicher Regelungen im nationalen und internationalen Bereich.

19.2.1 Umfang der Datenerhebung und -speicherung

Mangelnde Erforderlichkeit der Speicherung

Im folgenden nenne ich Fälle, in denen mir die Erforderlichkeit der Speicherung oder die dafür herangezogene Rechtsgrundlage zweifelhaft erscheint:

— Zum Teil werden personenbezogene Daten allein aufgrund der Anfrage einer anderen Dienststelle registriert (z. B. beim Bundesgrenzschutz, vgl. schon die Kritik im 6. TB S. 48).

— In der Haftdatei des BKA wird auch nach Ablauf der Haft die Speicherung von personenbezogenen Daten generell für fünf bzw. zwei Jahre aufrechterhalten (die Unterscheidung richtet sich danach, ob zu der betreffenden Person eine Speicherung im überregionalen Kriminalaktennachweis vorliegt oder nicht). Diese pauschale, wenn auch zeitlich abgestufte Speicherung nach Haftende kann weder aus § 4 BKAG noch aus Gründen konkreter Gefahrenabwehr gerechtfertigt werden.

— Ähnlich zu beurteilen ist die generelle Aufrechterhaltung der Speicherung von Daten vermißter und unbekannter, hilfloser Personen auch nach der jeweiligen Aufklärung des Falles.

— Häufig wird nur auf formale Feststellungen abgestellt, ohne deren Hintergründe zu berücksichtigen. Dies geschieht z. B. bei der Meldung und/oder Speicherung personenbezogener Daten von Begleitpersonen im Rahmen der polizeilichen Beobachtung, bei der Datenverarbeitung zu Personen im Zusammenhang mit ihrer Teilnahme an bestimmten Veranstaltungen, wegen des Aufenthalts oder der Wohnung in bestimmten Gegenden oder des einmaligen Betretens bestimmter Gebäude unter Umständen sogar auf Einladung der betreffenden Behörde selbst (jeweils bei Polizei und Nachrichtendiensten).

— Oft erfolgen unnötige Parallelspeicherungen. Ein Beispiel hierfür sind die in Dateien verschiedener Sicherheitsbehörden geführten Hinweise auf die im Bundeszentralregister eingetragenen Straftaten. Da die betreffenden Behörden jederzeit grundsätzlich Auskunft vom BZR erhalten können, besteht für die Parallelspeicherung kein Anlaß. Außerdem ist nicht auszuschließen, daß hierdurch die Regelungen des BZRG unterlaufen werden. Ein weiteres Beispiel für diese Fallgruppe ist die sogenannte personelle Vorbeugung durch den MAD (s. u. Nr. 21.3).

— Problematisch erscheint im polizeilichen Bereich die stetige Zunahme der Speicherung von Daten sogenannter „anderer Personen". Dies sind Personen, die weder Störer noch Straftatverdächtige oder Beschuldigte sind. Dieser Personenkreis ist prinzipiell zur Speicherung für die PIOS-Anwendungen und für Spurendokumentationsverfahren vorgesehen. Bedenken haben die Datenschutzbeauftragten dagegen schon anläßlich der Inkraftsetzung der Dateienrichtlinien erhoben, die die Speicherung dieser Personen in Nr. 4.2.11 vorsehen (s. GMBl. 1981 S. 114). Leider hat dies nicht zu einer Änderung oder wenigstens restriktiven Handhabung dieser Regelung geführt. Vielmehr ist zu befürchten, daß mehr und mehr Daten zur Verdachtsgewinnung, also im Vorfeld konkreter polizeilicher Gefahren oder — für die Nachrichtendienste — konkreter Anhaltspunkte verarbeitet werden. Vorhaben wie „Massendatenverarbeitung" für den polizeilichen Bereich oder die „personelle Vorbeugung" für den nachrichtendienstlichen Bereich (hier MAD), mögen dies verdeutlichen (näher hierzu Nr. 20.1 und 21.3).

— Gleiches gilt auch für die seit Jahren umstrittene Rasterfahndung. Hier wird nicht auf konkrete Verdachtsmomente, sondern auf die Kumulierung bestimmter Verhaltensweisen abgestellt, um mit Hilfe automatisierter Verfahren Anhaltspunkte für einen Straftat- oder Störerverdacht zu erhalten. Der (möglicherweise) konkrete Verdacht steht also am Ende, nicht am Anfang der Maßnahme. Das geltende Polizei- und Stafverfahrensrecht enthält hierfür keine Rechtsgrundlagen, zumindest keine solchen, die den Anforderungen der Normenklarheit entsprechen.

Zunehmende Dateienvielfalt

In immer größerem Umfange werden für die verschiedenen Deliktsgruppen oder für bestimmte nachrichtendienstliche Bereiche Spezialdateien eingerichtet. Dies führt dazu, daß die Daten über eine Person nicht mehr — wie in den Anfängen der Datenverarbeitung — in nur wenigen Aktenhinweisdateien verzeichnet sind. Vielmehr finden sie sich in aller Regel in einer Vielzahl von Dateien unter jeweils verschiedenen Aspekten wieder. Da die verschiedenen Dateien jeweils eigene Regelungen haben (z. B. für die Übermittlung oder für die Löschung), besteht die Gefahr von Fehlern bei der Pflege der Dateninhalte; dabei auftretende Probleme vervielfachen sich. Als Beispiel hierzu soll aufgeführt werden, in wie vielen Dateien die personenbezogenen Daten einer Person gespeichert sein können, die — kein seltener Fall — im Zusammenhang mit der Teilnahme an Gewalttätigkeiten bei Demonstrationen (nicht selten auch nur wegen der bloßen Teilnahme an einer solchen Demonstration) überprüft und ed-behandelt wurde: bei der sachbearbeitenden Dienststelle und beim LKA in den von Land zu Land in verschiedenem Umfang bestehenden Dateien; beim BKA in aller Regel im überregionalen KAN sowie in den Dateien Erkennungsdienst und Daktyloskopie; seitens der Abteilung Staatsschutz des BKA darüber hinaus zur Zeit (noch) in NADIS (künftig in APIS) und in der Datei Landfrie-

densbruch. Schließlich ist nicht ausgeschlossen, daß eine weitere Speicherung in PIOS unter dem jeweils einschlägigen Aspekt vorgenommen wird. Sofern eine spezielle Spurendokumentationsdatei unter den Aspekten der Strafverfolgung oder der Gefahrenabwehr im Zusammenhang mit solchen Demonstrationen eingerichtet ist, sind die Daten auch dort registriert. Daneben wird aufgrund der verschiedenen Meldedienste zwischen Polizei und Nachrichtendiensten dieser Person eine Speicherung sowohl durch das zuständige Landesamt als auch das Bundesamt für Verfassungsschutz erfolgen. Sofern die Demonstration im Zusammenhang mit militärischen Angelegenheiten steht, ist auch von verschiedenen Speicherungen beim MAD auszugehen; unter besonderen Umständen kann auch eine zusätzliche Speicherung beim BND stattfinden. Wurde in diesem Zusammenhang z. B. eine Erkenntnisfrage an die Grenzschutzdirektion des BGS gestellt, so ist nach der gegenwärtigen Praxis auch dort von einer Speicherung im Grenzaktennachweis auszugehen. Dies macht beispielhaft einerseits die Schwierigkeiten der datenschutzrechtlichen Kontrolle deutlich und zeigt andererseits auch auf, wie wichtig es ist, die übergreifenden Grundfragen sobald wie möglich für alle Behörden zu lösen.

Inhalt der Speicherung

Inhaltliche Probleme stellen sich bei der Speicherung personengebundener Hinweise (Merkmale, Wertungen etc.). Zu nennen sind aus dem polizeilichen Bereich die bereits in der Öffentlichkeit bekanntgewordenen Merkmale „Stadt- und Landstreicher", „häufig wechselnder Aufenthaltsort", „Prostituierte", „Freitodgefahr" und „gewalttätig". Merkmale vergleichbarer Art können insbesondere bei den Verfassungsschutzbehörden und beim MAD gespeichert werden. Es wird m. E. nicht ausreichend geprüft, ob es für die Sachentscheidung, z. B. eine Sicherheitsüberprüfung, nicht ausreicht, wenn die entsprechenden Hinweise sich in der Akte befinden. Auch muß die Erforderlichkeit in den verschiedenen Dateien differenziert betrachtet werden. So sind bestimmte personengebundene Hinweise wie etwa „Freitodgefahr", „gewalttätig" oder „Betäubungsmittelkonsument" in einer Fahndungsdatei der Polizei zu bejahen. Anders ist indes die Erforderlichkeit in Aktenhinweisdateien wie dem KAN oder in Aktenerschließungssystemen zu beurteilen. Hinzu kommt die Gefahr, daß schon aufgrund solcher Merkmale Entscheidungen getroffen werden, obwohl ein solcher Hinweis zwangsläufig verkürzt ist und — wie nicht selten festzustellen ist — sich nach dem Inhalt der Akte nicht immer rechtfertigen läßt. (Zu den Gefahren einer Entscheidung allein aufgrund der Speicherung vgl. schon 3. TB S. 16; in der Prüfpraxis wurden Beispiele beim MAD hierfür festgestellt im Zusammenhang mit den Kontrollen im Jahre 1982.)

Art der Speicherung

Es ist zu unterscheiden, ob eine Speicherung mehr verwaltungsmäßigen oder mehr nachrichtendienstlichen oder polizeilichen Charakter hat. Ist ersteres der Fall, so müssen die Daten streng von den polizeilichen oder nachrichtendienstlichen Informationen getrennt werden. Denn bei einer Anfrage zu einer bestimmten Person, die mit der betreffenden Behörde bisher nur einen allgemeinen oder verwaltungsmäßigen Kontakt hatte (z. B. als Petent, der um Auskunft nachsucht oder als Anzeigeerstatter), darf keine Auskunft aus dem System INPOL oder NADIS erteilt werden. Eine Vermischung solcher unverfänglichen Daten mit den Daten, die im Zusammenhang mit polizeilicher oder nachrichtendienstlicher Tätigkeit im engeren Sinn gespeichert wurden, wäre unzulässig (zum Sonderfall der Registrierung von ed-Unterlagen über Asylbewerber nach § 13 AsylVerfG siehe jedoch zu Nr. 20.1). Diesen von mir seit Jahren erhobenen Forderungen hat das BKA dadurch Rechnung getragen, daß es einen eigenen internen Vorgangsnachweis Personalien (VNP) eingerichtet hat, der nicht dem allgemeinen Zugriff auf das System INPOL unterliegt. Allerdings ist das BKA der Auffassung, daß dieser Nachweis jeder Stelle im BKA als interne Datei zur Verfügung stehen muß, so daß es möglich ist, im Zusammenhang mit jeder kriminalpolizeilichen Sachbearbeitung auch die Datei VNP abzufragen. Ich halte hier eine Änderung für geboten, die den Zugriff auf die allein mit allgemeiner Verwaltung befaßten Stellen beschränkt.

Wie wichtig diese Forderung ist, zeigt die Tatsache, daß bei den Polizeien die Dokumentation von Ablauf und Grundlagen polizeilichen Handelns zunehmend automatisiert und nicht mehr wie bisher in Tagebüchern, Listen usw. erfolgt (z. B. Einsatz-Leitsysteme). Dies bedeutet, daß alle personenbezogenen Daten, die im Zusammenhang mit der Ablaufdokumentation anfallen, künftig jederzeit in jeder beliebig auswertbaren Form zur Verfügung stehen. Deshalb ist dafür Sorge zu tragen, daß diese Daten nicht fälschlich in einen kriminalpolizeilichen Kontext gelangen. Dies ist gleichzeitig ein Beispiel für die Veränderung von Wertungen, wenn automatisierte Verfahren eingesetzt werden: Solange die Ablaufdokumentation manuell in Buchform oder in ähnlicher Weise stattfand, war dies kaum ein Problem. Mit der Automatisierung und der damit beliebig möglichen Auswertung ergeben sich nunmehr Fragestellungen, die rechtzeitig einer Lösung bedürfen.

19.2.2 Übermittlung, Verwertung, Zweckbindung

Da Daten durch eine Übermittlung in aller Regel den ursprünglichen Kontext verlassen, u. U. neuen Regelungen und neuen Beurteilungen unterliegen und außerdem eventuelle ursprüngliche Fehler vervielfältigt werden, ist die Übermittlung ein zentrales Problem des Datenschutzes. Hierzu wurden bereits im Sechsten Tätigkeitsbericht (S. 39f.) allgemeine Aussagen gemacht. In Ergänzung hierzu ist festzuhalten:

— Die Praxis der Übermittlung zwischen Polizeibehörden und Nachrichtendiensten bedarf einer sorgfältigen Analyse; nach meinen Erfahrungen

wird sie zu großzügig und insbesondere nicht immer mit dem Trennungsgebot vereinbar gehandhabt.

— Es muß sorgfältig geprüft werden, ob die vorhandenen Daten wirklich noch für die eigene Tätigkeit erforderlich und damit rechtmäßig gespeichert sind. Denn nur dann ist eine Übermittlung zulässig.

— Dieses Gebot gilt insbesondere dann, wenn ausländische Dienststellen nach Erkenntnissen bei inländischen Sicherheitsbehörden anfragen. Generell ist hier bei der Übermittlung besonders restriktiv zu verfahren.

— Hat eine Übermittlung stattgefunden, so ist grundsätzlich ein Nachbericht geboten, wenn nachträglich wichtige Änderungen eintreten oder bekannt werden, um der Stelle, die Auskunft erhalten hat, die Möglichkeit zur Überprüfung der Erforderlichkeit der eigenen Unterlagen zu eröffnen. In der Praxis geschieht dies überwiegend nicht. Selbst seit Jahren bestehende Regelungen, wie die Meldungen der Staatsanwaltschaften oder Gerichte an die Polizei nach Nr. 11 MiStra, werden bisher nur ungenügend beachtet.

— Die Relevanzprüfung für die Übermittlung setzt eine genaue Angabe des Zweckes der Anfrage voraus; hieran fehlt es noch oft. Im Berichtsjahr wurde z. B. festgestellt, daß seitens einer Behörde beim Anfragegrund keinerlei Differenzierung danach vorgenommen wurde, ob die erbetene Übermittlung für weitere eigene inländische Tätigkeit oder für die Weiterleitung an ausländische Dienste dienen sollte (näher s. u. Nr. 21.1).

— Die vom Bundesverfassungsgericht anerkannte „informationelle Gewaltenteilung" (BVerfGE 65, 1, 69) erfordert Zurückhaltung bei der Einrichtung von Online-Anschlüssen. Online-Verbindungen zwischen Sicherheitsbehörden verschiedener Art und Sicherheitsbehörden mit dritten Behörden müssen die Ausnahme sein. Zu Recht wurden daher z. B. bereits 1979 im Hinblick auf die Forderungen des BfD bestehende Online-Anschlüsse zwischen BfV und BKA aufgehoben bzw. weitgehend reduziert (s. 2. TB S. 45).

19.2.3 Löschen von Daten

Erzielte Fortschritte

— Altfälle, also solche, bei denen in der Regel seit mehr als zehn Jahren im polizeilichen oder mehr als 15 Jahre im nachrichtendienstlichen Bereich keine neue Erkenntnis angefallen ist, müssen vordringlich bereinigt werden. Die Sicherheitsbehörden des Bundes haben hier — allerdings in unterschiedlichem Umfang — erhebliche Anstrengungen unternommen. Die Bereinigung dient auch dem Interesse der Behörden selbst, die sich damit von unnötigem Ballast befreien. Vor allem aber bedeutet sie für den Bürger die Gewißheit, daß es wirklich ein „programmiertes Vergessen" gibt.

— Löschung heißt prinzipiell physikalisches Löschen: Dies kann u. a. geschehen durch Überschreiben des entsprechenden Bandes oder durch Vernichtung des Datenträgers. In den Sicherungsbändern muß die Löschung in einem vertretbaren zeitlichen Abstand zur Löschung im Auskunftsbestand erfolgen. Die Fristen liegen in der Regel zwischen vier Wochen und drei Monaten. Beim MAD sind die Fristen von zwei bis drei Jahren für die Löschung in den Sicherungsbändern derzeit noch zu lang. Hier sind die Gespräche noch nicht abgeschlossen; ich gehe davon aus, daß eine entsprechende Verkürzung erreichbar ist. Wichtig ist, daß Sicherungsbänder nur noch ausschließlich zur Datensicherung und nicht mehr zur Auskunftserteilung verwendet werden. Für die Polizei sei hierfür auch auf Nr. 6.1.2 der Dateienrichtlinien hingewiesen. Soweit Änderungsprotokolle und/oder Abfrageprotokolle gefertigt werden (auf letzteres wird zu Recht bisher beim BKA verzichtet), werden diese in einem angemessenen Zeitraum nach der Löschung im aktuellen Bestand bereinigt oder es ist sichergestellt, daß sie nur in speziellen Fällen (z. B. zur Spionageabwehr — einem der Hauptzwecke des Abfrageprotokolls im nachrichtendienstlichen Bereich) und nur unter erheblichen verfahrensmäßigen Sicherungen verwertet werden. Im BfV z. B. bedarf es dafür der Zustimmung des Präsidenten.

  Besteht eine Personenakte zu dem Datensatz, der gelöscht wird, so ist diese Akte zu vernichten. Bei Organisations- oder Sachakten ist dies regelmäßig nicht möglich, da hier der Sachkomplex oder die Organisation in Frage steht und die Löschung einzelner Daten nicht den Vorgang als solchen überflüssig macht. Ich bemühe mich hier aber darum, daß jedenfalls dann, wenn der Aufwand vertretbar ist, die Hinweise auf Personen, deren Daten gelöscht werden, in der Sach- oder Organisationsakte geschwärzt oder entsprechende Teilvorgänge vernichtet werden. Nur so läßt sich sicherstellen, daß die personenbezogenen Daten des Betroffenen nicht bei Bedarf doch wieder verwertet werden.

Noch offene Fragen zur Löschung

— Prüfung der Löschungsvoraussetzungen in allen Dateien

  Die Löschung personenbezogener Daten in einer Datei hat nicht zwangsläufig die Löschung auch in einer anderen Datei der gleichen Dienststelle oder gar anderer Dienststellen, an die Erkenntnisse übermittelt wurden, zur Folge. Daher muß die für die andere Datei verantwortliche Stelle von der Löschung benachrichtigt werden, damit sie ihrerseits überprüft, ob nicht auch sie löschen bzw. ihren Vorgang vernichten muß. Dies ist besonders wichtig bei Verbunddateien wie NADIS oder INPOL, wenn Daten zu einer Person auch bei angeschlossenen Teilnehmern

des Systems gespeichert sind. Unterschiedliche Notierungen beruhen oft auf dem gleichen Sachverhalt (vgl. das Beispiel oben zu Nr. 19.2.1 (zunehmende Dateienvielfalt)). Die Löschung nützt dann dem Betroffenen nichts, wenn seine personenbezogenen Daten im gleichen Kontext bei einer oder mehreren anderen Stellen gespeichert und für alle Teilnehmer abrufbar bleiben.

— Die Pflicht zum Nachbericht an Stellen, an die früher übermittelt wurde, wird zunehmend anerkannt.

  Bei folgender, durchaus häufiger Fallkonstellation ist inzwischen eine Verbesserung der Praxis erreicht: Fragt eine Stelle, die bereits früher Erkenntnisse zu einer bestimmten Person erhalten hat, erneut an und ergibt die dadurch veranlaßte Überüfung bei der angefragten Stelle, daß die vorhandenen Hinweise inzwischen irrelevant und deshalb zu löschen sind, so teilt sie dies der anfragenden Stelle mit. Ich gehe davon aus, daß dies in aller Regel auch zu einer Löschung bei der anfragenden Behörde führt, falls sie nicht aus anderen Gründen die Daten weiter benötigt. (In verschiedenen Fällen jedenfalls konnte ich die Löschung auch bei der anfragenden Stelle durch Einschaltung der Landesdatenschutzbeauftragten feststellen.)

— Von besonderer Bedeutung ist der *Nachbericht an ausländische Stellen.* Für den Interpolbereich gibt es hierfür eine im Februar 1984 in Kraft getretene Regelung, die die Interpolteilnehmer zu entsprechender Nachmeldung gegenüber dem Generalsekretariat und zur gegenseitigen Beachtung verpflichtet. Für das BKA wurde speziell eine ergänzende interne Anweisung erlassen, mit der die bei meinen Prüfungen in den Jahren 1982 und 1983 festgestellten Mängel bei der Nachberichtspflicht weitgehend behoben werden sollen (s. näher 6. TB S. 44 und unten zu Nr. 20.1). Dem BfV und dem BND habe ich empfohlen, ähnlich zu verfahren. Ich werde mich von der Einhaltung dieser Empfehlungen und der zwischenzeitlich ergangenen Erlasse überzeugen.

19.2.4 Transparenz und Auskunft an den Betroffenen

Das Recht auf Kenntnis hoheitlicher, gegen den Bürger gerichteter Datenverarbeitungsmaßnahmen ist Inhalt seines grundrechtlich geschützten informationellen Selbstbestimmungsrechts. Das Bundesverfassungsgericht hat dies im Volkszählungsurteil nochmals ausdrücklich bestätigt (BVerfGE 65, 1, 70 f.). Im Sicherheitsbereich ist es verständlicherweise nicht immer möglich, den Bürger voll darüber zu informieren, ob und in welchem Umfang personenbezogene Daten zu seiner Person gespeichert sind. Das gilt insbesondere für die Nachrichtendienste. Andererseits muß und darf dies nicht bedeuten, daß hier ausnahmslos die Auskunft oder eine Teilauskunft verweigert wird. Die Praxis der Auskunftserteilung durch die Polizeibehörden gegenüber dem Bürger ist für meinen Zuständigkeitsbereich recht zufriedenstellend. Für die Nachrichtendienste gilt dies jedoch nicht, auch wenn hier in letzter Zeit eine gewisse Besserung eingetreten ist. Für die Zukunft sollte im Rahmen der ohnehin erforderlichen gesetzgeberischen Maßnahmen versucht werden, Fallgruppen zu bilden, in denen eine Auskunft in der Regel erteilt werden kann oder in denen sie im Zweifel zu verweigern ist. Eine Fallgruppe, die grundsätzlich der vollen Auskunft unterliegen sollte, ist beispielsweise die Speicherung im Zusammenhang mit der Sicherheitsüberprüfung, an der der Betroffene selbst mitwirkt. Entsprechende Vorschläge habe ich dem Bundesminister des Innern für die Neuregelung der Richtlinien unterbreitet, und ich gehe davon aus, daß damit eine Änderung der bisherigen Praxis des BfV erreicht werden kann. Das gilt gleichfalls für den MAD und den BND, soweit diese Behörden für die Sicherheitsüberprüfung im jeweiligen Bereich zuständig sind. Eine weitere Fallgruppe wären die Personen, deren Daten deshalb bei einem Nachrichtendienst gespeichert sind, weil dies ihrem Schutz dient, wenn sie sich beispielsweise selbst dem betreffenden Dienst offenbart haben. Es besteht in solchen Fällen kein Grund, die Auskunft über Art und Umfang der Speicherung zu verweigern. Ein dritter Bereich könnte nach Altersgruppen gebildet werden. Entscheidend ist letztlich, daß die Pflicht zur Interessenabwägung sorgfältig wahrgenommen und nicht voreilig vom Recht der Auskunftsverweigerung nach § 13 Abs. 2 BDSG Gebrauch gemacht wird. Diese Bestimmung sollte ohnehin im Rahmen der Novellierung des BDSG ersatzlos gestrichen werden, da die Abwägungsklauseln des § 13 Abs. 3 BDSG auch für die Nachrichtendienste ausreichend erscheinen.

19.2.5 Notwendigkeit gesetzlicher Regelungen im nationalen Bereich

Der vorstehende Überblick hat nur einige Schwerpunktprobleme aufgezeigt, die für die Datenverarbeitung im Sicherheitsbereich bestehen. Daneben gibt es eine Reihe anderer Fragen, die noch nicht befriedigend gelöst sind. So haben die Datenschutzbeauftragten beispielsweise seit Jahren darauf hingewiesen, daß die Regelungen der Dateien- und Löschungsrichtlinien der verschiedenen Sicherheitsbehörden unzureichend sind. Ein großer Teil der vorstehend aufgeführten Probleme ist in den Richtlinien nicht angesprochen. Unabhängig davon ist es nach dem Volkszählungsurteil und nach gegenwärtigem Meinungsstand zur Regelungsbedürftigkeit der Datenverarbeitung im Sicherheitsbereich unerläßlich, die erforderlichen gesetzlichen Grundlagen mit der notwendigen Klarheit und Präzisierung zu schaffen. Dabei ist vordringlich die Zusammenarbeit von Polizei und Nachrichtendiensten zu behandeln. Eilbedürftig sind auch die immer noch ausstehenden allgemeinen Rechtsgrundlagen für die informationelle Tätigkeit von BND und MAD (s. näher Nr. 21.2 und 21.3).

19.2.6 Notwendigkeit internationaler Lösungen

Die Internationalisierung der Kriminalität nimmt unbestreitbar zu. Einer der Gründe hierfür ist die zunehmende Öffnung der Grenzen insbesondere im

Bereich der Europäischen Gemeinschaft. Gleichzeitig wird die bereits jetzt enge Zusammenarbeit der Sicherheitsbehörden über die nationalen Grenzen hinaus weiter anwachsen. Dies zwingt zu internationalen Lösungen des Datenschutzes für diesen Bereich. Verbesserungen auf diesem Gebiet wurden erreicht durch die Ergänzung der Interpol-Statuten in Form einer Datenschutzregelung für das Generalsekretariat von Interpol und den Verkehr mit den nationalen Zentralbüros. Zu nennen ist auch die Institutionalisierung einer internationalen Kontrollkommission von Interpol, die in einem Anhang zum neuen Sitzstaatsabkommen zwischen Interpol und der Republik Frankreich beschlossen wurde (vgl. hierzu 6. TB S. 44 f. und unten Nr. 20.1.4). Dies reicht jedoch nicht aus. Über Interpol und den allgemeinen polizeilichen Bereich hinaus sind einvernehmliche Regelung für die Voraussetzungen und Grenzen des internationalen Informationsaustausches der Sicherheitsbehörden anzustreben. Nur so kann der Gefahr begegnet werden, daß Vereinbarungen für den polizeilichen Bereich durch Datenaustausch der Nachrichtendienste unterlaufen werden können. Diese Gefahr besteht auch deshalb, weil die Organisation von Polizei und Nachrichtendiensten und deren Zusammenarbeit in den Mitgliedstaaten der Europäischen Gemeinschaft und erst recht darüber hinaus sehr unterschiedlich gestaltet sind. Auf längere Sicht müssen hier gemeinschaftsrechtliche und völkerrechtliche Lösungen angestrebt werden. Insbesondere muß versucht werden, wenigstens die wichtigsten Befugnisrechte der Sicherheitsbehörden einander anzugleichen; das gleiche gilt für die Datenschutzrechte des Betroffenen. Im Bereich der Europäischen Gemeinschaft wie auch des Europarats wird zwar seit längerer Zeit vom einheitlichen europäischen Rechtsraum gesprochen. Da dessen Realisierung jedoch auf absehbare Zeit nicht zu erwarten ist, müssen vordringlich Verwaltungsvereinbarungen getroffen werden, wie die vorstehend erwähnte Ergänzung der Interpol-Statuten. Nachdem ich die Vorschläge der internationalen Datenschutzkonferenz zu den Interpol-Datenschutzregelungen maßgeblich mitgestalten konnte, werde ich auch an der Lösung der weiteren datenschutzrechtlichen Probleme beim grenzüberschreitenden Informationsaustausch im Sicherheitsbereich mitarbeiten. Dies geschieht bereits in der Arbeitsgruppe „Datenschutz im Polizeibereich" beim Europarat, außerdem in der Arbeitsgruppe „Datenschutz bei den Sicherheitsbehörden" der internationalen Konferenz der Datenschutzkontrollinstitutionen, deren Einsetzung (unter Vorsitz Dänemarks) auf der Konferenz in Wien im Herbst 1984 beschlossen wurde. Dabei gilt es, die Erkenntnisse umzusetzen, die aufgrund der relativ großen Prüferfahrung des BfD vorliegen. Zu hoffen ist, daß diese Arbeit von den für den Verkehr mit dem Ausland zuständigen Sicherheitsbehörden unterstützt wird. Die Einhaltung gemeinsamer Grundregeln für den Datenschutz liegt nicht nur im Interesse des Bürgers; auch den Sicherheitsbehörden muß daran gelegen sein, daß übermittelte Erkenntnisse in einer Weise verwertet werden, wie sie Rechtsgrundsätzen des Inlands entspricht. (Im einzelnen siehe auch zu BKA Nr. 20.1 und BfV Nr. 21.1).

19.3. Sicherheitsüberprüfung

- Die Bundesregierung hat zugesagt, bei der Neufassung der Richtlinien für die Sicherheitsüberprüfung datenschutzrechtliche Gesichtspunkte „weitgehend" zu berücksichtigen. Aus datenschutzrechtlicher Sicht ist ein entscheidender Gesichtspunkt, daß die im Rahmen der Sicherheitsüberprüfung gesammelten Daten nur für diesen Zweck verwendet werden.

In ihrer Stellungnahme zu meinem Sechsten Tätigkeitsbericht (S. 41 f.) hat die Bundesregierung mitgeteilt, daß sie meinen Forderungen im Zusammenhang mit der Ausarbeitung des Entwurfs der neuen Sicherheitsrichtlinien „bereits weitgehend Rechnung" getragen habe. Dies gelte insbesondere für

— das Recht des Überprüften auf Einsicht in die Sicherheitsrichtlinien,

— den Hinweis auf die Speicherung von Daten des Überprüften (und eventuell seines Ehegatten, Verlobten bzw. der Person, mit der er in eheähnlicher Gemeinschaft lebt) durch das BfV,

— die Anforderung von Akten des Notaufnahme- oder Asylverfahrens nur mit Kenntnis und Einwilligung des Überprüften, wobei allerdings die Verweigerung der Einwilligung eine ausreichende Sicherheitsüberprüfung und somit eine Verwendung in sicherheitsempfindlicher Tätigkeit grundsätzlich unmöglich mache.

Eine Neufassung der Richtlinien ist mir bislang noch nicht zugegangen, da die Bundesregierung noch prüft, welche Konsequenzen sich aus dem Volkszählungsurteil des Bundesverfassungsgerichts für die Sicherheitsüberprüfung ergeben. Nach meiner Auffassung wird eine gesetzliche Regelung der Sicherheitsüberprüfung nunmehr unumgänglich sein (vgl. schon 2. TB S. 44 f.).

Es handelt sich bei der Sicherheitsüberprüfung um einen komplexen Vorgang, der datenschutzrechtlich von erheblicher Bedeutung ist. Im Rahmen einer Sicherheitsüberprüfung werden zum Teil hochsensible Daten beim Betroffenen erhoben. Diese Daten werden an die zuständige Sicherheitsbehörde weitergeleitet. Sie holt ihrerseits weitere Erkundigungen bei anderen Stellen ein. Die so gewonnenen Informationen werden zusammengeführt und das Resultat ihrer Bewertung an den zuständigen Geheimschutzbeauftragten zurückübermittelt. Auf diesem Wege entstehen an verschiedenen Stellen Datensammlungen, die auch zur Speicherung in Dateien führen.

Eine abschließende datenschutzrechtliche Bewertung dieses Vorgangs kann sich nicht auf die Sicherheitsrichtlinien beschränken, da diese nur Teilaspekte regeln. Vielmehr müssen in eine derartige Beurteilung weitere Gesichtspunkte einbezogen werden. Hierzu gehört insbesondere die Frage, wie lange wo welche Daten aus einer Sicherheitsüberprüfung gespeichert werden. Hierzu hat mir kurz vor Drucklegung dieses Berichts der Bundesminister des Innern einen Erlaß zugeleitet, durch den

die Löschung der Altfälle und die künftige laufende Bestandsbereinigung der hierfür betriebenen Dateien sichergestellt werden soll.

Wichtig ist auch die Frage, zu welchen Zwecken die insoweit gespeicherten Daten verwendet werden dürfen. Bei der Erhebung der Daten beim Betroffenen wird diesem zugesagt, daß die Angaben „vertraulich" behandelt werden. Dies und der vom Bundesverfassungsgericht im Volkszählungsurteil betonte Grundsatz der Zweckbindung stehen einer freien Verwendung dieser Daten für die Arbeit der Sicherheitsbehörden entgegen. Die Einhaltung dieses Zweckbindungsgebots scheint mir aber derzeit noch nicht gesichert.

Ich werde den Gesamtbereich der Sicherheitsüberprüfung mit seinen unterschiedlichen Aspekten in meine Kontrolltätigkeit im kommenden Jahr einbeziehen. Gegenstand dieser Prüfung wird auch die Frage sein, inwiefern die derzeitige Regelung der Sicherheitsüberprüfung in den entsprechenden Richtlinien abschließend sein kann. Im Zuge der Bearbeitung einer Einzeleingabe ist mir bekanntgeworden, daß auch das BKA vereinzelt „Sicherheitsüberprüfungen" vorgenommen hat, und zwar bei Arbeitskräften der Stationierungsstreitkräfte. Hierzu hat mir der Bundesminister des Innern inzwischen mitgeteilt, daß derartige Überprüfungen vom BKA in Zukunft nicht mehr durchgeführt werden. Einschlägige Ersuchen der amerikanischen Dienststellen werden entsprechend meiner Anregung künftig nur vom BfV unter Beachtung der Rechts- und Verfahrensgarantien für den Betroffenen beantwortet.

20. Polizeibehörden des Bundes

20.1 Bundeskriminalamt

Zusammenfassung

- Hervorzuheben ist, daß das Bundeskriminalamt auch im Berichtsjahr erhebliche Anstrengungen zur Bereinigung seiner Datenbestände unternommen hat. Im Bereich der Datei PIOS-TE sowie der Datenbestände bei der Abteilung Staatsschutz wurden mehrere zehntausend Personendatensätze gelöscht und die zugrundeliegenden Akten vernichtet. Dies verdient aus meiner Sicht volle Anerkennung.
- Im Bereich der Verarbeitung von ed-Unterlagen mit primär administrativem Charakter (Personenfeststellungsverfahren bei Asylbewerbern und im Notaufnahmeverfahren) wurden wesentliche Verbesserungen und Klarstellungen erreicht.
- Wegen der zunehmenden Notwendigkeit zur internationalen informationellen Zusammenarbeit der Polizei werden klare und völkerrechtlich verbindliche Regelungen des bereichsspezifischen Datenschutzes immer dringlicher. Durch eine neue Dienstanweisung des BKA sowie die inzwischen in Kraft getretenen und weitere in Vorbereitung befindliche Interpol-Datenschutzregelungen ist für die Übergangszeit eine Milderung der Probleme zu erwarten.

20.1.1 Bedeutung der DV-Anwendung für die Rechtslage im Sicherheitsbereich

- Der Trend zum stetigen Ausbau der elektronischen Datenverarbeitung beim Bundeskriminalamt hält weiter an.
- Neue PIOS-Anwendungen führen notgedrungen zur Speicherung nicht nur von Beschuldigten, Verdächtigen oder Störern, sondern auch von „anderen Personen".
- SPUDOK-Anwendungen werden in zunehmender Zahl eingesetzt. Dies ist nicht zuletzt durch die leichte Handhabbarkeit des Systems bedingt.
- Die Polizei hat konkrete Vorstellungen über die Verarbeitung von „Massendaten", entwickelt, d. h. auch von Daten, die nicht Spuren betreffen, sondern lediglich rein zufälligen Bezug zum Tatgeschehen haben.

Im fünften Tätigkeitsbericht (S. 84 ff.) habe ich über die Entwicklung der DV-Anwendungen beim Bundeskriminalamt berichtet. In den vergangenen zwei Jahren hat es erneut wesentliche Veränderungen gegeben. Über die Speicherung von Daten über Beschuldigte, Verdächtige oder Störer hinaus werden zunehmend auch Daten von „anderen Personen", Nichtstörern, Kontaktpersonen und von unter Umständen bloß zufällig Beteiligten erfaßt. Als wichtige Abschnitte dieser Entwicklung, die etappenweise verläuft, sind zu nennen:

Das *PIOS-Verfahren* wurde entwickelt, um Akten elektronisch auswerten zu können. Diese Funktion konnte und kann das Verfahren nur erfüllen, wenn nicht nur der Beschuldigte oder Verdächtige gespeichert wird, sondern auch andere in der Akte enthaltene Personendaten erfaßt werden. Durch die Verknüpfung der unterschiedlichen Personendaten untereinander sowie mit den Daten über Institutionen, Objekte und Sachen hat PIOS die Eigenschaft eines „Verdachtsverdichtungsinstruments" erhalten. Mit der Einführung des PIOS-Verfahrens in einem Kriminalitätsbereich ist in der Regel die Speicherung von Daten über einen erweiterten Personenkreis verbunden. Ursprünglich war PIOS für den Einsatz im Bereich der Terrorismusabwehr konzipiert. Inzwischen gibt es PIOS-Rauschgift, PIOS-Landfriedensbruch, PIOS-Landesverrat, PIOS-Waffen, PIOS-Arbeitsdatei Illegale Arbeitsvermittlung. Weiterhin ist geplant, die Daten von PIOS-Terrorismus mit den Daten aus dem Staatsschutzbereich in der PIOS-Datei „APIS" zusammenzuführen. Da nach Auffassung der Polizei das PIOS-Verfahren ein geeignetes Verfahren zur Bekämpfung der organisierten Kriminalität ist und da diese nach Einschätzung vieler Beobachter zunimmt, ist mit einem weiteren Ansteigen der PIOS-Anwendungen zu rechnen.

Das Konzept *PIOS-Neu* sieht eine Reihe von Weiterentwicklungen des bestehenden Verfahrens vor.

Von Bedeutung ist insbesondere, daß die gespeicherten Daten in einem hierarchischen Verhältnis stehen. Einzelinformationen über Personen sind beispielsweise einem Sachverhalt zugeordnet, der seinerseits wiederum zu einem übergeordneten Vorgang gehört. Hieraus wird der Trend sichtbar, die Speicherung von Personendaten mit den Zwecken einer Aufklärung komplexer Tatzusammenhänge zu verbinden. Nicht die Person und ihr vermuteter oder beweisbarer Tatbeitrag stehen im Mittelpunkt der Speicherung, sondern die Sachaufklärung. Damit ist zwar der Vorteil verbunden, daß alle gespeicherten personenbezogenen Daten im Zusammenhang mit einem Ereignis oder Vorgang leichter vollständig bereinigt werden können. Da die personenbezogenen Daten jedoch mit dem aufzuklärenden Fall automatisch verknüpft sind, dürfte eine Löschung einzelner Personendaten nur schwer durchzusetzen sein, ehe das Ereignis oder der Vorgang, dem die Speicherung zuzurechnen ist, vollständig aufgeklärt ist.

Auch die Zahl der *Spurendokumentationssysteme* (SPUDOK) hat stark zugenommen. Beim BKA waren binnen weniger Jahre 26 SPUDOK-Anwendungen zu verzeichnen. Hiervon sind 16 inzwischen wieder gelöscht worden. Es steht zu erwarten, daß die Tendenz zunehmen wird, das SPUDOK-Verfahren bei allen größeren Kriminalfällen einzusetzen. Insbesondere bei der Bildung von Sonderkommissionen besteht offenbar die Neigung, sich des SPUDOK-Verfahrens zu bedienen. Eine der Eigenheiten dieses Verfahrens ist, daß es neben der Erfassung aller relevanten Spuren auch die Funktion hat, das polizeiliche Handeln bei der Aufklärung des jeweiligen Straffalles zu dokumentieren. In SPUDOK sind deshalb im Grunde sämtliche von der Polizei aufgenommene Spuren einzugeben.

Das Verfahren erlaubt es, die zu erfassenden Informationen im freien Text einzugeben. Alle darin vorkommenden Wörter können im Dialog als Suchbegriffe für die dazu gehörenden Textstellen verwendet werden, es sei denn, daß sie ausnahmsweise in Klammern gesetzt worden sind. Dies gilt auch für alle im Text vorkommenden personenbezogenen Daten. Bei SPUDOK tritt also eine gegenüber der sonstigen Datenerfassung umgekehrte Situation ein: Es muß im Einzelfall entschieden werden, ob in einem erfaßten Text ausnahmsweise ein personenbezogenes Datum nicht als Suchbegriff dienen soll. Dies führt dazu, daß praktisch mit allen in einer Spurenmeldung vorkommenden Personendaten nach dieser Person und den dazugehörenden Textstellen gesucht werden kann. Es ist deshalb nicht ausreichend, wenn in den SPUDOK-Errichtungsanordnungen nach dem Muster der bisherigen Dateierrichtungsanordnungen noch genaue, differenzierte Voraussetzungen für die Erfassung von Personen in SPUDOK-Dateien aufgeführt sind, ohne die hier unbegrenzten Abrufmöglichkeiten zu berücksichtigen.

Die Formulierung in den Dateierrichtungsanordnungen für die Erfassung sogenannter „anderer Personen" wird jedenfalls in der Praxis in aller Regel so verstanden, daß alle im Text einer Spur vorkommenden Personendaten auch in den SPUDOK-Verfahren gespeichert werden dürfen. Im Ergebnis bedeutet dies die Erfassung einer Vielzahl von Personendaten, die in den bisherigen traditionellen Dateien nicht gespeichert werden. Zwar ist nicht zu verkennen, daß die SPUDOK-Dateien bislang nur für vergleichsweise kurze Fristen geführt werden. Allerdings ist noch keineswegs geklärt, in welchem Umfang es der Polizei erlaubt ist, derartige Dateien nach Abschluß der Ermittlungen ohne weiteres zu löschen. Hier sind Abstimmungen mit der Justiz bis hin zur Verteidigung in einem späteren Strafverfahren notwendig.

Das Bundeskriminalamt bemüht sich, in den Errichtungsanordnungen durch die Formulierung von *Zweckbindungsgrundsätzen* für die Daten über „andere Personen" die Gefährdung für das Grundrecht auf informationelle Selbstbestimmung, die in SPUDOK-Verfahren liegen können, auszuräumen. Allerdings greifen derartige Zweckbindungsgrundsätze nur bei (Einzel-) Auskunftsersuchen und auch nur dann, wenn der entsprechende Personenkreis in der jeweiligen Datei besonders gekennzeichnet wird. Kurz vor Drucklegung dieses Berichts hat der Bundesminister des Innern zugesagt, daß dies in Zukunft geschehen soll. Probleme könnten sich auch ergeben, wenn SPUDOK-Verfahren insgesamt miteinander abgeglichen werden.

Da es sich bei SPUDOK um ein vielseitig verwendbares Verfahren handelt, wird es auch zur Gefahrenabwehr eingesetzt. Dies geschah z. B. im Herbst 1983 in Form der Datei *„Lage 1"* (für ein früheres Beispiel vgl. 3. TB S. 50). In dieser Datei wurden Informationen über Aktionen gegen die NATO-Nachrüstung erfaßt. Sie ist inzwischen vollständig gelöscht worden. Zuvor habe ich eine datenschutzrechtliche Kontrolle dieser Datei vorgenommen. Sie hat zu einer Reihe von Beanstandungen geführt. Zwar ist im wesentlichen die Errichtungsanordnung für diese Datei eingehalten worden, in Einzelfällen wurden aber Anmelder und Teilnehmer von Demonstrationen, Flugblattverteiler und ähnliche Personen erfaßt, denen weder ein strafbares Verhalten noch sonst die Verursachung einer konkreten Gefahr vorzuwerfen war.

Ich habe dem Bundesminister des Innern in meinem Prüfbericht dargelegt, daß möglicherweise allein die Anwendung des SPUDOK-Verfahrens bei den Benutzern die Vorstellung hervorrufen könnte, es handele sich ja „nur" um die Speicherung in SPUDOK, so daß ein weniger strenger Maßstab anzulegen sei. Genährt werden könnte eine solche irrige Vorstellung durch Nr. 4.2.10 der Dateienrichtlinien, wonach nur in SPUDOK-Systemen Anzeigenerstatter, Hinweisgeber und Zeugen gespeichert werden dürfen.

Darüber hinaus habe ich dem Bundesminister des Innern gegenüber Zweifel an der Erforderlichkeit der gesamten Datei „Lage 1" geäußert. Da es sich um eine Datei im Bereich der Gefahrenabwehr handelte, hätte hier nach meiner Auffassung das Bundeskriminalamt nur in Unterstützungsfunktion für die Länder tätig werden dürfen. Von allen Bundes-

ländern hat sich aber lediglich das Bundesland Bayern unmittelbar an die Datei „Lage 1" anschließen lassen. Meines Erachtens ist die Datei „Lage 1" ein Beispiel dafür, wie vorhandene multifunktionale Technik eingesetzt wird, weil sie eben zur Verfügung steht.

Es ist vor allem diese multifunktionale Anwendbarkeit des SPUDOK-Verfahrens, die weitere Anwendungsbereiche erwarten läßt. In der Polizei wird zur Zeit die Speicherung sogenannter *„Massendaten"* diskutiert. Massendaten sind von der 99. Tagung der AG Kripo am 11. April 1984 wie folgt definiert worden: „Im Zusammenhang mit polizeilichen Maßnahmen (z. B. Ringalarmfahndungen, Einrichtungen von Kontrollstellen) können personen- oder sachbezogene Massendaten anfallen, bei denen aus sachbezogenen Gründen zu vermuten ist, daß die für die Fallaufklärung brauchbaren Daten darin enthalten sind. Im Gegensatz zu den von vornherein im engeren Fallzusammenhang erfaßten Hinweisen und Spuren werden Massendaten aufgrund rein zufälliger Bezüge zum jeweiligen Tagesgeschehen erhoben, um daraus für die Ermittlungen bedeutsame Hinweise zu gewinnen." Diese Definition macht deutlich, daß danach die entscheidende Voraussetzung für die Aufnahme von personenbezogenen Daten in ein SPUDOK-Verfahren, nämlich die Qualität einer „Spur", wegfallen würde. Bei den Massendaten geht es um „rein zufällige Bezüge" zum jeweiligen Tatgeschehen. Die erhobenen und gespeicherten Daten sollen dann unter bestimmten Voraussetzungen mit polizeilichen oder anderen Datenbeständen abgeglichen werden. Eingesetzt werden soll die „Massendatenverarbeitung" bei Vorliegen bestimmter Straftaten, die „wegen ihres Umfangs oder ihrer Bedeutung polizeiliche Maßnahmen zur Erhebung solcher Daten erfordern".

Eine Aktion wie die im Herbst 1983 in Rheinland-Pfalz durchgeführte *„Aktion Gitternetz"* könnte, wenn das Konzept realisiert wird, in Zukunft zur Speicherung von „Massendaten" führen. Bei der Aktion Gitternetz wurden in Rheinland-Pfalz zeitweise Kennzeichen von Kraftfahrzeugen notiert, die bestimmte Straßen befuhren. Nach Ermittlung der Halterdaten wurden die Halter durch Abfrage in polizeilichen Informationssystemen überprüft. Im Rahmen der Massendatenverarbeitung würde der nur „zufällige" Bezug zu einer Straftat genügen sowie die Erwartung, unter den gespeicherten Daten würden sich solche befinden, die für die Fallaufklärung „brauchbar" sind.

Auf der Sitzung des Arbeitskreises II der Innenministerkonferenz vom 27./28. September 1984 wurde die Beschlußfassung über die Massendatenverarbeitung vorläufig zurückgestellt, da zunächst die Ergebnisse des ad hoc-Ausschusses des Arbeitskreises II zur Frage der Schaffung von bereichsspezifischen Vorschriften für die polizeiliche Informationsverarbeitung abgewartet werden sollen.

Insgesamt läßt sich an den Stationen *PIOS, PIOS-Neu, SPUDOK, Massendatenverarbeitung* eine Entwicklung ablesen, die über die Verarbeitung von Daten über Verdächtige und Beschuldigte hinausführt, bis zur Verarbeitung von Daten über Randpersonen, „Szene"-Angehörige, Kontaktpersonen usw. Da nach dem Volkszählungsurteil in der Speicherung personenbezogener Daten in Polizeidateien unstreitig ein Eingriff zu sehen ist, bedeutet die zunehmende Inanspruchnahme von Personen, die weder Beschuldigte noch Verdächtige noch Störer sind, auch eine Zunahme der Verstöße gegen geltendes Recht, da die engen Grenzen der Voraussetzungen für die Inanspruchnahme des Nichtstörers (sogenannter polizeilicher Notstand) häufig überschritten sein dürften. Die Entwicklung der Datenverarbeitungstechnik und die Verfeinerung der hierdurch zu Verfügung gestellten Instrumente bringen es mit sich, daß traditionelle Denkansätze des Polizeirechts mehr und mehr in den Hintergrund gedrängt werden. Gerade im Hinblick auf die im Anschluß an das Volkszählungsurteil geführte Diskussion über neue Rechtsgrundlagen für die polizeiliche Datenverarbeitung ist aus datenschutzrechtlicher Sicht zu fordern, daß in diesen Rechtsgrundlagen nicht lediglich die technische Entwicklung juristisch nachvollzogen wird, sondern daß der technischen Entwicklung dem Grundrechtsverständnis entsprechende rechtliche Grenzen gezogen werden.

20.1.2 Wichtige Weiterentwicklungen in der Datenverarbeitung des Bundeskriminalamtes

- In Form der „Arbeitsdatei PIOS-Illegale Arbeitsvermittlung (AIA)" wird beim BKA nunmehr das PIOS-Verfahren auch zur Speicherung von Daten zur Aufklärung einzelner Strafverfahren und nicht nur zur Bekämpfung ganzer Kriminalitätsbereiche wie etwa Terrorismus oder Rauschgift eingesetzt.
- Gegen die Zusammenfassung von Daten des allgemeinen polizeilichen Staatsschutzes mit den Daten aus dem Bereich der Terrorismusbekämpfung in der Datei APIS bestehen erhebliche datenschutzrechtliche Bedenken.
- Die Zahl der SPUDOK-Anwendungen im BKA hat sich im Berichtszeitraum weiter erhöht.
- Für die Datei „Dokumentationssystem für terrorismus- und extremismusbezogene Schriften (TESCH)" sind in der endgültigen Fassung der Errichtungsanordnung datenschutzrechtlich bedenkliche Erweiterungen gegenüber dem Probebetrieb vorgesehen.
- In der Datei „Forensisches Informationssystem Handschriften (FISH)" werden der Sache nach erkennungsdienstliche Unterlagen gespeichert, ohne daß nach der Errichtungsanordnung die für die Aufbewahrung von ed-Material entwikkelten Rechtsgrundsätze zu beachten wären.

Der vorstehend beschriebene allgemeine Trend hat auch im Berichtsjahr in der Weiterentwicklung der Datenverarbeitung des BKA seinen Ausdruck gefunden. Im folgenden werden einige der wichtigsten mir bekanntgewordenen neuen Verfahren behandelt.

Auf der Basis des PIOS-Verfahrens wurde die Datei *„Arbeitsdatei PIOS-Illegale Arbeitsvermittlung (AIA)"* als Amtsdatei eingerichtet. Die Datei soll der Aufklärung und Verhütung von Straftaten der illegalen Einschleusung und Vermittlung von ausländischen Arbeitnehmern im Rahmen eines konkreten Ermittlungsverfahrens dienen. Damit wird nach meiner Kenntnis zum ersten Mal vom BKA das PIOS-Verfahren nicht nur für bestimmte Kriminalitätsbereiche, sondern konkret für die Aufklärung in einem einzelnen Ermittlungsverfahren eingesetzt. Dementsprechend „paßt" auch das Muster der gebräuchlichen Errichtungsanordnungen für auf Dauer eingerichtete Dateien wie PIOS nicht. Statt dessen ist pauschal bestimmt, daß eine Unterrichtung „anderer Personen" im Sinne der Nr. 4.3 der Dateienrichtlinien unterbleibt, „weil ihre Speicherung im Rahmen eines noch nicht abgeschlossenen Ermittlungsverfahrens erfolgt (...) und eine Unterrichtung die noch laufenden Ermittlungen gefährden würde". Außerdem wird noch auf die Sachleitungsbefugnis der Staatsanwaltschaft verwiesen.

Hinsichtlich der Speicherungsdauer wird nicht mehr nach den Gruppen der gespeicherten Personen und dem Verdachtsgrad (Beschuldigter/Verdächtiger/„andere Person") unterschieden, sondern die Löschung der gesamten Datei in Aussicht gestellt, „wenn das in Nr. 2.1 genannte Ermittlungsverfahren abgeschlossen und ausgewertet ist". Damit ist gleichzeitig ein wichtiges datenschutzrechtliches Prinzip, nämlich die möglichst auf die einzelne Person ausgerichtete Entscheidung über die Speicherung bzw. Löschung von Daten aufgegeben und die Speicherung aller erfaßten Personendaten dem Zweck des Verfahrens untergeordnet, was bisher bei PIOS nicht der Fall war. Parallel zu einer immer stärkeren Einbeziehung „anderer Personen", d. h. von Personen, die weder beschuldigt noch verdächtigt sind, ist eine schrittweise Zurücknahme solcher datenschutzrechtlicher Sicherungen zu beobachten, die die Probleme bei der „ausnahmsweisen" Erfassung anderer Personen mildern sollten.

Inzwischen ist mir auch die Errichtungsanordnung für die seit längerem geplante „Arbeitsdatei PIOS-Innere Sicherheit (APIS)" zugegangen. Die Datei APIS dient dem Zweck, auf der Basis des PIOS-Verfahrens die Daten aus dem Bereich der Abteilung Staatsschutz des BKA sowie aus der Abteilung TE (Terrorismusbekämpfung) zusammenzuführen und in einer einheitlichen Datei zu speichern. Gegen die seit Jahren bestehende Absicht hierzu habe ich wiederholt datenschutzrechtliche Bedenken geltend gemacht. Diese Bedenken richten sich insbesondere dagegen, daß Daten aus der Terrorismusbekämpfung, die zum Teil Schwerstkriminalität betreffen, mit Daten aus dem Bereich des polizeilichen Staatsschutzes (mögliches Beispiel: „wildes" Plakatieren im Rahmen der Friedensbewegung) in einen Topf geworfen werden. Die Zusammenführung derartiger Datenbestände stellt auch eine Veränderung des Kontextes und damit einen datenschutzrechtlich relevanten Vorgang dar.

Ein weiteres Bedenken gegen die Datei APIS erwächst daraus, daß die damit zur Verfügung stehenden technischen Möglichkeiten die Datenverarbeitung bei der Abteilung Staatsschutz des BKA entscheidend verändern dürften. Bislang hat die Abteilung Staatsschutz des BKA ihre Daten im nachrichtendienstlichen Informationssystem NADIS gespeichert. Die Eigenschaften dieses Systems brachten es mit sich, daß im wesentlichen nur solche Personen dort erfaßt werden konnten, gegen die ein konkretes Ermittlungsverfahren eingeleitet worden ist. Es handelte sich also in aller Regel um Beschuldigte oder Verdächtige. Die Erfassung sogenannter „anderer Personen" war nicht vorgesehen. Sinn und Zweck des PIOS-Verfahrens ist es aber gerade, die vorhandenen (gespeicherten) Akten so auszuwerten, daß auch andere Personen als nur die Beschuldigten oder Verdächtigen erfaßt werden. Dies bedeutet, daß in der Tendenz bei der Abteilung Staatsschutz des BKA ein erweiterter Personenkreis erfaßt werden kann als bisher.

Die erfaßten personenbezogenen Daten sind auch ganz anderen Recherchiermöglichkeiten ausgesetzt als dies bei NADIS der Fall gewesen ist. Die Erfassung in NADIS hatte im wesentlichen Hinweis- und Registraturfunktion. Die Erfassung in APIS geschieht aber vor allem zu dem Zweck, verbesserte Auswertungs- und Recherchiermöglichkeiten zu erhalten. Die im Rahmen von APIS erfaßten Daten insbesondere über „andere Personen" können dort ständig in Auswertungsvorgänge der Abteilungen Staatsschutz oder TE einbezogen werden.

So sehr ich es begrüße, daß die Abteilung Staatsschutz aus dem NADIS-Verbund herausgelöst wird, so sehr habe ich aber Bedenken gegen die Datei APIS in der Form, wie sie derzeit geplant ist.

Im Berichtsjahr sind eine Reihe neuer SPUDOK-Anwendungen angemeldet worden. Die Errichtungsanordnungen hierzu gingen mir zum Teil erst nach Aufforderung zu. Der vorstehend zu Nr. 20.1.1 allgemein beschriebene Trend, SPUDOK-Verfahren verstärkt einzusetzen, ist hier deutlich zum Ausdruck gekommen. Es handelt sich insbesondere um SPUDOK-Verfahren im Bereich der Bekämpfung der Rauschgiftkriminalität sowie im Bereich Terrorismus. Eine Prüfung jeder einzelnen dieser SPUDOK-Dateien ist mir aus Kapazitätsgründen nicht möglich.

Bereits in meinem Fünften Tätigkeitsbericht (S. 87) habe ich die geplante Datei „Dokumentationssystem für terrorismus- und extremismusbezogene Schriften (TESCH)" erwähnt. Nunmehr ist mir die endgültige Errichtungsanordnung für diese Datei zugegangen. Die von mir gegenüber der vorläufigen Errichtungsanordnung geltend gemachten datenschutzrechtlichen Bedenken sind im wesentlichen nicht berücksichtigt worden. Auch ist gegenüber der Errichtungsanordnung für den Probebetrieb bei der Festlegung des Zwecks der Datei eine neue Kategorie hinzugekommen, die nach meiner Auffassung eine wesentliche Erweiterung darstellt. Nach einem Katalog von Straftaten, in deren Zusammenhang Druckerzeugnisse, Handschriften, Ton- oder Bildträger in TESCH erfaßt werden können, ist nunmehr eingefügt, daß auch sonstige Straftaten,

„soweit sie sich direkt oder indirekt gegen die innere Sicherheit der Bundesrepublik Deutschland richten" mit einbezogen werden können. Ich halte diese Generalklausel für eine ganz erhebliche Erweiterung gegenüber dem bisherigen Zweck der Datei.

Meine allgemeinen Bedenken gegen das Verfahren TESCH werden dadurch noch verstärkt. Diese Bedenken richten sich insbesondere darauf, daß nach meiner Auffassung bislang noch nicht überzeugend dargelegt ist, weshalb in TESCH überhaupt personenbezogene Daten erfaßt werden müssen. Wenn die Datei insbesondere dem Zweck dient, den Inhalt von Druckerzeugnissen zu speichern und miteinander abzugleichen, so muß nach meiner Auffassung der Verweis auf die Aktenfundstelle, an der das Original der jeweiligen Druckschrift zu finden ist, genügen. Die Speicherung von personenbezogenen Daten, insbesondere von „Autoren, Verantwortlichen im Sinne der Pressegesetze, Herstellern, Verbreitern, soweit es sich um Beschuldigte oder Verdächtige im Sinne der Nr. 4 der Errichtungsanordnung handelt", Verlagen und Institutionen ist zum bloßen Auffinden und Vergleichen inkriminierter Texte nicht notwendig. Sie birgt die Gefahr in sich, daß die entsprechenden Personendaten neben den anderen in Betracht kommenden Dateien des BKA auch in TESCH erfaßt werden. Die Folge ist eine bereits an anderer Stelle beschriebene immer größere Dateienvielfalt, die es immer schwerer macht, erforderlich werdende Löschungen konsequent und mit Auswirkung auf alle in Betracht kommenden Dateien durchzuführen (s. o. Nr. 19.2.1).

Ähnliche Bedenken bestehen gegen die Datei *„Forensisches Informationssystem Handschriften (FISH)"*. In dieser Datei werden Schriftstücke aus allen Deliktsbereichen erfaßt, die dem Bundeskriminalamt von den Polizeidienststellen der Länder, Staatsanwaltschaften, Gerichten und gegebenenfalls von anderen Behörden zur Untersuchung übersandt werden. Die Datei dient nach dem Text der Errichtungsanordnung dem Zweck, die Identifizierung der Verfasser inkriminierter Schriftstücke und die Ermittlung regional und überregional tätig werdender schreibender Rechtsbrecher unter Feststellung von Tatzusammenhängen zu fördern.

Erfaßt werden sollen nur Schriftstücke, die im Zusammenhang mit Ermittlungsverfahren anfallen. Andererseits ist auch vorgesehen, daß Daten aus der Häftlingsüberwachung mit erfaßt werden. Gerade für die Daten aus dem Bereich der Häftlingsüberwachung ist aber eine Sonderregelung getroffen worden, die datenschutzrechtlichen Bedenken weitgehend Rechnung trägt. Es wird darauf zu achten sein, daß bei Erfassung von Daten aus der Häftlingsüberwachung auch in anderen Dateien die Einhaltung der speziellen Datenschutzbestimmungen für diese Daten nicht erschwert wird. Zwar ist in der vorläufigen Errichtungsanordnung zur Erprobung der Datei FISH vorgesehen, daß die Verwertung von Daten aus dem Bereich der Häftlingsüberwachung nur in Übereinstimmung mit den Regelungen für jene erfolgen darf. Auch für die Speicherung dieser Daten ist auf die entsprechende Regelung zur Häftlingsüberwachung verwiesen. Es erscheint aber zweifelhaft, ob hiermit eine befriedigende datenschutzrechtliche Praxis erreicht werden kann, da die Dateneingabe und die Datenbestandspflege für beide Dateien verschiedenen Polizeibehörden obliegen.

Hinzu kommt ein weiteres Bedenken: Bei den erfaßten Schriftstücken handelt es sich insbesondere um handschriftliche Unterlagen. Durch den Vergleich der Handschriften soll die Identität der betreffenden Personen geklärt werden. Im Grunde genommen handelt es sich deshalb nach meiner Auffassung in der Sache um erkennungsdienstliche Unterlagen. Aus datenschutzrechtlicher Sicht besteht vor allem die Sorge, daß mit solchen neuen Systemen unabhängig von der gewählten Bezeichnung die Regelungen für die Anfertigung und Aufbewahrung erkennungsdienstlicher Unterlagen, so wie sie sich in einer langjährigen Rechtsprechung herausgebildet haben und zum Teil gesetzlich festgelegt sind, mit Hilfe eines Verfahrens wie FISH ausgehöhlt werden könnten. Ich habe deshalb den Bundesminister des Innern auf meine Bedenken dieser Art hingewiesen und um Prüfung von Erforderlichkeit und Vertretbarkeit der Datei gebeten.

Ein weiteres Bedenken ergibt sich daraus, daß in FISH auch die Speicherung personenbezogener Daten von Geschädigten vorgesehen ist, ohne daß eine Einverständniserklärung der Betroffenen gefordert wird.

Insgesamt besteht bei der dargestellten Entwicklung über die im Einzelfall mit der Neueinführung der jeweiligen Verfahren bestehenden qualitativen Bedenken hinaus die Sorge, daß die zunehmende Dateienvielfalt beim BKA die Durchsetzung datenschutzrechtlicher Regeln erschwert. Es wurde bereits an anderer Stelle dargestellt (s. Nr. 19.2.1), daß ein und derselbe Sachverhalt zur Speicherung in sehr verschiedenen Dateien mit ganz unterschiedlichen Errichtungsanordnungen führen kann. So ist es sicher nicht übertrieben zu sagen, daß das Bundeskriminalamt heute über kaum weniger Dateien verfügt als zum Zeitpunkt der Abfassung des ersten Dateienberichts von 1979 des Bundesministers des Innern, der u. a. dazu dienen sollte, die Zahl der Dateien erheblich zu verringern. Gestiegen ist außerdem deutlich der Grad der Automatisierung dieser Dateien. Aus datenschutzrechtlicher Sicht bedeutet dies die stetige Verschärfung von Grundproblemen, die gelöst sein müßten, bevor an die laufende Erweiterung der Nutzung technischer Möglichkeiten gegangen wird.

20.1.3 Aufbewahrung von erkennungsdienstlichen (ed)-Unterlagen über Asylbewerber und Personen im Zusammenhang mit dem Notaufnahmeverfahren

Sowohl beim Verfahren um die Anerkennung als Asylbewerber beim Bundesamt in Zirndorf als auch im Zusammenhang mit dem Bundesnotaufnahmeverfahren in Gießen werden in der Regel ed-Unterlagen über die betreffenden Personen angefertigt. Im erstgenannten Fall werden die Polizeidienststellen der Länder in Vollzugshilfe für das Bundesamt

tätig; im zweiten Fall geschieht dies in der Verantwortung der hessischen Innenverwaltung durch den Polizeipräsidenten in Gießen. Hierbei handelt es sich jeweils um eine besondere Form der Personenfeststellung, weil die Identität der betreffenden Person nicht eindeutig bekannt ist. Es handelt sich nicht um Maßnahmen kriminalpolizeilicher Art.

Rechtsgrundlage für die ed-Behandlung bei Asylbewerbern war früher § 3 Ausländergesetz. Seit dem 1. August 1982 gilt hierfür § 13 AsylVerfG. Für die Maßnahmen des Polizeipräsidenten in Gießen ist dagegen hessisches Recht einschlägig (Ausführungsgesetz zum Personalausweisgesetz in Verbindung mit dem Hessischen Sicherheits- und Ordnungsgesetz).

In beiden Fällen wird jeweils eine Ausfertigung der ed-Unterlagen an das BKA übersandt. Dort wurden bisher diese Daten grundsätzlich gespeichert und die Unterlagen aufbewahrt. Dies geschah früher generell im allgemeinen Zentralen Personenindex des BKA, d. h. vermischt mit Daten über Personen, die aus kriminalpolizeilichen Gründen dort registriert waren. Ich habe seit langem darauf hingewiesen, daß dies eine unzulässige Vermengung von verwaltungsmäßigen mit kriminalpolizeilichen Unterlagen ist (vgl. auch oben Nr. 19.2.1). Das BKA hat daraufhin Ende 1980 die Speicherpraxis dahingehend geändert, daß die betreffenden Hinweise in den verwaltungsinternen Vorgangsnachweis Personalien eingestellt wurden, der nicht dem allgemeinen Zugriff der Polizeidienststellen unterliegt (vgl. hierzu 4. TB S. 52). Eine Einstellung in den kriminalpolizeilichen ZPI (heute KAN) erfolgte nur dann, wenn bereits in anderem Zusammenhang ein entsprechender kriminalpolizeilich relevanter Bestand vorhanden war. Für beide Fallgruppen wurde außerdem eine Speicherfrist von fünf Jahren festgelegt.

Mit dem Inkrafttreten des § 13 AsylVerfG zum 1. August 1982 änderte das BKA die Speicherpraxis zunächst dahingehend, daß die Hinweise über Asylbewerber wieder wie früher dem allgemeinen Zugriff der Polizeibehörden unterworfen und undifferenziert gespeichert wurden zusammen mit Unterlagen aus rein kriminalpolizeilichem Anlaß. Zur Begründung stützten sich BKA und BMI auf § 13 Absatz 3 AsylVerfG, wonach die Unterlagen, die für zehn Jahre nach unanfechtbarer Ablehnung oder nach Rücknahme des Antrags aufbewahrt werden dürfen, auch genutzt werden können „zur Feststellung der Identität oder der Zuordnung von Beweismitteln im Rahmen der Strafverfolgung und der polizeilichen Gefahrenabwehr". Gegen diese Auslegung bestehen erhebliche Bedenken, da die schon immer bestehende Möglichkeit der Nutzung zu kriminalpolizeilichen Zwecken im konkreten Einzelfall nicht gleichzusetzen ist mit der generellen Vermengung verwaltungsmäßiger Daten mit solchen kriminalpolizeilicher Art. Andererseits ist einzuräumen, daß der Wortlaut der fraglichen Bestimmung nicht eindeutig ist.

Nunmehr wurde für den von § 13 AsylVerfG betroffenen Personenkreis (zur Zeit immerhin rd. 200000 mit einem jährlichen Zuwachs von ca. 15000 bis 20000 Personen) eine Regelung vereinbart, die einerseits die prinzipielle Trennung von verwaltungsmäßigen Daten von solchen kriminalpolizeilicher Art unangetastet läßt, andererseits praktischen Bedürfnissen entgegenkommt, ohne schutzwürdige Belange der Betroffenen zu gefährden. Hiernach werden künftig die Hinweise über die aufgrund von § 13 AsylVerfG entstandenen ed-Unterlagen von Personen, zu denen nicht bereits kriminalpolizeilich relevante Hinweise gespeichert sind, ausschließlich in der ed-Datei registriert. Als Grund für die Anfertigung der ed-Unterlagen wird jeweils § 13 AsylVerfG angegeben, um damit den rein verwaltungsrechtlichen Charakter zu unterstreichen. Während sonst auf Anfrage an das INPOL-System ein Kurzhinweis auf eine Speicherung in der ed-Datei gegeben wird, und zwar auch dann, wenn keine Notierung im Kriminalaktennachweis vorliegt, wird dies hier künftig programmtechnisch ausgeschlossen. Eine Auskunft zu Personen, die ausschließlich aufgrund § 13 AsylVerfG beim BKA gespeichert sind, ist dann also nur noch durch gezielte Anfrage an die ed-Datei möglich; durch den in der Auskunft enthaltenen Hinweis auf § 13 AsylVerfG ist jede Verwechselung mit kriminalpolizeilichen Unterlagen ausgeschlossen. Ich hoffe, daß die programmtechnischen Voraussetzungen für die Realisierung dieser Vereinbarung baldmöglichst geschaffen werden.

Gleichzeitig hat mir der Bundesminister des Innern auf meine Anregung zugesagt, daß hinsichtlich der ed-Unterlagen, die im Zusammenhang mit dem Notaufnahmeverfahren angefertigt werden, ab sofort wie folgt verfahren wird: In der Regel werden die ed-Unterlagen nach Abgleich mit den beim BKA gespeicherten Daten sofort zurückgeleitet. Sofern ein umfangreicheres Personenfeststellungsverfahren durch den Polizeipräsidenten Gießen durchgeführt wird, werden die dem BKA zugeleiteten Unterlagen nur noch vorübergehend für die Dauer von drei Monaten aufbewahrt. Das BKA geht davon aus, daß das Personenfeststellungsverfahren dann beendet ist. Nur in diesem Fall erfolgt eine Speicherung in dem vom allgemeinen kriminalpolizeilichen System getrennten Vorgangsnachweis Personalien wie bisher. Ergibt der Abgleich im BKA oder das Personenfeststellungsverfahren keine kriminalpolizeilichen Hinweise zu der Person, dann werden die Daten nach Ablauf der vorgenannten Frist gelöscht und die Unterlagen an den Polizeipräsidenten in Gießen zurückgesandt. Dies entspricht im übrigen auch der in Nr. 6.2 der erkennungsdienstlichen Richtlinien vorgesehenen Verfahrensweise, wonach in solchen Fällen nach Durchführung der Personenfeststellung keine Speicherung zulässig ist.

Gegenüber der bisherigen Praxis der Speicherung für die Dauer von fünf Jahren ist dies eine erhebliche Verbesserung. Darüber hinaus hat das BKA in allen Fällen, in denen im Verlaufe des letzten Jahres Eingaben von Personen bearbeitet wurden, die allein im Zusammenhang mit dem Notaufnahmeverfahren ed-behandelt wurden, die gespeicherten Daten gelöscht und die ed-Unterlagen sofort vernichtet. Dies geschah im Vorgriff auf die nunmehr generelle Regelung. Die noch vorhandenen Speiche-

rungen, die länger als drei Monate zurücklagen (rd. 600 Personendatensätze), wurden inzwischen gelöscht. Damit ist für einen großen Personenkreis eine Gefährdung schutzwürdiger Belange für die Zukunft praktisch ausgeschlossen und für die Vergangenheit bereinigt. Grundsätzlich wird auch dann so verfahren, wenn eine Person nur ed-behandelt wurde, um die Identität einwandfrei feststellen zu können, und weder eine Sonderregelung wie § 13 AsylVerfG vorliegt noch zu der betreffenden Person kriminalpolizeilich relevante Unterlagen beim BKA vorhanden sind.

20.1.4 Interpol

Aus zeitlichen Gründen konnte in diesem Jahr die Tätigkeit des BKA als Nationales Zentralbüro von Interpol nicht erneut geprüft werden. Hier konzentrierte sich die Arbeit auf die Erörterung verschiedener Grundsatzfragen im Nachgang zu meiner Prüfung 1983 (vgl. 6. TB S. 44f.). Dabei ist für die Frage der Relevanzprüfung vor Auskunftserteilung, der Nachberichtspflicht bei wichtigen Änderungen sowie des Hinweises auf interne Löschungsfristen eine zufriedenstellende Lösung durch Erlaß einer neuen Weisung erreicht worden. Hiernach wird das BKA die bisher praktizierte sofortige Auskunft aus den überwiegend unvollständigen eigenen Unterlagen auf eilige Erkenntnismitteilungen beschränken. Nach einer Inlandsumfrage wird das BKA jedenfalls in Fällen bedeutender Abweichung von den ursprünglich übermittelten Erkenntnissen die erforderlichen Berichtigungen nachmelden. Im übrigen wird prinzipiell erst dann Auskunft erteilt, wenn aufgrund einer vorherigen Inlandsumfrage feststeht, daß die vorhandenen Unterlagen weiterhin erforderlich sind. Zusätzlich wird das BKA auf die eigene interne Löschungsfrist hinweisen.

Durch diese Regelung wird die Gefahr der Verletzung schutzwürdiger Belange durch die Übermittlung irrelevanter, veralterter oder unverhältnismäßiger Erkenntnisse entscheidend verringert. Ich werde mich von ihrer Einhaltung im Jahr 1985 überzeugen. Zur Beachtung der Auflagen, Fristen und Hinweise, die das BKA seinen Erkenntnissen beifügt, sind das Generalsekretariat und die anderen Nationalen Zentralbüros aufgrund der neuen und inzwischen in Kraft getretenen Interpol-Datenschutzrichtlinien verpflichtet (vgl. auch oben Nr. 19.2.6). Die noch ausstehenden Richtlinien über den Datenaustausch zwischen den einzelnen Nationalen Zentralbüros sowie die Löschungsrichtlinien für die Dateien des Generalsekretariats lassen eine weitere Besserung erwarten. Ich gehe davon aus, daß mich das BKA rechtzeitig vom Stand der Arbeiten der zuständigen Gremien von Interpol unterrichtet, damit ich meine Vorstellungen einbringen kann. Im übrigen erhoffe ich zusätzliche Verbesserungen und Anregungen durch die internationale Kontrollkommission für das Generalsekretariat, die im Jahr 1985 ihre Arbeit aufnehmen wird.

Auf längere Sicht werden völkerrechtlich verbindliche Regelungen unumgänglich sein. Diese müssen auch für Nachrichtendienste gelten, soweit hierfür nicht Regelungen eigener Art zu erlassen sind. Nur so ist eine Umgehung erreichter Verbesserungen im polizeilichen Bereich auszuschließen (s. o. Nr. 19.2.6). Wegen der rasch zunehmenden Bedeutung des internationalen Datenverkehrs gerade im polizeilichen Bereich in Westeuropa wird sich die datenschutzrechtliche Kontrolle in Zukunft mehr als bisher hierauf konzentrieren müssen. Dazu ist es notwendig, daß ich rechtzeitig von Planungen unterrichtet werde, die die internationalen Aspekte sicherheitsbehördlicher Datenverarbeitung betreffen.

20.2 Bundesgrenzschutz

20.2.1 Grenzaktennachweis (GAN)

In meinem Sechsten Tätigkeitsbericht (S. 48) habe ich dargestellt, daß es sich bei dem bereits im Aufbau befindlichen GAN um eine Datei handelt, in der sämtliche Akten, die bei der Grenzschutzdirektion vorhanden sind, registriert werden sollen. Die Datei wird in einem geschützten Index des Bundesgrenzschutzes beim Bundeskriminalamt geführt. Neben der Grenzschutzdirektion sollen auch die Grenzschutzämter und die Geschäftszimmer der Grenzschutzstellen auf den GAN zugreifen können. Aufgrund der mir im Jahre 1983 vorgelegten Unterlagen sowie einer datenschutzrechtlichen Kontrolle habe ich eine Reihe von Bedenken gegen verschiedene Aspekte des GAN erhoben, deren wichtigste ich im Sechsten Tätigkeitsbericht (S. 48) geschildert habe. Ende Dezember 1983 leitete mir der Bundesminister des Innern daraufhin einen neuen Entwurf für die Errichtungsanordnung des GAN zu, der lediglich bei den Speicherfristen für Kinder meine Anregungen aufgriff. Zu dem Entwurf habe ich unter Einbeziehung der Konsequenzen, die sich m. E. aus dem Volkszählungsurteil des Bundesverfassungsgerichts auch für die Datenverarbeitung des Bundesgrenzschutzes ergeben, Stellung genommen.

Inzwischen konnten bei mehreren Problemen Verbesserungen erzielt werden. Zu folgenden Punkten habe ich jedoch nach wie vor datenschutzrechtliche Bedenken:

— Wie beim Kriminalaktennachweis des Bundeskriminalamtes sollen auch im GAN des Bundesgrenzschutzes personengebundene Hinweise (z. B. bewaffnet, gewalttätig, Freitodgefahr, Betäubungsmittel-Konsument) gespeichert werden. Ich halte die Speicherung solcher Hinweise in der INPOL-Personenfahndungsdatei lediglich für die Dauer aktueller Fahndungen für zulässig (näher s. o. zu Nr. 19.2.1). Die Speicherung dieser Hinweise im GAN (insbesondere aus Gründen der Eigensicherung von Beamten des Bundesgrenzschutzes) ist dagegen schon deshalb nicht erforderlich, weil sie bereits aus dem Datenfeld „personengebundene Hinweise" in der INPOL-Personenfahndungsdatei zu entnehmen sind, auf die die Grenzschutzstellen Zugriff haben.

— Die beabsichtigte Zugriffsberechtigung der Grenzschutzstellen halte ich aufgrund der räumlichen Verhältnisse bei zahlreichen Grenzschutzstellen nicht für vertretbar, denn sie ermöglicht es, im Rahmen der normalen grenzpolizeilichen Personenkontrolle auch die Datei GAN abzufragen. So können die dort enthaltenen verkürzten Aktenhinweise Entscheidungen beeinflussen, die bei genauerer Kenntnis des Akteninhalts so möglicherweise nicht getroffen würden (vgl. auch oben Nr. 19.2.1). Soweit *im Einzelfall* eine Auskunft aus dem GAN in Verbindung mit den dazugehörigen Unterlagen benötigt wird, kann mittels des INPOL-Systems bereits seit längerem eine schnelle Anfrage bei Grenzschutzämtern oder bei der Grenzschutzdirektion durchgeführt werden. Zeitliche Verzögerungen sind dadurch nicht zu erwarten. Soweit sie im Ausnahmefall dennoch eintreten sollten, sind sie bei Abwägung mit den geschilderten Risiken hinzunehmen.

— Nach wie vor werden im GAN auch Anfragen anderer Polizeidienststellen registriert, die keinen grenzrelevanten Bezug haben, insbesondere keine grenzpolizeilichen Maßnahmen veranlassen (vgl. hierzu schon meine Kritik im 4. TB S. 30 f.).

Darüber hinaus ist auch darauf hinzuweisen, daß die ungelösten Probleme bei der Amtshilfe des BGS für die Nachrichtendienste (vgl. auch nachstehend Nr. 20.2.2) auch für den GAN Auswirkungen haben. Denn der Bundesgrenzschutz speichert im GAN Daten auch von Personen, die auf Antrag der Nachrichtendienste im Grenzfahndungsbestand ausgeschrieben waren. Diese Speicherung ist nach meiner Auffassung schon deshalb nicht zulässig, weil nach wie vor gesetzliche Grundlagen für die Amtshilfe des Bundesgrenzschutzes für die Nachrichtendienste fehlen. Darüber hinaus erscheint diese Speicherung auch nicht erforderlich.

Aus den gleichen Gründen halte ich auch die aus dem GAN vorgesehene Auskunftserteilung des Bundesgrenzschutzes an die Nachrichtendienste nach den Vorschriften der Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen nicht für zulässig.

Ich habe dem Bundesminister des Innern meine Bedenken nochmals schriftlich vorgetragen und um erneute Überprüfung gebeten. Diese Prüfung ist bisher nicht abgeschlossen.

20.2.2 Zur Amtshilfe des Bundesgrenzschutzes für die Nachrichtendienste

Anfang 1984 habe ich einen Entwurf für die Neufassung der Dienstanweisung zur Amtshilfe des Bundesgrenzschutzes für die Nachrichtendienste erhalten. In meiner Stellungnahme hierzu habe ich eine Reihe von Bedenken gegen die beabsichtigte Neuregelung geäußert. Unter Berufung auf das Volkszählungsurteil des Bundesverfassungsgerichts habe ich die Auffassung vertreten, daß vor einer Erweiterung des Umfangs der Amtshilfe des Bundesgrenzschutzes eine eindeutige und dem Gebot der Normenklarheit entsprechende gesetzliche Regelung für diese Form der Datenübermittlung Vorrang haben müsse. Dies war im übrigen bereits beim Erlaß der neuen Dienstanweisung im Herbst 1981 erklärtes Ziel der Bundesregierung (vgl. hierzu 4. TB S. 31).

20.3 Zollkriminalinstitut

Zusammenfassung

- Der Bundesminister der Finanzen hat meiner Auffassung zugestimmt, daß der Online-Zugriff der Polizei auf die Daten der zollrechtlichen Überwachung unzulässig ist, und vom Bundesminister des Innern die Beendigung dieses Zugriffs verlangt.
- Die Bemühungen um eine wirkungsvolle Datenschutzkontrolle scheiterten beim Zollkriminalinstitut wiederum daran, daß mir das Steuergeheimnis entgegengehalten wurde. Über einen von mir gemachten Kompromißvorschlag hinsichtlich des Bereiches der Steuer- und Zollfahndung hat der Bundesminister der Finanzen bisher nicht entschieden.

20.3.1

In den vergangenen Jahren habe ich jeweils über die zollrechtliche Überwachung berichtet (vgl. 5. TB S. 100 f., 6. TB S. 53) und kritisiert, daß die Polizeibehörden, die über einen Anschluß an die INPOL-Fahndungsdatei verfügen, damit zugleich Zugriff auf die Daten haben, die im Rahmen der zollrechtlichen Überwachung gespeichert sind. Ich halte dies für unvereinbar mit dem Steuergeheimnis nach § 30 der Abgabenordnung. Dieser Auffassung hat sich nunmehr der Bundesminister der Finanzen angeschlossen. Er hat deshalb dem Bundesminister des Innern mitgeteilt, daß es zwingend geboten sei, die Datenbestände der zollrechtlichen Überwachung von den anderen Datenbeständen der polizeilichen Beobachtung zu trennen. Außerdem soll bei einer Kontrolle an der Grenze die Grenzpolizei nur eine Anhaltemeldung im Rahmen der polizeilichen Beobachtung fertigen. Bei einer zollrechtlichen Kontrolle aufgrund einer Ausschreibung zur zollrechtlichen Überwachung darf nur beim Auffinden von Rauschgift eine Meldung an Polizeidienststellen nach der Polizeidienstvorschrift 386.1 erfolgen. Ein negatives Kontrollergebnis darf die Zollverwaltung der Polizei nicht mitteilen.

Der Arbeitskreis II der Innenministerkonferenz hat daraufhin auf seiner Sitzung am 27./28. November 1984 die AG Kripo beauftragt, unter Berücksichtigung der vom Bundesminister der Finanzen dargelegten Bedenken einen Lösungsvorschlag zu erarbeiten, der berücksichtigt, daß es aus polizeitaktischen Gründen erforderlich sein kann, des Rauschgift- oder Waffenschmuggels Verdächtige sowohl zur polizeilichen Beobachtung als auch zur zollrechtlichen Überwachung auszuschreiben.

Damit ist eine seit Jahren erhobene datenschutzrechtliche Forderung im Grundsatz als berechtigt anerkannt worden. Ich gehe davon aus, daß die Beendigung des Zugriffs der Polizeidienststellen des Inlands auf Ausschreibungen zur zollrechtlichen Überwachung nunmehr unverzüglich in Angriff genommen wird. Gegen eine Ausschreibung von Personen sowohl zur zollrechtlichen Überwachung als auch zur polizeilichen Beobachtung bestehen aus datenschutzrechtlicher Sicht keine grundsätzlichen Bedenken, sofern die jeweiligen Voraussetzungen nach den entsprechenden Vorschriften erfüllt sind. Für beide Bereiche bleibt es allerdings bei der grundsätzlichen und durch das Volkszählungsurteil in ihrer Richtigkeit bestätigten Forderung nach Schaffung einer bereichsspezifischen, präzisen gesetzlichen Grundlage, die dem Gebot der Normenklarheit entspricht.

20.3.2

Leider sind auch im Berichtsjahr meine Bemühungen um Vorlage aller für eine Datenschutzprüfung notwendigen Unterlagen ohne Erfolg geblieben. Der Bundesminister der Finanzen ist nach wie vor der Ansicht, daß das in § 30 AO garantierte Steuergeheimnis meiner Kontrollbefugnis entgegensteht. Ich habe wiederholt dargelegt (vgl. 3. TB S. 21, 4. TB S. 19, 5. TB S. 100, 6. TB S. 53), daß ich es als meine gesetzliche Aufgabe ansehe, gerade die Einhaltung dieser Geheimhaltungsvorschrift zu kontrollieren.

Im vergangenen Jahr habe ich erneut einen Vorstoß in dieser Streitfrage unternommen, um wenigstens zu einer pragmatischen Lösung in einem Teilbereich zu kommen. Ich habe dem Bundesminister der Finanzen vorgeschlagen, unter Wahrung der beiderseitigen Rechtsstandpunkte bis zur gesetzlichen Klärung wenigstens im Bereich der Steuer- und Zollfahndung datenschutzrechtliche Kontrollen zuzulassen. Die für die Steuer- und Zollfahndung zuständigen Behörden haben im Grunde die Aufgaben und Befugnisse von Polizeibehörden. Das ergibt sich bereits aus der Gleichstellung mit den „Behörden und Beamten des Polizeidienstes" gemäß § 404 AO.

Hierbei handelt es sich jedoch keineswegs um den klassischen Anwendungsbereich des Steuergeheimnisses. Das Steuergeheimnis hat seinen Ursprung in der Überlegung, daß der Staat nur dann vom Bürger vollständige und richtige Angaben für die Zwecke der Steuererhebung verlangen kann, wenn er die so gewonnenen Daten strikt zweckgebunden verwendet. Nur im Vertrauen auf den Schutz dieser Daten kann der Staat verläßliche Angaben der Bürger für das Besteuerungsverfahren erwarten.

Diese Voraussetzungen liegen in dieser Ausprägung bei einem Steuer- oder Zollstrafverfahren nicht vor. Es geht hier um ein eigenständiges Verfahren, bei dem die Fahndungsbehörden eigene Ermittlungen durchführen (§ 397 AO) so wie jede andere Polizeibehörde auch. Deshalb hat der Betroffene auch ein Auskunftsverweigerungsrecht, wie es jedem Beschuldigten zusteht (vgl. §§ 399, 404 AO i. V. m. § 136 StPO). Die Interessenlage ist also mit dem üblichen Besteuerungsverfahren nicht vergleichbar.

Dementsprechend sieht § 30 Abs. 4 Nr. 4 AO auch die Möglichkeit der Übermittlung von Daten zur Verfolgung sonstiger Straftaten vor, soweit die Daten im Verfahren einer Steuerstraftat oder Steuerordnungswidrigkeit oder ohne Bestehen einer steuerlichen Verpflichtung oder unter Verzicht auf ein Auskunftsverweigerungsrecht erlangt worden sind. Begründet wurde die Einfügung des § 30 Abs. 4 Nr. 4 AO im Finanzausschuß seinerzeit damit, daß der spezifische Schutzgedanke des Steuergeheimnisses nicht greife, sofern der Betroffene nicht durch Mitwirkungs- und Offenbarungspflichten zur Preisgabe von Daten verpflichtet sei.

Ich habe, gestützt auf diese Argumentation, dem Bundesminister der Finanzen vorgeschlagen, jedenfalls im Bereich der Steuer- und Zollfahndung wirkungsvolle datenschutzrechtliche Kontrollen zuzulassen, zumal das Bundesverfassungsgericht inzwischen im Volkszählungsurteil, also in einem Verfahren, in dem es um eine vergleichbare Geheimhaltungsvorschrift (Statistikgeheimnis) ging, die Bedeutung einer unabhängigen datenschutzrechtlichen Kontrolle betont hat. Der Bundesminister der Finanzen hat sich zu diesem Vorschlag noch nicht geäußert. Es bleibt daher gegenwärtig bei dem unbefriedigenden Zustand, daß im Bereich der Steuer- und Zollfahndung keine datenschutzrechtlichen Kontrollen möglich sind, obwohl es sich dort im Grunde um polizeiliche Datenverarbeitung handelt.

21. Nachrichtendienste des Bundes

21.1 Bundesamt für Verfassungsschutz

Zusammenfassung

- Der Bundesminister des Innern hat in seiner Stellungnahme zu meinem Bericht über die Prüfung bei der Abteilung III des Bundesamtes für Verfassungsschutz (BfV) Löschungen und Verfahrensänderungen angekündigt.
- Die verbleibenden Streitfragen beruhen zumeist auf unterschiedlicher Rechtsauslegung. Sie sind zum Teil von erheblicher praktischer Konsequenz. Es geht dabei vor allem um folgende Fragen:
  - Darf der Verfassungsschutz im Rahmen der Beobachtung verfassungsfeindlicher Bestrebungen auch einfache Mitglieder oder nur Träger extremistischer Organisationen registrieren?
  - Darf im Rahmen der Beobachtung des Einflusses extremistischer Bestrebungen auch die möglicherweise beeinflußte demokratische Organisation selbst beobachtet werden?
  - Unter welchen Voraussetzungen darf ein Verhalten, das sich als Ausübung von Grund-

rechten darstellt, zu einer Speicherung beim Verfassungsschutz führen?

- Dürfen Daten, die an sich zu löschen sind, vorher noch in irgendeiner Form verwertet werden?
- In welchem Umfang müssen in Dateien gelöschte Daten auch in Akten vernichtet werden?
- Ist das Trennungsgebot zwischen Polizei und Verfassungsschutz nur organisatorischer Natur oder hat es auch Auswirkungen auf die informationelle Zusammenarbeit?
- Gelten die für das Bundeszentralregister maßgebenden Fristen sinngemäß auch für das BfV, wenn dort Straftaten in Dateien gespeichert werden?

- Für den Datenaustausch mit ausländischen Stellen sind gesetzliche Regelungen zu erarbeiten. Bei der Prüfung der Übermittlungsfähigkeit einzelner Daten ist ein strengerer Maßstab anzulegen. Insbesondere muß vermieden werden, daß Rechtspositionen, die dem Bürger nach innerstaatlichen Regelungen zustehen, durch internationalen Datenaustausch der Nachrichtendienste gefährdet werden.
- Nach dem Beschluß des Bundesverfassungsgerichts vom 20. Juni 1984 zur Tätigkeit des BND aufgrund § 3 Gesetz zu Artikel 10 GG (näher hierzu s. Nr. 21.2.4) kann meine Kontrollkompetenz für Überwachungsmaßnahmen des BfV nach dem G 10 nicht mehr streitig sein.

21.1.1 Kontrolle bei der Abteilung III (Linksextremismus)

Im Jahre 1983 habe ich über einen längeren Zeitraum die Datenverarbeitung bei der Abteilung III (Beobachtung linksextremistischer Bestrebungen) des BfV kontrolliert. Zu dem von mir erstellten Prüfbericht hat nunmehr der Bundesminister des Innern Stellung genommen. Er hat in einer Reihe von Fragen wichtige Veränderungen der Datenverarbeitungspraxis und der zugrundeliegenden innerdienstlichen Vorschriften angekündigt. Meine Anregungen hierzu sind teilweise aufgegriffen worden. Die von mir beanstandeten Einzelfälle sind oder werden zum überwiegenden Teil gelöscht. Soweit dies nicht der Fall ist, beruht dies größtenteils auf unterschiedlichen Rechtsauffassungen. Einige dieser Rechtsfragen werden bereits seit Jahren zwischen dem BfV und mir kontrovers diskutiert, einige sind in dieser Deutlichkeit erst im Verlaufe der datenschutzrechtlichen Kontrolle zutage getreten. Im wesentlichen handelt es sich hierbei um folgende Fragen:

Kernpunkt der Tätigkeit des Verfassungsschutzes ist die Beobachtung extremistischer Bestrebungen. Die Speicherung *personenbezogener* Daten ist in diesem Zusammenhang nur zulässig, wenn sie zur Beobachtung der betreffenden Organisation notwendig ist. Dies ist nach meiner Auffassung nur bei „Trägern" der jeweiligen Organisation der Fall. Träger einer extremistischen Organisation können zwar nicht nur die Funktionäre, sondern auch einfache Mitglieder sein. Die bloße Mitgliedschaft als solche ohne besondere zusätzliche Aktivitäten macht aber nach meiner Ansicht die betreffende Person nicht automatisch zum Träger einer verfassungsfeindlichen Bestrebung.

Der Bundesminister des Innern vertritt demgegenüber die Auffassung, daß die Trägereigenschaft auch bei einfachen Mitgliedern in der Regel zu bejahen ist. Er geht deshalb davon aus, daß das BfV berechtigt sei, auch die Daten einfacher Mitglieder extremistischer Organisationen zu speichern. Dementsprechend hat der Bundesminister des Innern alle Beanstandungen ausdrücklich zurückgewiesen, die auf die fehlende „Trägereigenschaft" der betreffenden Person gestützt waren.

Das BfV interessiert sich auch für die Bestrebungen von Extremisten, Einfluß auf demokratische Organisationen zu gewinnen. Aus datenschutzrechtlicher Sicht kommt es dabei aber darauf an, daß bei der Beobachtung des Einflusses extremistischer Kräfte auf demokratische Organisationen nicht die betreffenden demokratischen Organisationen selbst und damit ihre Mitglieder durch den Verfassungsschutz beobachtet werden. Ich habe deshalb dem BfV vorgeschlagen, derartige Beeinflussungsversuche in einer Form zu dokumentieren, die jeden Anschein einer Beobachtung derjenigen Organisation und ihrer Mitglieder vermeidet, die Ziel derartiger Beeinflussungsversuche sind. Ich habe darüber hinaus eine Reihe von konkreten Vorschlägen gemacht, wie die Datenspeicherung von Personen vermieden werden kann, die in solchen demokratischen Organisationen, Kampagnen etc. mitarbeiten, auf die extremistische Organisationen Einfluß zu nehmen versuchen.

Der Bundesminister des Innern ist dagegen der Auffassung, daß sich extremistische Aktivitäten gegen demokratische Organisationen losgelöst vom demokratischen Umfeld weder beobachten noch beurteilen lassen, da eine sachgerechte Bewertung auch Kenntnisse über demokratische Zielobjekte von Extremisten erfordert. So sei z. B. zur Beurteilung des Erfolges extremistischer Beeinflussungsversuche oder von Bündnisbemühungen die Frage nach der Akzeptanz von Bedeutung. Der Auftrag des § 3 Abs. 1 BVerfSchG schließe daher die Aufgabe und Befugnis des BfV ein, auch in solchen Zusammenhängen — unter Beachtung des Verhältnismäßigkeitsgrundsatzes — personenbezogene Informationen zu sammeln und auszuwerten. Das BfV speichere jedoch keineswegs die Daten aller Personen, die in Sachakten genannt werden, welche die Beobachtung extremistischer Einflüsse auf demokratische Organisationen betreffen.

Bereits im Sechsten Tätigkeitsbericht (S. 49 f.) habe ich dargelegt, daß eine Verhaltensweise, die grundrechtlich besonders geschützt ist, nicht zu einer Speicherung in den Dateien des BfV führen darf, wenn kein weiterer Grund dafür hinzutritt. Eine Speicherung durch das BfV stellt einen Eingriff dar, der nur gerechtfertigt ist, wenn die Schranken des jeweils ausgeübten Grundrechts überschritten sind. Da die Grundrechte unterschiedliche Schrankenbe-

stimmungen aufweisen, sind nach meiner Ansicht Differenzierungen nach dem jeweiligen Grundrecht erforderlich. In dieser Auffassung fühle ich mich durch das Volkszählungsurteil des Bundesverfassungsgerichts bestärkt. Wenn dort gefordert wird, der Bürger müsse wissen, wer was wann bei welcher Gelegenheit über ihn speichere, und weiter die Befürchtung geäußert wird, wer damit rechne, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen könnten, werde möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Artikel 8, 9 GG) verzichten, so ist dies der Kern auch meiner Argumentation. Ich habe deshalb das BfV darauf hingewiesen, daß bei einer Speicherung, die die Ausübung von Grundrechten betrifft, besondere Sorgfalt geboten und besonders streng darauf zu achten ist, daß es sich nicht um eine Betätigung handelt, die innerhalb der Schranken des jeweiligen Grundrechts erlaubt ist.

Der Bundesminister des Innern folgt mir darin, daß die Grundrechtsausübung allein kein Speicherungsgrund sein dürfe. Er hat aber ausgeführt, daß die Tatsache, daß es sich um eine Grundrechtsausübung handelt, der Speicherung dann nicht entgegenstehe, wenn durch die Grundrechtsausübung extremistische Bestrebungen gefördert werden oder wenn die „Schwelle zum Extremismusverdacht" überschritten ist. Es komme deswegen nicht darauf an, ob der *Inhalt* der jeweiligen Grundrechtsausübung verfassungsfeindlicher Natur sei oder nicht, sondern insbesondere ob der Betroffene nach dem Erkenntnisstand des BfV als Extremist einzustufen sei. Ich halte diese Argumentation und diese Abgrenzungskriterien nach wie vor nicht für geeignet, unberechtigte Speicherungen zu vermeiden. Müßte schon immer dann, wenn eine Äußerung objektiv geeignet sein könnte, extremistische Bestrebungen zu fördern, eine Speicherung befürchtet werden, so wüßte der Bürger in der Tat nicht mehr, wer was wann bei welcher Gelegenheit über ihn speichert. Darüber hinaus bin ich der Auffassung, daß man die Diskussion über diesen Fragenkreis nur konkret anhand der einzelnen in Betracht kommenden Grundrechte führen kann.

Die Bereinigung der Datenbestände in den Dateien des BfV erfordert eine geraume Zeit. Nicht immer läßt es sich vermeiden, daß Daten dort noch gespeichert sind, die eigentlich bereits zu löschen gewesen wären. Meines Erachtens dürfen derartige Daten nicht mehr verwertet, insbesondere nicht mehr an Dritte übermittelt werden.

Der Bundesminister des Innern hat demgegenüber geäußert, es bestehe insoweit nur ein grundsätzliches, kein absolutes Verwertungsverbot. Ausnahmen seien dann möglich, wenn die Relevanz der beim BfV vorliegenden Informationen nicht abschließend beurteilt werden könne, die betreffende Information aber für die anfragende Stelle aufgrund dort vorliegender zusätzlicher Erkenntnisse oder im Hinblick auf den Anfragegrund von Bedeutung sein könnte. Unter anderem hat sich das BfV auf das sogenannte „Narr-Urteil" des Bundesverwaltungsgerichts vom 21. Februar 1984 berufen (DÖV 1984, S. 510). Dies erscheint mir auch deshalb nicht sachgemäß, weil in diesem Urteil über die Verwertung löschungsreifer Daten nichts ausgesagt ist.

Bei Personen, die zu Recht als Träger extremistischer Bestrebungen in der NADIS-Personenzentraldatei (PZD) registriert sind, halte ich es gleichwohl nicht für zulässig, deren Ausübung staatsbürgerlicher Rechte, soweit sie keinen extremistischen Bezug hat, hinzuzuspeichern. Auch die einzelne Information, die einem „Extremisten" zugeordnet und in den personenbezogenen Sammlungen des BfV gespeichert wird, muß extremistischen Bezug haben. Insoweit stimme ich mit der Auffassung des Bayerischen Datenschutzbeauftragten (vgl. dessen 6. TB S. 40 f.) überein. Der Bundesminister des Innern geht davon aus, daß bei sogenannten „Folgespeicherungen" ein großzügigerer Maßstab als bei der erstmaligen Speicherung von Daten einer Person anzulegen sei. Hiergegen wird im Grundsatz nichts einzuwenden sein. Gleichwohl muß auch bei großzügiger Handhabung die zu speichernde Information extremistischen Bezug haben.

In den Akten des BfV, insbesondere in den sogenannten „Sachakten", ist eine Vielzahl von personenbezogenen Daten erfaßt. Nur ein Teil hiervon ist auch in den Dateien des Bundesamtes gespeichert. Das Datenschutzinteresse konzentriert sich primär und nach dem BDSG auf eine Speicherung in Dateien, da von dieser Form der Speicherung personenbezogener Daten ein erheblich höherer Gefährdungsgrad ausgeht als von der Speicherung in Aktenform. Gleichwohl müssen auch für die Datenerfassung in Akten Lösungen gefunden werden, die datenschutzrechtlichen Belangen Rechnung tragen. Denn bei genauer Kenntnis des Sachgebiets können personenbezogene Daten in Sachakten gezielt aufgefunden werden, auch ohne daß Daten der betreffenden Person in der NADIS-PZD gespeichert sind. Außerdem wird die Fortentwicklung der automatisierten Datenverarbeitung den Unterschied zwischen automatisierter und aktenmäßiger Verarbeitung ohnehin verwischen, weil zunehmend auch freie Texte im Computer erfaßt werden können. Die Nutzung von Akteninhalten wird dann erheblich komfortabler werden. Schon im Hinblick auf diese Entwicklung, die vermutlich früher oder später auch beim BfV zum Tragen kommen wird, halte ich es für unumgänglich, sich schon jetzt mit diesem Fragenkreis zu befassen.

Der Bundesminister des Innern ist dagegen der Auffassung, daß die aktenmäßige Erfassung von politisch aktiven Bürgern zur Beobachtung extremistischer Einflüsse auf demokratische Organisationen datenschutzrechtlich nicht zu beanstanden ist. Dem kann ich in dieser Allgemeinheit nicht zustimmen. Im Volkszählungsurteil hat das Bundesverfassungsgericht die Dateiform der Verarbeitung personenbezogener Daten als nicht ausschlaggebend für datenschutzrechtliche Fragestellungen angesehen.

Nach wie vor umstritten ist zwischen dem Bundesminister des Innern und mir der Inhalt des verfas-

sungskräftigen Trennungsgebots zwischen Polizei und Verfassungsschutz (vgl. hierzu 5. TB S. 79 ff. und S. 93 ff.). Der Bundesminister des Innern geht davon aus, daß das Trennungsgebot eine rein organisationsrechtliche Vorschrift ist, die mit der organisatorischen Trennung von Polizei- und Verfassungsschutzbehörden erfüllt ist. Ich bin dagegen nach wie vor der Auffassung, daß das Trennungsgebot darüber hinaus eine Zusammenfassung der Befugnisse von Verfassungsschutz und Polizei verhindern soll. Unter den Bedingungen der modernen Informationsverarbeitung würde nach meiner Auffassung das Trennungsgebot zu wesentlichen Teilen ausgehöhlt werden, wenn es sich nur in der Behördenorganisation ausdrückte. Denn dem Verfassungsschutz ist nicht nur die Anwendung polizeilicher Befugnisse versagt, sondern unstreitig darf die Polizei auch nicht mit ihren Befugnissen für den Verfassungsschutz tätig werden, indem sie ihm gezielt Daten beschafft. Mit polizeilichen Befugnissen zu eigenen Zwecken erlangte Informationen darf sie nur unter engen und vom Gesetzgeber präzise festzulegenden Voraussetzungen an den Verfassungsschutz übermitteln. Der Bundesminister des Innern hat in seiner Stellungnahme angekündigt, daß als Konsequenz aus dem Volkszählungsurteil auch Regelungen zur Zusammenarbeit der Sicherheitsbehörden des Bundes und der Länder beabsichtigt sind.

Eng mit dem Vorstehenden hängt eine andere von mir ausgesprochene Beanstandung zusammen. Ich habe in Akten des Verfassungsschutzes von der Polizei angefertigte und an den Verfassungsschutz übermittelte erkennungsdienstliche Unterlagen gefunden. Meine Beanstandung gründet sich darauf, daß es für die Zulässigkeit der Aufbewahrung von erkennungsdienstlichen Unterlagen im polizeilichen Bereich Rechtsvorschriften bzw. eine gefestigte Rechtsprechung gibt. Ich betrachte diese Regelungen als abschließend. Die Löschung erkennungsdienstlicher Unterlagen bei der Polizei, z. B. nach Ablauf der KpS-Regelfrist von 10 Jahren, würde dem Betroffenen nur wenig nützen, wenn diese erkennungsdienstlichen Unterlagen im Wege der Amtshilfe an den Verfassungsschutz übermittelt und dort für in der Regel längere Fristen weitergespeichert werden dürften.

Ebenfalls zu diesem Fragenkreis gehört die Problematik der Übermittlung von Erkenntnissen aus Hausdurchsuchungen durch die Polizei an den Verfassungsschutz. Der Bundesminister des Innern vertritt dazu die Auffassung, daß die §§ 108, 110 StPO kein Verwertungsverbot enthalten. Er hat andererseits aber auch eingeräumt, daß aus diesen Vorschriften keine Rechtsgrundlage zur Übermittlung dieser Unterlagen zu entnehmen ist. Er hält aber die Übermittlung dieser Informationen an den Verfassungsschutz und ihre Verwertung durch das BfV für unverzichtbar. In der Praxis — dies hat meine Prüfung gezeigt — wird von dieser Möglichkeit auch Gebrauch gemacht.

In meinem Prüfbericht habe ich die Meinung vertreten, daß das BfV analog an die Fristen des Bundeszentralregistergesetzes gebunden ist, soweit es Straftaten in seinen Dateien speichert. Ich habe mich dabei von der Überlegung leiten lassen, daß der dem BZRG zugrundeliegende Resozialisierungsgedanke nur unzureichend verwirklicht werden kann, wenn zwar im Bundeszentralregister Verurteilungen gelöscht werden, es aber andere staatliche Register gibt, in denen diese Verurteilungen weiter gespeichert bleiben. Aus diesem Grund habe ich beanstandet, daß die derzeitige Struktur der Datenverarbeitung des BfV keine Gewähr dafür bietet, daß die BZR-Fristen bei der Speicherung von Straftaten in den Dateien des BfV eingehalten werden. Als Beispiel habe ich einen Fall angeführt, in dem die betreffende Person im Jahre 1969 wegen Körperverletzung im Zusammenhang mit einer vom BfV als linksextremistisch eingestuften Aktion verurteilt worden ist. Diese Verurteilung wurde als Zusatzinformation zu den Daten des Betroffenen gespeichert, die wegen extremistischer Aktivitäten registriert waren. Die weitere Aufrechterhaltung der Speicherung der Straftat aus dem Jahre 1969 habe ich beanstandet. Diese Beanstandung hat der BMI zurückgewiesen, weil nach seiner Meinung die BZR-Fristen für die Speicherung von Straftaten im BfV auch nicht analog angewandt werden können. Demgemäß will er auch die Speicherung in dem oben erwähnten Einzelfall aufrechterhalten. Im Ergebnis führt dies dazu, daß eine 1969 begangene Körperverletzung möglicherweise noch 20 Jahre danach und länger beim BfV gespeichert bleibt. Ich halte dies für unvereinbar mit dem Grundgedanken des BZRG.

In meinem Sechsten Tätigkeitsbericht (S. 50) habe ich Dateien des Verfassungsschutzes erwähnt, in denen für Zwecke der Identifizierung auch Daten gespeichert werden, die in erheblichem Maße in die Intimsphäre hineinreichen. Der Bundesminister des Innern hat Mängel dieser Spezialdateien eingeräumt und in Aussicht gestellt, daß diese Dateien in etwa drei Jahren durch ein neues Verfahren ersetzt werden sollen, das sich streng am Erforderlichkeitsprinzip orientieren soll. Für die Zwischenzeit hat der Bundesminister des Innern Übergangsvorschriften angekündigt. Als Sofortmaßnahme wurden einige besonders bedenkliche Merkmale gesperrt. Nach meiner Auffassung gibt es darüber hinaus noch weitere die Intimsphäre berührende Merkmale, die für die Aufgabenerfüllung der Abteilung III des BfV nicht erforderlich sind. Ich werde mich bemühen, für die Übergangszeit bis zur Einstellung des Verfahrens eine weitere Reduzierung des Datenumfangs zu erreichen.

21.1.2 Kontrolle der Übermittlung an ausländische Dienststellen

Wegen der zunehmenden internationalen Zusammenarbeit der Nachrichtendienste aus den zu Nr. 19.2.5 genannten Gründen habe ich erstmals die seit längerem beabsichtigte Prüfung der Übermittlung von Informationen durch das BfV an ausländische Dienststellen durchgeführt. Dabei wurde so vorgegangen, daß die Bedingungen einer umfassenden datenschutzrechtlichen Kontrolle einerseits erfüllt, die Beachtung des Quellenschutzes anderer-

seits gewahrt wurden. Ich habe im übrigen stets die Notwendigkeit des Quellenschutzes anerkannt, da es in aller Regel verzichtbar ist, die Identität einer Quelle zu kennen, um einen Sachverhalt aus datenschutzrechtlicher Sicht zu überprüfen.

Die Kontrolle selbst ergab ein überwiegend positives Bild. Anzuerkennen ist insbesondere das Bestreben des BfV, datenschutzrechtliche Belange der Betroffenen nicht zu gefährden. Das gilt vor allem auch für die Daten, die bei der Befragung von Asylbewerbern im Zusammenhang mit dem Asylverfahren von dem Bundesamt in Zirndorf erhoben werden. In der Öffentlichkeit geäußerte Befürchtungen, wonach das BfV mehr oder weniger umfangreiche Hinweise über solche Personen an die Verfolgerländer unmittelbar oder mittelbar weiterleite, haben sich nicht bestätigt.

Andererseits zeigten sich auch einige bedenkliche, zum Teil durch den organisatorischen Ablauf der Zusammenarbeit mit ausländischen Diensten bedingte Schwachstellen. Unter anderem sind zu nennen:

— unvertretbare personenbezogene Datenübermittlungen durch Übersendung zusammenfassender Berichte über bestimmte Ereignisse;

— Art und Umfang von Übermittlungen im Extremismusbereich;

— mangelnde Sorgfalt bei der Prüfung des Anfragegrundes und daraus resultierende unnötige Übermittlungen;

— ungenaue Formulierung des Anfragegrundes durch das BfV, wenn dieses bei inländischen Stellen um Auskunft bittet, um Anfragen ausländischer Dienste beantworten zu können;

— die teilweise Nichtbeachtung gesetzlicher Zuständigkeiten für Auskünfte über straf- und polizeirechtlich relevante Sachverhalte (vgl. § 57 BZRG, § 73 IRG, §§ 1 Abs. 2, 10 BKAG) mit der oben zu Nr. 19.2.6 und Nr. 20.1 dargelegten Folge, daß Regelungen, die im polizeilichen Bereich vereinbart sind und für die es bisher keine vergleichbare Regelung im nachrichtendienstlichen Bereich gibt, umgangen werden können;

— Verletzung der verfahrensmäßigen Rechte, die dem Betroffenen bei inländischen Sicherheitsüberprüfungen zustehen (insbesondere des Rechts auf Anhörung), bei der Beantwortung ausländischer Anfragen, die einer vergleichbaren Überprüfung dienen.

Ich habe eine Reihe von Verbesserungsvorschlägen gemacht und u. a. auf die im Interpolverkehr erreichten Regelungen hingewiesen. Es wäre zu prüfen, inwieweit deren Übernahme für die nachrichtendienstliche Tätigkeit möglich ist. Der Bundesminister des Innern hat mir inzwischen zugesagt, daß er mich bei der Neufassung der Dienstvorschrift für den Verkehr mit dem Ausland beteiligen und meinen Anregungen weitgehend folgen will. Bereits jetzt sollen diese Anregungen beim Auslandsauskunftsverkehr berücksichtigt werden. Ein besonders wichtiger Punkt ist auch die von mir geforderte größere Transparenz bei der Befragung von Asylbewerbern während ihres Verfahrens beim Bundesamt in Zirndorf.

21.2 Bundesnachrichtendienst

Zusammenfassung

- Die seit Jahren erhobene Forderung nach gesetzlichen Grundlagen für die informationelle Tätigkeit des Bundesnachrichtendienstes (BND) läßt sich nach dem Volkszählungsurteil des Bundesverfassungsgerichts auch verfassungsrechtlich begründen; eine entsprechende gesetzliche Regelung ist daher dringend geboten.
- Als Voraussetzung hierfür bedarf es noch einer kritischen Analyse der gegenwärtigen informationellen Praxis des BND für alle Stufen der Verarbeitung personenbezogener Daten.
- Die Kontrollen der Datenverarbeitung des BND ergaben in einigen Bereichen erneut die Notwendigkeit größerer Restriktion insbesondere beim Speichern personenbezogener Daten. Andererseits wurden zu den bisher erreichten datenschutzrechtlichen Verbesserungen weitere Fortschritte erzielt. Das betrifft vor allem Einschränkungen der Übermittlung sowie den Abbau von Altfällen.
- Nach dem Beschluß des Bundesverfassungsgerichts vom 20. Juni 1984 zur Tätigkeit des BND aufgrund § 3 Gesetz zu Artikel 10 GG — G 10 — (sogenannte strategische Kontrolle der Post- und Fernmeldeverkehrsbeziehungen) kann meine Kontrollkompetenz für diesen Bereich und generell für Überwachungsmaßnahmen der Nachrichtendienste des Bundes nach dem G 10 nicht mehr in Frage gestellt werden.

21.2.1 Notwendigkeit gesetzlicher Regelungen

Auf die Notwendigkeit gesetzlicher Grundlagen für die informationelle Tätigkeit des BND habe ich immer wieder, zuletzt im Sechsten Tätigkeitsbericht (S. 51), hingewiesen. Vereinzelt bestehen zwar gesetzliche Bestimmungen, die jeweils Teilbereiche regeln (so die Übermittlungsregelungen nach § 41 — früher § 39 — BZRG, § 72 SGB X, § 18 MRRG und die entsprechenden landesrechtlichen Bestimmungen sowie die Ausnahmeregelungen über bestimmte datenschutzrechtliche Pflichten nach §§ 12 Abs. 2, 13 Abs. 2, 19 Abs. 3 und 4 BDSG). Außerdem regelt das Gesetz zu Artikel 10 GG Einzelheiten besonders schwerwiegender Datenerhebung und -verwertung.

Eine umfassende bereichsspezifische Regelung, die klarstellt, unter welchen Voraussetzungen und in welchen Grenzen der BND Daten erheben, speichern, übermitteln und sonst verwerten darf, fehlt jedoch. Sie ist nach dem Volkszählungsurteil des Bundesverfassungsgerichts jedoch unerläßlich und auch Voraussetzung für die weitere Rechtsetzung, soweit darin Datenübermittlungen an den BND vorgesehen werden und dabei — wie bisher — allein

auf die Erfüllung der dem BND obliegenden Aufgaben abgestellt wird.

Solange diese Aufgaben nicht gesetzlich festgelegt sind, bleiben solche Datenübermittlungen, wenn sie auf die vorhandenen Spezialvorschriften (siehe oben) gestützt werden, problematisch; künftige Regelungen dieser Art könnte ich als alleinige Rechtsgrundlage für Datenübermittlungen an den BND nicht akzeptieren. In diesem Sinne habe ich mich auch in meiner Stellungnahme vom 25. April 1984 über die Auswirkungen des Volkszählungsurteils im Zusammenhang mit der Novellierung des Personalausweisgesetzes und den dort vorgesehenen Übermittlungsregelungen an den BND geäußert (B 6.3 und 10, S. 49 und 54; gleiches gilt für den MAD, hierzu nachstehend zu Nr. 21.3). Es liegt nicht nur im Interesse des Datenschutzes, sondern ebenso im Interesse des BND sowie aller an der informationellen Zusammenarbeit mit dem BND beteiligten Stellen, daß die entsprechenden Aufgaben- und Befugnisnormen für den BND mit der gebotenen Klarheit bald erlassen werden.

21.2.2 Praktische Grundlagen und Schwerpunkte gesetzlicher Regelungen

Eine wichtige Grundlage hierfür wird die auf meine Anregung hin in Bearbeitung befindliche genaue Zusammenstellung aller von der Datenverarbeitung des BND betroffenen Personenkreise sein. Diese Zusammenstellung ist noch nicht vollständig und konnte mir daher bei meiner letzten Prüfung noch nicht vorgelegt werden. Die Personenkreise, die von der gegenwärtigen Datenverarbeitung des BND betroffen sind, lassen sich nämlich mit der erforderlichen Klarheit aus der Dateienübersicht gemäß § 15 BDSG in Verbindung mit den dazu angeführten weiteren Unterlagen nicht entnehmen. Damit fehlt auch eine wichtige Grundlage für meine Kontrollaufgabe. Sie soll durch die von mir empfohlene Übersicht geschaffen bzw. vervollständigt werden und gleichzeitig eine wesentliche Ausgangsbasis für die künftigen Gesetzgebungsarbeiten sein. Auch die in vielen Teilbereichen bisher erreichten Verbesserungen können eine wertvolle Hilfe sein.

Vordringlich regelungsbedürftig erscheinen die „Außenbeziehungen" des BND, d. h. die Voraussetzungen, unter denen personenbezogene Daten an den BND durch andere Stellen und vom BND an solche übermittelt werden dürfen. Im ersten Fall ist gleichzeitig die Zulässigkeit der weiteren Verarbeitung beim BND zu regeln, so daß jedenfalls insoweit die gesetzliche Klarstellung des Informationsaustausches mit der Aufgaben- und Befugniszuweisung an den BND einhergehen muß, ähnlich wie dies auch im Gesetz zu Artikel 10 GG geschehen ist.

21.2.3 Kontrollergebnisse

Meine Kontrollen in diesem Jahr haben erneut sowohl bedenkliche als auch erfreuliche Aspekte ergeben.

Bedenklich sind nach wie vor folgende Praktiken, die bei der Erarbeitung gesetzlicher Grundlagen kritisch geprüft werden sollten:

- Art und Umfang der Informationserhebung im Zusammenhang mit dem Befragungswesen sowie bestimmte organisatorische Verbindungen mit anderen Behörden, die einem Online-Anschluß gleichkommen (hierzu schon 5. TB S. 97).

- Die Speicherung von Daten über bestimmte Personen zu Zwecken der Sicherheit des BND oft allein deshalb, weil sie in mehr oder weniger zufälligem, aber plausiblem Kontakt zum Umfeld von Bediensteten oder Liegenschaften des BND stehen. Eine im Berichtsjahr durchgeführte Auswertung ergab, daß es sich hier um einen relativ großen Personenkreis handelt. Bei künftigen Regelungen wäre zumindest zu fragen, ob in den meisten Fällen nicht eine Dateianfrage ausreicht und eine Speicherung entfallen kann, wenn keine Erkenntnisse zu der Person vorliegen. Auch wäre an kürzere Überprüfungsfristen als die Regelfrist von 15 Jahren zu denken. Gemildert ist die Problematik allerdings durch die mehrfach überprüfte Zusage des BND, über diesen Personenkreis grundsätzlich keine *inhaltliche* Auskunft an dritte Stellen zu erteilen (hierzu auch 6. TB S. 51). Allerdings ist die Tatsache, daß diese Personen beim BND gespeichert sind, der gegenwärtigen Formulierung der Auskunft zu entnehmen (vgl. auch unten). Ich habe daher empfohlen, daß künftig hier — wie zu einem anderen Personenkreis bereits früher vereinbart (vgl. 6. TB S. 51) — auch diese Art der Auskunftserteilung in der Regel entfällt, so daß kein Rückschluß auf die Speicherung mehr möglich ist. Im übrigen hat mir der BND zugesagt, die bisherigen Speicherungen dieser Art beschleunigt zu überprüfen und bei Neueinspeicherungen einen strengeren Maßstab als bisher anzulegen.

- Bei manchen Anfragearten, die m. E. überhaupt nicht an den BND gerichtet werden sollten (z. B. in einigen Fällen bei der Einstellungsüberprüfung), wird zwar ebenfalls keine inhaltliche Auskunft erteilt, der BND gibt aber durch die Formulierung der Auskunft zu erkennen, daß die Person — aus welchen Gründen auch immer — beim BND registriert ist. Meinem Vorschlag, in solchen Fällen prinzipiell die Auskunft „keine Erkenntnisse" zu erteilen, wurde bisher nicht entsprochen. Zu Unrecht wird hier auf die Verantwortung der anfragenden Stelle abgehoben.

- In einem bestimmten Bereich orientiert sich die Speicherung oft zu sehr an zusammenfassenden Berichten anderer Stellen. Da diese Stellen wiederum zu personenbezogenen Daten, die in solchen Berichten enthalten sind, keinen Nachbericht bei wichtigen Änderungen liefern, der BND andererseits keine kontinuierliche Überprüfung der Relevanz solcher Daten gewährleisten kann, bleiben die Speicherungen in der Regel bis zum Ablauf der 15-Jahres-Frist bestehen, soweit keine Zeitspeicherung vorliegt. Daran ändert sich auch dann nichts, wenn bei der ursprünglich berichtenden Stelle zwischenzeitlich die Hinweise vernichtet wurden.

Meinem mehrfach gemachten Vorschlag, diesen Problemen u. a. dadurch zu begegnen, daß eine Speicherung beim BND in diesem Bereich nur dann erfolgt, wenn Ermittlungen auf eigene Initiative oder auf Antrag einer dritten Stelle angestellt werden oder der BND sonst als Vermittler auftritt, wurde bisher nicht Rechnung getragen. Doch hat der BND zugesagt, bei der Speicherung auf der Grundlage von Berichten der genannten Art künftig einen strengeren Maßstab anzulegen, nachdem das Problem in einem aktuellen Fall im Rahmen der letzten Kontrollen besonders deutlich hervorgetreten ist.

— Bei der Frage der Notwendigkeit personenbezogener Speicherung im Bereich der Beobachtung des Internationalen Kommunismus (vgl. hierzu 6. TB S. 52) hat meine letzte Kontrolle eine Verbesserung insoweit gezeigt, als sich die Speicherung mehr auf die wichtigeren Angehörigen („Träger") einschlägiger Organisationen beschränkt.

— Die Fristen für die Überprüfung auf Löschungswürdigkeit der Daten sind mit generell 15 Jahren zu pauschal geregelt. Die nach den Löschungsrichtlinien vorgesehene Verlängerungsmöglichkeit in bestimmten Fallgruppen wird im Zweifel extensiv gehandhabt. Einigkeit besteht jedoch inzwischen für die Auslegung der nach den Richtlinien vorgesehenen Zugriffsbeschränkung (Sperrklausel) für bestimmte Datengruppen nach Ablauf von 15 Jahren. In diesem Fall besteht eine prinzipielle Auskunftssperre an dritte Stellen. Es darf dann auch kein Hinweis mehr auf die Tatsache der Speicherung erfolgen, sofern nicht besondere Gründe im Einzelfall vorliegen (vgl. hierzu auch 6. TB S. 51). Um die bei den Prüfungen dieses Jahres in mehreren Fällen festgestellten Verstöße gegen die Sperrklausel künftig zu vermeiden, hat der BND eine entsprechende Weisung gegeben.

— Wenn der Zeitpunkt des Ereignisses und der Zeitpunkt der Einspeicherung auseinanderliegen, ist bisher nicht sichergestellt, daß die zeitliche Diskrepanz bei der Regelüberprüfung berücksichtigt wird. Dies kann — wie Einzelfälle belegen — zu einer Fristverlängerung bis zu fünf Jahren und mehr führen. Lediglich für einen Bereich, bei dem dies häufiger vorkommt, konnte vereinbart werden, daß die Frist vom Zeitpunkt des Ereignisses und nicht der Speicherung ab berechnet und die entsprechende Wiedervorlage sichergestellt wird. Für einen anderen Bereich, in dem Ereignis und Zeitpunkt der Speicherung nach der Struktur des Meldeaufkommens ebenfalls häufiger differieren, wurde dieses Modell „aus technischen Gründen" dagegen bisher nicht übernommen.

Demgegenüber ist auf folgende positive Gesichtspunkte hinzuweisen:

— Der nunmehr zügig durchgeführte Abbau von Altfällen hat im Jahre 1984 zu Löschungen erheblichen Umfangs geführt. Allerdings ist die regelmäßige Überprüfung der 15-Jahres-Frist nach wie vor nicht vor 1991 sichergestellt, weil erst seit 1976 der Zeitpunkt der Erstspeicherung festgehalten wird (vgl. hierzu 5. TB S. 99 und 6. TB S. 51).

— Nach einer Prüfung der Speicherung von Daten über Personen unter 16 Jahren wurde vereinbart, daß dieser Personenkreis künftig — von besonders gelagerten Ausnahmefällen abgesehen — von der Speicherung ausgenommen wird. Die Zahl der gespeicherten Datensätze für diesen Personenkreis ist dadurch deutlich zurückgegangen.

— Bei den von mir durchgeführten Kontrollen von Einzelfällen und Querschnittsanfragen konnten öfter als früher Löschungen erreicht werden oder der BND hat die sofortige Überprüfung bei einer größeren Zahl problematischer Fälle zugesagt.

— Die Möglichkeit der Zeitspeicherung wird wenigstens in einem Bereich zunehmend genutzt. Dadurch können für die sehr häufigen Grenzfälle kürzere Überprüfungsfristen vorgesehen werden.

— Generell muß hervorgehoben werden, daß der BND trotz aller vorstehend erwähnten Problempunkte den Erfordernissen des Datenschutzes aufgeschlossen gegenübersteht, was meine Kontrolltätigkeit erleichtert.

21.2.4 Kontrollkompetenz für Maßnahmen nach dem G 10

Für die Frage meiner Kontrollkompetenz im G 10-Bereich hat das Bundesverfassungsgericht im Beschluß vom 20. Juni 1984 zur Verfassungsmäßigkeit von § 3 G 10 (1 BvR 1494/78) eine entscheidende Klarstellung vorgenommen. Das Bundesverfassungsgericht hat ausdrücklich auf meine früheren Kontrollen in diesem Bereich Bezug genommen (hektographierte Fassung S. 28), deren Ergebnisse ich im Zweiten Tätigkeitsbericht geschildert habe (S. 50). Es hat darüber hinaus festgestellt, daß die Befugnis nach § 3 G 10 „nur deshalb hingenommen werden kann, weil die Kontrolle der Maßnahmen ... durch unabhängige und an keine Weisung gebundene staatliche Organe und Hilfsorgane (Kontrollkommission und Datenschutzbeauftragte) sichergestellt ist" (hektographierte Fassung S. 30). Hierbei hat das Bundesverfassungsgericht an die bereits im Volkszählungsurteil allgemein betonte Bedeutung der „Beteiligung unabhängiger Datenschutzbeauftragter ... für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung" (BVerfGE 65, 1, 46) erinnert. Damit wurde meine im Dritten Tätigkeitsbericht (S. 47 f.) näher dargelegte Auffassung zu der bisher von der G 10-Kommission bestrittenen parallelen Kontrollbefugnis bestätigt. Dies muß über § 3 G 10 hinaus für die Datenverarbeitung aller Nachrichtendienste nach dem G 10 gelten. Denn das Bundesverfassungsgericht hat nicht nur vom Bundesbeauftragten für den Datenschutz, sondern unter Bezugnahme auf das Volkszählungsurteil von den „Datenschutzbeauftragten" generell gesprochen, womit auch die Kontrollbefug-

nis der Landesbeauftragten umfaßt ist. Diese haben jedoch keine Zuständigkeit für die Kontrolle von Maßnahmen nach § 3 G 10. Ihnen obliegt vielmehr die Kontrolle der G 10-Maßnahmen des jeweiligen Landesamtes für Verfassungsschutz nach Maßgabe der Landesdatenschutzgesetze (mit Ausnahme des Saarländischen Datenschutzbeauftragten, vgl. § 20 Saarl. Datenschutzgesetz).

Im übrigen ergibt sich diese Kontrollkompetenz für meinen Bereich auch aus dem eindeutigen Wortlaut von § 19 Abs. 1 und 3 BDSG. Hiernach hat der BfD die Einhaltung der Vorschriften des BDSG sowie anderer Vorschriften über den Datenschutz bei allen Behörden und öffentlichen Stellen des Bundes zu kontrollieren. Hiervon ausgenommen sind lediglich die Gerichte, soweit sie nicht in Verwaltungsangelegenheiten tätig werden (§ 19 Abs. 1 BDSG). Für die Nachrichtendienste des Bundes ist also für kein Tätigkeitsfeld eine Einschränkung der datenschutzrechtlichen Kontrolle vorgesehen. Die einzige Ausnahme kann sich aufgrund von § 19 Abs. 3 Satz 4 BDSG ergeben, nämlich dann, wenn im Einzelfall von der obersten Bundesbehörde festgestellt wird, daß die Einsicht in Unterlagen die Sicherheit des Bundes oder eines Landes gefährdet. Das kann vorübergehend auch bei einer G 10-Maßnahme der Fall sein (z. B. besonders wichtige laufende operative Maßnahme), keinesfalls aber generell im Anwendungsbereich des G 10. Im Gegenteil: Nach dem Beschluß des Bundesverfassungsgerichts steht fest, daß die unabhängige Kontrolle der Datenschutzbeauftragten zur Wahrung des informationellen Selbstbestimmungsrechts gerade bei G 10-Maßnahmen unverzichtbar ist.

Ich gehe davon aus, daß ich entsprechend meinem gesetzlichen Auftrag Kontrollen auch in diesem Bereich nunmehr ungehindert durchführen kann.

21.3 Militärischer Abschirmdienst

Zusammenfassung

- Nach dem Volkszählungsurteil des Bundesverfassungsgerichts ist eine klare und präzise Regelung der Aufgaben und Befugnisse des Militärischen Abschirmdienstes (MAD) unumgänglich.
- Die Bereinigung der Datenbestände beim MAD hat weitere Fortschritte gemacht, die „Basiskartei Zersetzung" ist vollständig gelöscht.
- Im Rahmen der „personellen Vorbeugung" werden auf Vorrat Daten gespeichert, die zum Teil keinen unmittelbaren Bundeswehrbezug haben. Die Notwendigkeit für derartige Parallelspeicherungen zu den Staats- und Verfassungsschutzbehörden ist nach meiner Auffassung nicht überzeugend dargetan.
- Derzeit ist die Einhaltung des Zweckbindungsgrundsatzes vor allem im Bereich der Sicherheitsüberprüfung nicht gewährleistet.
- Neue DV-Vorhaben des MAD werfen neue datenschutzrechtliche Fragen auf.
- Nach dem Beschluß des Bundesverfassungsgerichts vom 20. Juni 1984 zur Tätigkeit des BND aufgrund § 3 Gesetz zu Artikel 10 GG (vgl. Nr. 21.2.4) kann meine Kontrollkompetenz für Überwachungsmaßnahmen des MAD nach dem G 10 nicht mehr streitig sein.

21.3.1 Notwendigkeit gesetzlicher Grundlagen

Die Aktivitäten des Militärischen Abschirmdienstes (MAD) im Zusammenhang mit der vorzeitigen Pensionierung eines Generals der Bundeswehr haben heftige öffentliche Diskussionen über Aufgaben und Befugnisse des MAD hervorgerufen. Von den vielen in diesem Zusammenhang öffentlich diskutierten Aspekten scheinen mir besonders zwei von Bedeutung zu sein: Der Fall hat verdeutlicht, welche Probleme es aufwirft, wenn eine Polizeibehörde im Auftrag eines Nachrichtendienstes ermittelt. Aufgaben und Befugnisse von Polizei und Nachrichtendiensten sind so unterschiedlich, daß zwangsläufig Komplikationen auftreten müssen, wenn auf dem sogenannten „kleinen Dienstweg" gegenseitig bei der Informationserhebung ausgeholfen wird.

Zum anderen ist in der öffentlichen Diskussion die auch von mir seit Jahren erhobene Forderung nach einer klaren, präzisen Regelung von Aufgaben und Befugnissen des MAD unterstützt worden. Insbesondere der Abschlußbericht der sogenannten „Höcherl-Kommission" kommt zu demselben Ergebnis. Es bleibt zu hoffen, daß der Gesetzgeber diesen Forderungen Rechnung trägt. Aus datenschutzrechtlicher Sicht würde damit der unerfreuliche Zustand beendet, daß beim MAD in großem Umfang personenbezogene Daten verarbeitet werden, ohne daß dafür eine Rechtsgrundlage besteht. Dies ist nicht nur ein formaler Aspekt. Wo Aufgaben und Befugnisse nicht klar und präzise beschrieben sind, bleibt immer Raum für verschiedene, auch extensive Interpretationen des Aufgabenverständnisses. So wäre zu wünschen, daß der Gesetzgeber nicht nur die gewachsenen Strukturen und Aufgabenbereiche des MAD nachträglich sanktioniert, sondern eine an den konkreten Bedürfnissen eines Dienstes zur Wahrung der militärischen Sicherheit orientierte Lösung findet.

21.3.2 Weitere Verbesserungen und Erfolgskontrolle

Ich habe mich auch im Berichtsjahr auf der Grundlage der bestehenden innerdienstlichen Weisungen und Richtlinien um weitere konkrete Verbesserungen des Datenschutzes beim MAD bemüht. Die Bereitschaft zur Zusammenarbeit auf diesem Gebiet hat beim MAD trotz personeller Fluktuation unvermindert angehalten. So sind weitere bemerkenswerte Konsequenzen aus meiner datenschutzrechtlichen Prüfung aus dem Jahr 1982 gezogen worden. In der Tendenz laufen diese Konsequenzen auf die Löschung zu Unrecht gespeicherter personenbezogener Daten, auf die Einschränkung der Übermittlung von Daten an andere Behörden sowie auf die Neutralisierung von Aktenzeichen und damit auf die Verminderung der Gefahr von Entscheidungen nur aufgrund von Computerauszügen hinaus (vgl.

auch oben 19.2.1). Bei einem Kontrollbesuch im Frühjahr 1984 mußte ich allerdings feststellen, daß die gebotene Bereinigung manchmal zu formalistisch und am Buchstaben meiner Prüfbemerkungen orientiert durchgeführt worden war, ohne zu berücksichtigen, daß die von mir aufgegriffenen und beispielhaft herausgestellten Fälle stets auch für alle anderen vergleichbaren Fälle gelten. Eine Datenschutzkontrolle kann aus der Vielzahl der gespeicherten Daten immer nur einige wenige einbeziehen und anhand dieser Einzelfälle allgemeine Lösungen aufzeigen. Durch entsprechende Löschungsanordnungen ist inzwischen sichergestellt worden, daß auch die weitere Bereinigung in der Folge zügig und gründlich vorgenommen wird.

Die von mir insgesamt beanstandete und in der Öffentlichkeit besonders kritisierte *„Basiskartei Zersetzung"* ist nach Mitteilung des MAD mit dem gesamten Bestand von ca. 45 000 Karteikarten vernichtet worden. Es wurden weder Ersatzkarteien angelegt noch sonstwie in ähnlicher Weise Informationen aus der „Basiskartei Zersetzung" gespeichert.

21.3.3 Probleme der „Personellen Vorbeugung"

Umstritten ist zwischen dem MAD und mir nach wie vor das Instrument der sogenannten *personellen Vorbeugung* (vgl. auch oben Nr. 19.2.1). Nach Auffassung des MAD muß die Bundeswehr wissen, welche „Extremisten" im jeweiligen wehrpflichtigen Jahrgang auf sie zukommen, um hierauf gezielt reagieren zu können. Der MAD speichert in diesem Zusammenhang Daten über Personen, die vom Alter her noch als Wehrpflichtige eingezogen werden können. Die Informationen werden ihm zumeist von anderen Sicherheitsbehörden ohne Rechtsgrundlage im Wege der Amtshilfe übermittelt. Sie sind also auch bei der übermittelnden Stelle bereits gespeichert. Dies hat eine Verdoppelung der Speicherung über ein und dasselbe Ereignis zur Folge. Handelt es sich beispielsweise um einen Jugendlichen, so kann es sein, daß seine Daten aufgrund besonderer Datenschutzbestimmungen bei der betreffenden Polizeibehörde oder beim Verfassungsschutz nach fünf Jahren wieder gelöscht werden. Beim MAD hingegen, der eigentlich für die Speicherung derartiger Informationen gar nicht zuständig ist, bleiben sie unter Umständen länger gespeichert. Da der MAD auch seinerseits im Wege der Amtshilfe Daten weitergibt, können derartige Daten an dritte oder vierte Stellen gelangen, obwohl die ursprünglich erhebende Behörde sie längst gelöscht hat. Wirksame Datenschutzmaßnahmen, insbesondere die vollständige Löschung personenbezogener Daten, sind bei einer derartigen Praxis nur schwer durchzusetzen (vgl. auch allgemein oben Nr. 19.2.1).

Ich habe mich gegenüber dem MAD auf den Standpunkt gestellt, daß Informationen über Personen, die der Bundeswehr noch nicht angehören, nur dann vom MAD gespeichert werden dürfen, wenn ihre extremistische Betätigung unmittelbaren Bundeswehrbezug hat, wenn es sich also insoweit um zersetzende Tätigkeit, d. h. um verfassungsfeindliche Bestrebungen mit unmittelbarem Bundeswehrbezug handelt. Dies würde eine ganz erhebliche Reduzierung der Speicherungen im Bereich der Zersetzungsabwehr generell zur Folge haben. Da der MAD nicht allgemeine Staatsschutz- bzw. Verfassungsschutzbehörde ist, läßt sich seine gegenteilige Auffassung nicht damit begründen, der Betreffende könne ja einmal Soldat in der Bundeswehr werden. Dies wäre eine Vorratsspeicherung, die das Bundesverfassungsgericht — in einem anderen Zusammenhang — für unzulässig erklärt hat.

Ich sehe im übrigen auch keine Notwendigkeit für das Instrument der personellen Vorbeugung in dieser Ausgestaltung. Von den jährlich einberufenen Wehrpflichtigen wird etwa die Hälfte ohnehin einer Sicherheitsüberprüfung unterzogen, weil sie Umgang mit Verschlußsachen erhält. Im Rahmen dieser Sicherheitsüberprüfungen werden auch Anfragen bei Polizeibehörden und den Behörden für Verfassungsschutz vorgenommen. Etwaige dort zu Recht gespeicherte Informationen können auf diesem Wege an den MAD übermittelt werden. Im Gegensatz zum Verfahren bei der personellen Vorbeugung werden sie dann aber aus einem konkreten Anlaß im Rahmen einer Überprüfung übermittelt, die dem Betroffenen eröffnet wird und ihm die Chance bietet, zu belastenden Informationen Stellung zu nehmen.

Da sicherheitsrelevante Informationen in der Bundeswehr nicht nur beim Umgang mit Verschlußsachen im eigentlichen Sinne anfallen können, wurde im Jahre 1980 die Möglichkeit einer sogenannten *„Sicherheitsanfrage"* geschaffen. Für Soldaten, die in besondere Vertrauensstellungen oder in besonders sicherheitsrelevante Tätigkeiten eingewiesen werden, besteht danach die Möglichkeit, eine verkürzte Sicherheitsüberprüfung vorzunehmen. Auch dabei erfolgt eine Nachfrage bei den Behörden des Verfassungsschutzes. Datenübermittlungen sind hier aber weniger bedenklich, weil es sich um konkrete Auskunftsersuchen zu einem konkreten Zweck handelt und der Betroffene von dieser Überprüfung Kenntnis hat. Freilich ist bei beiden Alternativen eine klare gesetzliche Regelung für solche Übermittlungen erforderlich.

Lediglich für den verbleibenden Rest von ca. einem Drittel der Wehrpflichtigen besteht eine „Überprüfungslücke". Sinn und Zweck der personellen Vorbeugung kann es also nur sein, über jenen begrenzten Personenkreis, der keinen Umgang mit Verschlußsachen erhält und keine besondere sicherheitsrelevante Vertrauensstellung bekleidet, schon vor der Einberufung zu wissen, ob sich einzelne aus ihm bereits extremistisch betätigt haben, um gegebenenfalls geeignete Abwehrmaßnahmen zu ergreifen. Meine datenschutzrechtliche Prüfung im Jahre 1982 hat ergeben, daß jedenfalls nicht ausgeschlossen werden kann, daß einzelnen Soldaten durch das praktizierte Verfahren Nachteile erwachsen können, obwohl sie sich in der Bundeswehr selbst nicht extremistisch betätigen. Tun sie es wirklich, so wird dies dem MAD im Rahmen seiner Aufgabenerfüllung ohnehin bekannt, so daß eine Vorratsspeicherung unnötig und unverhältnismäßig ist.

Die möglichen Vorteile, die mit dem derzeitigen Verfahren der personellen Vorbeugung verbunden sind, vermögen nach meiner Auffassung die datenschutzrechtlichen Nachteile nicht aufzuwiegen. Leider konnte in diesen Fragen bislang noch keine Einigung mit dem MAD erzielt werden.

21.3.4 Sicherheitsüberprüfung und Zweckbindung

Ein weiterer, bislang nicht abschließend geklärter Punkt ist die Frage der *Zweckbindung*. Schon vor Erlaß des Volkszählungsurteils habe ich im Bericht über meine datenschutzrechtliche Kontrolle des Jahres 1982 die Beachtung des Grundsatzes der Zweckbindung verlangt. Aus ihm folgt nach meiner Auffassung, daß sich ein Nachrichtendienst mit ganz unterschiedlichen Aufgaben nicht in jeder Hinsicht als Einheit begreifen darf.

Konkret habe ich vor allem die Beachtung des Grundsatzes der Zweckbindung für den Bereich der Sicherheitsüberprüfung verlangt. Bei einer Sicherheitsüberprüfung ist der Betroffene gezwungen, in erheblichem Ausmaß personenbezogene Auskünfte über sich und gegebenenfalls nahe Verwandte zu geben. Einzelne Fragen in dem entsprechenden Erklärungsbogen können auf eine Selbstbezichtigung hinauslaufen, so wenn z. B. nach strafbaren Handlungen gefragt wird, nach Mitgliedschaften in extremistischen Organisationen oder danach, ob der Betreffende sich in wirtschaftlichen Schwierigkeiten befindet. Im Erklärungsbogen wird dem zu Überprüfenden zugesichert, die geforderten Angaben würden „streng vertraulich" behandelt.

Der MAD steht auf dem Standpunkt, daß die im Wege der Sicherheitsüberprüfung beim Betroffenen selbst erhobenen Daten auch für seine sonstigen Aufgaben frei zur Verfügung stehen. Im Ergebnis kann dies z. B. zu einer Speicherung im Rahmen der Zersetzungsabwehr führen. Da der MAD im Rahmen der Zusammenarbeit mit anderen Sicherheitsbehörden auf dem Wege der Amtshilfe auch Daten aus Sicherheitsüberprüfungsakten übermittelt, kann es im Einzelfall vorkommen, daß die Angaben im Erklärungsbogen zur Sicherheitsüberprüfung letztlich zu einer Speicherung beim Verfassungsschutz führen. Auch im Hinblick auf die Zusicherung vertraulicher Behandlung der im Rahmen der Sicherheitsüberprüfung abverlangten Daten vertrete ich die Auffassung, daß sie nur für diesen Zweck verwendet werden dürfen. Eine Übermittlung an eine andere Sicherheitsbehörde halte ich nur für zulässig, wenn auch diese die Daten für die Durchführung einer Sicherheitsüberprüfung verwenden will.

21.3.5 Entwicklung der Datenverarbeitung beim MAD

Der *weitere Ausbau* der *elektronischen Datenverarbeitung* geht auch beim MAD zügig voran. So wie bei allen anderen Sicherheitsbehörden werden auch dort neue Verfahren entworfen, erprobt und angewandt. In der Tendenz läuft dies auf die Erfassung von mehr und detaillierteren Daten in den automatisierten Dateien hinaus. Die Entwicklung der Datenverarbeitung auch beim MAD zielt immer mehr darauf ab, über die Funktion eines Aktennachweissystems hinaus auch Akteninhalte dateimäßig und damit nach den unterschiedlichsten Gesichtspunkten auswertbar darzustellen. Hieraus können sich neue datenschutzrechtliche Probleme ergeben. Werden Akteninhalte teilweise oder überwiegend in Dateiform automatisiert gespeichert, so wächst die Versuchung, sich auf diese Informationen zu verlassen und die Originalbelege in der Akte nicht mehr nachzulesen. Besonderheiten des Einzelfalls, atypische Fallvarianten, möglicherweise Entlastendes könnten zu kurz kommen. Auch könnte die Neigung entstehen, möglichst alle Daten zu erheben, die in der entsprechenden Datei gespeichert werden können. Diese Bedenken, die nicht spezifisch für die Entwicklung beim MAD sind, habe ich dem MAD vorgetragen.

Die Gespräche über die neuen DV-Verfahren beim MAD sind noch nicht abgeschlossen. Der kooperative Stil, in dem sich bislang die Zusammenarbeit mit dem MAD gestaltet hat, läßt mich hoffen, daß auch bei den neuen DV-Verfahren deutliche datenschutzrechtliche Korrekturen erreichbar sind.

22. Nicht-öffentlicher Bereich

22.1 Grundsätzlicher Regelungsbedarf

Das grundsätzlich gewährleistete Recht des einzelnen auf informationelle Selbstbestimmung gilt nicht nur im Verhältnis zwischen Bürger und Staat, es muß grundsätzlich auch im nicht-öffentlichen Bereich Gültigkeit haben. Darauf habe ich in meiner Stellungnahme zum Volkszählungsurteil gegenüber dem Innenausschuß des Deutschen Bundestages hingewiesen. Diese Auffassung wird auch vom Bundesminister der Justiz geteilt (vgl. Bulletin vom 18. September 1984).

Das Bundesverfassungsgericht hat in seinem Urteil die Bedeutung der Datenschutzkontrollen unterstrichen, mit deren Hilfe der Gefahr einer Verletzung des Persönlichkeitsrechts entgegengewirkt werden soll. In der Praxis bestehen jedoch in einigen Fällen für die Aufsichtsbehörden gesetzliche Hinderungsgründe, Vorgänge datenschutzrechtlich zu überprüfen, obwohl Datenschutzverstöße bekannt sind oder doch gravierende Anhaltspunkte für die Beeinträchtigung schutzwürdiger Belange vorliegen. So dürfen die Aufsichtsbehörden im nicht-öffentlichen Bereich nach § 30 BDSG nur dann tätig werden, wenn ein Betroffener begründet darlegt, in seinen Rechten verletzt zu sein (sogenannte Anlaßaufsicht). Solange es also an einer Beschwerde fehlt, besteht für die Datenschutzaufsicht keine Möglichkeit der Überprüfung. Ebenso verhält es sich, wenn der Betroffene Beschwerde führt, aber keine konkreten Tatsachen darlegen kann. Selbst mit konkreten Tatsachen belegten Beschwerden kann die Aufsichtsbehörde nicht nachgehen, wenn der Beschwerdeführer nicht in eigener Person von der Datenschutzverletzung betroffen ist. Ein vorbeugendes Tätigwerden, um Persönlichkeitsverletzungen

„entgegenzuwirken", wie es nach dem Verfassungsgerichtsurteil gefordert wird, ist von vornherein nicht möglich, da die gesetzliche Formulierung in § 30 BDSG voraussetzt, daß schon jemand in seinen Rechten „verletzt worden ist". So war den Aufsichtsbehörden die teilweise Nichtbeachtung des Datenschutzes bei der Erteilung von Bankauskünften seit Jahren bekannt, sie konnten jedoch nicht einschreiten, da es an Beschwerden Betroffener fehlte.

Ein weiteres Defizit beim Datenschutz ergibt sich aus der gesetzlichen Voraussetzung, daß die zu überprüfende Datenverarbeitung in Form einer Datei erfolgt. Diese Abhängigkeit der Anwendung der Schutzbestimmungen von der Art der Verarbeitung räumt dem Betroffenen bei sonst gleichem Sachverhalt im einen Falle die Wahrnehmung seiner Datenschutzrechte ein, im anderen Falle schließt sie ihn davon aus. Dies widerspricht dem vom Bundesverfassungsgericht aufgestellten Grundsatz, daß der Bürger erkennen können muß, wer was wann bei welcher Gelegenheit über ihn weiß.

Ein Wirtschaftsbereich, in dem diese willkürliche Unterscheidung Bedeutung erlangt, ist der der Handels- und Wirtschaftsauskunfteien. Einige große Auskunfteien haben in Verhandlungen mit den Datenschutzaufsichtsbehörden anerkannt, daß die Regelungen des BDSG auf sie Anwendung finden. Sie machen allerdings einschränkend geltend, daß nicht alle gesammelten Unterlagen und recherchierten Informationen unter den Datenschutz fielen, sondern nur diejenigen, die in einem „Datenspiegel" festgehalten seien. Damit fällt der größte Teil des vorhandenen Datenmaterials aus dem Schutzbereich des Gesetzes heraus. Andere Unternehmungen dieses Wirtschaftsbereichs entziehen sich dem Datenschutz dadurch, daß sie auf die Art ihrer Datensammlung in Akten und Mappen verweisen und den Aufsichtsbehörden — bisher erfolgreich — die Prüfungsbefugnis streitig machen.

Für eine Verbesserung des Datenschutzes im nichtöffentlichen Bereich ist weiterhin die Einbeziehung jeglichen Umgangs mit personenbezogenen Daten in Erwägung zu ziehen, nachdem das Bundesverfassungsgericht das Recht auf informationelle Selbstbestimmung unabhängig von bestimmten Verarbeitungsformen anerkannt hat. Aufgrund der Beschränkung der Anwendung des BDSG auf die in § 2 BDSG definierten Phasen der Verarbeitung bleiben Datenverarbeitungsvorgänge innerhalb einer speichernden Stelle unberücksichtigt. Wie das Beispiel der Verwendung von Inkassodaten für Auskunfteizwecke unter Nr. 9.6.2 zeigt, kann sich jedoch eine solche „interne" Zweckänderung für den Betroffenen wie eine unbefugte Übermittlung auswirken und sollte deshalb vom Gesetz erfaßt werden.

22.2 Bankauskunft

Das herausragende positive Datenschutzereignis des abgelaufenen Jahres im nicht-öffentlichen Bereich ist die neue Regelung der Bankauskünfte. Die mit den Datenschutzinstanzen abgestimmten neuen Grundsätze für das Bankauskunftsverfahren signalisieren ein Umdenken bei Banken und Sparkassen hin zu einer stärkeren Berücksichtigung des Persönlichkeitsschutzes der Betroffenen.

Während die Kreditwirtschaft bislang davon ausging, daß die Erteilung von Bankauskünften stillschweigender Bestandteil des Vertragsverhältnisses mit der Bank sei, einer Verkehrssitte entspreche und sich implizit auch aus dem Angebot der Kreditinstitute ergebe, dem Kunden mit allen bankmäßigen Auskünften zur Verfügung zu stehen (Nr. 10 Allgemeine Geschäftsbedingungen [AGB] der Banken, Nr. 7 Sparkassen-AGB, jeweils in der alten Fassung), steht bei der neuen Vereinbarung die Selbstbestimmung des Bankkunden im Vordergrund. Von der Seite des Datenschutzes hat man der Auffassung, daß § 24 BDSG Bankauskünfte gestatte, von Anfang an widersprochen, weil diese Auskünfte außerhalb der Zweckbestimmung des Vertragsverhältnisses liegen und die Belange des Bankkunden, der auf das Bankgeheimnis vertraut, nicht den Interessen Dritter untergeordnet werden können; daraus folgt, daß Bankauskünfte nur mit ausdrücklicher Zustimmung des Betroffenen (§ 3 BDSG) zulässig sind (1. TB S. 42, 4. TB S. 40, 5. TB S. 75).

Diese Position hat die Kreditwirtschaft nunmehr anerkannt. Im Oktober 1984 erläuterten Kreditwirtschaft und Datenschutzinstanzen der Öffentlichkeit in einem gemeinsamen Kommuniqué die datenschutzrechtlichen Voraussetzungen und Grenzen für die Erteilung von Bankauskünften. Danach dürfen Bankauskünfte nur noch erteilt werden, sofern dies dem Willen des Kunden entspricht. Für den Privatkunden bedeutet dies, daß über ihn Auskünfte nur erteilt werden, wenn er allgemein oder im Einzelfall ausdrücklich zugestimmt hat; über Geschäftskunden (juristische Personen und Kaufleute) werden Auskünfte erteilt, sofern keine anderslautende Weisung des Kunden vorliegt. Weiterhin enthalten die Vereinbarungen Abgrenzungen bezüglich des Inhalts einer Bankauskunft, die Verpflichtung zu ausschließlich zweckgebundener Verwendung der Daten beim Auskunftsempfänger sowie die Verpflichtung, den Betroffenen über die Bedingungen und die Durchführung von Bankauskünften aufzuklären.

Die Texte des Kommuniqués und der Kundeninformation „Bankauskunftsverfahren" sind in der *Anlage 2* wiedergegeben.

22.3 Adreßhandel

Die unverlangte Zusendung persönlich adressierter Werbung ist für viele Betroffene ein fortwährendes Ärgernis. Die einen ärgert der verstopfte Briefkasten. Andere beunruhigt, daß ihre Namen und Adressen, verbunden mit zusätzlichen Informationen über die persönlichen Verhältnisse, verkauft, vermietet oder sonst zur Auswertung überlassen werden, ohne daß sie den Urheber ermitteln und damit den Datenhandel eindämmen können. Die

vom Adressenverleger- und Direktwerbeunternehmerverband (ADV) geführte „Robinson-Liste", auf die sich die von der Werbewirtschaft so bezeichneten „Werbemuffel" setzen lassen können, hat nur einen begrenzten Wirkungsgrad, weil nur ein Teil der Werbewirtschaft die Eintragungen berücksichtigt.

Der Betroffene sieht sich bei der Durchsetzung seines (von der Rechtsprechung anerkannten) Rechts auf Unterlassung weiterer Werbesendungen (BGH-Urteil vom 16. Februar 1973 — I ZR 160/71, NJW 1973, S. 1119) in erster Linie der Schwierigkeit gegenüber, die Datenquelle festzustellen, d. h. zu ermitteln, wer tatsächlich im Besitz seiner Adresse ist und diese Dritten für Werbezwecke zur Verfügung stellt. Kennt man die Datenquelle, dann besteht die zweite Schwierigkeit darin, dem Adressennutzer eine vollständige Auflistung aller Schreibvarianten der eigenen Anschrift mitzuteilen. Diese Forderung an den Betroffenen wird damit begründet, daß anderenfalls nicht sichergestellt werden könne, daß der Betroffene nicht doch noch weitere Werbesendungen unter (leicht) veränderter — mitunter auch falscher — Schreibweise erhält.

Für das erste Problem habe ich bereits in meinem Ersten Tätigkeitsbericht (Nr. 4.4) auf eine einfache und praktikable Lösungsmöglichkeit hingewiesen: Jede Werbezusendung mit einer Anschrift, die nicht unmittelbar vom Betroffenen selbst stammt, muß die Datenquelle nennen, damit der Betroffene seine Datenschutzrechte wahrnehmen kann. Eine solche Verfahrensweise ist in Schweden, in den Vereinigten Staaten und auch in der Bundesrepublik Deutschland erfolgreich erprobt worden, ohne daß dadurch der Werbeerfolg geschmälert worden wäre.

Der ADV-Verband hat nach Verhandlungen mit den Datenschutzaufsichtsbehörden im Jahre 1981 in diesem Sinne seinen Mitgliedern empfohlen, Werbesendungen so aufzubereiten, daß der Betroffene die Datenquelle erfahren kann. Darüber hinaus sollte im Werbeschreiben erläutert werden, nach welchen Gesichtspunkten die Anschriften für diese Werbemaßnahme ausgewählt wurden (z. B. Münzsammler, Weintrinker, Besser-Verdienender, Hausbesitzer, Katalog-Käufer, Geldspender). Leider blieb die Empfehlung ohne nennenswerte Wirkung. Der Versandhandel, der maßgeblich am Adreßhandel beteiligt ist, lehnte bereits das Gespräch mit den zuständigen Datenschutzaufsichtsbehörden über diese Thematik ab.

Somit bleibt es dabei, daß der Bürger die Ansprüche auf Auskunft und Löschung, die ihm das BDSG eingeräumt hat, im Regelfall nicht ausüben kann. Dies ist außerordentlich bedauerlich, nicht nur, weil im Werbebereich im großen Umfang personenbezogene Daten verarbeitet werden, sondern vor allem, weil die Bürger gerade in solchen Alltagsangelegenheiten ihre Erfahrungen mit der Datenverarbeitung und dem Datenschutz sammeln. Sind diese Erfahrungen durchweg negativ, so darf es nicht verwundern, wenn Vorhaben wie die Volkszählung am mangelnden Vertrauen der Bürger scheitern. Ich appelliere daher erneut an den Gesetzgeber, Abhilfe zu schaffen.

Mit dem zweiten Hemmnis bei der Durchsetzung der Datenschutzrechte bei der Direktwerbung hatte sich das Oberlandesgericht München zu befassen (Urteil vom 29. Mai 1984 — 13 U 5583/83). Nach diesem Urteil trägt der Werbende die Verantwortung dafür, daß ein Widerspruch des Betroffenen gegen weitere Zusendungen streng beachtet wird.

Ein Kreditkarten-Unternehmen hatte von einem Rechtsanwalt eine Liste aller möglichen Schreibweisen seiner Anschrift verlangt, weil der Computer nur so die ihn betreffenden Anschriften aus den verschiedenen Adressenbeständen aussortieren könne. So hatte das Datenverarbeitungsprogramm des Kreditkarten-Unternehmens beim automatischen Anschriftenvergleich z. B. Anschriften nicht aussortiert, wenn der Punkt hinter dem abgekürzten Doktortitel fehlte oder andere geringfügige Abweichungen vorlagen. Das Gericht akzeptierte diese Begründung nicht; es verpflichtete vielmehr das Unternehmen, seine Arbeitsweisen so einzurichten, daß sich keine unzumutbaren Belastungen für den Betroffenen ergeben, andernfalls liege ein Organisationsmangel vor. Ein Datenverarbeitungsprogramm, das nur Zeichen für Zeichen vergleichen kann, reicht danach nicht aus. Es muß vielmehr imstande sein, alle Varianten einer Anschrift zu erkennen, wenn dies auch einem Sachbearbeiter ohne weiteres möglich wäre.

Der Grundgedanke dieser Entscheidung verdient allgemeine Beachtung: Niemand darf sich auf die „Dummheit" seines Computers berufen, wenn er schutzwürdige Belange Betroffener beeinträchtigt. Wer mit personenbezogenen Daten umgeht, muß seinen Computer entweder „intelligent" programmieren oder auf ihn verzichten.

22.4 Mieterfragebögen

Für den Datenschutz von Mietinteressenten hatte ich in früheren Tätigkeitsberichten gesetzgeberische und organisatorische Maßnahmen gefordert, da in zahlreichen Fällen die formularmäßige Befragung bei der Wohnungssuche tief in die Privatsphäre hineinreicht und dadurch ungerechtfertigte Angaben über die persönlichen Verhältnisse der Betroffenen erhoben und gespeichert werden. Der Bundesminister für Raumordnung, Bauwesen und Städtebau hatte mir im vergangenen Jahr zugesagt, die Problematik mit den Ländern zu beraten. Dies ist geschehen und hat zu der Anregung der zuständigen Fachkommission geführt, „bei Gesprächen und Verhandlungen mit wohnungswirtschaftlichen Verbänden auf das Problem hinzuweisen, damit die Verbände den Wohnungsunternehmen und Hauseigentümern empfehlen, bestimmte Fragen nicht zu stellen".

Ich möchte nicht die gute Absicht der Fachkommission verkennen; ich habe jedoch erhebliche Zweifel, ob „Anregungen" und „Empfehlungen" ausreichen werden, in der Praxis einen angemessenen Datenschutz durchzusetzen.

Einen gewissen Lichtblick für eine stärkere Berücksichtigung schutzwürdiger Belange von Mietinteressenten bietet der vom Bundesminister der Justiz vertretene Standpunkt, daß die Entwicklung der Rechtsprechung zur Befragungspraxis im Bereich des Arbeitsrechts übertragbar sei auf die Grundsätze für die Befragung durch Vermieter. Leider fehlt es bisher aber noch an entsprechenden Entscheidungen der Obergerichte, die die Praxis im Sinne des Datenschutzes prägen könnten.

23. Datensicherung

Die notwendige Sicherheit bei der Verarbeitung personenbezogener Daten entsteht nicht schon allein daraus, daß alle mit der Datenverarbeitung beauftragten Mitarbeiter und alle, die Daten zur Kenntnis nehmen und entsprechende Unterlagen erhalten, die ihrer Meinung nach angemessene Sorgfalt walten lassen. Vielmehr ist es erforderlich, daß die Organisation der Datenverarbeitung planmäßig Sicherungsmaßnahmen vorsieht, mit denen die Abläufe möglichst datenschutzgerecht gestaltet werden, und daß die Empfänger von Daten eindringlich auf ihren Beitrag zur Sicherung hingewiesen werden. Ferner müssen angemessene Kontrollen die Einhaltung der angeordneten Maßnahmen sichern und mit dazu beitragen, daß nie ganz auszuschließende Fehler rechtzeitig erkannt werden. Dieses bewußte und planmäßige Organisieren von Sicherheit bei der Verarbeitung personenbezogener Daten wird zwar vom Bundesdatenschutzgesetz gefordert, es wird aber noch nicht von allen Stellen und nicht immer mit der notwendigen Sorgfalt durchgeführt.

Zuweilen mußte ich sogar feststellen, daß speichernde Stellen mit der Organisation des Schutzes der ihnen anvertrauten Daten erst im Zusammenhang mit meiner Überprüfung beginnen. Sie verletzen damit bestehende, für sie geltende gesetzliche Vorschriften. Sich darauf zu verlassen, daß ihnen bei einer Kontrolle der Umfang ihres gesetzlichen Auftrags schon erklärt wird, ist ein erhebliches Mißverständnis meiner Aufgabe. Abgesehen davon, daß ich dies schon aus Kapazitätsgründen nicht kann, ist die Auswahl und die Durchführung angemessener Sicherungsmaßnahmen einschließlich ihrer Organisation eine Aufgabe der speichernden Stelle selbst sowie der in diesen Fragen nicht immer wirksamen Fachaufsicht. Meine Aufgabe ist es, die Bemühungen der datenverarbeitenden Stellen durch Beratung zu unterstützen und durch stichprobenartige Kontrollen ihre Wirksamkeit zu überprüfen.

Entgegen mancher Erwartung ergeben sich aus den bei Beratungen und Kontrollen gewonnenen Erfahrungen außer allgemeinen Feststellungen kaum Erkenntnisse, die von anderen Stellen *unmittelbar* in Maßnahmen für den eigenen Bereich umgesetzt werden können. Denn die angemessenen Maßnahmen richten sich stets nach den Aufgaben der Stelle, nach den Datenarten und dem Umfang sowie dem Kontext der Verarbeitung und nicht zuletzt auch nach den gewachsenen Strukturen in der einzelnen Behörde, zu denen auch die örtlichen und baulichen Verhältnisse gehören.

23.1 Die Sicherung nicht mehr benötigter Daten

Wenn Daten nicht mehr zur Erfüllung der Aufgabe benötigt werden, sind sie „nur noch" zu sichern bzw. gesichert zu vernichten. Der hierfür zu leistende Aufwand liefert keinen unmittelbaren Beitrag zur Aufgabenerfüllung der speichernden Stelle, und auch den organisatorischen Vorkehrungen steht als Ertrag nichts außer dem Gewinn an Sicherheit gegenüber. Deshalb wird den nicht mehr benötigten Daten gelegentlich noch immer zu wenig Aufmerksamkeit geschenkt. So konnte es z. B. geschehen, daß die Rückseiten von Ausdrucken personenbezogener Daten als Notizzettel verwendet wurden und als solche die speichernde Stelle verließen. In einem anderen Fall führte die fehleranfällige Behandlung freigegebener Magnetbänder dazu, daß außer den auf einem Magnetband planmäßig und zulässig weitergegebenen Daten sich noch Daten aus einer vorangegangenen Verarbeitung befanden, die nicht hätten übermittelt werden dürfen. Ein besonderes Problem wurde deutlich, als eine alte Liste mit personenbezogenen Daten gefunden wurde, die von einer Stelle der Bundesverwaltung in mehreren Exemplaren gedruckt und (zulässig) an verschiedene Empfänger verschickt worden war.

Diese Empfänger brauchten bezüglich der Liste vermutlich kein Datenschutzgesetz anzuwenden, weil sie selbst diese Daten nicht in Dateien — sondern eben nur in Listenform — speicherten. Es kann nicht ausgeschlossen werden, daß diese rechtliche Schwachstelle mit dazu beigetragen hat, daß die Liste nicht ordnungsgemäß vernichtet wurde.

Alle Fälle hätten durch die gebotene Sorgfalt leicht vermieden werden können. Sie wurden zum Anlaß genommen, die Organisation zu überprüfen und den Sicherungsanforderungen anzupassen und auch die an der Datenverarbeitung Beteiligten entsprechend zu belehren. Es kommt aber darauf an, solche Maßnahmen schon vorbeugend zu ergreifen, also bei jeglicher Art von personenbezogener Datenverarbeitung jeden einzelnen Verarbeitungsschritt sicher zu gestalten und die Löschung oder Archivierung konsequent mitzuplanen.

23.2 Versand von Datenträgern, Ausdrucken und Mitteilungen

In einer Reihe von Einzeleingaben haben Betroffene sich darüber beschwert, daß auf Zusendungen an sie außer der Anschrift noch weitere personenbezogene Daten sichtbar waren. In einem Fall war das Druckbild so unpassend gestaltet und das gewählte Papier so durchsichtig, daß im Anschriftenfenster Zahlungsdaten erkennbar waren, obwohl die Zusendung im verschlossenen Briefumschlag erfolgte. In anderen Fällen waren außer der Anschrift im Anschriftenfeld die Mitgliedsnummer oder andere „sprechende" Kennziffern enthalten,

die zum Teil das Geburtsdatum der Empfänger erkennen ließen. Es mag in Sonderfällen zwar geboten sein, außer der Anschrift des Empfängers weitere personenbezogene Daten von außen sichtbar anzugeben. Es sollte aber stets sorgfältig geprüft werden, ob dies erforderlich ist, denn manchem ist es schon unangenehm, wenn der Postbote sein Geburtsdatum erfährt, und oft kann auch nicht sichergestellt werden, daß die Zusendungen den Empfänger direkt erreichen und nicht erst einen Umweg über Mitbewohner oder andere Ersatzempfänger machen.

Ein anderes Problem ist die Entscheidung über die angemessene *Versandart* von Daten in einzelnen Fällen und bei der Übersendung von Datenträgern oder Ausdrucken mit einer Vielzahl von Fällen. Eine gegenüber dem einfachen Brief, Päckchen oder Paket sicherere Versandart, z. B. Einschreiben oder Wertsendung, verursacht Mehrkosten und Mehrarbeit beim Absender und beim Empfänger, die außer mehr Sicherheit keinen weiteren Nutzen haben. Deshalb wird hier gern gespart, was unter Berücksichtigung der Sicherheit der Postbeförderung je nach Art der transportierten Daten und Datenträger auch vertretbar sein kann. Nicht vertretbar ist es jedoch, wenn die Annahme von Sendungen nicht oder so schlecht organisiert ist, daß sie zwar von der Post abgeliefert, vom Empfänger aber nicht sofort gesichert verwahrt oder richtig weitergeleitet werden. Ein solcher Organisationsmangel hat es möglicherweise begünstigt, daß eine umfangreichere Sendung ausgedruckter Mitgliederdaten von der Zentrale einer Krankenkasse an eine Zweigstelle in der Nähe dieser Zweigstelle auf der Straße gefunden wurde.

Eine weitere Schwierigkeit, die mit dem Versand von Mitteilungen zusammenhängt, tritt häufig bei der Behandlung der Posteingänge beim Empfänger auf. Ist der Empfänger eine größere Firma oder Behörde, so gibt es im allgemeinen eine Posteingangsstelle, die alle ankommenden Schreiben öffnet und je nach Inhalt an die jeweils zuständige Abteilung weiterleitet. Dieses Verfahren ist aber für einige Zusendungen wie z. B. Auskünfte aus dem Bundeszentralregister, psychiatrische und ärztliche Gutachten oder andere Sozialdaten völlig ungeeignet. Hier muß der Absender durch entsprechende und deutliche Hinweise der empfangenden Stelle die sachgerechte interne Zustellung ermöglichen. Dazu sind häufig Absprachen mit dem Empfänger und leider auch eine etwas aufwendigere Organisation erforderlich. Einige Stellen — z. B. das Bundeszentralregister — bemühen sich hier, die Wünsche der Empfänger soweit wie möglich zu berücksichtigen. Aus anderen Bereichen erhalte ich dagegen noch immer Beschwerden darüber, daß Sendungen beim Empfänger falsch behandelt werden, weil die notwendigen Leitvermerke fehlen.

23.3 Kontrollierbarkeit von Massenabrufen

Im Berichtsjahr gab es zum ersten Mal ausführliche Berichte über unerlaubte Zugriffe von sogenannten Hackern auf solche Datenkommunikationssysteme, die besonders zur Unterstützung von Massenverfahren geeignet sind. Auf Wunsch des Innenausschusses des Deutschen Bundestages habe ich deshalb die Probleme der Sicherheit bei der Datenkommunikation und die Möglichkeiten, diese Probleme zu lösen, beschrieben. Diese „Problemskizze zur Sicherheit bei der Datenkommunikation" habe ich dem Innenausschuß im Dezember 1984 vorgelegt, sie ist als *Anlage 1* diesem Bericht beigefügt.

Die Tatsache, daß sich die allgemeine Aufmerksamkeit besonders auf die Probleme richtet, die mit der Automatisierung des Informationsaustausches verbunden sind, darf aber nicht darüber hinwegtäuschen, daß auch die konventionelle, schriftliche oder auch telefonische Beantwortung von Anfragen zumindest dann besondere Sicherungsmaßnahmen erfordert, wenn dabei regelmäßig in erheblichem Umfang und in einem standardisierten Verfahren Auskunftsersuchen beantwortet werden. Typisch sind dafür z. B. die Auskunftsverfahren des Kraftfahrt-Bundesamtes und des Bundeszentralregisters. Solchen Verfahren ist gemeinsam, daß nur geprüft wird, ob die anfragende Stelle berechtigt ist, (für den meist nur stichwortartig beschriebenen Zweck) die gewünschte Auskunft zu erhalten. Ob die Angaben der anfragenden Stelle im Einzelfall zutreffen, wird vor der Auskunftserteilung nicht geprüft, und in der Regel führt die abgebende Stelle auch keine Aufzeichnungen über erteilte Auskünfte, so daß für nachträgliche Kontrollen jeder Anhaltspunkt fehlt. Deswegen bestehen im wesentlichen zwei Risiken:

— Bei der anfragenden Stelle kann es aus alter Gewohnheit üblich sein, auch in solchen Fällen anzufragen, in denen die Auskunft (voraussichtlich) nicht erforderlich ist, ohne daß die befragte Stelle dies erkennen kann. In der anfragenden Stelle wird das unangemessene Vorgehen möglicherweise dadurch begünstigt, daß die Datenschutzorganisation unzureichend oder zu eng am Dateibegriff ausgerichtet ist, und die überflüssigen Auskünfte in Akten eingehen.

— Bei der anfragenden Stelle kann im Einzelfall das eingespielte und unkontrolliert ablaufende Verfahren für gezielte Mißbräuche angewendet werden, etwa dadurch, daß Auskünfte eingeholt werden, die zur rechtmäßigen Aufgabenerfüllung nicht erforderlich sind, sondern dem Privatinteresse des anfragenden Mitarbeiters dienen. Über verschiedene Fälle dieser Art hat der Landesbeauftragte für den Datenschutz in Baden-Württemberg in seinem Vierten Tätigkeitsbericht (S. 55 f.) berichtet.

Beide Risiken ließen sich erheblich vermindern, wenn die beteiligten Stellen gemeinsame Regelungen zur Zweckbindung und zur Kontrolle z. B. durch gelegentliche Stichproben träfen. Diese organisatorischen Vorkehrungen sind geboten, auch schon bevor in der anstehenden Novellierung des BDSG entsprechend gesetzliche Auflagen formuliert sind.

23.4 Personal Computer

Die Miniaturisierung elektronischer Bauteile (Chips), die Integration mehrerer Funktionen in einem Bauteil und die damit fast parallel verlaufenden Verbesserungen des Preis-Leistungs-Verhältnisses von DV-Anlagen machen es möglich, kleine, leistungsfähige und preiswerte Computer zur persönlichen Benutzung durch einen oder wenige Mitarbeiter einzusetzen. Einige in der bisherigen automatisierten Datenverarbeitung bewährte Prinzipien wie z. B. „Funktionentrennung", „Vier-Augen-Prinzip" oder „interne Auftragskontrolle" sind auf die neue Art der Datenverarbeitung praktisch nicht übertragbar, und auch die sonstigen Sicherheitswirkungen einer notwendigerweise planmäßigen Zusammenarbeit mehrerer Personen entfallen weitgehend. Damit können weder die Rechtmäßigkeit noch die Sicherheit der Datenverarbeitung gewährleistet werden, es sei denn, daß die dafür Verantwortlichen rechtzeitig durch entsprechende Anordnungen sicherstellen, daß sich aus den neuen Möglichkeiten kein Wildwuchs entwickelt.

Die hier beschriebenen Probleme verschärfen sich erheblich, wenn einzelne Mitarbeiter zur Erledigung der Aufgaben privateigene Computer benutzen, weil dann zum einen die Trennung zwischen dienstlichen und privaten Daten und Datenverarbeitungen leicht verwischt wird und zum anderen die organisatorischen Vorgaben schwerer durchzusetzen sind.

Im Rahmen meiner Beratungstätigkeit sind konkrete Fragen des Einsatzes von Personal- oder Homecomputern noch nicht aufgetreten; es gab jedoch schon einige ähnliche Unklarheiten über die Verarbeitung personenbezogener Daten mit neueren Textautomaten, die sich nicht nur zur Textverarbeitung, sondern auch zur sonstigen Datenverarbeitung eignen.

Diese Probleme werden zunehmen, und das Fortschreiten der Miniaturisierung und der Verbilligung der elektronischen Datenverarbeitungsanlagen werden auch den Einsatz kleinerer Geräte an vielen verschiedenen Stellen für jeweils individuelle Anwendungen begünstigen. Deshalb begrüße ich, daß für den Bereich der Steuerverwaltung die zuständigen Automationsreferenten (Steuer) für die arbeitsplatzorientierte Datenverarbeitung einheitliche Regelungen zur Vermeidung von Fehlentwicklungen vorgeschlagen haben. Außerdem hat sich der Arbeitskreis „Datenschutz und neue Technologien" der Arbeitsgemeinschaft für wirtschaftliche Verwaltung e. V. (AWV), an dem ich beteiligt bin, mit den Risiken und Chancen dieser Technologien für den Datenschutz beschäftigt. Erste Arbeitsergebnisse dazu werden voraussichtlich Anfang 1985 veröffentlicht.

24. Novellierung des Bundesdatenschutzgesetzes

24.1 Sachstand

In fast allen meinen bisherigen Tätigkeitsberichten habe ich über den Sachstand der Novellierung des BDSG, über dazu vorliegende Gesetzentwürfe und über meine Vorschläge zur Änderung dieses Gesetzes berichtet. Keiner dieser Entwürfe und Vorschläge ist bisher, soweit sie überhaupt in das Gesetzgebungsverfahren eingebracht wurden, bis zur Ausschußberatung im Deutschen Bundestag gelangt. Auch der in meinem Sechsten Tätigkeitsbericht (vgl. dort S. 56 f.) erwähnte Referentenentwurf des Bundesministers des Innern vom 23. Juni 1983 ist nach Verkündung des Urteils des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 offenbar nicht weiterverfolgt worden, vielmehr hat dieses Urteil den BMI veranlaßt, neue Überlegungen zur Novellierung des BDSG anzustellen. Nach gegenwärtigem Sachstand soll ein Entwurf zur Änderung des BDSG jedoch nicht von der Bundesregierung, sondern von den Fraktionen der CDU/CSU und der FDP eingebracht werden. An den Vorbereitungen bin ich nicht beteiligt.

Die Fraktion der SPD hat am 27. März 1984 einen eigenen Gesetzentwurf zur Änderung des BDSG im Deutschen Bundestag eingebracht (BT-Drucksache 10/1180); die erste Lesung hat am 20. September 1984 stattgefunden, eine Beratung im federführenden Innenausschuß steht noch aus. Nach der Begründung des Entwurfs sollen damit die Vorschriften des BDSG den vom Bundesverfassungsgericht aufgestellten verfassungsrechtlichen Anforderungen an die Datenverarbeitung angepaßt werden. Da meine Stellungnahme zu den Auswirkungen des Volkszählungsurteils erst später vorgelegt wurde, konnte sie in dem Entwurf nicht berücksichtigt werden. Ich gehe davon aus, daß ich nach Vorlage des angekündigten Novellierungsentwurfs der Koalitionsfraktionen in die parlamentarischen Beratungen beider Entwürfe eingeschaltet werde, und möchte deshalb gegenwärtig auf eine vorweggenommene Bewertung des SPD-Entwurfs verzichten.

24.2 Auswirkungen des Volkszählungsurteils

Wie in der Einleitung zu diesem Bericht erwähnt, bin ich in meiner auf Anforderung des Innenausschusses des Deutschen Bundestages vorgelegten Stellungnahme zu den Auswirkungen des Volkszählungsurteils des Bundesverfassungsgerichts auch auf die Novellierung des BDSG eingegangen. Meine dort dargestellten Überlegungen und Vorschläge seien hier in verkürzter Form und thesenartig nochmals wiedergegeben:

a) Die *freie Selbstbestimmung* des Betroffenen über Preisgabe und Verwendung seiner Daten und die dieses Recht sichernden Regelungen und Vorkehrungen — Aufklärung, Zweckbindung, Auskunftsrechte usw. — müssen im Vordergrund eines „Schutzgesetzes" stehen, nicht aber die Einschränkungen des Selbstbestimmungsrechts, die das BDSG *auch* regelt und weiterhin zu regeln hat. Das Gesetz sollte in seiner Anlage und Konzeption deutlicher zum Ausdruck bringen, daß Freiwilligkeit von Angaben und freie Einwilligung in die nachfolgende Datenverarbeitung den von der Verfassung gewollten Regelfall darstellen.

b) Nachdem das BVerfG nunmehr bestätigt hat, daß Gegenstand der Datenschutzregelungen die Sicherung und Einschränkung des Rechts auf informationelle Selbstbestimmung ist, sollten die an dieser Zielrichtung vorbeigehende und auf den *Mißbrauch* abstellende Bezeichnung des Gesetzes sowie aus dem gleichen Grunde auch die Definition des Begriffs Datenschutz in § 1 Abs. 1 geändert werden. Dies entspräche nicht nur dem Gebot präziser Gesetzessprache, sondern würde einen auch in Datenverarbeitungskreisen immer noch verbreiteten Irrtum ausräumen, daß das BDSG nur Mißbrauchsfälle betreffe.

c) Nach den Feststellungen des BVerfG gilt das Recht auf informationelle Selbstbestimmung gegenüber jeder nicht von dem Willen des Betroffenen getragenen Datenverwendung, unabhängig davon, ob die Daten in *Dateien* verarbeitet werden oder nicht. Das BDSG muß also auch die Verwendung von personenbezogenen Daten regeln, die nicht in Dateien verarbeitet werden. Das bedeutet jedoch nicht, daß für personenbezogene Daten, die sich z. B. in Akten oder Listen befinden, generell dieselben Vorschriften gelten müssen wie für Daten in Dateien. Es ist vielmehr zu berücksichtigen, daß die Gefährdung für Rechte des Betroffenen und die angemessenen Maßnahmen zu seinem Schutz je nach der Art des Datenträgers unterschiedlich sein können. Die für die Datenverarbeitung außerhalb von Dateien notwendigen Vorschriften sollten in einem besonderen Abschnitt zusammengefaßt werden.

d) Die wesentlichen Aussagen des BVerfG gelten der *Datenerhebung*, die im BDSG nur insoweit geregelt ist, als der Betroffene, falls Daten aufgrund einer Rechtsvorschrift erhoben werden, auf diese hinzuweisen ist, sonst auf die Freiwilligkeit seiner Angaben. Demgegenüber stellt das Gericht für den Fall eines Auskunftszwangs des Bürgers fest,

   — daß die Rechtsvorschrift, die im überwiegenden Allgemeininteresse den Bürger zur Auskunft zwingt, den Umfang der Beschränkung, also seiner Auskunftspflicht, erkennen lassen muß,

   — daß der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmen muß,

   — daß die Angaben für diesen Zweck geeignet und erforderlich sein müssen,

   — daß, sofern mehrere Verwendungszwecke festgelegt werden, diese nicht tendenziell unvereinbar sein dürfen,

   — daß es sich nicht um Daten ohne Sozialbezug, nicht um unzumutbare intime Angaben, nicht um Selbstbezichtigungen und nicht um eine Vorratsdatensammlung zu unbestimmten oder noch nicht bestimmbaren Zwecken handeln darf,

   — daß Aufklärungs- und Belehrungspflichten der datenerhebenden Stelle bestehen.

   Angesichts dieses verfassungsrechtlichen Forderungskatalogs erscheint es geboten, die allgemeinen Anforderungen an die Datenerhebung, insbesondere soweit sie sich an den Gesetzesvollzug wenden, im BDSG in Form von Zulässigkeitsvoraussetzungen zu regeln und die Datenerhebung damit in Erweiterung des Datenverarbeitungsbegriffs zur eigenständigen Verarbeitungsphase zu erklären. Die künftige BDSG-Vorschrift zur Datenerhebung sollte festlegen, daß Daten unter Auskunftszwang nur erhoben werden dürfen, wenn und soweit dies eine spezialgesetzliche Vorschrift erlaubt und wenn in dieser Vorschrift der Verwendungszweck präzise angegeben ist. Ferner sollten die Ausschlußtatbestände für zwangsweise Datenerhebungen genannt werden. Besonders eingehend sollten im BDSG die Aufklärungspflichten gegenüber dem Betroffenen festgelegt werden, da dieser nach dem Urteil Anspruch darauf hat zu erfahren, wer was wann und bei welcher Gelegenheit über ihn weiß. Das bedeutet, daß ihm erklärt werden muß — und zwar nicht nur durch Hinweis auf eine ihm möglicherweise nur schwer zugängliche Gesetzesvorschrift —, ob er zur Auskunft verpflichtet ist, wie weit diese Pflicht reicht und für welche Zwecke die angegebenen Daten verwendet werden sollen. Dabei sind auch eventuelle Datenempfänger zu nennen. Schließlich sollten auch die Folgen einer Auskunftsverweigerung mitgeteilt werden müssen. Diese inhaltlichen Festlegungen der Aufklärungspflicht datenerhebender Stellen müssen selbstverständlich auch gelten, wenn vom Bürger aufgrund von Mitwirkungspflichten oder freiwillig Angaben erhoben werden.

   Die BDSG-Regelung der Datenerhebung darf sich nicht auf den Fall beschränken, daß die erhobenen Daten anschließend in Dateien gespeichert werden. Informationelle Selbstbestimmung und ihre Einschränkungen sind nicht vom Datenträger abhängig, zumal vielfach im Zeitpunkt der Datenerhebung gar nicht abzusehen ist, welche organisatorischen Mittel für die weitere Verarbeitung gewählt werden.

e) Für die *Datenspeicherung* reicht die bisherige Generalklausel des § 9 Abs. 1 aus. Eine Ergänzung wäre dann notwendig, wenn die wohl auch auf die Datenspeicherung abzielende Aussage des Gerichts, daß die Sammlung personenbezogener Daten auf Vorrat zu unbestimmten und nicht bestimmbaren Zwecken nicht zulässig ist, anstatt in der Datenerhebungsvorschrift in der Speicherungsvorschrift des BDSG ihren Niederschlag finden soll.

f) Das BVerfG sieht die entscheidenden Bezüge zum Recht auf informationelle Selbstbestimmung in der *Verwendung* der Daten, weil darin — ähnlich wie bei der Datenerhebung — die Betroffenheit des Bürgers, sei es in Form von belastenden Verwaltungsmaßnahmen, sei es in der Gewährung von Leistungen, unmittelbar Ausdruck findet. Abgesehen von § 5 Abs. 1 enthält das BDSG keine Bestimmung zur Datenver-

wendung. Zulässigkeitsvoraussetzungen für die Verwendung der Daten ist — ähnlich wie für die Datenerhebung — daß der Datenverwender dabei rechtmäßig handelt, sich im Rahmen seiner Zuständigkeit hält und die Daten für die Verwendung erforderlich sind. Als wesentliches zusätzliches Erfordernis muß entsprechend der zentralen Aussage des Gerichts festgelegt werden, daß die Verwendung der Daten grundsätzlich auf den *gesetzlich bestimmten Zweck* begrenzt ist. Damit kann zunächst der Zweck gemeint sein, der in der bereichsspezifischen Erhebungsvorschrift festgelegt ist, bei freiwilliger Datenangabe der Zweck, der dem Betroffenen genannt wurde, um ihn zu Angaben zu veranlassen. Denkbar ist jedoch auch, daß sich der Verwendungszweck der Daten aus der gesetzlichen Aufgaben- und Befugnisbeschreibung der Stelle, die die Daten erhoben hat bzw. sie speichert, mit hinreichender Normenklarheit ergibt. Auch dieser Fall sollte in einer Vorschrift des BDSG, die die Datenverwendung regelt, berücksichtigt werden. Der Verwendungszweck selbst kann allerdings im BDSG, das seinen Charakter als Auffang- und Rahmenvorschrift behalten soll, nicht festgelegt werden.

Ausnahmen von dem Grundsatz der Zweckbindung müssen so geregelt werden, daß eine *Zweckänderung* bei der Stelle, die über die Daten verfügt, nur dann erfolgen darf, wenn eine gesonderte zwangsweise Datenerhebung für diesen anderen Zweck nach den dafür oben angeführten Bedingungen zulässig wäre. Weitere Voraussetzung wäre es, dem Bürger Kenntnis darüber zu verschaffen, zu welchen weiteren Zwecken seine Daten nunmehr verwendet werden sollen. Dies wird regelmäßig nur durch eine individuelle Benachrichtigung möglich sein.

Wurden die Daten für den primären Zweck vom Betroffenen freiwillig angegeben, so wird es für eine Zweckänderung seiner Einwilligung bedürfen. Das gleiche muß gelten, wenn Daten für den primären Zweck zwar zwangsweise erhoben wurden, die Verwendung derselben Daten für einen anderen Zweck aber nicht durch eine eigene bereichsspezifische Erhebungsvorschrift gedeckt ist, so daß dafür nur freiwillige Angaben in Betracht kämen. Für Fälle minimaler Zweckabweichung könnte eine Bestimmung ausreichen, nach der die Einwilligung in eine andere Verwendung der Daten unterstellt werden darf, wenn der Betroffene nach Benachrichtigung über die beabsichtigte Verwendung in angemessener Frist nicht widerspricht.

g) Da das Gericht der Verwendung der Daten und ihrem Verwendungszusammenhang entscheidende Bedeutung beimißt, kann es nicht darauf ankommen, ob die Daten bei der speichernden Stelle nur *intern genutzt* oder ob sie weiterübermittelt werden. Ein — wenn auch begrenzter — datenschutzrechtlicher Freiraum, wie er in § 1 Abs. 2 Satz 2 BDSG eingeräumt wird, ist damit nicht vereinbar. Vielmehr muß auch die nur interne Verarbeitung personenbezogener Daten Zulässigkeitsvoraussetzungen unterworfen werden, insbesondere muß die zweckgebundene Verwendung sichergestellt sein. Das Auskunftsrecht des Betroffenen muß auch diese Daten umfassen, damit er erfahren kann, wer Daten über ihn besitzt, und die Datenschutzkontrolle muß sich auf die Eigennutzung der Daten durch die speichernde Stelle erstrecken, um den damit angestrebten „vorgezogenen Rechtsschutz" zu gewährleisten.

h) Das BVerfG fordert angesichts der Gefahren der automatischen Datenverarbeitung einen amtshilfefesten Schutz gegen Zweckentfremdung durch *Weitergabe- und Verwertungsverbote.* Übermittlungsvorschriften, die — wie § 10 BDSG — lediglich an die rechtmäßige Aufgabenerfüllung der an einer *Übermittlung* beteiligten Stellen oder — wie § 11 BDSG — an das berechtigte Interesse des Empfängers anknüpfen, können keinen ausreichenden Schutz gegen Zweckentfremdung bieten. Sie können eine Übermittlung allenfalls dann rechtfertigen, wenn mit der Übermittlung keine Zweckentfremdung verbunden ist, d. h. wenn der Empfänger die Daten für den gleichen Zweck verwenden will wie die übermittelnde Stelle. Für diesen Ausnahmefall müßte eine gesetzliche Pflicht zur Benachrichtigung des Betroffenen geschaffen werden.

Führt — wie im Regelfall — eine Datenübermittlung zu einer Zweckentfremdung der Daten, so ist dafür eine präzise bereichsspezifische gesetzliche Grundlage erforderlich, weil sie das Recht auf informationelle Selbstbestimmung einschränkt. Der Grad der Bestimmtheit der Norm hängt von Art, Umfang und den beabsichtigten Verwendungen der Daten sowie der Gefahr ihres Mißbrauchs ab. Das Vorhandensein einer solchen Spezialregelung muß im BDSG zur Zulässigkeitsvoraussetzung für die Datenübermittlung bestimmt werden. Eine Datenübermittlung kann also künftig nicht mehr allein auf die §§ 10, 11 BDSG bzw. auf die Amtshilfevorschriften der Verwaltungsverfahrensgesetze gestützt werden.

Erweist sich eine Datenübermittlung an eine Stelle als zweckmäßig, die sich nicht auf eine präzise bereichsspezifische Übermittlungsvorschrift berufen kann, die aber befugt wäre, aufgrund einer für sie geltenden Erhebungsvorschrift selbst die Daten zu erheben, so wird dasselbe zu gelten haben wie bei einer Zweckänderung bei der speichernden Stelle. Das BDSG muß allerdings für diesen Fall zulässiger Datenübermittlung zugleich eine Pflicht zur Benachrichtigung des Betroffenen vorschreiben.

In den Fällen der Datenübermittlung im *Direktzugriffsverfahren (Online)* ist es besonders dringlich, daß der Gesetzgeber für Transparenz und für angemessene organisatorische und verfahrensrechtliche Vorkehrungen zum Schutz des Betroffenen sorgt. Auf die vom Bundesbeauftragten für den Datenschutz hierzu schon früher gemachten Vorschläge wird verwiesen (vgl. 4. TB S. 56, 5. TB S. 113 und oben Nr. 23.3).

Aus Artikel 19 Abs. 4 GG hat das BVerfG die *Pflicht zur Protokollierung* von Datenübermittlungen abgeleitet, damit der Bürger von der Weitergabe seiner Daten gemäß den einschlägigen Vorschriften der Datenschutzgesetze Kenntnis erlangen und dagegen u. U. den Rechtsweg beschreiten kann. Eine gesetzliche Bestimmung über eine solche Protokollierungspflicht sollte Ausnahmen für die Fälle vorsehen, in denen die Protokollierung die Wahrnehmung des Rechts auf informationelle Selbstbestimmung nicht zu fördern geeignet ist, sondern im Gegenteil zu einer weiteren Gefährdung dieses Rechts führt. Dies ist immer dann der Fall, wenn das Übermittlungsprotokoll einen zusätzlichen Informationsgehalt aufweist, der über die Kontrollierbarkeit der Übermittlung und die Unterrichtungsmöglichkeit des Betroffenen hinaus weitere Verwendungszwecke der Daten eröffnet.

i) Aus der Feststellung des Gerichts, daß die Vorschrift des § 9 Abs. 4 VZG 1983 über die *Übermittlung von Einzelangaben für wissenschaftliche Zwecke* das allgemeine Persönlichkeitsrecht nicht verletzt, ergibt sich, daß gegen eine Übermittlungsregelung zugunsten der wissenschaftlichen Forschung keine prinzipiellen Bedenken bestehen.

   Akzeptabel wäre beispielsweise eine Forschungsklausel, die sich in den Grenzen des § 9 Abs. 4 VZG 1983 bewegt und gleichwertige Sicherungen vorsieht. Dies würde insbesondere bedeuten:

   — Die Übermittlung muß sich auf die erforderlichen Angaben beschränken.

   — Das Gesetz muß den Empfänger einer strikten Zweckbindung unterwerfen, die auch strafrechtlich abzusichern ist.

   — Eine effektive Kontrolle durch die Datenschutzbeauftragten muß gewährleistet sein.

   — Die Übermittlung von Angaben mit Namen und Anschriften oder anderen Identifikationsmerkmalen darf nur mit Einwilligung des Betroffenen erfolgen. Ausnahmen davon sollten bereichsspezifischen Regelungen vorbehalten bleiben; eine Ermächtigung durch das BDSG wäre allenfalls akzeptabel, wenn sie mit weiteren Einschränkungen und zusätzlichen grundrechtssichernden Vorkehrungen verbunden wäre.

j) *Aufklärungs- und Auskunftspflichten* sind eine wesentliche Voraussetzung für eine verfassungsgemäße Verwendung personenbezogener Daten, die unter Zwang erhoben und ohne Zustimmung des Betroffenen verwendet werden. Damit verträgt es sich nicht, die Auskunftserteilung, wie bisher, von der Zahlung eines Entgelts abhängig zu machen. Die Auskunftserteilung muß vielmehr im BDSG generell kostenfrei geregelt sein.

   Eine Rechtsordnung, in der die Betroffenen nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß, wäre mit dem von der Verfassung garantierten Recht auf informationelle Selbstbestimmung nicht vereinbar. Deshalb dürfen bestimmte Behörden nicht generell von der Pflicht zur Auskunftserteilung ausgenommen werden. Dies gilt insbesondere für die Sicherheitsbehörden, deren Datenverarbeitung häufig im besonderen Maße geeignet ist, Rechte des Betroffenen zu beschränken. Anstelle des den Sicherheitsbehörden in § 13 Abs. 2 BDSG eingeräumten Auskunftsverweigerungsrechts ist gesetzlich festzulegen, daß Gründe der Geheimhaltung aus überwiegendem Allgemeininteresse, die gegebenenfalls gegen eine Auskunftserteilung sprechen, wegen der grundlegenden Bedeutung des Auskunftsanspruchs für die Verhältnismäßigkeit der Datenverwendung nur bei einer *Abwägung im Einzelfall* berücksichtigt werden können, wie dies schon jetzt in den internen Richtlinien für die polizeiliche Datenverarbeitung vorgesehen ist. Wegen der Rechtsschutzgarantie des Artikels 19 Abs. 4 GG sollte das BDSG entsprechend neuerer verwaltungsgerichtlicher Rechtsprechung außerdem festlegen, daß eine ablehnende Entscheidung angemessen begründet werden muß, damit sie durch die Gerichte überprüfbar ist. Für den Fall einer (zulässigen) Auskunftsverweigerung sollte das BDSG vorschreiben, daß die Auskunft nach Wegfall der Hinderungsgründe nachträglich erteilt werden muß.

   Soweit eine Protokollierung von Datenübermittlungen vorzunehmen ist oder die Weitergabe von Daten auf andere Weise festgestellt werden kann, muß sich die Auskunft an den Betroffenen auch auf die Übermittlung und den Übermittlungsempfänger beziehen. Gleiches gilt für die Herkunft der Daten. Ausnahmen von der Verpflichtung, über die Herkunft und den Empfänger der Daten Auskunft zu geben, können allenfalls zugelassen werden, wenn überwiegende berechtigte Interessen dieser Personen oder der Allgemeinheit entgegenstehen.

k) Das BVerfG fordert für den Bereich der Statistik, daß die Handhabung der allgemeinen *Löschungspflichten* nach § 11 Abs. 7 BStatG nicht dem Ermessen der Exekutive überlassen bleiben darf. Für Daten, die vergleichbaren Geheimhaltungspflichten unterliegen, werden deshalb gleichfalls spezielle Löschungsvorschriften notwendig sein. Dabei wird es sich aber um Vorschriften außerhalb des BDSG handeln müssen, die die Rahmenvorschrift des BDSG für einen bestimmten Bereich konkretisieren.

   Von einer Löschungsvorschrift im BDSG wird man fordern müssen, daß unter den Voraussetzungen des § 14 Abs. 3 personenbezogene Daten nicht nur — wie dort vorgesehen — gelöscht werden *können*, sondern daß dann eine Löschungs*pflicht* besteht. Wenn die Kenntnis von Daten zur Erreichung des gesetzlich festgelegten Verwendungszweckes nicht mehr erforderlich ist, kann eine fortwirkende Beschränkung des Rechts auf informationelle Selbstbestimmung, die in der weiteren Verfügbarkeit der Daten zu sehen ist, nicht mehr gerechtfertigt werden.

Um den Rechtsetzungsaufwand für bereichsspezifische Löschungsfristen in Grenzen zu halten, könnte daran gedacht werden, in § 14 BDSG eine Regelfrist vorzuschreiben, nach deren Ablauf Daten spätestens gelöscht werden müssen, falls sie nicht schon vorher zur Aufgabenerfüllung entbehrlich und deshalb früher zu löschen sind. Eine solche Regelfrist wäre empirisch zu ermitteln und sollte der Aufbewahrungsdauer für Daten in möglichst vielen Verwaltungsbereichen entsprechen.

l) Die Betonung der *Datenschutzkontrolle* im Urteil als wesentliche Bedingung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung unterstützt meine früheren Verbesserungsvorschläge zur Stellung des Bundesbeauftragten für den Datenschutz (vgl. 4. TB S. 57, 5. TB S. 114):

- Die vom BVerfG geforderte Beteiligung unabhängiger Datenschutzbeauftragter setzt deren Unterrichtung über geplante Veränderungen in der Struktur staatlicher Informationsbeschaffung und -verwendung voraus. Eine gesetzliche Unterrichtungspflicht über die Planung von Informationssystemen sollte die Wahrnehmung der Beratungsaufgabe des Bundesbeauftragten sicherstellen, ohne ihn so präjudizierend in den Planungsprozeß einzubinden, daß eine nachgehende Kontrolle nicht mehr effektiv wahrgenommen werden kann.
- Die Betonung der Unabhängigkeit der Datenschutzbeauftragten wirft die Frage auf, ob damit die der Bundesregierung gesetzlich übertragene Rechtsaufsicht über den Bundesbeauftragten noch vereinbar ist. Sollte sie erhalten bleiben, muß klargestellt sein, daß sie nicht auch die Letztentscheidung über auslegungsfähige Datenschutzvorschriften umfaßt. Mit der Unabhängigkeit des Bundesbeauftragten wäre es nicht vereinbar, wenn ihm die Bundesregierung — gegebenenfalls im Interesse der kontrollierten Stellen — eine ihr richtig erscheinende Auslegung einer Vorschrift aufzwingen könnte.
- Der gelegentlich diskutierte Gedanke, dem Bundesbeauftragten für den Datenschutz einen Beirat an die Seite zu stellen, erscheint auch unter dem Gesichtspunkt seiner Unabhängigkeit nicht geeignet, die Datenschutzkontrolle zu stärken.
- Die Unabhängigkeit muß auch dahingehend gesichert sein, daß der Bundesbeauftragte nach eigenem Ermessen vor Gericht das Zeugnis verweigern darf. Dieses Recht sollte ihm sowohl im Interesse Betroffener als auch — wie die Erfahrung zeigt — im staatlichen Geheimhaltungsinteresse eingeräumt und auf Aussagen seiner Mitarbeiter erstreckt werden.
- Nach den Feststellungen des BVerfG sind Vorkehrungen zum Schutz des Rechts auf informationelle Selbstbestimmung, wie sie die Tätigkeit der Datenschutzbeauftragten darstellt, in den Fällen besonders dringlich, in denen die Daten wegen ihres besonders sensiblen Informationsgehalts oder ihres Verwendungszusammenhanges speziellen Geheimhaltungspflichten (z. B. dem Statistik-, Steuer- oder Fernmeldegeheimnis) unterliegen. Daher ist klarzustellen, daß spezielle Geheimhaltungsvorschriften die Datenschutzkontrolle nicht ausschließen und das Fernmeldegeheimnis insoweit eingeschränkt ist.
- Die Kontrollbefugnis des Bundesbeauftragten für den Datenschutz darf nicht auf die Rechtmäßigkeit derjenigen Datenverarbeitung, die in Dateien stattfindet, beschränkt werden, insbesondere dann nicht, wenn es sich um Datenschutzvorschriften außerhalb des BDSG handelt, die keinen Dateibezug kennen. Andernfalls könnte die vom BVerfG geforderte Grundrechtssicherung durch eine effektive Datenschutzkontrolle nicht verwirklicht werden. Die mehrdeutige Fassung des § 19 Abs. 1 BDSG muß daher geändert werden. Im Regelfall wird eine Datenschutzkontrolle in bezug auf Daten, die sich in Akten und sonstigen Unterlagen befinden, nur dann in Betracht kommen, wenn Beschwerden Betroffener oder sonstige Anhaltspunkte vorliegen.

m) Grundrechte oder grundrechtsgleiche Rechtspositionen wirken als Abwehrrechte grundsätzlich nur im Verhältnis Staat-Bürger. Sie können aber als Ordnungsgrundsätze bzw. objektive Wertentscheidungen der Verfassung mittelbare Drittwirkung insofern entfalten, als Regelungen der *Rechtsbeziehungen zwischen Privaten* in ihrem Geiste ausgelegt werden müssen (BVerfGE 7, 205 f.), insbesondere nicht im Widerspruch zu Grundrechten stehen dürfen. Auch der private Bereich zählt zu der „sozialen Umwelt" des einzelnen, in der ohne seine Kenntnis Wissen über ihn angesammelt und gegen ihn verwendet werden kann, was ihn möglicherweise davon abhält, aus eigener freier Selbstbestimmung zu planen oder zu entscheiden. Das gilt insbesondere in bezug auf große private Organisationen, die allein durch ihre Machtposition soziale Kontrolle ausüben können.

Somit ist auch im privaten Bereich das informationelle Selbstbestimmungsrecht bei jedem Umgang mit personenbezogenen Informationen zu beachten. Die Beschränkung des BDSG auf bestimmte Verarbeitungsformen ist daher zu überprüfen. Allerdings ist zu berücksichtigen, daß auch der Umgang mit personenbezogenen Informationen im Anwendungsbereich des Privatrechts Grundrechtsschutz genießen kann. Dies kann es rechtfertigen, es bei dem auf Dateien abstellenden Regelungsansatz für solche Bereiche zu belassen, in denen die Auswirkungen auf die informationelle Selbstbestimmung eher gering zu veranschlagen sind. Soweit dagegen die Verwendung personenbezogener Informationen nach Zweck und Auswirkung oder wegen besonders großer Mißbrauchsrisiken die informationelle Selbstbestimmung der Betroffenen nach-

haltig einschränkt, ist — entsprechend dem öffentlichen Bereich — der Geltungsbereich des Datenschutzes umfassend anzulegen. Dies gilt beispielsweise für die Informationsverarbeitung durch Arbeitgeber und für den geschäftsmäßigen Umgang mit Angaben zur Kreditwürdigkeit sowie für die Verwendung medizinischer und anderer besonders empfindlicher Angaben, wie sie in Artikel 6 der Datenschutzkonvention des Europarats umschrieben werden.

Die zentralen Regelungsansätze des BDSG — Einwilligung und Vertragsverhältnis — sind aufrechtzuerhalten. Gesetzliche Korrekturen sind jedoch dort geboten, wo sich diese Instrumente als wirkungslos herausgestellt haben. Banken- und Versicherungsverträge sind Beispiele, die deutlich zeigen, daß die Einwilligung des Kunden in die Weitergabe seiner Daten nicht immer Ergebnis informationeller Selbstbestimmung, sondern häufiger Folge einseitiger Interessendurchsetzung ist. Nicht anders verhält es sich bei Mieterfragebögen und Krankenhaus-Aufnahmeverträgen, mit denen Mieter und Patienten nicht selten zum Verzicht auf Datenschutz veranlaßt werden. Zu erwägen wäre hier eine Ergänzung des § 3 BDSG, die eine mißbräuchliche Verwendung von Einwilligungsklauseln unterbindet; dabei könnte man an die Regelungen des Gesetzes über Allgemeine Geschäftsbedingungen anknüpfen. Auch im Arbeitsrecht muß berücksichtigt werden, daß die typische Abhängigkeit des Arbeitnehmers einer freien und gleichberechtigten Gestaltung der Informationsbeziehungen sowohl bei der Bewerbung als auch bei bestehendem Arbeitsverhältnis entgegensteht. Personenbezogene Daten über Arbeitnehmer sowie Bewerber sollten daher nur insoweit erhoben und verwendet werden dürfen, als die Durchführung des Arbeitsverhältnisses oder die Erfüllung von dem Arbeitgeber durch Gesetz auferlegten Pflichten davon abhängen.

Auch im privaten Bereich orientiert sich die Zulässigkeit der Verwendung personenbezogener Daten entscheidend an den Zwecken, zu denen die Daten erhoben und gespeichert worden sind. Im BDSG ist daher der Grundsatz der Zweckbindung auch für den nicht-öffentlichen Bereich als allgemeines Regelungsprinzip zugrunde zu legen.

Die Regelungen, welche sicherstellen sollen, daß der Betroffene sich Kenntnis von den ihn betreffenden privaten Datenspeicherungen verschaffen kann, bedürfen der Überprüfung. Dies gilt z. B. für die im 4. Abschnitt bestehende Regelung, den Betroffenen erst im Falle einer Übermittlung von der Speicherung seiner Daten zu benachrichtigen, und für die De-facto-Ausnahme von der Benachrichtigungspflicht zugunsten der Adressenverlage. Außerdem fehlt die Pflicht, den Betroffenen über den Zweck der Verarbeitung aufzuklären. Dies sollte bereits bei der Benachrichtigung geschehen. Um dem Betroffenen eine sachgerechte Entscheidung zu ermöglichen, ob er sein Auskunftsrecht ausüben soll, ist es darüber hinaus notwendig, bereits bei der Benachrichtigung mitzuteilen, welche Arten von Daten zu seiner Person vorliegen. Benachrichtigung und Auskunft sollten grundsätzlich die Quellen sowie die Empfänger der Daten umfassen.

Der Grundsatz der Effektivität von Grundrechtsschutz und Grundrechtsvorsorge ist auch im privaten Bereich zu beachten, allerdings mit unterschiedlichen Mitteln zu verwirklichen. Am wichtigsten erscheint es, die Aufsichtsbehörden der Länder in den Stand zu setzen, effektiv zu ermitteln und festgestellte Verstöße abzustellen. Aber auch die unternehmensinterne Datenschutzkontrolle durch Datenschutzbeauftragte und mit den Mitteln der betrieblichen Mitbestimmung bzw. Personalvertretung sollte verstärkt werden.

24.3 Regelungsbedarf für die Datenverarbeitung außerhalb von Dateien

Zu dieser Frage habe ich mich in meiner Stellungnahme (s. o.) wie folgt geäußert:

Da ein Eingriff in das Recht auf informationelle Selbstbestimmung auch vorliegt, wenn die personenbezogenen Angaben nicht in Dateien verarbeitet werden, sondern z. B. in Listen eingetragen oder in Akten gesammelt werden, sollten die Rahmenbedingungen auch für diese Datenverarbeitung in das BDSG aufgenommen werden. Dabei müssen im Grunde dieselben Prinzipien wie für die Datenverarbeitung in Dateien gelten; sie werden aber teilweise zu abweichenden, den anders gearteten Verarbeitungsverhältnissen angepaßten Regelungen führen müssen. Für solche Regelungen können hier nur erste Überlegungen angeboten werden, die der weiteren Vertiefung insbesondere im Hinblick auf die Anforderungen der Verwaltungspraxis bedürfen.

a) Datenerhebung

Soweit Daten erfragt oder auf andere Weise erhoben werden, müssen dieselben Regeln gelten, wie für Daten, die in Dateien gespeichert werden sollen. Denn zum einen ist bei der Datenerhebung häufig nicht gesichert, daß die erhobenen Daten nicht doch in Dateien verarbeitet werden, und zum anderen kann die Grundrechtsposition des einzelnen insoweit nicht durch die formalen Strukturen der weiteren Datenverarbeitung beeinflußt werden.

Weil die Datenerhebung stets als besonderer Vorgang zu regeln ist und die weitere Verarbeitung erst danach erfolgt, ergibt sich auch aus den unterschiedlichen Formen der Weiterverarbeitung kein Unterschied im Regelungsbedarf.

b) Datenspeicherung

Werden Daten nicht in (planmäßig strukturierten) Dateien gespeichert, so ist es häufig schwer, die wirklich benötigten Angaben von außerdem vorhandenen Darstellungen oder Mitteilungen zu tren-

nen. So können im Schriftwechsel, aber auch in Listen, Plänen oder anderen Unterlagen personenbezogene Angaben enthalten sein, die zwar für die Aufgabe nicht im strengen Sinne erforderlich sind, dort aber auch nicht mit vertretbarem Aufwand entfernt werden können.

Aus diesen Gründen müssen die Zulässigkeitskriterien für die Speicherung weiter gefaßt sein, insbesondere muß auf die Vollständigkeit und den Zusammenhang der Darstellung Rücksicht genommen werden. Damit ließe sich der Handlungsspielraum für die speichernde Stelle so erweitern, daß eine praktikable Lösung erreicht werden kann.

c) Übermittlung

Gerade dann, wenn nicht aus Dateien übermittelt wird, ist die Übermittlung ein Einzelvorgang, der eine Prüfung der Zulässigkeit erlaubt. Trotzdem werden die entsprechenden Vorschriften, die auf die Erforderlichkeit der Kenntnis der Daten abstellen, nicht ohne weiteres übertragbar sein. Denn ähnlich wie bei der Speicherung kann es gelegentlich unmöglich sein, die zu übermittelnden Daten von anderen körperlich zu trennen. Auch läßt es sich bei der Überlassung von Akten in der Praxis kaum vermeiden, daß neben erforderlichen und zulässigerweise übermittelten Bestandteilen von Akten auch andere Daten „mitgehen", für die diese Zulässigkeitsvoraussetzungen nicht vorliegen. Eine an sich gebotene Trennung stößt oft auf erhebliche praktische Hindernisse. Deshalb sind auch hier der Zusammenhang der Darstellung und die Vollständigkeit zu berücksichtigen.

d) Datenverwendung

Da mit *jeder* Datenverwendung ein bestimmter Zweck verfolgt wird, können die für die Verwendung von Daten in Dateien geltenden Grundsätze auch auf andere Formen der Verarbeitung Anwendung finden. Aus verfassungsrechtlichen Gründen erscheint das auch geboten, denn bei der Beurteilung eines Eingriffs in das Recht auf informationelle Selbstbestimmung durch die Verwendung von Daten kommt es auf die genutzte Technik nicht an.

Die Übernahme der engen Zweckbindungsvorschriften mildert überdies auch die unvermeidbare Lockerung bei den Zulässigkeitsvoraussetzungen für die Speicherung und die Übermittlung.

e) Auskunft an den Betroffenen

Anders als bei der Datenverarbeitung in Dateien dürfte es praktisch unmöglich sein, in Akten, Zeitungsausschnittssammlungen und ähnlichen unstrukturierten Unterlagen alle zur Person des Betroffenen gehörenden Daten unter seiner Anschrift, seinem Namen, dem Geburtsdatum oder anderen identifizierenden Angaben aufzufinden.

Deshalb wird die Auskunft in diesen Fällen regelmäßig nur dann erteilt werden können, wenn der Betroffene ausreichende Angaben zu dem Zusammenhang macht, in dem seine Daten bei der speichernden Stelle geführt werden. Die Auskunftspflicht muß sich deshalb auf diejenigen Daten beschränken, die nach den Angaben des Betroffenen mit vertretbarem Aufwand gefunden werden können.

Eine andere denkbare Lösung könnte darin bestehen, dem Betroffenen Einsicht in die in Betracht kommenden Unterlagen zu gewähren, allerdings ohne die im Verwaltungsverfahrensgesetz dafür vorgesehene Voraussetzung, daß er Beteiligter an einem laufenden Verwaltungsverfahren ist. Zu berücksichtigen wäre dabei auch, daß durch die Einsicht schutzwürdige Belange Dritter nicht verletzt, insbesondere nicht fremde Angaben zur Kenntnis genommen werden dürfen.

f) Berichtigung und Löschung

Die Verpflichtung, unrichtige Daten zu berichtigen, kann grundsätzlich auch auf die Datenverarbeitung außerhalb von Dateien übertragen werden. Die Methoden der Berichtigung werden aber andere sein, weil die unrichtigen Darstellungen häufig Urkunden sind oder ähnliche Beweiskraft haben oder für den nachzuvollziehenden Ablauf eines Verfahrens unverzichtbar sind. In diesen Fällen müßte die Berichtigung im Hinzufügen der richtigen Darstellung bestehen. Das Löschen unrichtiger Daten wird also wegen der notwendigen Vollständigkeit nicht immer gefordert werden können.

Sind Einzelangaben für die Zweck- oder Aufgabenerfüllung nicht mehr erforderlich, sind sie aber mit anderen Teilen desselben Komplexes, für die dies nicht zutrifft, nur schwer trennbar verbunden, so sollte eine Löschungspflicht nur bestehen, wenn eine Abwägung ergibt, daß die für eine Löschung sprechenden Gründe die Gesichtspunkte der Vollständigkeit und des Sinn- bzw. Sachzusammenhangs überwiegen.

g) Transparenz

Die Verfahren der Verarbeitung personenbezogener Daten außerhalb von Dateien dürften eine Beschreibung, wie sie für die Datei-Veröffentlichungen gemäß § 12 BDSG oder das Dateienregister des BfD gemäß § 19 Abs. 4 BDSG vorgesehen ist, weitgehend ausschließen. Auch die Benachrichtigung des Betroffenen dürfte häufig an praktischen Schwierigkeiten scheitern. Deshalb müssen hier Einschränkungen der Transparenz nach außen hingenommen werden.

Mit welchen Mitteln wenigstens ein gewisses Maß an innerer Transparenz — also für die speichernde Stelle und die dort für den Datenschutz Verantwortlichen — erreicht werden kann, bedarf noch der weiteren Diskussion. Denkbar wäre auch eine Aufzeichnungspflicht, die sich nur auf besonders sensible Datenarten oder besondere Verarbeitungsformen (z. B. Listen) erstreckt.

h) Datensicherung

Eine allgemeine Pflicht zur sicheren Verwahrung und zur Kontrolle des Umgangs mit Daten sollte nicht auf Daten in Dateien beschränkt sein. Gerade Akten mit ihren oft recht detaillierten Schilderungen von persönlichen Verhältnissen bedürfen der gesicherten Unterbringung, zumal auf sie ohne besondere Sachkunde zugegriffen werden kann. Die Datensicherungsvorschriften sollten deshalb nur zwischen automatisierten und nicht-automatisierten Verfahren unterscheiden.

i) Datenschutz-Kontrolle

Gerade weil die Verarbeitung personenbezogener Daten außerhalb von Dateien in sehr unterschiedlichen Formen erfolgt, ist sie für den Betroffenen kaum übersehbar. Die Kontrolle durch unabhängige Datenschutzbeauftragte sollte für diesen Mangel einen Ausgleich schaffen. Auch wenn sie sich nach denselben Vorschriften vollziehen soll, wie sie für Dateien gelten, muß jedoch schon aus Kapazitätsgründen mit einer wesentlich geringeren Stichprobendichte gerechnet werden. Der gegenwärtige unbefriedigende Zustand, daß Anfragen und Beschwerden Betroffener oft nur unzureichend behandelt werden können, weil die entsprechenden Daten nicht in Dateien verarbeitet werden, sollte aber auf jeden Fall beseitigt werden.

25. Ausland und Internationales

25.1 Datenschutz-Konvention des Europarats

Der Entwurf eines Ratifikationsgesetzes zur Datenschutz-Konvention des Europarats vom 28. Januar 1981 wird zur Zeit im Parlament beraten. Ich begrüße es sehr, daß die Verabschiedung nunmehr in greifbare Nähe gerückt ist, denn ich verspreche mir davon wesentliche Impulse für die Weiterentwicklung des Datenschutzes. Für den Datenschutz in Europa und auch darüber hinaus ist die Ratifikation durch die Bundesrepublik von besonderer Bedeutung, weil damit der fünfte Zeichnerstaat ratifizieren und dadurch die Konvention endlich — über vier Jahre nach ihrem Zustandekommen — in Kraft treten wird. Länder, deren Datenschutzstandard noch nicht den in der Konvention normierten Anforderungen entspricht, werden sich dann noch stärker mit der Notwendigkeit konfrontiert sehen, zu diesem Standard aufzurücken, weil andernfalls eine Behinderung des grenzüberschreitenden Datenflusses aufgrund von Datenschutzvorschriften eines Vertragsstaates nicht ausgeschlossen werden kann.

Auch innerhalb der Bundesrepublik Deutschland erwarte ich einen positiven Effekt für den Datenschutz, da die Regelungen der Konvention in einigen Punkten präziser sind als das deutsche Datenschutzrecht. So verbietet die Konvention beispielsweise die Verwendung von Daten zu einem Zweck, der mit dem (ursprünglichen) Zweck ihrer Verarbeitung nicht vereinbar ist. Insgesamt wird die Konvention im gleichen Sinne wie die Volkszählungs-Entscheidung des Bundesverfassungsgerichts zu einer noch konsequenter an den Interessen der Betroffenen orientierten Datenschutzpraxis führen.

Der Europarat setzt seine Bemühungen fort, die Grundsätze der Konvention durch bereichsspezifische Empfehlungen inhaltlich auszufüllen und zu konkretisieren. Nach der Verabschiedung einer Empfehlung zum Schutz personenbezogener Daten für Zwecke der wissenschaftlichen Forschung und Statistik im Jahre 1983 (abgedruckt als Anlage 3 zum 6. TB) sind zwei weitere Empfehlungen zu den Bereichen Direktwerbung/Adressenhandel und soziale Sicherung vom Expertenkomitee Datenschutz, an dessen Arbeit ich mich beteilige, vorbereitet worden. Mit ihrer Verabschiedung durch den Ministerrat wird im Laufe des Jahres 1985 gerechnet.

Der Europarat beschäftigt sich weiter mit den Problemen der polizeilichen Informationsverarbeitung und dem Arbeitnehmerdatenschutz. Darüber hinaus will er den Einfluß der informationstechnologischen Veränderungen auf den Datenschutz untersuchen.

25.2 Die Datenschutzgesetzgebung im Ausland

Nach einigen Jahren der Stagnation zeigen sich in der Datenschutzgesetzgebung des Auslandes wieder verstärkte und aussichtsreiche Aktivitäten.

Ein wichtiger Markstein war die Verabschiedung des britischen Datenschutzgesetzes im vergangenen Jahr. Dieses Gesetz übernimmt zum Teil wörtlich die Datenschutzprinzipien der Europarats-Konvention. Die Datenschutzaufsicht liegt, zusammengefaßt für den öffentlichen und den privaten Bereich, beim Data Protection Registrar. Bei ihm sind alle Datenbestände zu einem zentralen Register anzumelden. Die Verwendung der Daten muß den Registereintragungen entsprechen. Der Registrar soll darauf hinwirken, daß Wirtschaftsverbände und andere Organisationen jeweils für ihre Mitglieder besondere Datenschutzrichtlinien aufstellen. Gegen Entscheidungen des Registrar kann Beschwerde beim neu eingerichteten Data Protection Tribunal eingelegt werden, welches paritätisch aus Vertretern der datenverarbeitenden Stellen und der Betroffenen zusammengesetzt ist.

In Belgien wurden, da der Entwurf eines Datenschutzgesetzes noch nicht verabschiedet ist, in das neue Gesetz über das Bevölkerungsregister ausführliche Datenschutzvorschriften aufgenommen. Dazu gehört auch die Einrichtung eines Datenschutz-Ausschusses.

Kanada hat sein Datenschutzrecht grundlegend umgestaltet und ausgebaut. Der Datenschutz ist nicht mehr in einem Abschnitt des Human Rights Act geregelt, sondern in einem besonderen Privacy Act. Auch das (allgemeine) Recht auf Zugang zu Regierungsinformationen wurde in einem gesonderten Gesetz, dem Access to Information Act, gere-

gelt und seine Kontrolle dem Information Commissioner anvertraut. Der Privacy Commissioner, bisher nur Ombudsmann, ist seit der Gesetzesänderung auch für die präventive Kontrolle des Datenschutzes bei allen Regierungseinrichtungen des Bundes zuständig.

In mehreren Ländern sind die Vorbereitungen so weit gediehen, daß mit der Verabschiedung eines Datenschutzgesetzes innerhalb der nächsten ein bis zwei Jahre gerechnet werden kann; hierzu zählen die Niederlande, Italien, Spanien und Portugal.

25.3 Zusammenarbeit der Datenschutz-Kontrollinstanzen

Die internationale Konferenz der Datenschutz-Kontrollinstanzen beschäftigte sich auf ihrer Sitzung in Wien im September 1984 mit einer Reihe von Fachfragen, u. a. im Zusammenhang mit Kreditauskunfteien, der Personaldatenverarbeitung, der Direktwerbung und der Polizei. Bereichsübergreifende Konferenzthemen waren die Kontrollverfahren der Datenschutzaufsicht, die Entwicklung und Verbreitung maschinenlesbarer Ausweise und die Fortentwicklung des Datenschutzrechts, wobei das Volkszählungsurteil des Bundesverfassungsgerichts auf besonderes Interesse der Teilnehmer stieß.

25.4 Europäische Gemeinschaft

In meinem letzten Tätigkeitsbericht (6. TB S. 58) habe ich auf den wachsenden Einfluß supranationaler Aktivitäten auf die Datenverarbeitung und den Datenschutz in der Bundesrepublik Deutschland hingewiesen. Dieser Einfluß hat sich im vergangenen Jahr weiter verstärkt. Die Entwicklung fordert nunmehr grundsätzliche Überlegungen, wie der Datenschutz für die Bürger der Bundesrepublik Deutschland angesichts dieser zunehmenden externen Einflußfaktoren gewährleistet werden kann. Für den nachhaltigen Einfluß der Europäischen Gemeinschaft auf den Datenschutz in der Bundesrepublik Deutschland möchte ich einige Beispiele anführen.

a) Durch Zufall erfuhr ich von Bemühungen der Mitgliedsländer der Europäischen Gemeinschaft, für den grenzüberschreitenden Warenverkehr ein Einheitspapier einzuführen, durch welches die zollrechtlichen, die statistischen und die versendungstechnischen Angaben in einem einzigen Dokument zusammengefaßt werden sollen. Dadurch erhält jede beteiligte Stelle die Kenntnis aller Daten, auch solcher, die sie nicht benötigt. Auf meinen Hinweis, daß dabei der Datenschutz — insbesondere die Grundsätze der rechtlichen Aufklärung bei der Datenerhebung und der Erforderlichkeit bei der Datenübermittlung — zu beachten sei, entgegneten die zuständigen Ressorts, die Entscheidung innerhalb der Europäischen Gemeinschaft stehe kurz bevor, datenschutzrechtliche Einwendungen von deutscher Seite gefährdeten das Gesamtprojekt und seien angesichts der wirtschaftlichen und politischen Bedeutung des Projekts nicht zu vertreten. Das EG-Einheitspapier wurde beschlossen; es muß nun versucht werden, durch Maßnahmen auf nationaler Ebene den Datenschutz zu verwirklichen, soweit dies möglich ist.

b) Das Statistische Amt der Europäischen Gemeinschaft in Luxemburg erhält, zum Teil auf der Grundlage von EG-Vorschriften, von den Statistischen Ämtern der Mitgliedsstaaten Daten, deren Struktur teilweise so beschaffen ist, daß daraus Angaben über einzelne Auskunftspflichtige gewonnen werden können. Es gibt jedoch keine Rechtsvorschrift der Europäischen Gemeinschaft, welche die Daten ihres Statistischen Amtes strikt gegen eine Offenbarung an Außenstehende oder eine Verwendung für nichtstatistische Zwecke schützt, wie dies in der Bundesrepublik Deutschland nunmehr beispielhaft gewährleistet ist. Der Konflikt zwischen EG-rechtlicher Datenlieferungspflicht und nationalem Statistikgeheimnis kann zu einer schweren Belastung der statistischen Arbeit führen.

c) Das Presse- und Informationsbüro der Europäischen Gemeinschaft in Bonn informiert die Presse regelmäßig über Förderungsmaßnahmen des Europäischen Ausrichtungs- und Garantiefonds für die Landwirtschaft. Dabei werden für jede Förderungsmaßnahme nicht nur der genaue Förderungsbetrag und der individuelle Förderungszweck genannt, sondern auch Name und/oder Firma und Ort des Förderungsempfängers. So heißt es etwa in der Agrardokumentation (Fischerei) Nr. 57 vom 26. Juli 1984: „... 7. Friedrich P. (Namen im Original ausgeschrieben) in 2251 Finkhaushallig erneuert sein Schiff in Husum mit 90 000 DM, wofür 22 500 DM aus Brüssel bereitgestellt werden." Dem beschwerdeführenden Landesfischerei-Verband Schleswig-Holstein konnte ich mangels Zuständigkeit nicht weiterhelfen; ich habe allerdings das Presse- und Informationsbüro der Europäischen Gemeinschaft von den Beschwerden in Kenntnis gesetzt und auf die Bedenken aus der Sicht des Datenschutzes hingewiesen.

d) Im Bereich des Weinbaues müssen Erzeuger und Händler nach Vorschriften der Europäischen Gemeinschaft jährlich Meldungen über erzeugte Mengen und Lagerbestände machen. Zweck dieser Meldungen war es bisher allein, sie statistisch auszuwerten, damit die EG auf der Basis der Ergebnisse globale marktbeeinflussende Maßnahmen treffen kann. Mit der Verordnung (EWG) Nr. 2102/84 der Kommission vom 13. Juli 1984 wurde als weiterer Verwendungszweck vorgesehen, daß die Angaben des einzelnen Meldepflichtigen „außer zu statistischen Zwecken (auch) für die Durchführung der Verordnungen (EWG) Nr. 337/79 und 338/79 des Rates verwendet" werden dürfen. Insbesondere ist die Aufschlüsselung nach einzelnen Weinarten künftig verbindlich für etwaige individuelle Interventionsmaßnahmen.

   Damit erfolgt die Erhebung zu zwei ganz verschiedenen Zwecken. Das Volkszählungsurteil des Bundesverfassungsgerichts verbietet aber

zusammengefaßte Erhebungen, wenn die Erhebungszwecke nicht miteinander vereinbar sind. Jedenfalls hätte die vorgesehene Weiterleitung der Einzelangaben an eine Verwaltungsbehörde (Bundesamt für Ernährung und Forstwirtschaft) für Zwecke des Verwaltungsvollzugs in entsprechender Anwendung der Vorschriften des Bundesstatistikgesetzes (§§ 12, 11 Abs. 1 und 3) auf den Erhebungsunterlagen bekanntgegeben werden müssen. Weder bei der Vorbereitung der erwähnten EG-Vorschriften noch bei Erlaß der innerstaatlichen Durchführungsvorschriften bin ich beteiligt worden.

Um einen effektiven Datenschutz des deutschen Bürgers auch dann zu gewährleisten, wenn seine personenbezogenen Daten durch Einrichtungen der Europäischen Gemeinschaft oder aufgrund von EG-Regelungen verarbeitet werden, empfehle ich folgendes:

1. Die Bundesrepublik Deutschland sollte eine Initiative mit dem Ziel ergreifen, daß die Europäische Gemeinschaft für die personenbezogene Datenverarbeitung durch ihre eigenen Organe Datenschutzregelungen erläßt.

2. Die Bundesregierung sollte darauf hinwirken, daß die Europäische Gemeinschaft — entsprechend der Entschließung des Europäischen Parlaments vom 9. März 1982 (vgl. 5. TB S. 117) — die Datenschutz-Konvention des Europarats ratifiziert.

3. Die Bundesregierung sollte weiter darauf hinwirken, daß innerhalb der Europäischen Gemeinschaft durch geeignete organisatorische Vorkehrungen auch schon im Vorgriff auf künftige EG-rechtliche Regelungen sichergestellt wird, daß sowohl bei der Verarbeitung personenbezogener Daten durch die Organe der Europäischen Gemeinschaft selbst als auch bei Rechtsetzungsakten, die eine Verarbeitung personenbezogener Daten durch die Mitgliedsländer auslösen, der Datenschutz beachtet wird.

4. Unabhängig von diesen Maßnahmen der Europäischen Gemeinschaft wäre es wünschenswert, daß die Bundesregierung im Rahmen ihrer Mitwirkung an Entscheidungsprozessen der Europäischen Gemeinschaft dem Datenschutz verstärkte Bedeutung zumißt und dazu insbesondere eine ausreichende Beteiligung des Bundesbeauftragten für den Datenschutz sicherstellt.

26. Bilanz

In meinem Sechsten Tätigkeitsbericht habe ich über mehrere offene Probleme berichtet sowie über einige Entwicklungen, die noch nicht abgeschlossen waren. Wie die nachfolgende Aufstellung zeigt, wurden die Bemühungen, gemeinsam mit den zuständigen Stellen vertretbare Lösungen zu erarbeiten, überwiegend erfolgreich fortgesetzt, sie konnten häufig aber noch nicht zum Abschluß gebracht werden. Nur in wenigen Punkten stehen sich im wesentlichen unveränderte, gegensätzliche Rechtspositionen gegenüber.

1. Auf die Notwendigkeit, vor der Einführung des neuen Personalausweises weitere Datenschutzregelungen zu treffen, habe ich hingewiesen (6. TB S. 6 ff.). Diese Forderungen wurden bisher nur zum Teil berücksichtigt, siehe dazu Nr. 2.1 in diesem Bericht.

2. Über den Beginn der Arbeiten an der Neukonzeption des Ausländerzentralregisters habe ich berichtet (6. TB S. 9). Die Arbeitsgruppe, an der ich beteiligt bin, hat die in das Register aufzunehmenden Inhalte im wesentlichen abschließend diskutiert, andere Fragen — insbesondere zur Kommunikationsstruktur und zu den Rechtsgrundlagen — sind noch offen, siehe dazu Nr. 2.2 in diesem Bericht.

3. Gegen die Auffassung, daß die Bezeichnung „Verwaltungsangelegenheit", gegebenenfalls mit einem Aktenzeichen, als Zweckangabe für eine unbeschränkte Auskunft aus dem Bundeszentralregister ausreiche, habe ich Bedenken geltend gemacht (6. TB S. 12). Diese Angabe wird nun nicht mehr als ausreichend akzeptiert.

4. Ich habe bedauert, daß meine schon seit Jahren vorliegenden Vorschläge zur Novellierung des Bundeszentralregistergesetzes nicht berücksichtigt worden sind (6. TB S. 12). In die jüngste Novellierung ist vom Bundesminister der Justiz nur einer meiner Vorschläge aufgenommen worden, siehe dazu Nr. 4.1 in diesem Bericht.

5. Die Schaffung einer bereichsspezifischen Rechtsgrundlage für die Datenübermittlungen durch die Standesbeamten habe ich angeregt (6. TB S. 12 f.). Ich begrüße es, daß der Bundesminister des Innern dies inzwischen gleichfalls als notwendig ansieht und als Vorbereitung dazu bestimmte Mitteilungspflichten aus der bestehenden Dienstanweisung gestrichen hat, siehe dazu Nr. 2.5 in diesem Bericht.

6. Auf die Notwendigkeit von Verbesserungen bei den Mitteilungen in Zivilsachen, den Mitteilungen in Strafsachen sowie den Richtlinien für das Straf- und Bußgeldverfahren habe ich hingewiesen (6. TB S. 13 f.). Diese Arbeiten erweisen sich besonders wegen der Abstimmung mit den Ländern als schwierig. Ich begrüße es, daß sich jetzt erste Fortschritte erkennen lassen, siehe dazu Nr. 4.5 in diesem Bericht.

7. Über Tendenzen zur Verbesserung des Datenschutzes im Grundbuchwesen habe ich berichtet (6. TB S. 15). Leider ist bisher nicht erkennbar, in welchen Zeiträumen mit Lösungsvorschlägen des Bundesministers der Justiz zu rechnen ist, siehe dazu Nr. 4.7 in diesem Bericht.

8. Über datenschutzrechtliche Verbesserungen in Vorschlägen zur Novellierung der Abgabenordnung habe ich berichtet (6. TB S. 16). Die Erörterung ist noch nicht abgeschlossen. Nach wie vor fehlt auch eine positive Klärung meiner Kontrollbefugnisse für durch das Steuergeheimnis geschützte Daten, siehe dazu Nr. 5.1 in diesem Bericht.

9. In Bußgeldsachen habe ich der Zollverwaltung einen Verzicht auf Auskunftsersuchen an das Bundeszentralregister empfohlen und zugleich angeregt, bei Auskunftsersuchen in Steuerstrafsachen nicht die mißverständliche Zweckangabe „Steuersache" zu verwenden (6. TB S. 17). Die Zollverwaltung ist diesen Vorschlägen gefolgt, vgl. auch Nr. 4.1 in diesem Bericht.

10. Auf die Notwendigkeit einer Neuregelung für das Personalaktenrecht und für die Behandlung der Daten über Beihilfen im Krankheitsfall habe ich hingewiesen (6. TB S. 18 und S. 20). Der Bundesminister des Innern hat inzwischen dafür eine interministerielle Arbeitsgruppe gebildet, an der ich beteiligt bin, siehe dazu Nr. 7.3.1 in diesem Bericht.

11. Über Schritte zur Verbesserung der Situation bei der Bekanntgabe von Telefonverbindungsdaten, z. B. wenn Gebühren strittig sind, habe ich berichtet (6. TB S. 22 f.). Meinen mit dem Bundespostministerium abgestimmten Lösungsvorschlag hat der Ausschuß für das Post- und Fernmeldewesen akzeptiert; es wird aber noch nicht danach verfahren, siehe dazu Nr. 8.3 in diesem Bericht.

12. Über die Entwicklung beim Bildschirmtext-System habe ich berichtet (6. TB S. 23). Auch aufgrund meiner Prüfung der Bildschirmtext-Leitzentrale habe ich weitere Empfehlungen gegeben, siehe dazu Nr. 8.5 in diesem Bericht.

13. Über den Beginn der Arbeiten an einer gesetzlichen Grundlage für das Zentrale Verkehrsinformationssystem (ZEVIS) habe ich berichtet (6. TB S. 25 f.). An der Erörterung eines Entwurfs für ein Fahrzeugregistergesetz bin ich beteiligt, die Abstimmungsgespräche zwischen den Ressorts sind noch nicht abgeschlossen, siehe dazu Nr. 9.1 in diesem Bericht.

14. Auf Probleme des Schutzes von Einzelangaben aus Bundesstatistiken, die an oberste Bundesbehörden weitergeleitet werden, habe ich hingewiesen (6. TB S. 29). Zur Zeit werden durch das Statistische Bundesamt keine Einzelangaben mehr übermittelt.

15. Gegen das Verfahren bei der Gewährung von Arbeitslosenhilfe habe ich Bedenken geäußert (6. TB S. 31). Die Bundesanstalt für Arbeit prüft zur Zeit, ob diesen Bedenken Rechnung getragen werden kann, siehe dazu Nr. 13.3 in diesem Bericht.

16. Über Schwierigkeiten bei der Gewährung des Akteneinsichtsrechts gemäß § 25 SGB X habe ich berichtet (6. TB S. 31). Der inzwischen verabschiedete Erlaß der Bundesanstalt für Arbeit regelt das Verfahren zufriedenstellend.

17. Eine Prüfung der Zulässigkeit der Auftragsdatenverarbeitung der Volkswagenwerk AG (VW AG) für die Betriebskrankenkasse VW AG habe ich angekündigt (6. TB S. 34). Diese Prüfung hat die zunächst bestehenden Bedenken ausgeräumt, siehe dazu Nr. 15.1.1 in diesem Bericht.

18. Auf Unzulänglichkeiten bei der Erteilung von Bankauskünften über Kunden habe ich hingewiesen (6. TB S. 37 f.). Die Verhandlungen der Datenschutzbeauftragten und -aufsichtsbehörden mit Vertretern der Kreditwirtschaft haben zu befriedigenden Lösungen geführt, siehe dazu Nr. 22.2 in diesem Bericht.

19. Auf die Notwendigkeit, im internationalen Informationsaustausch im Rahmen von Interpol die internationalen Regelungen zum Schutz des Betroffenen stärker zu beachten, habe ich hingewiesen (6. TB S. 44). Das Bundeskriminalamt hat zugesagt, durch entsprechende Schulung dies zukünftig sicherzustellen.

20. Eine inhaltliche Prüfung der im Hinblick auf den erwarteten „heißen Herbst" vom Bundeskriminalamt eingerichteten Datei „Lage 1" habe ich angekündigt (6. TB S. 47). Diese Prüfung hat zu Beanstandungen Anlaß gegeben, siehe dazu Nr. 20.1.1 in diesem Bericht.

21. Gegen die Speicherung von die Intimsphäre berührenden Merkmalen durch das Bundesamt für Verfassungsschutz habe ich Bedenken erhoben (6. TB S. 50). Das Bundesamt für Verfassungsschutz hat zugesagt, einige dieser Merkmale künftig nicht mehr zu speichern, siehe dazu Nr. 21.1.1 in diesem Bericht.

22. Verzögerungen bei der Bereinigung von Altfällen beim Bundesnachrichtendienst habe ich bemängelt (6. TB S. 52). Im Berichtsjahr konnten hier erhebliche Verbesserungen festgestellt werden, siehe dazu Nr. 21.2.3 in diesem Bericht.

23. Eine Prüfung, ob im Institut für Wehrmedizinalstatistik und ärztliches Berichtswesen der Bundeswehr die Daten über die ärztliche Behandlung von Soldaten von den Gutachten über die Verwendungsfähigkeit getrennt werden können, habe ich angeregt (6. TB S. 54). Der Bundesminister der Verteidigung hat als Ergebnis seiner Prüfung mitgeteilt, daß dies nicht möglich sei, siehe dazu Nr. 18.4 in diesem Bericht.

24. Über Zwischenergebnisse eines Forschungsprojekts der Gesellschaft für Mathematik und Datenverarbeitung, in dem Methoden zur Anonymisierung personenbezogener Daten für Forschungszwecke untersucht wurden, habe ich berichtet (6. TB S. 60). Der inzwischen vorliegende Schlußbericht bestätigt die Vermutung, daß nur bei kleinen Stichproben und einer eng begrenzten Anzahl von Merkmalen eine ausreichende Anonymisierung so erfolgen kann, daß das Analysepotential der Daten weitgehend erhalten bleibt. In allen anderen Fällen müssen also andere Wege des Ausgleichs zwischen Forschungsinteressen und Datenschutzrechten gefunden werden.

Bonn, den 22. Januar 1985

Dr. Baumann

Anlage 1 (zu Nr. 23)

Problemskizze zur Sicherheit bei der Datenkommunikation *)

Gliederung

1. Einleitung

Die modernen Formen der Informationsverarbeitung haben einerseits die schon immer bestehenden Gefahren der Informationsverarbeitung vergrößert, andererseits neue Gefahren geschaffen, aber unter anderen Aspekten auch zu mehr Sicherheit geführt.

Ziel dieser Problemskizze ist es, die Sicherheit bei automatisch unterstützten Kommunikationsvorgängen abzuschätzen, die unter Bezeichnungen wie Telekommunikation, Datenfernverarbeitung oder Online-Datenübertragung im Rahmen privat oder öffentlich betriebener Netze zunehmend eingesetzt werden.

Unberücksichtigt bleiben die internen Sicherheitsprobleme der Rechenzentren und Datenspeicher, zu denen solche Verbindungen bestehen, sowie die Risiken gesellschaftlicher Veränderungen durch „Verdichtung von Datennetzen". Auch kann im Rahmen dieser Darstellung nicht auf alle Feinheiten eingegangen werden.

Den Anlaß zu dieser Arbeit gaben zum einen Berichte über sogenannte Hacker, vorwiegend jugendliche Computerexperten, die mit im Handel erhältlichen Geräten (Home-Computern) über Telefon-Wählleitungen meist aus technisch-sportlichem Ehrgeiz Verbindungen zu komplexen Datenverarbeitungssystemen aufgebaut, dort Daten abgerufen und zum Teil durch Datenänderungen erheblichen Schaden angerichtet haben.

Zum anderen besteht aber auch unabhängig von solchen „Erfolgsberichten" und ihrem Wahrheitsgehalt ein Interesse an einer zumindest qualitativen Beurteilung der Risiken und an einer Darstellung von möglichen und wirksamen Sicherheitsmaßnahmen. Dabei kann außer Betracht bleiben, ob — i. S. des BDSG — schutzwürdige Belange eines Betroffenen tatsächlich beeinträchtigt werden oder ob ein Schaden (nur) beim Betreiber des Systems eintritt. Denn es ist die Aufgabe des Betreibers, die notwendigen Sicherheitsmaßnahmen gegen die mögliche Gefährdung unabhängig von beobachteten Angriffen zu treffen, und für einen erheblichen Vertrauensschaden können schon begründete Vermutungen über die Unsicherheit eines Systems ausreichen.

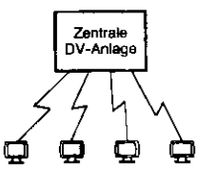
Bezogen auf die Arbeit der Bundesverwaltung gilt dies sowohl für neue Systeme, wie z. B. für Bildschirmtext, als auch für schon länger bestehende Verfahren, wie z. B. INPOL oder andere DV-Anwendungen, die durch Datenfernübertragung neue Strukturen bekommen, wie z. B. ZEVIS.

2. Strukturen von Datenkommunikationsnetzen

2.1 Beteiligte Anlagen

Die Mehrzahl der Datenkommunikationsnetze hat zwei unterschiedliche Arten von beteiligten DV-Anlagen, die gemeinsam das Kommunikationssystem bilden, und zwar

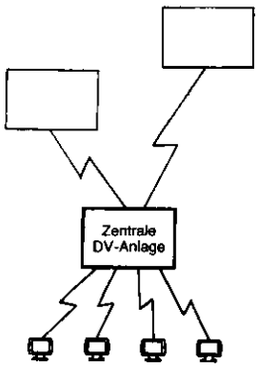
- eine Zentrale, in der die Daten und die (größeren) Auswertungsprogramme zur Verfügung stehen, und
- mehrere, gegenüber der Zentrale mit deutlich weniger Leistungs- und Speicherungsfähigkeit ausgestattete Daten(end)stationen (Terminals).



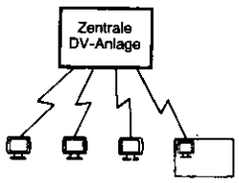
*) vorgelegt dem Innenausschuß des Deutschen Bundestages am 21. Dezember 1984

Dabei steht im allgemeinen die Zentrale ständig oder in festgelegten Betriebszeiten zur Verfügung. Die Terminals werden dagegen oft nur gelegentlich benutzt, um Daten an die Zentrale zu schicken oder von dort Daten abzurufen oder um Verarbeitungen zu veranlassen, deren Ergebnisse an das Terminal ausgegeben oder in anderer Form (z. B. Listenausdrucke) verschickt werden. Abweichungen von diesem Grundmuster sind insofern möglich, als

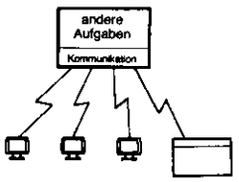
— die „Zentrale" aus mehreren untereinander verbundenen Anlagen bestehen kann. Das Benutzerterminal ist mit einer dieser Anlagen verbunden, die bei Bedarf als Vermittler zu den anderen Anlagen arbeitet. Ein Beispiel dafür ist das Btx-Netz, in dem ein Benutzeranschluß mit „seiner regional zuständigen Vermittlungsstelle" verbunden ist, die bei Bedarf mit anderen Rechnern Daten austauscht, um solche Anforderungen des Benutzers weiterleiten und erfüllen zu können, die über den eigenen — vorrätigen — Datenbestand der Vermittlungsstelle hinausgehen;



— statt einfacher Benutzerterminals leistungsfähige DV-Anlagen oder Arbeitsplatz-Computer vorhanden sein können, die im Rahmen dieses Datenverkehrs die Rolle von Terminals spielen (simulieren) oder auch mit anderen Verfahren den Datenverkehr bewirken;



— sowohl in der Zentrale bzw. in den ihr zugeordneten DV-Anlagen als auch in den Terminals außer diesem Daten*verkehr* noch andere Verarbeitungen (ohne Fernverarbeitungsleistung) ablaufen können, so daß die Kommunikation mit anderen Stellen unter Umständen nur einen geringen Anteil an der Gesamtleistung hat.



2.2 Verbindungsarten

Je nach Art der angeschlossenen DV-Anlagen, dem Volumen des anfallenden Datenverkehrs und den zu überbrückenden Entfernungen werden unterschiedliche Arten von Verbindungen genutzt:

— Verbindungen mit Hilfe des *Telefonnetzes*

Das installierte Telefonnetz ist nicht nur geeignet, das gesprochene Wort zu übertragen, sondern auf den zu einer Verbindung geschalteten Leitungen können auch digitale Signale (Daten) übertragen werden. Diese Signale sind im Prinzip „Töne", die je nach Art der Übertragungstechnik hörbar sind oder außerhalb des hörbaren Frequenzbereichs liegen, und zum Teil auch auf einer Leitung gesendet werden können, auf der gleichzeitig gesprochen wird.

Die Umsetzung der Daten aus der Form, in der sie von Datenverarbeitungsanlagen abgeschickt oder empfangen werden können, in die Form, in der sie auf Telefonleitungen übertragbar sind, geschieht durch einen Modem (Kunstwort aus *Mo*dulator und *Demo*dulator), der direkt an die Telefonleitung angeschlossen ist, oder durch einen Akustikkoppler, auf den der Telefonhörer gelegt wird. Die Modem-Funktion ist dann in den Akustikkoppler integriert oder es ist zwischen Koppler und Terminal ein Modem zwischengeschaltet.

Jeder Leitung entspricht im Prinzip ein Paar von Drähten, es ist aber auch möglich, mit Hilfe verschiedener Trägerfrequenzen verschiedenen Leitungen auf demselben Drahtpaar zu realisieren oder statt eines Drahtpaares eine (Richt-) Funkstrecke und seit kurzem auch Lichtwellenleiter (Glasfaser) zu verwenden. Häufig weiß der Benutzer einer Leitung nicht, welche Verfahren die einzelnen Abschnitte „seiner Leitung" realisieren. Der große Vorteil des Telefonnetzes ist, daß durch mehr als 30 Millionen „Sprechstellen" für die Bundesrepublik ein praktisch flächendeckendes Netz vorhanden ist, mit dem von jedem Anschluß und zu jedem Anschluß eine Datenübertragung möglich ist. Außer der Nutzung dieses Netzes als Wählnetz können von der Post Leitungen auch fest angemietet werden. Diese Punkt-zu-Punkt-Verbindungen, die auch Standleitungen genannt werden, stehen dem Mieter dauernd zur alleinigen Nutzung zur Verfügung. Mit mehreren solcher Leitungen können eigene, isolierte Teilnetze aufgebaut werden, Beispiele dafür sind das Bonner Bundesbehördennetz und das Standleitungsnetz für die Bundeswehr.

Die im öffentlichen Telefonnetz oder auf entsprechenden Standleitungen möglichen Datenübertragungsraten liegen im Bereich von etwa 50 bit/s bis 4 800 bit/s. Dies ist für die unmittelbare Dateneingabe von Hand schnell genug, für die Übertragung großer Datenmengen aber recht langsam.

— Datenübertragung
im *Fernschreibnetz und Teletex*

Das Fernschreibnetz ermöglicht eine Zeichenübertragung von einem Fernschreiber zu einem anderen. Dabei werden die Zeichen zwar durch sonst unüblich kurze Folgen (5 bit) digitaler Signale dargestellt, weshalb der darstellbare Zei-

chenvorrat auch sehr gering ist, es handelt sich aber von der Technik her gesehen stets um Datenübertragung im modernen Sinne. Diese Datenübertragung erfolgt im Prinzip auf eigenen — vom Telefonnetz getrennten — aber technisch gleichartigen Wegen. Auf Funkstrecken und in Glasfaserkabeln werden aber auch Telefon- und Fernschreibleitungen parallel auf demselben Medium realisiert.

Es ist schon seit langem üblich, Fernschreibverbindungen nicht nur zum Fernschreiben, sondern auch zum Datenverkehr mit Datenverarbeitungsanlagen zu nutzen. Ein typisches Beispiel für diese Nutzung ist das System des Ausländerzentralregisters, in dem u. a. von den örtlichen Ausländerbehörden und von Grenzstellen mit Fernschreibern und über Fernschreibleitungen direkt auf das zentrale Datenverarbeitungssystem zugegriffen werden kann.

Das Fernschreibnetz ist mit nur ca. 150 000 Anschlüssen weniger geeignet, eine Verbindung zu Haushalten herzustellen, größere und mittlere Firmen und Behörden sind aber gut erreichbar.

Seit 1982 bietet die Post den neuen, komfortableren Dienst Teletex an, der die übliche 8-bit-Zeichendarstellung verwendet und darauf ausgelegt ist, komplette, im absendenden Gerät schon fertiggestellte Briefe von einer Station zu einer anderen zu übertragen. Stationen können dabei geeignete Textverarbeitungssysteme oder auch große Computer sein, so daß dieser Weg für den kommerziellen Briefverkehr sehr attraktiv ist.

Die erreichbaren Datenübertragungsraten sind für den Fernschreibbetrieb 50 bit/s und für Teletex 2 400 bit/s. Damit kann eine volle DIN-A4-Seite im Teletex-Dienst in ca. 10 Sekunden übertragen werden.

— Datenübertragung im *Datex-Netz*

Speziell für die Datenübertragungen zwischen Computern betreibt die Post das Datex-Netz (*Data-ex*change).

Dabei ist zwischen einem Leitungs- und einem Paketdienst zu unterscheiden. Im Leitungsdienst (Datex-L) wird wie bei Telefon und Fernschreiben für die Dauer einer gewählten Verbindung eine Leitung zwischen den Teilnehmern zur Verfügung gestellt. Einzelne Leitungen können auch auf Dauer gemietet werden, diese Anschlüsse werden als Hauptanschlüsse für Direktruf (HfD) bezeichnet.

Im Paketnetz (Datex-P) — einem Wählnetz — werden einzelne, sogenannte Datenpakete an das Netz abgegeben, dort von Netzknoten zu Netzknoten weitergegeben, wobei in den Knoten auch eine kurzzeitige Zwischenspeicherung erfolgt, bis der Adressat erreicht wird. Dabei wird die Route jeweils nach den aktuellen Gegebenheiten bestimmt, so daß auch mehrere Pakete einer logisch zusammenhängenden Folge über verschiedene Wege an denselben Empfänger geleitet werden können. Eine Anmietung auf Dauer ist hier nicht möglich.

Die Leitungsführung für das Datex-Netz erfolgt so wie für das Fernschreibnetz. Die Post spricht deshalb auch von verschiedenen „Diensten" auf demselben Netz. Die im Datex-Netz erreichbaren Datenübertragungsraten betragen für angewählte Verbindungen 9 600 bit/s, für HfD-Verbindungen und den Paketdienst 48 000 bit/s.

Allen diesen Verbindungen ist gemeinsam, daß sie im Prinzip abgehört werden können, wobei der technische Aufwand dazu unterschiedlich ist, näheres dazu wird unter 3.1 ausgeführt.

Eine weitere Gemeinsamkeit der modernen Verbindungen zur Datenübertragung liegt in der Standardisierung der Darstellung:

Während beim Telefongespräch die Eigenarten der Stimme, der Akzent und die Sprechweise dazu beitragen, daß die Partner sich gegenseitig erkennen, und unter Bekannten häufig persönliche oder private Bemerkungen („small talk") auch einem Sachgespräch vorausgehen und damit unbewußt zum sicheren Erkennen der Partner beitragen, ist die Datenübertragung standardisiert und folgt auch inhaltlich abstrakten Normen und Strukturvereinbarungen (sogenannten Protokollen), so daß persönliche Eigenheiten ausgefiltert werden. Auch die früher gegebene Möglichkeit, an der Morsehandschrift den bekannten Partner wiederzuerkennen, fehlt bei den modernen Datenübertragungsverfahren. Der Ersatz für diese früher beiläufig nutzbaren Sicherungen muß durch bewußt eingerichtete Sicherungsmaßnahmen geleistet werden.

Dabei können die Netze selbst als Leistungsmerkmal vorsehen, daß dem angewählten Partner vom Betreiber des Netzes (zuverlässig) mitgeteilt wird, von welchem Anschluß aus er angewählt wurde. Dies ist im Fernschreibnetz und bei den Datex-Netzen möglich, im Telefonnetz bis auf weiteres aber nicht. Hier kann nur durch (automatisierten) Rückruf eine Hilfe gegeben werden.

Die Kenntnis, woher eine Abfrage oder eine andere Nachricht kommt, reicht aber zum Erkennen, wer dafür verantwortlich ist, häufig nicht aus. Dies trägt auch in den Fällen nichts zur Sicherung bei, in denen es auf den Anschluß, von dem eine Nachricht gesendet wird, nicht ankommt und dies auch nicht für nachträgliche Kontrollen aufgezeichnet wird.

Die Maßnahmen zur Erkennung des Partners müssen deshalb unabhängig vom Netz, z. B. durch Vereinbarung von — geheimen — Erkennungszeichen, getroffen werden. Dazu genügt es in der Regel, daß der Angerufene sich über die Identität des Anrufers vergewissert. Wenn aber die Gefahr besteht, daß der Verbindungsaufbau nicht den gewünschten Empfänger, sondern einen anderen erreicht, dann müssen zusätzliche Maßnahmen getroffen werden, die verhindern, daß der nicht gewünschte Empfänger die — geheimen — Zugangsvereinbarungen erfährt (etwa dadurch, daß er sich wie der gewünschte Empfänger verhält) und danach in der Weise mißbrauchen kann, daß er sich beim unzulässigen Verbindungsaufbau wie der (falsch geleitete) Anrufer verhält.

2.3 Funktionen in Datenkommunikationssystemen

In einem komplexen Datenverarbeitungssystem (DV-System) gibt es im wesentlichen vier Klassen von Funktionen, die im Einzelfall weiter differenziert sein können. Die hierfür verwendeten Bezeichnungen

— System-Management,

— Anwendungsprogrammierung,

— Dateneingabe und

— Datenauswertung

sind nicht normiert, sie sind jedoch im Bereich der Datenverarbeitung (mit leichten Abwandlungen) gebräuchlich. Diese Funktionen werden nicht nur bei der Datenkommunikation unterschieden, sondern ebenso in jeder anderen Art der automatisierten Datenverarbeitung, auch wenn bei kleinen Datenverarbeitungsanlagen — wie z. B. Personal- oder Home-Computern — sämtliche Funktionen von einer Person wahrgenommen werden können.

In einem Datenkommunikationssystem gilt für alle Funktionen, daß sie im Prinzip über jedes Terminal, das an das DV-System angeschlossen ist, wahrgenommen werden können. In einem ausgedehnten Online-System wäre es somit möglich, daß selbst die sicherheitsrelevanten Funktionen des System-Management von beliebig weit entfernten Datenstationen ausgeübt werden können, wenn keine Restriktionen programmiert sind.

— Das *System-Management* umfaßt alle Teilfunktionen, die erforderlich sind, um überhaupt mit einem DV-System arbeiten zu können.

  Zum DV-System gehören u. a. der oder die Rechner (Computer), die Eingabegeräte wie Datensichtgeräte, Magnetbandstationen, Magnetbplattenstationen, die Ausgabegeräte (Drucker sowie dieselben, wie für die Eingabe von Daten) und die Leitungen. Die Arbeit der einzelnen Teile und ihr Zusammenwirken werden geregelt durch Programme, die *Systemsoftware* oder *Betriebssystemsoftware* genannt werden. Die Systemsoftware wird von *Systemprogrammierern* verwaltet. Sie entscheiden, wie die gekaufte oder gemietete Software auf dem Datenverarbeitungssystem eingesetzt wird (Implementation der Software), und damit auch, ob und wie die im Betriebssystem vorgesehenen Sicherungen wirken.

  Zum System-Management soll hier auch die Betreuung der *Sicherheitssoftware* und der (sicherheitsrelevanten) *Datenbanksoftware* gezählt werden, sowie die Verwaltungstätigkeiten, mit denen geregelt wird, von welchem Terminal aus welche Aktionen möglich sind und wer worauf zugreifen kann.

  Den Funktionen des System-Managements ist gemeinsam, daß ihnen für die Sicherheit im DV-System eine Schlüsselrolle zukommt. Eine umfassende Kontrolle dieser Tätigkeiten und der damit beauftragten Personen ist kaum möglich. Durch eine entsprechende Organisation der Zugangs- und Zugriffskontrolle kann aber dafür gesorgt werden, daß nur bestimmte Personen sicherheitsrelevante Eingaben vornehmen können.

— Die *Anwendungsprogrammierung* umfaßt alle Teilfunktionen, die erforderlich sind, um ein Datenverarbeitungssystem für die Erfüllung von Aufgaben der Anwender bzw. der Benutzer verwenden zu können. Der *Anwendungsprogrammierer*, der diese Programme erstellt, sollte stets nur mit einer Testversion des Programms und nur mit Testdaten, also nicht mit echten Daten arbeiten. Insbesondere sollten zur Anwendung freigegebene Programme nicht ohne erneute Freigabe geändert werden können.

— Die *Dateneingabe* umfaßt die Teilfunktionen

  — Ersteingabe einschließlich des Anlegens von Dateien,

  — Ändern und Ergänzen eingegebener Daten,

  — Löschen von Daten.

  Die Funktionen sind häufig so verteilt, daß die Massenarbeiten von einer besonderen Datenerfassungsstelle erledigt werden, aber auch einzelne Eingaben durch die Benutzer des Systems erfolgen können.

  Die Eingabedaten können auch danach unterschieden werden, ob die eingegebenen Daten vom System zu verarbeitende Inhalte darstellen, oder ob die Daten Programmbefehle sind, die Einfluß auf die Art der Verarbeitung haben.

— Bei der *Datenauswertung* können — auch wenn die Übergänge fließend sind — Massenauswertungen und Einzelfallbearbeitungen unterschieden werden. Massenauswertungen werden in der Regel durch das Aufrufen eines im System vorhandenen Programms bewirkt, gelegentlich kann der Anwender die Auswertung innerhalb bestimmter Grenzen auch selbst programmieren. Die durchzuführende Verarbeitung und das Ergebnis (der sogenannte output) sind oft umfangreich. Die Organisation der Verarbeitung und die Übergabe des Ergebnisses richten sich im wesentlichen nach den technischen Möglichkeiten, den Kosten, der Eilbedürftigkeit und den notwendigen Sicherheitsmaßnahmen.

  Die Bearbeitung eines oder weniger Einzelfälle erfolgt in der Regel so, daß für vorgegebene Such- oder Arbeitsvorgänge die erforderlichen Daten in ein Schema (z. B. eine Maske auf einem Bildschirm) eingetragen werden und das Ergebnis nach kurzer Bearbeitungszeit dem Benutzer angezeigt wird. Außer möglichen Änderungen im Datenbestand hinterlassen solche Verarbeitungen nur dann erkennbare Spuren im System, wenn dies besonders veranlaßt (programmiert) ist.

3. Risiken

Bei den Risiken sind drei Schwerpunkte zu unterscheiden:

— Auf den Übertragungswegen können Unbefugte die Daten zur Kenntnis nehmen oder den Datenverkehr beeinflussen. Dazu bedarf es neben genauen Kenntnissen, die sicherlich zunehmend verbreitet sein werden, auch technischer Einrichtungen, deren Preise tendenziell sinken. Das Vorgehen ist im allgemeinen strafbar, die Wahrscheinlichkeit, entdeckt zu werden, ist unterschiedlich und zum Teil sehr gering.

— Von denselben Geräten, mit denen der reguläre Datenverkehr abgewickelt wird, oder mit Geräten, die bei der Datenübertragung genauso arbeiten, können Unbefugte sich mit erschlichenen Berechtigungen als zugelassene Systempartner ausgeben. Die dazu erforderlichen Kenntnisse werden durch die Beschäftigung mit Computern beinahe beiläufig erworben. Der erfolgreiche Angriff ist kaum zu entdecken, weil der Unbefugte fälschlich für einen zugelassenen Partner gehalten wird. Vorausgehende mißglückte Versuche sind zwar relativ leicht zu entdecken, aber nicht strafbar.

— Wer zur Erfüllung einer bestimmten Aufgabe berechtigt ist, ein Datenverarbeitungssystem zu benutzen, kann dies verhältnismäßig leicht auch für andere Zwecke tun. Die räumliche Entfernung und die meist unterschiedlichen Aufgaben der Partner bei der Datenübertragung erschweren die Kontrolle und machen den Mißbrauch für den Angreifer dadurch ungefährlicher.

3.1 Technische Risiken der Übertragungswege

Bei den technischen Risiken sind zwei Arten von Angriffen zu unterscheiden. Relativ einfach, aber in der Wirkung begrenzt sind *passive Angriffe*, die ähnlich wie das Abhören eines Telefongesprächs die Datenübertragung nicht beeinflussen, sondern nur Kenntnisse des Inhalts vermitteln.

Es ist allgemein bekannt, daß Telefongespräche zufällig durch eine Fehlschaltung oder planmäßig durch entsprechende Einrichtungen abgehört werden können. Ein gutes Muster einer eindringlichen Warnung enthält das interne Telefonverzeichnis des Bundesministeriums des Innern:

„*Abhörgefahr*

Telefongespräche können auf vielfältige Weise abgehört werden. Insbesondere die gegnerischen Nachrichtendienste nutzen dies für ihre Zwecke.

Ein Großteil der Telefongespräche wird — ohne daß dies für die Teilnehmer erkennbar ist — auf Richtfunktstrecken der Deutschen Bundespost übertragen. Diese werden durch die gegnerischen Nachrichtendienste mit modernen elektronischen Geräten Tag für Tag gezielt abgehört. Es muß davon ausgegangen werden, daß in den computergesteuerten Empfangseinrichtungen neben anderen nachrichtendienstlich interessanten Stellen/Personen auch die Telefonnummer des Bundesministeriums des Innern (ggf. mit verschiedenen Apparat-Nr.) eingespeichert ist.

Besonders abhörgefährdet sind auch alle Gespräche über *Autotelefon*. Um sie mitzuhören, genügt ein einfacher Allwellenempfänger.

Die Abhörgefahr bei hausinternen Gesprächen und Ortsgesprächen ist zwar geringer, aber keinesfalls ausgeschlossen.

Telefongespräche, die Verschlußsachen zum Inhalt haben, sind deshalb grundsätzlich untersagt. Ausnahmen unter bestimmten Voraussetzungen regelt § 47 Abs. 2 VSA.

Zu einigen Behörden bestehen verschlüsselte Fernsprechverbindungen. Nutzen Sie diese. Nähere Auskunft erteilt die Fernschreibstelle im Haus 6."

Das für das Abhören Gesagte gilt grundsätzlich auch für die Datenübertragung, jedoch bedarf es anderer Geräte zur Aufzeichnung des Datenverkehrs. Diese sind aber leicht beschaffbar, zumal in einfachen Fällen dieselben Geräte genügen, die zur regulären Teilnahme geeignet sind. Für das systematische Auswerten des Datenverkehrs auf Funkstrecken oder in anderen Bündeln ergeben sich durch die neuen Techniken sogar Erleichterungen. Anders als beim Abhören kann man hier die Informationen einer automatischen Vorauswertung (z. B. nach Adressaten oder Stichworten) unterwerfen und danach nur das voraussichtlich Verwertbare so speichern, daß man es bei Bedarf leicht wieder verwenden kann. Die Schwierigkeiten, die verschiedenen Leistungen eines Bündels richtig zu entmischen, stellen aber wie beim Abhören erhebliche Anforderungen an die technischen Einrichtungen.

Der technische Aufwand für *aktive Angriffe* auf die Datenübertragung auf Leitungen ist im primitiven Fall des Durchschneidens eines Drahtes sehr gering. Eingriffe dieser Art oder vergleichbare Störungen, die eine Verbindung so unterbrechen, daß wenigstens einer der Partner dies erkennen kann, führen jedoch zu schnellen Gegenmaßnahmen. Gezielte Eingriffe mit kalkulierter und andauernder Wirkung sind weit schwieriger vorzunehmen. So ist es z. B. schon von der Leitungstechnik her sehr schwierig, eine abgesendete Mitteilung so auf den eigenen Anschluß umzuleiten, daß die Manipulation nicht bemerkt wird. Denn durch den Eingriff wird in der Regel entweder der Absender oder der Empfänger von der Teilnahme am allgemeinen Verkehr ausgeschlossen, was nach kurzer Zeit auffällt.

Innerhalb des Vermittlungssystems des jeweiligen Netzes — also im allgemeinen bei der Post — sind aber auch Eingriffe möglich, die gezielt nur auf einzelne Mitteilungen wirken.

Das Verfälschen des Inhalts einer Datenübertragung verlangt erheblichen Aufwand. Dazu muß die Übertragung unterbrochen und beiden Partnern auf (gewisse) Dauer vorgetäuscht werden, daß sie unmittelbar verbunden sind. Der Angreifer muß also die Übertragungen abfangen und statt dessen plausibel geänderte Daten weiterschicken. Der apparative Aufwand ist schon wegen der Zeitbedingungen bei hohen Übertragungsgeschwindigkeiten

erheblich. In einfachen und verhältnismäßig langsamen Verbindungen, z. B. beim Btx-Banking, sind aber gezielte Verfälschungen (z. B. der Ziel-Kontonummer bei Überweisungen) nicht ausgeschlossen.

Die Möglichkeiten, Angriffe der hier beschriebenen Art durchzuführen, sind in erheblichem Maß abhängig von den Medien, auf denen die Leitungen realisiert werden:

Dienen Drähte als Träger von Leitungen, so erzeugen die Datenübertragungen im Umfeld der Drähte Abstrahlungen, die zuverlässig analysiert werden können. Die Drähte müssen weder unterbrochen werden noch ergibt sich eine erkennbare Beeinträchtigung der Übertragung, der Abstand zum Draht muß aber gering sein (höchstens wenige Meter, für Datenübertragungen, die nur schwache Abstrahlung verursachen, wenige Zentimeter). Man kann Drähte aber auch unterbrechen und Geräte so zwischenschalten, daß die Leitungen scheinbar unterbrechungsfrei weiterlaufen. Damit sind dann auch aktive Eingriffe möglich. Die während der Montage auftretende Störung bleibt unerkannt, wenn in dieser Zeit keine Verbindung über die Drähte läuft.

Leitungen auf Funkstrecken können mit geeigneten Empfängern leicht und unbemerkt abgehört werden, wobei die Abstände zwischen Empfänger und Funkstrecke mehrere Kilometer betragen können. Dies ist wegen der geographischen Situation besonders für den Datenverkehr von und nach Berlin von Bedeutung.

Am sichersten werden Leitungen über Lichtwellenleiter (Glasfaserkabel) geführt. Hier gibt es keine praktisch verwertbare Abstrahlung. Das Unterbrechen und Zwischenschalten ist wegen der komplizierten Technik schwierig und die zeitweilige Störung wird voraussichtlich deswegen bemerkt, weil wegen der hohen Übertragungsdichte (mehrere Leitungen auf einem Kabel) kaum übertragungsfreie Zeiten existieren.

3.2 Erschleichen von Berechtigungen

Es ist eine wirksame Methode zum unbefugten Benutzen von Datenverarbeitungssystemen, daß Unbefugte sich wie berechtigte Benutzer verhalten. Dies ist relativ ungefährlich für den Unbefugten, wenn er die Angriffsversuche von außen, am besten von einem Ort aus, den das System nicht feststellen kann oder nicht registriert, unternimmt. Es wird dadurch erleichtert, daß er — anders als bei herkömmlicher Kommunikation — nicht beiläufig (z. B. an der Stimme) als unberechtigt erkannt wird (siehe 2.2).

Sieht man einmal davon ab, daß ein Unberechtigter sich Zugang zu einem Terminal oder einem anderen Gerät verschafft, das über eine Standleitung mit dem System verbunden ist, so sind die Ziele solcher Angriffe diejenigen Systeme, die über Wählleitungen erreichbar sind. Die dazu benötigten Terminals sind weitgehend standardisiert, die Datenübertragungsprozeduren sind weitgehend normiert, zumindest in der Regel nicht geheim. Auch die Rufnummern von anwählbaren Computern sind im allgemeinen nicht geheim, viele sind in den Teilnehmerverzeichnissen der Datendienste der Post verzeichnet, andere sind zumindest den Berechtigten bekannt und werden unter Interessierten ausgetauscht.

Nur wenig schwieriger ist es, selber Telefonnummern herauszufinden, über die Datenverarbeitungssysteme anwählbar sind. Häufig liegt die Nummer „in der Nähe" der im Telefonbuch stehenden Telefonnummer des Betreibers. Bei automatischer Durchwahl liegt die Durchwahlnummer häufig in der Nähe der Durchwahlnummer der Rechenzentrumsleitung, die z. B. leicht durch einen Anruf in der Zentrale zu ermitteln ist. Das Ausprobieren von Nummern wird dadurch erleichtert, daß die Anschlüsse von Rechnern sich in Sekundenschnelle mit einem besonderen Datenton melden, während bei Fehlversuchen das übliche Freizeichen ertönt. Das Finden eines solchen Anschlusses ist also nicht schwierig, für Interessierte ist es ein erster motivierender Erfolg.

Deshalb ist grundsätzlich davon auszugehen, daß Systeme, die anwählbar sind, auch von Unbefugten angewählt werden können.

Ist die Verbindung zu einem Datenverarbeitungssystem (schalttechnisch) hergestellt, so ist eine Reihe mehr oder minder systembezogener Formalitäten zu erledigen, bevor man an die gespeicherten Informationen gelangt. Weil früher diese Formalitäten wenig bekannt waren, vertraut man auch heute gelegentlich noch darauf, daß hier abschreckende und sicherheitswirksame Schwierigkeiten liegen. Das ist aber in der Regel nicht der Fall. Zum einen gibt es hier weitgehend bekannte Standards, deren einfache Variationen leicht herauszufinden sind, insbesondere wenn der Unbefugte Erfahrungen mit vergleichbaren Systemen hat. Auch die Fachliteratur und die Systembeschreibungen der Hersteller liefern die erforderlichen Hinweise. Deshalb ist insgesamt davon auszugehen, daß die Zahl der kenntnisreichen Angreifer steigt. Zum anderen sind moderne Systeme oft so benutzerfreundlich, daß die gewünschten Funktionen aus einer Übersicht wie aus einer Speisekarte nur noch auszuwählen sind (Menue-Technik) und der Benutzer auch sonst weitgehend über alle in einer bestimmten Dialogphase möglichen Entscheidungen bzw. Eingaben informiert wird. Zusätzlich wird gelegentlich eine allgemeine Erklärung des Systems angeboten und an schwierigen Stellen kann der Benutzer sich oft durch Aufrufen einer Help-Funktion über das systemgerechte Verhalten vom System selbst informieren lassen. Weil die Formalitäten aus diesen Gründen praktisch keine Sicherungswirkung haben, die richtige Systembenutzung also kein Beweis für die Berechtigung dazu ist, müssen andere Beweise vom System verlangt werden. Diese bestehen im wesentlichen aus dem Zwang für den Benutzer, sich dem System vorzustellen (Identifikation) und zu beweisen, daß er derjenige ist, für den er sich ausgibt (Authentifikation), näheres dazu wird unter Nr. 4.3.2 ausgeführt. Das System kann danach seine

Reaktionen daran ausrichten, welche Berechtigung der vorgestellte (und ausgewiesene) Benutzer hat.

3.3 Mißbrauch einer erteilten Berechtigung

Wer zur Benutzung eines Datenverarbeitungssystems berechtigt ist, der kann diese Berechtigung um so leichter mißbrauchen, je weniger das System dagegen gesichert ist und je geringer die Benutzungskontrollen des Systems wirken. Dabei sind unterschiedliche Arten von Gefährdungen zu beachten.

Zum einen kann es durchaus sachgerecht sein, einem Benutzer den Zugriff auf Millionen von Datensätzen zu gestatten, obwohl er für seine Aufgabe immer nur einzelne Datensätze oder Teile davon benötigt, weil man von vornherein nicht festlegen kann, welche der Informationen gerade dieser Benutzer für die von ihm jeweils zu bearbeitende Einzelaufgabe benötigt. In diesen Fällen ist es kaum zu verhindern, daß ein Berechtigter z. B. auch Daten abruft, bei denen ein Zusammenhang mit der rechtmäßigen Aufgabenerfüllung nicht besteht. Diese Art des Mißbrauchs wird besonders dadurch begünstigt, daß die Zugriffsberechtigungen in automatisierten Systemen streng formalisiert und so angelegt sein müssen, daß sie dem *möglichen* Bedarf Rechnung tragen, ohne daß bei den damit durchführbaren Einzelaktionen das Vorliegen bzw. die Richtigkeit einer Begründung geprüft werden kann. Dies ist zwar nicht erst eine Folge der Einrichtung automatisierter Fernverarbeitung, sondern eine häufig zu beobachtende Erscheinung bei formalisierten Massenverfahren für Einzelauskünfte; gerade für diese ist aber die Einrichtung automatisierter Abrufverfahren besonders sinnvoll.

Ein Mißbrauch von Berechtigungen kann aber dadurch erfolgen, daß der Berechtigte seine Zugriffsberechtigung einem Unbefugten überläßt, so daß der Unbefugte gegenüber dem System als der Berechtigte auftreten kann.

Ein weiteres Risiko liegt darin, daß es nicht ohne weiteres ausgeschlossen ist, daß ein zu bestimmten Nutzungen Berechtigter seine eingeschränkte Berechtigung eigenmächtig erweitert. So könnte z. B. jemand, der nur zum Abfragen von Daten berechtigt ist, die Daten abfragen, die der Eigensicherung des Systems dienen, um damit herauszubekommen, welche Eingaben zu tätigen sind, um Daten auch ändern zu können. Und wer nur zum Abfragen und Ändern von Einzeldaten berechtigt ist, könnte durch Ändern der Berechtigungstabellen des Systems die Möglichkeit zum Programmieren erhalten. Es erscheint selbstverständlich, daß die Sicherungsverfahren in Datenverarbeitungssystemen solche Umgehungen ausschließen. Untersuchungen des TÜV Bayern e. V. haben aber ergeben, daß auch insoweit mangelhafte Systeme eingesetzt werden.

Sehr schwierig abzuschätzen und für den Systembetreiber manchmal auch nur schwer beherrschbar ist das Risiko der Fernwartung. Fernwartung ist ein sich auch und gerade für kleine DV-Anlagen durchsetzendes Verfahren der Betreuung durch eine Wartungsfirma (meist Teil des Herstellerservice), bei dem die zur Wartung notwendigen Informationen durch Datenfernübertragung abgerufen werden und — soweit möglich — die Fehlerbehebung ebenfalls durch Datenfernübertragung (in das System hinein) vorgenommen wird. Bei der Fernwartung treffen also die ohnehin in der Wartung von DV-Systemen liegenden Risiken mit denen der Datenkommunikation zusammen. Weil es sich hier aber um ein Sonderproblem handelt, wird im Rahmen dieser Darstellung darauf nicht weiter eingegangen.

4. Sicherungsmaßnahmen

4.1 Maßnahmen zur Sicherung der Leitungen

Die Beschränkung der Datenfernübertragung auf Standleitungen oder auf „eigene" Netze aus mehreren Standleitungen macht ein System zwar sicher gegen das Anwählen von außen, es erschwert aber keineswegs die Angriffe auf die Leitungen. Im Gegenteil: weil immer dieselben Wege benutzt werden, können gezielte Angriffe sogar etwas leichter geführt werden. Insgesamt sind Standleitungsverbindungen aber als sicherer anzusehen als der Anschluß an ein Wählnetz.

Welche Art der Verbindung jeweils eingerichtet wird, hängt jedoch nicht allein von der erreichbaren Sicherheit ab, vielmehr sind die mit dem System zu erfüllenden Aufgaben und die Kostenaspekte meist ausschlaggebend für die Entscheidung Stand- oder Wählleitung.

Auch die Erkenntnis, daß eine Leitungsführung über Funkstrecken das Abhörrisiko erhöht und Leitungen in Glasfaserkabeln am sichersten sind, kann die Auswahlentscheidung nur selten beeinflussen. Denn dazu müßten nicht nur auf der fraglichen Strecke Alternativen überhaupt verfügbar sein, sondern man müßte auch auf die Art der Leitungsführung durch die Post Einfluß nehmen können. Und für den vom Systembetreiber zu verantwortenden Teil der Übertragungsstrecke (zwischen dem Abschluß des posteigenen Netzes und den Datenverarbeitungsanlagen) kommen schon aus Kostengründen praktisch nur drahtgeführte Leitungen in Frage. Hier ist es allerdings möglich, durch Kontrolle der Leitungsführung und der eigenen Schalteinrichtungen das Abhörrisiko zu vermindern. Trotzdem bleibt die Angreifbarkeit der Leitungen insgesamt ein Risiko für die Datenfernübertragung.

Es gibt allerdings die Möglichkeit, den Erfolg eines Angriffs auf die Leitungen so zu reduzieren, daß nur noch die Störung als Risiko bleibt. Dies ist durch Verschlüsselung mit kryptographischen Verfahren erreichbar.

Exkurs: Datenverschlüsselung

Es gibt einige Verfahren, bei denen mit bekannten Algorithmen (= mathematische Formeln und Vor-

schriften über ihre Anwendung) und geheimzuhaltenden Schlüsseln (= Parametern, die in die Formeln eingesetzt werden) digitale Zeichenfolgen so verschlüsselt werden können, daß das Ergebnis (= Kryptogramm) ohne Kenntnis des Schlüssels praktisch nicht in den Klartext zurückverwandelt werden kann. Dabei bedeutet „praktisch nicht", daß trotz erheblicher Bemühungen von Experten zur Zeit kein Dechiffrier-Verfahren bekannt ist, das mit Aussicht auf Erfolg angewendet werden kann. Natürlich ist es immer möglich, alle denkbaren Schlüssel zu probieren. Die in modernen Verfahren vorgesehenen Schlüssellängen und damit die Zahl der denkbaren Schlüssel ist aber so groß, daß dies auch mit schnellsten Computern im Durchschnitt mehrere Jahrzehnte bis zum Erfolg braucht. Zufallstreffer schon beim ersten Probelauf sind natürlich möglich, aber etwa so wahrscheinlich wie das Ergebnis, daß jemand bei drei aufeinander folgenden Lottoziehungen jeweils 6 Richtige hat. Die Unwahrscheinlichkeit ließe sich bei Bedarf durch längere Schlüssel auch noch steigern.

Auf der Basis kryptographischer Verfahren ließen sich nicht nur der Verkehr auf Leitungen und alle anderen Methoden des Datentransports sichern, es könnten auch bisher offene Probleme der Beweisbarkeit, bezogen auf den Inhalt erhaltener Nachrichten einschließlich Zeit und Absender, technisch sicher gelöst werden (s. dazu Rihaczek, Karl: Datenverschlüsselung in Kommunikationssystemen, Vieweg-Verlag, 1984).

Daß trotz dieser Vorteile die Datenverschlüsselung (außerhalb des militärischen Bereichs) nur zögernd Anwendung findet, liegt nur zum Teil an den noch hohen Kosten, die zur Zeit einige tausend Mark je Gerät betragen dürften, bei Masseneinsatz aber in der Größenordnung hundert Mark liegen könnten. Die entscheidenden Hindernisse, die den breiten Einsatz von Verschlüsselung erschweren, sind

a) die fehlende Normung

Es gibt noch keine deutsche oder internationale Norm über einen Algorithmus und die Modalitäten der Anwendung. Da zur Datenübertragung aber beide Partner sich genau über die Methode der Verschlüsselung einig sein müssen, sind für jeden Anwendungsfall diese Vereinbarungen jeweils fallweise zu treffen.

b) die fehlende Organisation der Schlüsselverteilung

Für jeden Datenaustausch zwischen zwei Partnern muß die Verschlüsselung so organisiert werden, daß diese Partner verschlüsseln und entschlüsseln können, sonst aber niemand mitlesen kann. Dazu bedarf es einer Vereinbarung, die nur für diese beiden Partner wirkt, und das auch in Netzen mit vielen, zum Teil Tausenden von Partnern. Die — abgesehen von den Kosten — denkbare Lösung, daß für jedes Partnerpaar eine besondere Schlüsselvereinbarung getroffen wird, ist schon wegen der Unübersichtlichkeit der Beziehungen unsicher. Verfahren mit halboffenen Schlüsseln, bei denen jeder Teilnehmer einen Schlüssel für das Verschlüsseln veröffentlichen kann und mit einem anderen dazu passenden Schlüssel, den nur er kennt, die ihm verschlüsselt gesendeten Mitteilungen entschlüsseln kann, scheinen zwar mathematisch sicher zu sein. Es gibt aber erhebliche — wenn auch theoretisch gesehen unbegründete — Vorbehalte, daß bei vielen Teilnehmern einige der Schlüssel zufällig erraten oder bei der Suche nach geeigneten Paaren aus offenem und geheimem Schlüssel gefunden werden könnten. Auch müßte ein solches Verfahren genormt und zumindest die Schlüsselveröffentlichung organisiert werden, bevor es allgemein anwendbar ist.

Die gedanklich einfachste Lösung ist die Errichtung einer Schlüsselverteilzentrale. Diese müßte mit jedem, der am Krypto-Verkehr teilnehmen möchte, einen Hauptschlüssel vereinbaren. Um dann eine logisch und zeitlich zusammenhängende Folge von Datenübertragungen (Session) verschlüsselt mit einem Partner abwickeln zu können, beauftragt der „Anrufende" zunächst die Schlüsselzentrale, ihm und seinem gewünschten Partner für diese Session einen Sessionsschlüssel zu übersenden. Zur Verschlüsselung dieses Schlüssels benutzt die Schlüsselzentrale den mit dem jeweiligen Partner vereinbarten Hauptschlüssel.

Wird diese Art der Schlüsselzuteilung in den Aufbau einer Wählverbindung integriert, so liegt der Zeitbedarf dafür bei wenigen Sekunden. Deshalb wäre es sachgerecht, die Schlüsselzuteilung als besonderen Dienst der Post zu betreiben. Damit wären sowohl die Leistungsfähigkeit als auch die Vertrauenswürdigkeit gegeben, die eine Schlüsselverteilzentrale braucht. Beinahe als Abfallprodukt könnte die Post auch Beweisfunktionen für den Datenverkehr (Einschreiben, Postzustellurkunde) anbieten. Auch die Probleme des internationalen Krypto-Verkehrs erscheinen auf der Basis nationaler Zentralen mit Zusammenarbeitsrichtlinien lösbar. Die Post läßt aber zur Zeit wenig Interesse an einer solchen Dienstleistung erkennen.

Wegen dieser ungelösten Probleme der Verschlüsselung, die weder im mathematisch-theoretischen noch im technisch-konstruktiven sondern überwiegend im administrativen bzw. organisatorischen Bereich liegen, wird die Verschlüsselung (außer für militärische Zwecke) bisher nur vereinzelt (für Punkt-zu-Punkt-Verbindungen) eingesetzt, z. B. für den Datenaustausch zwischen größeren Teilen von Unternehmen und seit März 1984 auch für die Übertragung von Versichertendaten von der Bundesversicherungsanstalt für Angestellte (in Berlin) zu ihren Auskunfts- und Beratungsstellen in verschiedenen größeren Städten.

4.2 Sicherung des Systemzugangs

Eine erste Schranke gegen die unberechtigte Benutzung von Datenverarbeitungssystemen kann dadurch errichtet werden, daß Unberechtigten schon der Zugang zum System verwehrt wird. Dazu ist es erforderlich, ihnen den Zugang zu den Geräten zu

verwehren, von denen aus der Datenverkehr betrieben werden kann. Dies ist möglich durch das Einschließen der Geräte oder Verschließen der Räume, in denen diese Geräte stehen, aber auch durch technische Einrichtungen an den Geräten selbst (Schlüsselschalter zum Einschalten oder für besondere Funktionen). Diese Maßnahmen können sehr wirksam gestaltet werden, sie sind aber nur dann mit Erfolg einsetzbar, wenn oder soweit bestimmte Funktionen an bestimmte Geräte gebunden werden können. Denn wenn ein System für seine planmäßige Benutzung über Wählanschlüsse erreichbar sein muß, ist der Zugang auf der Ebene der Geräte so nicht einschränkbar, und deshalb ist der Zugang zum System auch Unberechtigten möglich. Der darin liegenden Gefährdung muß auf andere Weise begegnet werden.

4.3 Sicherung durch Berechtigungsprüfung

Viele, die zu einem Datenverarbeitungssystem mit Hilfe der Datenfernübertragung Zugang erlangen können, haben überhaupt keine Berechtigung zur Benutzung dieses Systems, und oft sind auch die Arten der vergebenen Berechtigungen unterschiedlich. Bevor das System also eine Anfrage beantwortet oder eine Anweisung ausführt, ist zu prüfen, ob der jeweilige Partner dazu auch berechtigt ist. Nur in Extremfällen offener Systemnetze sind bestimmte Funktionen jedem erlaubt. So darf z. B. ein automatisches Auskunftssystem für Telefonnummern (ein entsprechender Großversuch mit speziellen Terminals, die zugleich aber auch zur Kommunikation mit anderen Systemen geeignet sind, wird zur Zeit in Frankreich durchgeführt) wie ein Telefonbuch von jedem ohne Berechtigungsprüfung benutzt werden, weil jeder dazu als berechtigt gilt. Ähnliches kann für wissenschaftliche und vergleichbare Informationssysteme gelten, möglicherweise mit dem Unterschied, daß dafür Benutzungsvergütungen zu entrichten sind — ein Problem auf das hier nicht weiter eingegangen werden soll. Abgesehen von solchen Systemen, die zur Veröffentlichung dienen, ist aber eine Prüfung der Berechtigung möglichst bald nach der Kontaktaufnahme geboten.

4.3.1 Zuteilung von Berechtigungen

Für die Zuteilung und Verwaltung von Berechtigungen an mehrere Personen gibt es prinzipiell zwei Ansätze: Entweder weist ein Benutzer direkt nach, daß er zur Ausführung einer Funktion berechtigt ist, dann erbringen alle zur gleichen Funktion Berechtigten denselben Nachweis, ohne daß das System erkennt, mit wem es verbunden ist. Oder die Benutzer müssen sich einzeln dem System vorstellen (und auch nachweisen, daß die „Vorstellung" richtig war) und das System prüft dann anhand von Berechtigungstabellen, wozu der jeweilige Benutzer berechtigt ist.

In der tatsächlichen Wirkung ist das erste Verfahren dem zweiten weit unterlegen. Denn in der Praxis besteht der Nachweis im Nennen eines Erkennungs- oder Codewortes (im weiteren in Anlehnung an den englischen Ausdruck password „Paßwort" genannt), das umso gefahrloser an Dritte weitergegeben werden kann, je mehr Personen dieses Paßwort kennen und damit als Verdächtige für die Weitergabe in Frage kommen. Auch andere, im Prinzip erlaubte Aktionen lassen sich dem einzelnen Benutzer nicht zuordnen, so daß einer sinnvollen Nachkontrolle die sachdienlichen Anhaltspunkte fehlen. Trotzdem werden solche organisatorisch sehr einfachen Verfahren gelegentlich angewandt, sie sind aber nur für Berechtigungen angemessen, bei denen schon wegen der geringen Bedeutung ein Mißbrauch nicht zu erwarten ist. Sonst ist es stets geboten, die Berechtigungen und besonders die Nutzungen jeweils mit einzelnen Personen zu verbinden. Es sollte auch keine Dienststellen-Paßwörter geben, die in einer Dienststelle wahlweise jeweils von dem benutzt werden, der gerade z. B. mit einem Auskunftssystem arbeitet, weil sonst die persönliche Verantwortung für die Systemnutzung nicht mehr nachvollziehbar ist.

4.3.2 Identifikation und Authentifikation

Die (berechtigten und) einem DV-System bekannten Benutzer haben für die Arbeit mit dem System eine Benutzerkennung (englisch: user-identification, abgekürzt user-id), die der allgemeinen Verwaltung, z. B. der Abrechnung und dem Adressieren von Mitteilungen dient. Der Benutzer identifiziert sich dem System gegenüber durch Angabe dieser Kennung, die schon wegen ihrer allgemeinen Verwendung nicht geheim bleiben kann und deshalb nur wenig zur Sicherheit beiträgt.

Damit das System „sicher" sein kann, daß der Teilnehmer am Dialog auch wirklich derjenige Benutzer ist, für den er sich ausgibt, also zur Authentifikation, muß eine Prüfung vorgesehen sein, die jeweils nur dieser Benutzer bestehen kann, oder bei der es jedenfalls diesem Benutzer zuzurechnen (vorhaltbar) ist, daß ein anderer „die Prüfung bestanden hat".

Die denkbaren Möglichkeiten für eine sichere Authentifikation sind sehr vielfältig:

— Gegenstände, wie z. B. Schlüssel oder Magnetkarten, lassen sehr viele Variationen zu, sind aber eine Inhaber-Authentifikation, bei der ein erhebliches Risiko im Verlieren und auch ein gewisses Risiko im Nachmachen liegt. Als Berechtigungsnachweis in Datenübertragungssystemen hat sie auch deshalb kaum Bedeutung erlangt, weil zum Erkennen der Gegenstände ein spürbarer technischer Aufwand erforderlich ist.

— Das Stimmprofil des Berechtigten, seine Fingerabdrücke, Handmaße oder ähnliches wären zur Authentifikation sehr gut geeignet, wenn mit vertretbarem Aufwand sichergestellt werden könnte, daß der Berechtigte stets als berechtigt anerkannt und jeder andere abgewiesen wird. Soweit bekannt, gibt es bisher keine Verfahren, um mit vertretbaren Mitteln eine brauchbare Authentifikation zu erreichen.

— Paßwörter, die zwischen dem Berechtigten und dem System vereinbart sind und die geheimzuhalten und vom Benutzer nur bei der Berechtigungsprüfung einzugeben sind, werden in der Datenverarbeitung in großem Umfang zur Authentifikation eingesetzt.

  Es mag verwundern, daß die „gute alte Parole" auch in den modernsten Kommunikationsverfahren noch nicht ausgedient hat. Und wenn man weiter bedenkt, daß Paßwörter zufällig, durch gezieltes Probieren oder durch Abhören auch Unberechtigten bekannt werden können, sind Zweifel an der Wirksamkeit eines darauf aufbauenden Schutzes auch angebracht. Durch eine die Sicherheit unterstützende Organisation läßt sich aber ein hohes Maß an Sicherheit erreichen. Wirksame unterstützende Maßnahmen habe ich in meinem Sechsten Tätigkeitsbericht (Nr. 25, S. 54 ff.) beschrieben.

— Parameter, die zugleich in kryptographischen Verfahren als Schlüssel eingesetzt werden, wirken im Prinzip wie Paßwörter, sie sichern zugleich aber auch die Datenübertragung. Obwohl die allgemeinen Hindernisse für den Einsatz der kryptographischen Verfahren einer breiten Anwendung im Wege stehen (s. o. Nr. 4.1), gibt es besonders im Zusammenhang mit Mikrochips, die in handlichen Karten untergebracht werden können (Chipkarten), aussichtsreiche Entwicklungen, die in einigen Jahren zu wirksamen Sicherungsverfahren führen können.

Alle heute eingesetzten Verfahren der Authentifikation sind in ihrer Wirkung wesentlich davon abhängig, daß der Berechtigte die Authentifikationsmittel nicht ausleiht oder weitergibt und sich so verhält, daß Unberechtigte nicht seine Berechtigung erschleichen können. Es ist deshalb wichtig, daß der Betreiber eines Systems alle berechtigten Benutzer auf das hinweist, was sie selbst zur Sicherheit im Rahmen des jeweiligen Sicherungskonzepts beitragen können.

Eine beliebte und leider gelegentlich auch erfolgreiche Methode zum Aufspüren eines Paßwortes ist das telefonische Erfragen vom Berechtigten unter dem Vorwand, man sei gerade mit der Suche nach einem Systemfehler oder mit seiner Behebung beschäftigt und brauche dazu dringend das Benutzerpaßwort. Um dieses Vorgehen, das auch als social engineering bezeichnet wird, wirkungslos zu machen, müssen alle Inhaber von Paßwörtern darüber informiert sein, ob überhaupt und wenn ja, unter welchen Umständen und auf welchem Weg sie ihr Paßwort im Notfall dem Betreiber des Systems offenbaren müssen. Dieser Weg sollte auf jeden Fall ein anderer sein als der Anruf eines Unbekannten.

4.4 Kontrolle der Systemnutzung

Weil Datenverarbeitungssysteme und insbesondere solche mit umfangreichen Datenkommunikationsbeziehungen nicht so sicher gestaltet werden können, daß ein Mißbrauch allein durch vorbeugende Maßnahmen völlig ausgeschlossen ist, muß die tatsächliche Nutzung der Systeme ständig auf Anhaltspunkte für Mißbräuche kontrolliert werden. Dabei muß sich die Kontrolle sowohl darauf richten, ob Unberechtigte, möglicherweise zu Lasten eines Berechtigten, das System nutzen oder zu nutzen versuchen, als auch darauf, ob die Berechtigten stets im Rahmen ihrer Berechtigung arbeiten und nicht ihre Berechtigung mißbrauchen.

4.4.1 Kontrollen mit dem Benutzer

Jeder Benutzer hat ein Interesse daran, daß seine Berechtigung nicht (zumindest nicht gegen seinen Willen) mißbraucht wird. Abgesehen davon, daß man ihn dazu anhält, alle Vorbeugungsmaßnahmen zu unterstützen, ist es deshalb sinnvoll, ihn regelmäßig über die unter seiner Berechtigung durchgeführten Aktivitäten zu unterrichten. Aus dem Vergleich dieser Berichte mit seiner Erinnerung oder seinen Aufzeichnungen über seine Systemnutzung kann er dann feststellen, ob in der Zwischenzeit seine Berechtigung von Dritten genutzt wurde. In der Regel genügt es dabei, ihn auf das Ende seiner letzten Benutzung hinzuweisen. Damit diese Maßnahme nicht an Wirkung verliert, ist vom System her sicherzustellen, daß keine Berechtigung zeitweilig doppelt genutzt wird, was auch aus anderen Gründen zu den regelmäßigen Überwachungsmaßnahmen gehören sollte.

Es ist darüber hinaus zweckmäßig, dem Benutzer bei jeder (erfolgreichen) Anschaltung, außer der unmittelbar vorangegangenen Anschaltung auch die seit Ende dieser letzten Nutzung erfolgten Zugangs-Fehlversuche anzuzeigen, die zu seiner Benutzernummer unternommen wurden. Damit erfährt er von jedem Versuch, unter seiner Identität mit dem System zu arbeiten, und kann damit auch bei allen mißglückten Zugangsversuchen beurteilen, ob es sich um seinen eigenen Irrtum bei der Authentifikation oder um einen Versuch handelt, seine Berechtigung zu erschleichen. Sind solche Versuche erkannt, so können daraufhin sowohl Sicherungsmaßnahmen wie z. B. Paßwortwechsel als auch Maßnahmen zum Feststellen des potentiellen Angreifers bei Wiederholung getroffen werden. Das Feststellen des potentiellen Angreifers setzt allerdings voraus, daß das (angerufene) System ermitteln kann, von welchem Anschluß aus der Angreifer tätig ist. Dies ist beim heutigen Stand der Technik von Wählverbindungen zum Teil schwierig, aber auch nicht unmöglich. Insbesondere wiederholte Versuche vom selben Anschluß aus werden dadurch sehr riskant — was die Entdeckung angeht. Strafbar sind solche Versuche aber nicht.

4.4.2 Kontrolle der Benutzer

Wesentlich leichter als Außenstehende sind die Berechtigten in der Lage, ein Datenverarbeitungssystem mißbräuchlich zu benutzen. Dies kann z. B. dadurch eingeleitet werden, daß ein Benutzer versucht, die ihm erteilte Berechtigung zu überziehen, d. h. Zugang zu solchen Datenbeständen oder Funktionen sucht, die ihm planmäßig nicht zur Verfügung stehen. Versuche dieser Art sollten nicht nur

abgewiesen sondern auch aufgezeichnet und verfolgt werden. Denn wer berechtigt ist, mit einem System zu arbeiten, kennt es im allgemeinen so gut, daß seine Angriffe als gefährlich anzusehen sind.

Während der Versuch, eine zugeteilte Berechtigung der Art nach auszudehnen, verhältnismäßig leicht bemerkt wird, ist es weit schwieriger, die Zweckentfremdung einer zugeteilten Berechtigung zu entdecken. Denn hier liegt der Mißbrauch in der formal richtigen Nutzung einer zugeteilten Berechtigung für andere Zwecke als diejenigen, für die diese Berechtigung gedacht war. Dazu kann der Benutzer in einer Folge in jeder Hinsicht zulässiger Aktionen, z. B. Datenabfragen über Personen, auch Fälle miterledigen lassen, die seiner Berechtigung nach zulässig, wegen des Fehlens eines die Einzelaktion rechtfertigenden Grundes (z. B. bei dienstlicher Berechtigung kein Zusammenhang mit einer dienstlichen Aufgabe) aber mißbräuchlich sind.

Um derartige Mißbräuche wenigstens nachträglich erkennen zu können — und durch die Gefahr der nachträglichen Entdeckung Benutzer vom möglichen Mißbrauch abzuhalten — müssen nachträgliche Kontrollen von Einzelfällen durchgeführt werden. Denn anders als z. B. bei der Beantwortung schriftlicher Anfragen durch Sachbearbeiter fallen in automatisierten Verfahren grundsätzlich niemandem irgend welche Besonderheiten auf, weil kein Sachbearbeiter mehr an der Bearbeitung beteiligt ist.

Bei der Durchführung nachträglicher Kontrollen gibt es im wesentlichen drei Probleme:

— Weil sich die Kontrolle auf Einzelfälle beziehen muß, ist es notwendig, daß vom System Aufzeichnungen über Einzelfälle erstellt werden, die dem jeweiligen Verursacher (Benutzer) zurechenbar und vorhaltbar sind. Der Benutzer muß — um im Kontrollfall die Zulässigkeit der Einzelaktion belegen zu können — Aufzeichnungen über jede seiner Systemaktivitäten führen oder auf andere Weise eine wenigstens plausible Begründung bringen können. Dies erfordert sowohl beim System als auch beim Benutzer entsprechenden Aufwand, dem oft außer der Kontrollierbarkeit kein weiterer Nutzen gegenübersteht. Auch aus Gründen des Datenschutzes kann z. B. bei Abfragen aus Dateien mit personenbezogenen Daten eine ausführliche Protokollierung unerwünscht sein. Auf der Seite des Systems könnte man zwar die Aufzeichnungen auf die Fälle beschränken, die wirklich auch Gegenstand einer Nachprüfung sein sollen, auf der Seite des Benutzers ist eine solche Einschränkung aber nicht sachgerecht. Kann man keine ohnehin vom Benutzer zu führenden Unterlagen heranziehen, so müssen die Kontrollen so bald nach den Aktionen folgen, daß der Benutzer sich an die rechtfertigenden Gründe noch erinnern können müßte, was nur schwer zu realisieren ist.

— Schon aus Aufwandsgründen können Kontrollen nur stichprobenweise durchgeführt werden. Die Häufigkeit und der Umfang der Stichproben müssen sich dabei nach dem für die Einzelkontrolle erforderlichen Aufwand und nach der Bedeutung der zu verhindernden Mißbräuche richten. Daneben können detaillierte Betriebsstatistiken Anhaltspunkte für Kontrollbedarf liefern. Solche Anhaltspunkte ergeben sich aus einer Statistik allerdings erst dann, wenn der Mißbrauch dem Umfang nach auffällig gewesen ist.

— Die Durchführung von Kontrollen wird besonders erschwert, wenn der Betreiber des Systems kein Kontrollrecht bei den Benutzern besitzt oder es wegen der oft großen Entfernungen selbst nicht geltend machen kann. Und auch bei der Verarbeitung personenbezogener Daten, die aufgrund gesetzlicher Vorschriften von Datenschutzbeauftragten zu kontrollieren ist, kommt es dann nicht zur Kontrolle der Benutzer großer Systeme, wenn der Benutzer bezüglich der im System verarbeiteten Daten selbst keine Datei führt. Deshalb ist es geboten, z. B. für die notwendigen Kontrollen von Online-Abrufverfahren durch Vereinbarungen oder durch gesetzliche Regelungen die Kontrolle der tatsächlich erfolgten Nutzung zu sichern.

Wegen der bestehenden Schwierigkeiten werden zur Zeit wirksame Kontrollen der Systembenutzung oft noch unterlassen. Daß aber nachträgliche Kontrollen durchaus angebracht sein können, zeigt — auf einem anderen Gebiet — das Angebot einer Kopiergerätefirma: Durch einen Zufallsgenerator im Kopiergerät werden Stichproben ausgewählt. In den damit bestimmten Fällen wird eine weitere Kopie gefertigt und in einem Tresor abgelegt, nur damit ein besonders Beauftragter die Zulässigkeit dieses Kopiervorgangs nachträglich überprüfen kann.

4.5 Begrenzung des Risikos

Mit entsprechend hohem Aufwand läßt sich theoretisch jedes Maß an Sicherheit erreichen, tatsächlich existierende Datenkommunikationssysteme werden aber nie absolut sicher sein. Neben den Maßnahmen zur Sicherung ist es deshalb auch wichtig, den durch Mißbrauch erreichbaren Nutzen für den Angreifer und den Schaden für das System bzw. für die Interessen, die vom Systembetreiber zu schützen sind, so weit wie möglich zu begrenzen.

Ein wichtiges Mittel dazu ist, zu verhindern, daß jede Funktion in einem Datenkommunikationssystem über jeden Kommunikationsweg aufgerufen werden kann. Es muß die Regel gelten, daß die Veranlassung einer Aktion um so kontrollierter geschehen muß, je mehr Schaden im Fall des Mißbrauchs dadurch angerichtet werden kann.

— Die zum System-Management gehörenden Funktionen einschließlich der Sicherheitsverwaltung sollten stets an bestimmte, in überwachten Räumen aufgestellte Eingabegeräte gebunden sein, damit es z. B. nicht möglich ist, durch Zugriff von außen Berechtigungstabellen zu lesen oder gar zu ändern.

— Für die Anwendungsprogrammierung gilt — zumindest soweit die Programme für das Gesamt-

system von Bedeutung sind und nicht nur Teile (z. B. einzelne Auswertungen) betreffen — dasselbe wie für das System-Management. Auf jeden Fall sollte sichergestellt werden, daß die Übernahme eines fertiggestellten Programms und aller Programmänderungen in die Bibliothek der auf Echt-Daten anzuwendenden Programme nur von bestimmten, kontrollierten Eingabegeräten veranlaßt werden kann.

Das Erstellen von Programmen, das Übersetzen von Programmen in Maschinensprache und auch das Testen mit Testdaten können von beliebigen Geräten und auch über Wählleitungen abgewickelt werden, wenn ein Übergreifen auf andere Funktionen zuverlässig verhindert wird. Dies ist besonders beim Testen — dabei laufen „ungeprüfte" Programme ab, deren Wirkungen nicht über den Testbereich hinausgreifen dürfen — nicht selbstverständlich, mit modernen Betriebssystemen aber erreichbar.

— Die Dateneingabe mit ihren Teilfunktionen Ersteingabe, Ergänzen, Ändern und Löschen kann oft nicht an von vornherein festgelegte Arbeitsplätze gebunden werden. Es kann sogar zu den notwendigen Leistungen des Systems gehören, die Dateneingabe auch über Wählleitungen zu ermöglichen. Dies gilt jedoch praktisch nie für alle Datenarten und Funktionen in gleicher Weise. Deshalb sollten auch diese Funktionen nur so frei wie notwendig sein, um die Möglichkeiten des Mißbrauchs so eng zu begrenzen, wie es mit den Systemleistungen vereinbar ist. Außerdem dient es der Sicherheit, Änderungen im Datenbestand so zu protokollieren, daß nach beabsichtigten oder unbeabsichtigten Falscheingaben bzw. Löschungen der alte, richtige Datenbestand dann rekonstruiert werden kann, wenn der Fehler bemerkt wurde. Dies ist besonders für Eingaben wichtig, die z. B. im Rahmen der Aktualisierung der Datenbasis von Bedeutung sind.

— Die Datenabfrage und andere Formen der reinen Systemnutzung können zwar an Berechtigungen, aber oft nicht an bestimmte, vom Betreiber des Systems kontrollierte Geräte und Zugangswege gebunden werden, denn es ist ja gerade der Zweck eines Datenkommunikationssystems, diesen Zugriff möglichst komfortabel einer Vielzahl von Berechtigten anzubieten. Hier kann nur der Umfang des nicht völlig zu verhindernden Mißbrauchs begrenzt werden. Zu diesen Maßnahmen gehören z. B. Summenbegrenzungen für die Verfügung über Geld sowohl für die Einzeltransaktion als auch in der Form des Limits pro Zeiteinheit. Analog dazu kann auch sonst das Maß der Nutzung bestimmt werden, etwa dadurch, daß nur eine festgesetzte, aller Voraussicht nach ausreichende Anzahl von bestimmten Aktionen pro Zeiteinheit zugelassen wird, oder daß Massenabfragen nicht durch Datenfernübertragung, sondern durch Versenden von Ausdrucken beantwortet werden, die vor der Absendung eine besondere Kontrolle durchlaufen.

Einige dieser Maßnahmen schränken nicht nur die Flexibilität ein, sondern sie verlangen auch einen gewissen Programmier- und Organisationsaufwand. Wie ich durch meine Kontrolltätigkeit festgestellt habe, werden sie deshalb manchmal auch dann unterlassen, wenn die Einbuße an Flexibilität keine oder nur geringe Erschwerungen zur Folge hätte.

5. Beurteilung der Lage

In den USA hat es schon einige spektakuläre Angriffe auf Systeme mit umfangreicher Datenfernverarbeitung gegeben, die aus spielerisch-sportlichen Motiven von sogenannten Hackern geführt wurden. Diese haben zu Beunruhigung und auch zu Vertrauensschäden geführt, der unmittelbare Schaden war aber jeweils im Verhältnis zur Größe der Systeme gering. Ziel der Angriffe waren weniger die Datenbanken der Verwaltung als vielmehr solche Informationssysteme, die zumindestens der Fachöffentlichkeit zur relativ freien Verfügung standen und in denen zum Teil auch Informationen für einen kleineren Personenkreis vorbehalten waren. Der unerlaubte Zugang wurde in den bekannt gewordenen Fällen stets über das Telefonwählnetz erreicht. Dieses neue Spiel mit dem Telefon ist eine Variante des in den USA beliebten Sports, innerhalb des von mehreren Gesellschaften betriebenen Telefonnetzes unter Ausnutzung von Schwachstellen gebührenfrei oder zum Ortstarif Ferngespräche zu führen.

In der Bundesrepublik Deutschland waren die Voraussetzungen für Hacker bisher weit schlechter. Die Monopolstellung der Post und die vergleichsweise sichere Bauweise des Telefonnetzes haben den Mißbrauch mit dem Ziel der Gebührenersparnis so erschwert, daß eine entsprechende Szene sich nicht gebildet hat.

Außerdem gab es hier erst sehr viel später über das öffentliche Telefon-Wählnetz erreichbare Computer, die als Ziel eines Angriffs interessant sind, und auch die Zahl der verfügbaren Geräte hat erst in letzter Zeit — auch wegen der Preissenkungen — stark zugenommen. Diese Verzögerung führte dazu, daß erst in diesem Jahr in nennenswertem Umfang über erfolgreiche Hacker-Angriffe berichtet wurde. Die Aktionen waren stets auf Publizität ausgerichtet und trugen deshalb im Ergebnis eher zur Verbesserung der Sicherungsmaßnahmen bei. Doch kann nicht ausgeschlossen werden, daß es unentdeckte oder nicht allgemein zugänglich beschriebene Fälle des Mißbrauchs von Datenkommunikationssystemen gegeben hat und noch gibt, in denen erkannte Schwachstellen nicht aufgedeckt, sondern ausgenutzt werden.

Über das Ausmaß, in dem Sicherheitsmaßnahmen von den jeweils verantwortlichen Betreibern und von den Benutzern getroffen worden sind, liegen mir keine auch nur annähernd repräsentative Erkenntnisse vor. Soweit ich im Rahmen meiner Kontrolltätigkeit — also beschränkt auf öffentliche Stellen des Bundes — große Datenkommunikationssy-

steme geprüft habe, ist das Bild, wie die folgenden Beispiele zeigen, uneinheitlich:

— Im Geschäftsbereich des Bundesministers der Verteidigung werden zwei große Informations- und Kommunikationssysteme mit personenbezogenen Daten betrieben, nämlich das *Per*sonal*f*ührungs- und *I*nformationssystem für *S*oldaten (PERFIS) und das *W*ehr*e*rsatz*w*esen-*I*nformations*s*ystem (WEWIS). Beide Systeme sind von außen kaum angreifbar, weil die Kommunikation ausschließlich auf Standleitungen — also außerhalb des öffentlichen Netzes — geführt wird. Die inneren Kontrollen bei PERFIS sind sorgfältig durchdacht und angemessen. Bei WEWIS gab es zunächst Schwachstellen im Bereich der Paßwortorganisation, der Abgrenzung von Zugriffsberechtigungen und der Kontrolle der Benutzeraktivitäten. Ohne daß Anhaltspunkte für tatsächliche Mißbräuche vorlagen, sind die Schwachstellen im wesentlichen beseitigt worden, an der Lösung der noch offenen Probleme wird zur Zeit gearbeitet.

— Das erst in den letzten Jahren konzipierte und zur Zeit noch im Aufbau befindliche offene Kommunikationssystem Bildschirmtext enthält noch mehrere Schwachstellen, die nach dem Kenntnisstand über mögliche Sicherungsmaßnahmen vermeidbar gewesen wären. Dies gilt sowohl für die Information der Benutzer über sicherheitsbewußtes Verhalten und die Organisation des Paßwortverfahrens als auch für fehlende Begrenzungen des Risikos. Nicht zuletzt unter dem Eindruck meiner Hinweise auf diese Mängel bemüht sich die Post als Betreiber des Systems, durch Nachbesserungen die Sicherheit zu erreichen, die für den erhofften Massenbetrieb mit mehreren Millionen Teilnehmern geboten ist.

— Ein älteres System hatte erhebliche Schwachstellen im Bereich der Zugriffssicherung und praktisch keine Kontrolle der Benutzer. Verbesserungen waren nur begrenzt möglich, so daß erst die bevorstehende Umstellung auf ein grundlegend neues Verfahren die gebotene Sicherheit bieten wird.

Diese Beispiele lassen erkennen, daß Sicherheit und Kontrollierbarkeit in großen Datenkommunikationssystemen nicht immer zu den selbstverständlich zu erfüllenden Anforderungen gerechnet, sondern zum Teil als lästige Auflagen empfunden und von den Systembetreibern nur notgedrungen akzeptiert werden. Unter dem Druck der Berichte über erfolgreiche Angriffe und im Zuge meiner Beratungs- und Kontrolltätigkeit steigt die Bereitschaft, Sicherheitsmaßnahmen zu ergreifen. Entscheidend ist indes, daß diese Maßnahmen auch so rechtzeitig und so wirksam getroffen werden, daß die voraussichtlich zunehmenden Mißbrauchsversuche nicht auch zunehmende Erfolge haben werden.

Anlage 2 (zu Nr. 22.2)

Bankauskunftsverfahren

Gemeinsames Kommuniqué über das Bankauskunftsverfahren

Einigkeit über die Erteilung von Bankauskünften haben die Kreditwirtschaft, die für den Datenschutz im privaten Bereich zuständigen Behörden (Düsseldorfer Kreis) und die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erzielt. Ziel der Verhandlungen war es, die datenschutzrechtlichen Voraussetzungen und Grenzen des Bankauskunftsverfahrens zu präzisieren, die Kunden über Inhalt und Zweck dieses Verfahrens umfassend zu unterrichten und sie auf ihre Rechte hinzuweisen. In die Gespräche ist auch das Schufa-Verfahren einbezogen worden.

I. In der Diskussion haben sich die Beteiligten von dem Grundsatz leiten lassen, daß dem Vertrauensverhältnis zwischen Kunden und Kreditinstitut (Bankgeheimnis) — unverändert — wesentliche Bedeutung zukommt. Deshalb dürfen Bankauskünfte nur erteilt werden, sofern dies dem Willen des Kunden entspricht. Darüber hinaus können Kreditinstitute aufgrund gesetzlicher Bestimmungen verpflichtet sein, Auskünfte zu erteilen (z. B. im Strafverfahren, Steuerverfahren). Für das Bankauskunftsverfahren gelten nunmehr folgende Anforderungen:

   1. Das Kreditinstitut ist berechtigt, über Geschäftskunden (juristische Personen und Kaufleute) Bankauskünfte zu erteilen, sofern ihm keine anderslautende Weisung des Kunden vorliegt.
   2. Bankauskünfte über Privatkunden erteilt das Kreditinstitut nur dann, wenn diese allgemein oder im Einzelfall ausdrücklich zugestimmt haben.
   3. Bankauskünfte sind allgemein gehaltene Feststellungen und Bemerkungen über die wirtschaftlichen Verhältnisse des Kunden, seine Kreditwürdigkeit und Zahlungsfähigkeit; betragsmäßige Angaben über Kontostände, Sparguthaben, Depot- oder sonstige dem Kreditinstitut anvertraute Vermögenswerte sowie Kreditinanspruchnahmen werden nicht gemacht.
   4. Bankauskünfte erhalten nur eigene Kunden sowie andere Kreditinstitute für deren eigene Zwecke und die ihrer Kunden; sie werden nur dann erteilt, wenn der Anfragende ein berechtigtes Interesse an der gewünschten Auskunft glaubhaft darlegt.

II. Für die Durchführung des Bankauskunftsverfahrens wird ergänzend auf folgendes hingewiesen:

   1. Die Auskunftsverweigerung wegen fehlender Einwilligung ist so zu formulieren, daß sie nicht als negative Auskunft verstanden werden kann. Liegt bei Privatkunden eine Einwilligung nicht vor oder hat bei Geschäftskunden der Kunde die Erteilung einer Auskunft untersagt oder hat die angefragte Stelle keinen Einblick in die wirtschaftlichen Verhältnisse des Kunden, ist dies in der Antwort deutlich zum Ausdruck zu bringen.
   2. Die Auskunft darf sich nur auf die wirtschaftlichen Verhältnisse des Kunden und sein Verhalten im Geschäftsleben beziehen.
   3. Bankauskünfte werden nur aufgrund von Erkenntnissen erteilt, die der auskunftgebenden Stelle vorliegen. Es werden keine Recherchen (etwa mit Hilfe von Wirtschaftsauskunfteien) angestellt.
   4. Hat das Kreditinstitut eine von Anfang an unrichtige Auskunft erteilt, so ist es zur Richtigstellung gegenüber dem Auskunftsempfänger verpflichtet.
   5. Der Kunde, der eine Auskunft erhält, ist ausdrücklich darauf hinzuweisen, daß er empfangene Informationen nur für den angegebenen Zweck verwenden und nicht an Dritte weitergeben darf.
   6. Mündlich erteilte Bankauskünfte werden dokumentiert und sollen in der Regel schriftlich bestätigt werden.
   7. Auf Verlangen des Betroffenen hat das Kreditinstitut den Inhalt einer erteilten Auskunft mitzuteilen.
   8. Wirtschaftsauskunfteien erhalten keine Bankauskünfte.

III. Schufa-Verfahren

   1. Es besteht Einvernehmen, daß der Kunde auch über das Schufa-Verfahren ausführlicher und deutlicher unterrichtet werden soll. Die Schufa-Klausel wurde noch nicht abschließend erörtert, weil zunächst der Ausgang eines beim BGH schwebenden Rechtsstreits abgewartet werden soll, der über die Wirksamkeit der Schufa-Klausel geführt wird.
   2. Die Datenschutzbehörden weisen darauf hin, daß eine Datenübermittlung an die Schufa ein Geschäft mit Kreditrisiko voraussetzt. Sie folgern hieraus, daß für die Eröffnung eines Girokontos, das nur auf Guthabenbasis geführt werden soll, die Unterzeichnung der Schufa-Klausel nicht verlangt werden darf. Sie fordern deshalb die Kreditwirtschaft auf, die Errichtung von Girokonten, die nur auf Guthabenbasis geführt werden sollen, auch ohne Schufa-Klausel zu ermöglichen.

Die Vertreter der Kreditwirtschaft weisen demgegenüber darauf hin, daß ein ausschließlich auf Guthabenbasis zu haltendes Konto von seiten des Kreditinstituts eine spezielle Beobachtung erfordert, was die organisatorischen Möglichkeiten eines automatisierten Massengeschäfts überschreiten kann. Außerdem machen sie darauf aufmerksam, daß der Kunde auf verschiedene moderne Formen des Zahlungsverkehrs (ec-Scheck, GAA-Karte) verzichten müßte.

Kundeninformation „Bankauskunftsverfahren"

Die Kreditwirtschaft hat die Auskunftserteilung durch Kreditinstitute mit den Datenschutzbehörden eingehend erörtert. Es besteht Einigkeit darüber, daß dem Bankgeheimnis für die Wahrung des Persönlichkeitsrechts in den Geschäftsbeziehungen zwischen Kunde und Kreditinstitut — unverändert — wesentliche Bedeutung zukommt. Deshalb dürfen Bankauskünfte nur erteilt werden, sofern dies dem Willen des Kunden entspricht. Darüber hinaus können Kreditinstitute aufgrund gesetzlicher Bestimmungen verpflichtet sein, Auskünfte zu erteilen (z. B. im Strafverfahren, Steuerverfahren). Für das Bankauskunftsverfahren (Nr. 7/10 AGB) gelten nunmehr folgende Regeln:

1. Das Kreditinstitut ist berechtigt, über Geschäftskunden (juristische Personen und Kaufleute, die im Handelsregister eingetragen sind) Bankauskünfte zu erteilen, sofern ihm keine anderslautende Weisung des Kunden vorliegt.
2. Bankauskünfte über Privatkunden (alle sonstigen Personen und Vereinigungen) erteilt das Kreditinstitut nur dann, wenn diese allgemein oder im Einzelfall ausdrücklich zugestimmt haben.
3. Bankauskünfte sind allgemein gehaltene Feststellungen und Bemerkungen über die wirtschaftlichen Verhältnisse des Kunden, seine Kreditwürdigkeit und Zahlungsfähigkeit; betragsmäßige Angaben über Kontostände, Sparguthaben, Depot- oder sonstige dem Kreditinstitut anvertraute Vermögenswerte sowie Kreditinanspruchnahmen werden nicht gemacht.
4. Bankauskünfte erhalten nur eigene Kunden sowie andere Kreditinstitute für deren eigene Zwecke und die ihrer Kunden; sie werden nur erteilt, wenn der Anfragende ein berechtigtes Interesse an der gewünschten Auskunft glaubhaft darlegt.

Im übrigen werden unter bestimmten Voraussetzungen auch Daten über Kunden an die Schutzgemeinschaft für allgemeine Kreditsicherung (Schufa) weitergegeben. Über Einzelheiten des Schufa-Verfahrens erteilen die Kreditinstitute auf Wunsch nähere Auskunft.

Sachregister

Abkürzungsverzeichnis

ADV	Automatisierte Datenverarbeitung
AGB	Allgemeine Geschäftsbedingungen
AFG	Arbeitsförderungsgesetz
AO	Abgabenordnung
APIS	Arbeitsdatei PIOS-Innere-Sicherheit
AZR	Ausländerzentralregister
BAG	Bundesarbeitsgericht
BBG	Bundesbeamtengesetz
BDSG	Bundesdatenschutzgesetz
BfA	Bundesversicherungsanstalt für Angestellte
BfD	Bundesbeauftragter für den Datenschutz
BfV	Bundesamt für Verfassungsschutz
BGB	Bürgerliches Gesetzbuch
BGBl	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGS	Bundesgrenzschutz
BKA	Bundeskriminalamt
BKAG	Gesetz über die Errichtung eines Bundeskriminalpolizeiamtes
BKGG	Bundeskindergeldgesetz
BLG	Bundesleistungsgesetz
BMA	Bundesminister für Arbeit und Sozialordnung
BMI	Bundesminister des Innern
BMP	Bundesminister für das Post- und Fernmeldewesen
BMV	Bundesminister für Verkehr
BND	Bundesnachrichtendienst
BStatG	Bundesstatistikgesetz
BT	Bundestag
BetrVG	Betriebsverfassungsgesetz
Btx	Bildschirmtext
BVerfG	Bundesverfassungsgericht
BVerfGE	Bundesverfassungsgerichtsentscheidung
BWO	Bundeswahlordnung
BZR	Bundeszentralregister
BZRG	Bundeszentralregistergesetz
DA	Dienstanweisung für die Standesbeamten und ihre Aufsichtsbehörden
DATEX	DATa EXchange
DBP	Deutsche Bundespost
DEVO	Datenerfassungsverordnung
DÜVO	Datenübermittlungsverordnung
DV	Datenverarbeitung
ed	erkennungsdienstlich
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
EWG	Europäische Wirtschaftsgemeinschaft
FAG	Gesetz über Fernmeldeanlagen
FISH	Forensisches Informationssystem Handschriften
G 10	Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses
GAN	Grenzaktennachweis
GG	Grundgesetz
GMBl	Gemeinsames Ministerialblatt
INPOL	Informationssystem der Polizei
IRG	Gesetz über die Internationale Rechtshilfe in Strafsachen

KAN	Kriminalaktennachweis
KBA	Kraftfahrt-Bundesamt
KONTES	Kundenorientierte Neugestaltung der Teilnehmerdienste mit EDV-Systemen
KpS-Richtl.	Richtlinien über die Errichtung und Führung kriminalpolizeilicher personenbezogener Sammlungen
LBA	Luftfahrt-Bundesamt
LKA	Landeskriminalamt
MAD	Militärischer Abschirmdienst
MiStra	Mitteilungen in Strafsachen
MiZi	Mitteilungen in Zivilsachen
MRRG	Melderechtsrahmengesetz
NADIS	Nachrichtendienstliches Informationssystem
NJW	Neue Juristische Wochenschrift
OVG	Oberverwaltungsgericht
P-Anfrage	Anfrage an das KBA mit Personendaten zur Feststellung der Anschrift und der Fahrzeuge dieser Person
PIOS	Auskunftssystem über Personen, Institutionen, Objekte und Sachen
RiStBV	Richtlinien für das Strafverfahren und das Bußgeldverfahren
RVO	Reichsversicherungsordnung
SCHUFA	Schutzgemeinschaft für allgemeine Kreditsicherung GmbH
SGB	Sozialgesetzbuch
SGB X	Sozialgesetzbuch Zehntes Buch
SPUDOK	Spurendokumentationssystem
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
StVG	Straßenverkehrsgesetz
StVZO	Straßenverkehrs-Zulassungs-Ordnung
TB	Tätigkeitsbericht*)
Telebox	Elektronisches Postfach für Datenfernübertragung
TEMEX	TEleMetry EXchange (Fernwirkdienst der DBP)
TESCH	Dokumentationssystem für terrorismus- und extremismusbezogene Schriften
VDR	Verband Deutscher Rentenversicherungsträger
VSA	Verschlußsachenanweisung
VSG	Verkehrssicherstellungsgesetz
VZG	Volkszählungsgesetz
VZR	Verkehrszentralregister
VZRG	Verkehrszentralregistergesetz
WEWIS	Wehrersatzweseninformationssystem
ZEVIS	Zentrales Verkehrsinformationssystem
ZPO	Zivilprozeßordnung

*) Erster Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 8/2460
Zweiter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 8/3570
Dritter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 9/93
Vierter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 9/1243
Fünfter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 9/2386
Sechster Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 10/877

Druck: Bonner Universitäts-Buchdruckerei, 5300 Bonn
Alleinvertrieb: Verlag Dr. Hans Heger, Postfach 20 08 21, Herderstraße 56, 5300 Bonn 2, Telefon (02 28) 36 35 51
ISSN 0722-8333