Deutscher Bundestag
11. Wahlperiode

Drucksache 11/1693
20. 01. 88

Sachgebiet 204

Unterrichtung

durch den Bundesbeauftragten für den Datenschutz

Zehnter 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 192 111/12 — vom 20. Januar 1988 gemäß § 19 Abs. 2 des Bundesdatenschutzgesetzes.

1. Einleitung

Der bevorstehende Ablauf der zweiten Amtsperiode des Bundesbeauftragten für den Datenschutz seit der Einrichtung dieser Behörde ist Anlaß genug, Bilanz zu ziehen, eine Standortbestimmung vorzunehmen und Perspektiven für die Zukunft aufzuzeigen.

Die Amtszeit von 1983 bis 1988 wurde maßgeblich geprägt durch das Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983, durch dessen Einfluß auf das Datenschutzverständnis in der Bevölkerung und seine Auswirkungen auf die Gesetzgebung, Rechtsprechung und Verwaltung. In den dem Urteil vorausgegangenen Monaten habe ich sowohl im gerichtlichen Verfahren der einstweiligen Anordnung wie auch im Hauptverfahren in umfangreichen Schriftsätzen meine Rechtsauffassung zum Volkszählungsgesetz 1983 dargelegt und in den mündlichen Verhandlungen vor dem Bundesverfassungsgericht Stellung genommen.

Das Volkszählungsurteil war letztlich die durch das Grundgesetz vorgezeichnete Antwort auf die Entwicklung zur Informationsgesellschaft, die gerade im vergangenen Jahrzehnt weltweit einen stürmischen Verlauf genommen hat. Zwar erging das Urteil zum Volkszählungsgesetz, also zum Bereich der Statistik. Es ist jedoch unbestritten, daß das Bundesverfassungsgericht mit dieser Entscheidung weit über den konkreten Anlaß hinaus allgemeine Grundsätze und Regeln zur Datenverarbeitung und zum Datenschutz aufgestellt hat, und zwar im Hinblick auf die Gefährdungen, denen das Grundrecht auf freie Entfaltung der Persönlichkeit durch die Nutzung vor allem der automatisierten Datenverarbeitung ausgesetzt ist. Das Gericht hat Verarbeitungsbedingungen in einem Umfang und in einer Tiefe formuliert, die die Datenschutzlandschaft bereits erheblich verändert haben und noch weiter verändern werden.

Natürlich konnte es nicht ausbleiben, daß über die Auslegung des Volkszählungsurteils alsbald eine heftige Diskussion entbrannte, bei der die Vertreter einer maximalistischen Betrachtungsweise das Urteil als magna charta des Datenschutzes priesen, während die Minimalisten aus ihm — abgesehen vielleicht von dem nachzubessernden Volkszählungsgesetz — keinen konkreten Handlungsbedarf ableiten wollten. Die zuletzt genannte Auffassung hat sich ersichtlich nicht durchsetzen können, und nur einige wenige Unverbesserliche beharren auf ihrer strikt verneinenden Haltung, so wenn beispielsweise in einem Kommentar — erschienen in einer großen deutschen Tageszeitung am 29. Dezember 1987 — von der „unglückseligen Entscheidung des Bundesverfassungsgerichts, jeder müsse wissen können, was wer wann über ihn wisse" die Rede ist.

Der Streit um die Auslegung des Volkszählungsurteils soll an dieser Stelle nicht fortgeführt werden. Jedoch erscheint es wichtig und notwendig, anhand von markanten Beispielen darzustellen, welche Veränderungen in den vier Jahren nach Erlaß des Urteils, insbesondere im Bereich von Gesetzgebung, Rechtsprechung und Verwaltung bereits eingetreten sind, welche Fortschritte erzielt wurden und wo Defizite zu verzeichnen sind.

1.1 Gesetzgebung

Im Bereich der Gesetzgebung liegt zwischen verfassungsrechtlichem Anspruch und gesetzgeberischer Verwirklichung noch eine lange und vor allem mühsame Wegstrecke, so daß die Frage gerechtfertigt erscheint, ob Motivation und gesetzgeberische Kräfte ausreichen, um sie in angemessener Zeit zu bewältigen.

Zu dem Anspruch selbst ist zuletzt in der Koalitionsvereinbarung vom März vergangenen Jahres insoweit ein eindeutiges Bekenntnis abgegeben worden, als dort mehr als 15 Gesetze aufgeführt werden, die in der anstehenden Legislaturperiode aus datenschutzrechtlichen Gründen entweder erstmals erlassen oder aber dringend novelliert werden müssen. Entsprechende Anstrengungen sind verstärkt notwendig, da heute — vier Jahre nach Erlaß des Urteils — erst einige wenige Gesetze verabschiedet werden konnten, in die die grundsätzlichen Anforderungen des Volkszählungsurteils Eingang fanden. Wenn man die nach dem Urteil notwendige Anlaufzeit für dessen Umsetzung in Rechnung stellt, dann scheint zwar dieses Ergebnis auf den ersten Blick nicht schlecht zu sein. Die Bilanz der ersten vier Jahre sieht jedoch dann weniger günstig aus, wenn man in Betracht zieht, daß es sich bei diesen Gesetzen — abgesehen von dem Bundesstatistikgesetz — ausnahmslos um Gesetze zur Verwirklichung bestimmter, zum Teil schon seit langem geplanter Vorhaben handelt, hinter denen ein entscheidender politischer Wille stand: Volkszählung, Mikrozensus, Ausgabe von neuen Personalausweisen und Pässen sowie die vollständige Inbetriebnahme des Zentralen Verkehrsinformationssystems ZEVIS. Selbst der Erlaß des Bundesarchivgesetzes stand in erster Linie unter politischem Handlungsbedarf und nicht unter dem Druck, den Datenschutz zu verbessern.

Die erwähnten Gesetze sind daher noch kein Beweis dafür, daß es dem Gesetzgeber bei diesen Vorhaben vor allem um die Umsetzung von Grundvorstellungen über einen besseren Persönlichkeitsschutz ging. Die datenschutzrechtliche Nagelprobe wird spätestens dann zu bestehen sein, wenn das Bundesdatenschutzgesetz zu novellieren ist und die bereichsspezifischen Datenschutzgesetze im Sicherheitsbereich zu erlassen sind. Der Gesetzgeber steht hierbei unter Zeitdruck, da die vom Bundesverfassungsgericht zur Bereinigung derartiger nicht verfassungsmäßiger Situationen zugestandene Übergangsfrist wohl am Ende dieser Legislaturperiode abgelaufen sein wird. Schon jetzt liegen Gerichtsentscheidungen vor, in denen ein zunächst anerkannter Übergangsbonus den beteiligten Verwaltungen nicht mehr zugestanden wurde. Es erscheint daher unbedingt notwendig, daß die entsprechenden Gesetzentwürfe noch vor der parlamentarischen Sommerpause eingebracht werden, um eine angemessene und zeitgerechte Beratung in den Ausschüssen zu gewährleisten.

Ich wünsche mir, daß bei diesen Beratungen genau so großer Wert auf meine Beteiligung gelegt wird, wie beispielsweise bei der Beratung des Volkszählungsgesetzes 1987, als es darum ging, ein Gesetz zu erlassen, das den datenschutzrechtlichen Anforderungen des Volkszählungsurteils in allen Punkten gerecht wird.

Die Ausschüsse des Deutschen Bundestages, vor allem der Innenausschuß, haben sich den nach Erlaß des Volkszählungsurteils verstärkt auftretenden datenschutzrechtlichen Problemen mit zunehmender Intensität und Sensibilität angenommen. Häufig wurden die anstehenden Themen auch durch Sachverständigen-Anhörungen vorbereitet, an denen ich beteiligt wurde. Wenn auch bei der jeweils endgültigen Gesetzesfassung meinen datenschutzrechtlichen Vorstellungen nicht immer in allen Punkten entsprochen wurde, so ist doch festzustellen, daß bei den Ausschußberatungen der Datenschutz stets eine wesentliche Rolle gespielt hat, und daß die in dieser Hinsicht erreichten Verbesserungen, die gerade auch in der Ausschußarbeit erzielt wurden, zum Teil beachtlich sind. Erinnert sei in diesem Zusammenhang z. B. an das Personalausweisgesetz. Der erste Regierungsentwurf zur Einführung eines fälschungssicheren und maschinenlesbaren Ausweises, der aus dem Jahre 1979 stammte, enthielt noch keine einzige den Datenschutz betreffende Bestimmung. Das im April 1986 verabschiedete Gesetz enthält hingegen eine Reihe sehr eingehender datenschutzrechtlicher Vorschriften, die zum Teil erst nach langwierigen parlamentarischen Beratungen aufgenommen wurden. Die gesetzgeberische Entstehungsgeschichte gerade dieses Gesetzes zeigt die bedeutende Rolle, die der Datenschutz insbesondere in der letzten Phase des Gesetzgebungsverfahrens gespielt hat, und sie stellt gleichzeitig ein Stück Geschichte des Datenschutzes im Bedeutungswandel der aktuellen Gesetzgebungsarbeit dar.

Gerade die datenschutzrechtlichen Erörterungen in den Ausschüssen des Deutschen Bundestages anläßlich der anstehenden Gesetzgebungsarbeit oder aber anläßlich aktueller Ereignisse sind eindrucksvolle Gradmesser des ständig wachsenden Problembewußtseins für Fragen des Datenschutzes. Und für den Bundesbeauftragten für den Datenschutz sind diese Beratungen, insbesondere auch im Innenausschuß des Deutschen Bundestages, nicht selten der Ort, wo datenschutzrechtliche Kontroversen, die mit der Verwaltung bestehen, nochmals diskutiert und vernünftigen Lösungen zugeführt werden können. Aber auch für den Gesetzgeber ist es bei der häufig bestehenden Brisanz dieser Materie von wesentlicher Bedeutung, den materiellen Gehalt einer von ihm zu beschließenden Regelung genau zu kennen, um deren Risiko — auch was die gesellschaftliche Akzeptanz anbelangt — abschätzen zu können.

1.2 Rechtsprechung

Die immer wieder zu hörende Auffassung, das Volkszählungsurteil werde — gerade auch von den Datenschutzbeauftragten — überinterpretiert und das Bundesverfassungsgericht selbst habe ja eine so weitreichende Entscheidung gar nicht treffen wollen, kann sich zumindest nicht auf die zwischenzeitlich ergangene Rechtsprechung stützen.

So hat das Bundesverfassungsgericht in seinen nach dem Volkszählungsurteil erlassenen Entscheidungen immer wieder auf dort enthaltene Grundsätze entweder ausdrücklich oder inhaltlich Bezug genommen, und in seinem auf eine Verfassungsbeschwerde zur Volkszählung ergangenen Beschluß vom 18. Dezember 1987 hat es den gelegentlich mit Kritik bedachten Grundsatz von der informationellen Gewaltenteilung erneut herausgestellt. Dort ist ausgeführt, daß aus der Einheit der Gemeindeverwaltung keine informationelle Einheit folgt und der Grundsatz der informationellen Gewaltenteilung auch innerhalb der Gemeindeverwaltung gilt.

Als besonders folgenreiche Auswirkung des Volkszählungsurteils ist es zu werten, daß die Gerichte dazu übergehen, insbesondere Teile polizeilicher Datenverarbeitung für unzulässig zu erklären, weil es an den hierfür erforderlichen Rechtsgrundlagen fehlt, wie sie nach den Grundsätzen des Volkszählungsurteils unerläßlich sind (so die Verwaltungsgerichte Frankfurt, Wiesbaden, Hannover und München).

Auch wenn solche Entscheidungen noch Einzelfälle sein mögen, müssen sich die Verantwortlichen darüber im klaren sein, daß die Tendenz zu einer solchen Einschätzung der Rechtslage zunimmt und der Zeitpunkt abzusehen ist, zu dem die Gerichte in vielen Bereichen die gegenwärtigen Rechtsgrundlagen nicht mehr als ausreichend anerkennen und daher Datenverarbeitung in großem Umfang für rechtswidrig erklären werden.

Niemand sollte sich der Hoffnung hingeben, daß insoweit noch eine Trendwende eintreten könnte; hierfür sind die im Volkszählungsurteil enthaltenen Grundsätze zu eindeutig. Als Lösung bleibt daher nur der bereits aufgezeigte Weg, die ausstehenden Gesetze so schnell wie möglich zu erlassen.

1.3 Verwaltung

Der Datenschutz ist in der öffentlichen Verwaltung im Rahmen der Ausführung bestehender Gesetze zu gewährleisten — aber auch in der Beachtung und Anwendung sonstigen geltenden Rechts, was sowohl Verfassungsgrundsätze als auch ungeschriebenes Recht und untergesetzliche Rechtsnormen sein können.

Im Zusammenhang mit der Anwendung dieses Rechts kommt der Exekutive hinsichtlich der Gestaltung der Datenschutzpraxis eine maßgebliche Rolle zu, da sie sowohl die Auslegung der einzelnen Vorschriften bestimmt, als auch für den Erlaß der zahlreichen Verwaltungsvorschriften und Dienstanweisungen verantwortlich ist. Soweit das Volkszählungsurteil Inhalt und Ziele des Datenschutzes authentisch bestimmt, ist es von der Verwaltung in ihrer täglichen Arbeit umzusetzen. Das bedeutet, daß

ihre Amtsträger — unabhängig von den notwendigen aber noch ausstehenden Gesetzesänderungen — sich ständig Rechenschaft darüber ablegen müssen, ob ihre gegenwärtige datenschutzrechtliche Praxis mit den Grundsätzen dieses Urteils noch im Einklang steht. Denn diese sind für die Verwaltung bereits heute insoweit verbindlich, als ihrer unmittelbaren Anwendung keine strikten Gesetzesbefehle entgegenstehen.

Die gegenwärtige Verwaltungspraxis bedarf danach der Überprüfung vor allem bezüglich folgender Problembereiche:

— Einbeziehung auch der lediglich in Akten enthaltenen personenbezogenen Daten in den Schutzbereich des Rechts auf informationelle Selbstbestimmung;

— deutliche Begrenzung des Umfangs der Datenverarbeitung unter dem Gesichtspunkt der Erforderlichkeit und der Verhältnismäßigkeit;

— kein Unterlaufen datenschutzrechtlicher Bestimmungen insbesondere durch unveränderte Anwendung der Amtshilfegrundsätze;

— Informationelle Gewaltenteilung, d.h. Datenschutz auch innerhalb einer Behörde durch Funktionstrennung;

— mehr Transparenz für den Betroffenen durch Erweiterung der Auskunftspraxis schon im Rahmen des geltenden Rechts.

Außerdem muß die Verwaltung vorhandene Vorschriften, die aber nach den Grundsätzen des Volkszählungsurteils als nicht mehr verfassungsmäßig anzusehen sind, bis zur Herstellung eines einwandfreien Rechtszustandes restriktiv auslegen. Auch wird z.B. von der Einführung neuer Verarbeitungsmethoden stets dann abzusehen sein, wenn diese den durch das Bundesverfassungsgericht konkretisierten verfassungsrechtlichen Anforderungen nicht entsprechen.

Ich verkenne nicht und will dies gerne deutlich aussprechen, daß sich das Datenschutzbewußtsein in nicht wenigen Bereichen der Verwaltung erfreulich verbessert hat, und daß dort Bemühungen unternommen werden, die Datenverarbeitung und den Datenschutz auch vor Erlaß entsprechender Gesetze den Grundsätzen des Volkszählungsurteils anzupassen. Auf einige dieser Beispiele habe ich in meinen Tätigkeitsberichten hingewiesen. Doch kann dies nicht darüber hinwegtäuschen, daß die meisten Behörden noch auf den Gesetzgeber und seine Signale warten, bevor sie die ihr zur Gewohnheit gewordene Praxis ändern, und daß Datenschutz vielfach immer noch als eine lästige Behinderung der Aufgabenerfüllung empfunden und oft falsch oder gar nicht verstanden wird.

Durch die Bereinigung von Gesetzgebungsdefiziten allein werden im übrigen die Datenschutzprobleme nicht gelöst, da deren Schwere auch durch den Zustand des Verhältnisses zwischen Verwaltung und Bürger bestimmt wird. Flankierend zu den Gesetzen hinzukommen muß daher ein Bewußtmachen und ein Bewußtwerden der datenschutzrechtlichen Problematik, also die Bildung eines entsprechenden Datenschutzbewußtseins sowohl bei den Datenverarbeitung betreibenden Personen wie auch bei den hierfür Verantwortlichen. Dem Bürger muß nicht allein durch Gesetze — die er häufig nicht versteht — sondern gerade durch die handelnde Verwaltung das Gefühl gegeben werden, daß er nicht als Objekt der Datenverarbeitung angesehen, sondern als Grundrechtsträger behandelt wird. Je mehr der Bürger darauf vertrauen kann, daß mit seinen personenbezogenen Daten genau so pfleglich umgegangen wird wie beispielsweise mit fremdem Eigentum, desto eher wird er auch bereit sein, seine Daten der öffentlichen Verwaltung zur gesetzlichen Aufgabenerfüllung anzuvertrauen. Transparenz und Fairnis sind hierfür unverzichtbare Voraussetzungen.

In Gesprächen mit Vertretern der Exekutive weise ich immer wieder auf diese inneren Zusammenhänge zwischen Datenschutz, Akzeptanz und gesetzlicher Aufgabenerfüllung hin und auf die auch in ihrem eigenen Interesse liegende Notwendigkeit, gerade bei den datenverarbeitenden Stellen und Personen das Bewußtsein hierfür zu entwickeln und zu schärfen. Denn der Schlüssel für eine generelle Lösung der Problematik liegt letztlich in der Erkenntnis, daß eine für den Betroffenen durchschaubare und von ihm akzeptierte Verarbeitung seiner personenbezogenen Daten zusammen mit einem angemessenen Datenschutz die besten Voraussetzungen auch für eine erfolgreiche gesetzliche Aufgabenerfüllung sind.

Wenn die hier von mir gegebene Bilanz aus der zweiten Amtszeit des Bundesbeauftragten für den Datenschutz sich fast ausschließlich mit dem Volkszählungsurteil des Bundesverfassungsgerichts und seinen Auswirkungen beschäftigt, so deshalb, weil dies das herausragende und bedeutungsvollste Ereignis dieser Jahre gewesen ist, mit dem ich sofort nach meinem Amtsantritt konfrontiert wurde und das mich ständig bei meiner Arbeit begleitet hat. Es wird noch auf Jahre hinaus die Amtsführung des BfD nachhaltig beeinflussen.

1.4 Bürgerfreundlichkeit

Ich möchte an dieser Stelle aber noch eine weitere Erfahrung wiedergeben, die ich in den letzten fünf Jahren gewonnen habe, und die ich den Verantwortlichen in Politik, Regierung und Verwaltung zugleich als Zukunftsperspektive eindringlich nahebringen möchte: Datenschutz ist ein wesentliches und überaus wirksames Instrument, Bürgerfreundlichkeit zu praktizieren. Ich stelle immer wieder fest, wie häufig — und meist auch wie abstrakt — manchmal auch mit ideologischem Anspruch, in Reden, sonstigen öffentlichen Verlautbarungen oder Arbeitsprogrammen die Forderung nach mehr Bürgerfreundlichkeit der Verwaltung erhoben wird. Vom Datenschutz, der ja für den Bürger geschaffen wurde, ist dabei leider fast nie die Rede, obwohl die Verwaltung gerade damit ihre bürgerfreundliche Haltung unter Beweis stellen kann. Dabei geht es weniger

um die richtige und oft schwierige Anwendung komplizierter Rechtsvorschriften, sondern darum, die bürgerbezogene Tätigkeit der Verwaltung transparent zu machen.

Denn Verwaltungstätigkeit ist fast immer auch Informationsverarbeitung, die bei Nutzung moderner Techniken noch weniger durchschaubar ist als sonst, und so leicht zum Ärgernis für den Bürger werden kann, wenn es dabei um seine personenbezogenen Daten geht. In zahlreichen Beschwerdefällen, die mir Bürger in Sorge um den richtigen Umgang mit ihren Daten vorgetragen haben, und gerade auch in Diskussionen mit den vielen Besuchergruppen, die sich für meine Arbeit interessierten, erlebe ich es immer wieder, daß die Bürger ihre zunächst eingenommene Abwehrhaltung, die sich oft bis zur Empörung steigert, aufgeben und auch belastende Maßnahmen akzeptieren, wenn man sie ihnen nur verständlich erklärt. Diese Auskunfts- und Belehrungspflicht ist im Datenschutzrecht angelegt. Es wäre aber falsch, sie vornehmlich den Datenschutzbeauftragten vorzubehalten. Würde die Verwaltung diese Aufklärungsarbeit, die sie — sicherlich ungewollt — vorläufig noch weitgehend den Datenschutzbeauftragten überläßt, selbst übernehmen, könnte sie das Postulat Bürgerfreundlichkeit schon an der ersten Nahtstelle zwischen Bürger und Staat demonstrieren und dabei ein Stück verlorengegangenes Vertrauen und Respekt zurückgewinnen. Als der Gesetzgeber die Datenschutzbeauftragten als Kontrollorgane institutionalisierte, lag es sicherlich nicht primär in seiner Absicht, dadurch den in der Bevölkerung wachsenden Erklärungsbedarf für ständig komplizierter werdende Verwaltungsabläufe zu befriedigen. Im nachhinein kann gesagt werden — und das weiß ich von vielen Bürgern —, daß die Einsetzung der Datenschutzbeauftragten allein wegen dieser — ihnen im Prinzip gar nicht aufgetragenen — Funktion als wesentlicher Schritt auf dem Weg zur Bürgerfreundlichkeit der öffentlichen Verwaltung betrachtet wird. Doch das reicht noch nicht aus. Diese Öffnung im Informationsverhalten des Staates gegenüber seinen Bürgern muß erweitert werden. Das gilt — mit selbstverständlichen Einschränkungen — auch im Bereich der öffentlichen Sicherheit. Denn insgesamt ist festzustellen: Dieser Staat hat nichts zu verbergen, er kann sich mehr Transparenz leisten, und er wird dadurch nicht schwächer, sondern stärker. Diese Erkenntnis beruht auf der dem Datenschutzbeauftragten in besonderem Maße möglichen Einsicht in die Arbeit vieler Behörden mit den unterschiedlichsten Aufgaben und — korrespondierend dazu — aus dem unmittelbaren Kontakt mit dem „verwalteten" Bürger, wenn dieser ihm seine Betroffenheit mitteilt.

Dem Bürger ist nicht primär daran gelegen, daß sich die Verwaltung für ihr Handeln rechtfertigt — dafür gibt es Instanzenzüge und Kontrollorgane —, sondern er möchte verstehen können, warum und wie im einzelnen sich die Verwaltung um ihn kümmert. Dazu bedarf es einer Einstellung im öffentlichen Dienst, die dessen gesetzliche Auskunftspflichten lediglich als das Minimum dessen begreift, was dem Bürger an Information geschuldet wird. Ich wünsche mir, daß dieses Potential zur Herstellung bürgerfreundlicher Verwaltung erkannt und besser genutzt wird.

1.5 Das beherrschende Ereignis im Berichtsjahr: Die Volkszählung 1987

Die Volkszählung war das zentrale datenschutzpolitische Ereignis im Berichtsjahr. Vorbereitung und Durchführung dieses Unternehmens fand unter großer Anteilnahme der Öffentlichkeit statt. In den Wochen um den Zählungsstichtag vom 25. Mai 1987 wurden die Dienststellen der Datenschutzbeauftragten mit telefonischen Anfragen und schriftlichen Eingaben überhäuft. Auch bei mir sind in dieser Zeit ungewöhnlich viele Anfragen besorgter Bürger eingegangen, die ich in der überwiegenden Mehrzahl selbst beantwortet habe. Ich habe insbesondere ein Informationspapier erarbeitet, in dem ich deutlich gemacht habe, daß nach meiner Auffassung das Volkszählungsgesetz die verfassungsrechtlichen Vorgaben des Volkszählungsurteils berücksichtigt hat; dieses Papier habe ich allen denjenigen zugesandt, die Zweifel in dieser Richtung geäußert haben. Eingaben, die sich schwerpunktmäßig mit Problemen der Durchführung der Volkszählung befaßten, habe ich an die Landesbeauftragten für den Datenschutz weitergeleitet; diese waren insoweit zuständig, weil die Durchführung der Volkszählung den Bundesländern obliegt, die hierfür auch den rechtlichen Rahmen zu schaffen hatten (vgl. 9. TB S. 45).

Auf die wichtigsten im Laufe des Berichtsjahres aufgetretenen Zweifelsfragen gehe ich weiter unten näher ein (s. u. Nr. 10). Zum Teil sind sie in den Konferenzen der Datenschutzbeauftragten des Bundes und der Länder gemeinsam diskutiert worden. Ich habe vor allem auch mit dem Bundesminister des Innern und dem Statistischen Bundesamt Gespräche geführt. Im allgemeinen konnten dabei einvernehmliche Lösungen gefunden werden.

Ich vermag im gegenwärtigen Zeitpunkt noch nicht zu beurteilen, ob die Volkszählung die gewünschten Ergebnisse erbracht hat und als Erfolg bewertet werden kann. Denn zuverlässige Erkenntnisse über die Vollständigkeit der Erfassung und die Qualität der Angaben liegen noch nicht vor.

Ich hatte zwar nicht erwartet, daß die Volkszählung 1987 ohne Widerstand seitens einzelner Bürger vonstatten gehen würde. Die dann aber bei einem Teil der Bevölkerung zutage getretene Skepsis, die bis zur offenen Ablehnung reichte, kam auch für mich überraschend. Mich hat betroffen gemacht, in welchem Ausmaße hier Ängste und Befürchtungen der Bürger sichtbar geworden sind. Dies kann nicht darauf beruhen, daß etwa gerade im Bereich der Statistik besondere staatliche Defizite vorhanden gewesen wären. Es wird wohl einzuräumen sein, daß das Volkszählungsgesetz für den Laien schwer verständlich ist. Es hat sich darüber hinaus bei diesem Gesetz erwiesen, daß in ihm auch manches geregelt ist, was in der Praxis so wohl nicht immer durchführbar ist.

Man kann z. B. die personelle und organisatorische Abschottung der Erhebungsstellen in kleineren Kommunen nur schwer gewährleisten, und auch das Gebot, Zähler nicht in unmittelbarer Nähe ihrer Wohnung einzusetzen, läßt sich dort kaum einhalten.

Dies mag dazu beigetragen haben, daß die Akzeptanz der Volkszählung gelitten hat. Damit können aber nicht alle in der Bevölkerung vorhandenen Zweifel erklärt werden.

Die Vorbehalte der Bürger sind wohl in dem allgemeinen Unbehagen dem Staat gegenüber und dem Gefühl des Ausgeliefertseins an die moderne Technik — insbesondere an die elektronische Datenverarbeitung — begründet. Solche Empfindungen sind nicht zuletzt auch vor dem Hintergrund der Einführung des maschinenlesbaren Personalausweises, der Ausweitung der Nutzung von ZEVIS und der gesetzlichen Absicherung der sog. Schleppnetzfahndung — alles Ereignisse der jüngsten Zeit — zu sehen. Die Volkszählung gab die Gelegenheit, sich des latent vorhandenen Mißtrauens bewußt zu werden und dieses zum ersten Mal wirkungsvoll und für den Staat schmerzlich zu artikulieren. Es reicht eben nicht aus, den einzelnen über die Notwendigkeit von Datenerhebungen erst dann zu unterrichten, wenn man Daten von ihm haben will.

Im übrigen dürfte nach den Erfahrungen des Berichtsjahres die Bundesregierung gut beraten sein, der Empfehlung des Deutschen Bundestages nachzukommen, für künftige Zählungen nach Alternativen zur Totalerhebung zu suchen. Dies entspricht nicht nur einer verfassungsgerichtlichen Forderung im Volkszählungsurteil. In diese Richtung weist auch der Entwurf einer Richtlinie des Rats der EG (KOM [86] 775 endg.; Ratsdok. 4219/87), mit der anstelle der früher vorgeschriebenen Totalerhebung für die 1991 geplanten allgemeinen Volkszählungen in der Gemeinschaft nunmehr auch alternative Verfahren — z. B. durch Stichprobenerhebungen — zugelassen sind. Die Suche nach Alternativen ist darüber hinaus eine Frage der politischen Vernunft. Denn es ist nicht vorstellbar, daß sich zukünftig eine Bundesregierung noch einmal dem politischen Risiko des Gelingens einer Volkszählung in der bisherigen Art ohne zwingende Not aussetzen wird.

2. Überblick über das Berichtsjahr

2.1 Kontrollen und Beratungen

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

Bundeszentralregister

Bundesdruckerei

Bundesgesundheitsamt

Bundesverwaltungsamt

Bundesanstalt für Arbeit

Bundesamt für den Zivildienst

Deutsche Bundesbank

Deutsche Bundesbahn

Bundesnachrichtendienst

Bundesamt für Verfassungsschutz

Bundeskriminalamt

Grenzschutzdirektion

Kraftfahrt-Bundesamt

Zentrale Militärkraftfahrtstelle

Umweltbundesamt

Statistisches Bundesamt

Bundesamt für Wirtschaft

Bundesversicherungsanstalt für Angestellte

Filmförderungsanstalt

Deutsche Bundespost u. a. mit folgenden Dienststellen

- ein Postgiroamt
- eine Oberpostdirektion
- mehrere Fernmeldeämter
- eine Rentenrechnungsstelle

Bundesamt für die Anerkennung ausländischer Flüchtlinge

Bundesbaudirektion

Bundesknappschaft

Krankenversorgung der Bundesbahnbeamten

eine Bank unter Aufsicht des Bundes

eine Berufsgenossenschaft

eine Ersatzkasse

mehrere Arbeitsämter

eine Grenzschutzstelle

Nachfolgend sind wichtige bearbeitete Themen und die Art ihrer Erledigung aufgeführt:

Thema	**Art der Erledigung**
Datenschutz bei der Volkszählung	— Beratungen des Innenausschusses des Deutschen Bundestages — Herausgabe eines Informationsblattes — Teilnahme an Diskussionsveranstaltungen
Verhältnis des Bundesstatistikgesetzes 1987 zum Volkszählungsgesetz 1987	— Beratung des Innenausschusses des Deutschen Bundestages — Schriftliche Stellungnahme und Beratung gegenüber dem BMI
Speicherung von AIDS-Daten	— Beratung des Innenausschusses und der Enquête-Kommission „AIDS" des Deutschen Bundestages — Schriftliche Stellungnahme gegenüber dem BMI — Teilnahme an Beratungen des nationalen AIDS-Beirates
Speicherung von Ein- und Ausreisedaten von Bürgern arabischer Staaten	— Beratung des Innenausschusses des Deutschen Bundestages — Beratung und schriftliche Stellungnahme gegenüber dem BMI
Zunehmende Automatisierung der Datenverarbeitung und Dateienvielfalt beim BKA	Schriftliche Stellungnahme gegenüber dem Innenausschuß des Deutschen Bundestages und dem BMI
Neufassung des Verkartungsplanes der Abt. III (Linksextremismus) des BfV	Fortsetzung der Beratung im Innenausschuß des Deutschen Bundestages
Entwurf eines Bundesarchivgesetz	Beratung und schriftliche Stellungnahme gegenüber dem Innenausschuß des Deutschen Bundestages und dem BMI
Beteiligung in zwei Verfassungsbeschwerden betr. Volkszählungsgesetz 1987	Schriftliche Stellungnahmen gegenüber dem Bundesverfassungsgericht
Wiederholungsbefragung nach dem Volkszählungsgesetz 1987	Beratung und schriftliche Stellungnahme gegenüber dem BMI, dem Statistischen Bundesamt und dem Wissenschaftlichen Beirat für Mikrozensus und Volkszählung
Verletzung des Arztgeheimnisses (AIDS)	Beratung des Auswärtigen Amtes
PARLAKOM	Beratung der Verwaltung des Deutschen Bundestages
Entwürfe von Rechtsverordnungen und Allgemeinen Verwaltungsvorschriften zum Paßgesetz	Schriftliche Stellungnahme gegenüber dem BMI
Vorentwurf eines Fünften Gesetzes zur Änderung und Ergänzung des Personenstandsgesetzes	Schriftliche Stellungnahme gegenüber dem BMI
Entwurf eines Dritten Gesetzes zur Änderung des Waffengesetzes	Schriftliche Stellungnahme gegenüber dem BMI
Regelung des Personalaktenrechts	Beratung in der interministeriellen Arbeitsgruppe im BMI und schriftliche Stellungnahme gegenüber dem BMI
Übermittlung von Straßenverkehrsunfalldaten des Statistischen Bundesamtes an die Bundesanstalt für Straßenwesen	Beratung und schriftliche Stellungnahme gegenüber dem BMI, dem BMV, dem Statistischen Bundesamt und der Bundesanstalt für Straßenwesen
Entwurf eines Geheimschutzgesetzes	Beratung gegenüber dem BMI
Errichtungsanordnungen für neue Dateien des BfV	Schriftliche Stellungnahme gegenüber dem BMI
Sicherheits-Richtlinien	Beratung und schriftliche Stellungnahme gegenüber dem BMI
Datenverarbeitung der Zentralstelle zur Bekämpfung der unerlaubten Einreise von Ausländern bei der Grenzschutzdirektion	Beratung und schriftliche Stellungnahme gegenüber dem BMI

Thema	Art der Erledigung
Änderungen des Bundeszentralregistergesetzes	Schriftliche Stellungnahme gegenüber dem BMJ
Vorbereitung datenschutzrechtlicher Ergänzungen zur Strafprozeßordnung	Schriftliche Stellungnahme gegenüber dem BMJ
Arbeitsentwurf eines Gesetzes zur Regelung der rechtlichen Grundlagen für Fahndungsmaßnahmen, Fahndungshilfsmittel und für die Akteneinsicht im Strafverfahren	Schriftliche Stellungnahme gegenüber dem BMJ
Planungen zum Aufbau eines länderübergreifenden staatsanwaltlichen Informationssystems (SISY)	Schriftliche Stellungnahme gegenüber dem BMJ
Arbeitsentwurf eines Vierten Gesetzes zur Änderung des Strafvollzugsgesetzes	Schriftliche Stellungnahme gegenüber dem BMJ
Entwurf eines Gesetzes über Mitteilungen der Justiz von Amts wegen in Zivil- und Strafsachen (Justizmitteilungsgesetz)	Schriftliche Stellungnahme gegenüber dem BMJ
Neufassung der Richtlinien des Bundesgesundheitsamtes für die Erstattung von Blutgruppengutachten	Schriftliche Stellungnahme gegenüber dem BMJ und dem BMJFFG
Entwurf einer Kontrollmitteilungsverordnung	Beratung gegenüber dem BMF
Entwurf einer Steuerdaten-Abruf-Verordnung	Beratung und schriftliche Stellungnahmen gegenüber dem BMF
Filmabgabe der Videowirtschaft	Beratung und schriftliche Stellungnahme gegenüber dem BMWi und der Filmförderungsanstalt
Förderung der Unternehmensberatung	Beratung und schriftliche Stellungnahme gegenüber dem BMWi und dem Bundesamt für Wirtschaft
Einführung eines Sozialversicherungsausweises	Beratung des BMA
Einsatz von PC in der Sozialversicherung	Erörterung mit dem BMA und Spitzenverbänden der Sozialversicherung
Neukonzeption der Merkmalsspeicherung beim MAD	Schriftliche Stellungnahme gegenüber dem BMVg
Einführung eines computergestützten Verfahrens der Eignungs- und Verwendungsprüfung nach dem Wehrpflichtgesetz	Beratung und schriftliche Stellungnahme gegenüber dem BMVg
Laborberichtsverordnung (AIDS)	Schriftliche Stellungnahmen gegenüber dem BMJFFG und Beratung des Bundesgesundheitsamtes
Aufbewahrung von Anerkennungsunterlagen beim Bundesamt für den Zivildienst	Schriftliche Stellungnahme gegenüber dem BMJFFG
Innerbehördliche Schweigepflicht bei Berufsgeheimnissen	Schriftliche Stellungnahme gegenüber dem BMJFFG
Novellierung des Straßenverkehrsunfallstatistikgesetzes	Beratung des BMV
Fahrzeugregisterverordnung (Ausführung des Gesetzes zur Änderung des Straßenverkehrsgesetzes — ZEVIS)	Beratung und schriftliche Stellungnahme gegenüber dem BMV
Richtlinien für die Sicherheitsüberprüfung von Personal in kerntechnischen Anlagen	Schriftliche Stellungnahme gegenüber dem BMU
Moderne Verfahren der Telefongesprächsvermittlung und -abrechnung	Beratung des Bundesministers für das Post- und Fernmeldewesen
Anzeigen und Benachrichtigungen nach § 14 Kreditwesengesetz	Beratung der Deutschen Bundesbank
Datensicherheit im Statistischen Bundesamt	Beratung des Statistischen Bundesamtes
Grundfragen der Arbeitsvermittlung/-beratung einschließlich des Ärztlichen/Psychologischen Dienstes, Reha-Verfahren	Beratung und schriftliche Stellungnahmen gegenüber der Bundesanstalt für Arbeit

Thema	Art der Erledigung
Auskunftserteilung aus dem Rentenkonto an Bevollmächtigte	Beratung der Bundesversicherungsanstalt für Angestellte
Einsatz von PC in Kurkliniken	Beratung der Bundesknappschaft
Automatisierte Personaldatenverarbeitung einschließlich PC-Einsatz und entsprechende Dienstvereinbarungen	Beratung und schriftliche Stellungnahmen gegenüber mehreren Behörden und Personalvertretungen
SCHUFA-Klauseln, SCHUFA-Verfahren	Zusammenarbeit mit den Aufsichtsbehörden der Länder, Beratung des Bundeskartellamtes, Beratung der Kreditwirtschaft
Datenschutz in der Versicherungswirtschaft	Zusammenarbeit mit den Aufsichtsbehörden der Länder
Datenschutz beim Versandhandel, Adressenhandel und Direktwerbung	Zusammenarbeit mit den Aufsichtsbehörden der Länder
Durchführung klinischer Arzneimittelprüfungen	Beratung des Bundesverbandes der pharmazeutischen Industrie
Grundfragen des Datenschutzes	Beratung ausländischer Stellen

2.2 Beanstandungen

Der Deutsche Bundestag hat in seinem Beschluß zu meinem Sechsten und Siebenten Tätigkeitsbericht (Beschlußempfehlung und Bericht des Innenausschusses, Drucksache 10/6583, Nr. 2) darum gebeten, festgestellte Rechtsverstöße stärker von Anregungen und Verbesserungsvorschlägen zu unterscheiden. Diesem Zweck soll die nachfolgende Zusammenstellung der im Berichtsjahr ausgesprochenen Beanstandungen dienen.

Wenn ich feststelle, daß eine Behörde oder öffentliche Stelle des Bundes gegen Datenschutzvorschriften verstoßen hat, so habe ich dies nach § 20 BDSG zu beanstanden. Diese Rechtsverstöße können sich gegen Bestimmungen des Bundesdatenschutzgesetzes, aber auch gegen andere Gesetze wie z. B. das Sozialgesetzbuch richten. Ich bin in diesen Fällen gesetzlich verpflichtet, Beanstandungen auszusprechen; lediglich bei unerheblichen Mängeln kann ich darauf verzichten (§ 20 Abs. 2 BDSG).

Bei dieser Rechtslage, die bei festgestellten Rechtsverletzungen keine Differenzierung erlaubt, kann allein aus der Tatsache der Beanstandung nicht auf die Schwere des Rechtsverstoßes geschlossen werden. Auch aus der folgenden Übersicht ergibt sich insoweit keine Gewichtung, da es dazu der Kenntnis des konkreten vollständigen Sachverhaltes bedarf. Deshalb wird wegen der Einzelheiten auf den jeweiligen Berichtsteil verwiesen, in dem die beanstandeten Vorgänge beschrieben sind.

Beanstandungen wurden im Berichtsjahr ausgesprochen gegenüber:

Bundesminister des Innern	Verstöße gegen das Bundesdatenschutzgesetz und gegen untergesetzliche Normen beim Bundeskriminalamt und der Grenzschutzdirektion (s. Nrn. 19.1, 19.2, 19.4, 19.5, 22.1, 22.2)
Bundesminister der Justiz	Verstöße gegen § 41 Abs. 1 Bundeszentralregistergesetz beim Bundeszentralregister (s. Nr. 5.1)
Bundesminister der Finanzen	Verstöße gegen das Bundesdatenschutzgesetz und gegen untergesetzliche Normen beim Zollkriminalinstitut und sonstigen Zollfahndungsdienststellen (s. Nr. 23)
Bundesminister für Wirtschaft	Nicht ordnungsmäßige Führung der Übersicht nach § 15 BDSG durch das Bundesamt für Wirtschaft (s. Nr. 25.1)
Bundesminister für Jugend, Familie, Frauen und Gesundheit	Verstoß gegen das Recht auf Auskunft nach § 13 BDSG durch das Ministerium (s. Nr. 17.3)

Bundesminister für Verkehr	— Unzulässige Datenübermittlung nach § 35 StVG durch das Kraftfahrt-Bundesamt (s. Nr. 9.3) — Unzulässige Datenübermittlung nach dem Straßenverkehrsunfallstatistikgesetz durch das Statistische Bundesamt (s. Nr. 10.2.2)
Bundesminister für das Post- und Fernmeldewesen	— Nicht ordnungsmäßiger PC-Einsatz in einem Fernmeldeamt (s. Nr. 7.5) — Nicht ordnungsmäßige Führung der Übersicht nach § 15 BDSG und Anmeldung der Dateien nach § 19 Abs. 4 BDSG bei der Deutschen Bundespost (s. Nr. 8.2.2) — Verstoß gegen § 6 BDSG im Zusammenhang mit der Nutzung des Bildschirmtextdienstes durch eine Postdienststelle (s. Nr. 8.4) — Verstoß gegen das Sozialgeheimnis durch eine Rentenrechnungsstelle (s. Nr. 8.7)
Bundesanstalt für Arbeit	Verstoß gegen das Sozialgeheimnis durch Arbeitsämter (s. Nr. 14.5 und auch Nr. 10.1)
Betriebskrankenkasse	Verstoß gegen das Sozialgeheimnis (s. Nr. 15.3)
Technikerkrankenkasse	Verstoß gegen das Sozialgeheimnis (s. Nr. 15.3)

2.3 Kooperation

Die Zusammenarbeit mit den Landesbeauftragten für den Datenschutz bzw. der Datenschutzkommission Rheinland-Pfalz sowie mit den Aufsichtsbehörden nach § 30 BDSG ist für mich nicht nur eine selbstverständlich zu erfüllende gesetzliche Pflicht, um durch den Austausch von Erfahrungen und das Bemühen um gemeinsame Beurteilungen für vergleichbare Sachverhalte eine möglichst einheitliche Anwendung der Datenschutzbestimmungen zu erreichen. Diese Zusammenarbeit liefert mir darüber hinaus Hinweise für meine Arbeit, und die erfolgenden Abstimmungen machen die dann gemeinsam geleistete Arbeit auch wirksamer. Dabei kommt der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und den von ihr eingesetzten Arbeitsgruppen besondere Bedeutung zu.

Die Hauptthemen der Konferenz waren

— am 23. Februar 1987
die Volkszählung 1987 und die dabei geplanten Datenschutzkontrollen

— am 4. und 5. Mai 1987
das Zentrale Verkehrsinformationssystem ZEVIS, die Neukonzeption des Ausländerzentralregisters und die Rückmeldungen durch die Justiz an die Polizei über den Ausgang von Strafverfahren

— am 7. Dezember 1987
die Speicherung von Hinweisen auf AIDS-Infektionen in polizeilichen Informationssystemen.

Auch außerhalb der Sitzungen der Konferenz kommt es besonders in den Fällen, in denen Behörden des Bundes mit denen der Länder Daten austauschen, häufig zur wechselseitigen Unterstützung bei der Klärung datenschutzrelevanter Sachverhalte, so zuletzt bei den Untersuchungen zur Mehrfachvergabe von Seriennummern für die neuen Personalausweise.

Die Zusammenarbeit mit den Aufsichtsbehörden der Länder für den Datenschutz im nicht-öffentlichen Bereich erfolgt — abgesehen von Arbeitskontakten — im sogenannten Düsseldorfer Kreis, an dessen Sitzungen meine Mitarbeiter regelmäßig teilnehmen. Schwerpunkte der Beratungen dort waren insbesondere

— die Weitergabe und Nutzung von Daten für Zwecke der Direktwerbung

— die datenschutzrechtlichen Pflichten der Wirtschafts- und Handelsauskunfteien

— die von den Versicherungen vorgeschriebenen Klauseln zum Datenschutz und zur Entbindung von der ärztlichen Schweigepflicht

— die von den Verbänden der Versicherungswirtschaft geführten Dateien zur Unterrichtung ihrer

Mitglieder über besondere Versicherungsrisiken und zur Vermeidung von Doppelversicherungsfällen.

Insbesondere auf dem Gebiet der technischen und organisatorischen Maßnahmen zur Datensicherung arbeite ich auch mit einigen Einrichtungen außerhalb der öffentlichen Verwaltung zusammen, die hier besondere Aktivitäten entwickeln. Dazu gehört seit Jahren die Arbeitsgemeinschaft für Wirtschaftliche Verwaltung e.V. (AWV), die in ihren Arbeitskreisen insbesondere Hilfen für die Praxis entwikkelt. Im Berichtsjahr wurde dort die AWV-Schrift 08/434 über „Datensicherheit in Netzen — Risiken und Maßnahmen" fertiggestellt. Auch in Arbeitsausschüssen des Deutschen Instituts für Normung e.V. (DIN) habe ich meine Mitwirkung, insbesondere bei der Normung von Einsatzbedingungen für Verschlüsselungsverfahren, fortgesetzt.

Schließlich konnte ich auch in diesem Jahr anläßlich eines Besuches bei einem bedeutenden Hersteller von Datenverarbeitungsanlagen und in mehreren Kontakten zu verschiedenen Computerfirmen mich über die Entwicklung auf dem Gebiet der Datenverarbeitung informieren und um Verständnis für die Forderung nach möglichst sicherer und kontrollierbarer Datenverarbeitung werben.

2.4 Öffentlichkeitsarbeit

Die von mir herausgegebenen Broschüren

— Bürgerfibel Datenschutz

— Der Bürger und seine Daten

— Der Bürger und seine Daten im Netz der sozialen Sicherung

sind abgesehen von gelegentlichen Überarbeitungen, seit Jahren unverändert geblieben; dennoch ist das Interesse daran nach wie vor groß. Im Berichtsjahr wurden davon insgesamt etwa 110000 Exemplare verschickt oder auf Veranstaltungen abgegeben. Nach der Art der Anfragen gehe ich davon aus, daß die Broschüren sehr oft als Unterrichtsmaterial sowohl an Schulen als auch durch Einrichtungen zur Erwachsenenbildung verwendet werden.

Von meinem Neunten Tätigkeitsbericht habe ich insgesamt etwa 6500 Exemplare an Journalisten und Behörden, aber auf Anfrage auch an interessierte Bürger verschickt, außerdem – meist zur Information über Einzelprobleme – auch Tätigkeitsberichte über weiter zurückliegende Berichtsjahre, soweit sie noch nicht vergriffen waren.

Mit der Betreuung von 46 Besuchergruppen im abgelaufenen Jahr hat diese Art der Öffentlichkeitsarbeit wiederum zugenommen. Die Besuche von Gruppen mit oft bis zu 50 Teilnehmern wurden fast immer auf Wunsch von Abgeordneten aus allen Fraktionen des Deutschen Bundestages im Rahmen von Bonn-Besuchen durch das Bundespresseamt oder auch im direkten Kontakt vereinbart. Auch wenn vor allem in reisegünstigen Wochen die Belastung der für die Betreuung eingesetzten Mitarbeiter recht hoch ist, halte ich diese Art von meist sehr offenen Diskussionen sowohl zur Information von Bürgern über meine Aufgaben und die Art ihrer Durchführung als auch zu meiner eigenen Information über die Besorgnisse und Meinungen der Bürger für sehr wichtig. Sie sind für mich eine nützliche Ergänzung zu den schriftlichen Kontakten, die weit überwiegend Fragen oder Beschwerden von Bürgern zu einzelnen speziellen Datenverarbeitungsfällen betreffen.

Teils aus besonderem Anlaß, aber auch zur allgemeinen Information haben meine Mitarbeiter und ich auf Wunsch von Journalisten zahlreiche Presse- und Rundfunkinterviews gegeben, und außer zur Vorstellung meines Neunten Tätigkeitsberichts habe ich mich auch sonst von mir aus an die Öffentlichkeit gewandt, wenn dies sachlich geboten war.

Bei verschiedenen Gelegenheiten, so z. B. auf der Datenschutz-Fachtagung DAFTA, in Vorträgen und im Rahmen von Fortbildungsveranstaltungen der Bundesakademie für öffentliche Verwaltung haben meine Mitarbeiter und ich für den Datenschutz geworben. Das Interesse an solchen Referaten ist groß, weil mit dem Vordringen von automatisierten Datenverarbeitungsverfahren an immer mehr Arbeitsplätze die Notwendigkeit zur entsprechenden Schulung der Mitarbeiter wächst. Ich nehme solche Gelegenheiten im Rahmen meiner Möglichkeiten gern wahr, weil sie mehr als die Kontrolltätigkeit geeignet ist, Verständnis für die Sicht der von Datenverarbeitung betroffenen Bürger zu wecken und damit Datenschutz zu einem regelmäßig zu beachtenden Prinzip zu machen.

2.5 Die Dienststelle

Die Personalsituation in meiner Dienststelle hat sich weiter verbessert. Für das Haushaltsjahr 1988 wurde mir auf parlamentarische Initiative eine weitere Stelle des höheren Dienstes bewilligt; dafür danke ich an dieser Stelle ausdrücklich. Dem in den letzten Jahren infolge der Ausweitung der Datenverarbeitung in der Bundesverwaltung zunehmend wachsenden Aufgabenvolumen entspricht der damit erreichte Personalstand indessen noch nicht, er bleibt auch immer noch hinter der Personalplanung des Jahres 1977 zurück. Die wesentlichen Gründe für den anhaltenden Personalbedarf meiner Dienststelle habe ich in meinem Neunten Tätigkeitsbericht (S. 11f.) geschildert. Zur Vermeidung von Wiederholungen verweise ich auf diese Ausführungen und beschränke mich hier auf zwei ergänzende Bemerkungen:

In den nächsten Jahren wird meine Dienststelle zusätzlich mit Kontrollen der Rechtmäßigkeit der aus dem Zentralen Verkehrsinformationssystem (ZEVIS) durch Bundesbehörden getätigten Abrufe, mit der Auswertung der aufgrund des § 36 Abs. 6 und 7 Straßenverkehrsgesetz (StVG) entstandenen Protokolle sowie mit der Erarbeitung von Hinweisen für mögliche Protokollauswertungen befaßt sein. Darüber hinaus wird ein weiterer Schwerpunkt meiner Tätigkeit in der Mitwirkung an dem dem Deutschen Bun-

destag zu erstattenden ZEVIS-Bericht liegen. Diese Mitwirkung erfordert vorherige systematische Kontrollen der ZEVIS-Abrufe, die sowohl die bundes- als auch die landesspezifischen Belange abdecken. Deshalb sind neben Einzelkontrollen des Bundes- und der Landesbeauftragten für den Datenschutz auch gemeinsame Kontrollen durchzuführen. Dies macht koordiniertes Vorgehen erforderlich. Sowohl die hierfür notwendigen vorbereitenden Arbeiten und die daraufhin durchzuführenden Kontrollen als auch die Umsetzung der gewonnenen Erkenntnisse werden Arbeitskapazitäten binden, die zu Lasten anderer Kontrollaufgaben und der Beratungstätigkeit gehen werden.

Nachdem mir im November 1987 der Entwurf eines Gesetzes zur Neufassung des Bundesdatenschutzgesetzes und des Verwaltungsverfahrensgesetzes zugegangen ist (s. u. Nr. 28) und weitere Gesetzentwürfe mit erheblicher datenschutzrechtlicher Bedeutung insbesondere für den Bereich der inneren Sicherheit oder beispielsweise auch auf dem Gebiet der gesetzlichen Krankenversicherung angekündigt worden sind, erwarte ich für die nächsten Jahre einen hohen Beratungsbedarf seitens der Gesetzgebungsorgane, aber auch seitens der Bundesressorts, die die Gesetzentwürfe vorbereiten. Dies wird ebenfalls erhebliche Arbeitskapazitäten meiner Dienststelle beanspruchen. Anders als den zuständigen Bundesressorts stehen mir für diese Aufgaben nur wenige Mitarbeiter zur Verfügung, die damit den Routinearbeiten gänzlich entzogen werden müssen. Dies läßt sich aus meiner Sicht auf die Dauer – und ich rechne mit langen Beratungszeiten dieser Gesetzgebungsvorhaben – nicht vertreten. Ich werde daher meine bisherigen Personalanforderungen auch in Zukunft mit Nachdruck weiterverfolgen.

3. Deutscher Bundestag

3.1 Neue Informations- und Kommunikationstechniken im Deutschen Bundestag (PARLAKOM)

Bereits in meinem Neunten Tätigkeitsbericht habe ich über die Einführung neuer Informations- und Kommunikationstechniken und -medien im Deutschen Bundestag (PARLAKOM) berichtet und auf einige Datenschutzprobleme aufmerksam gemacht. Die PARLAKOM-Planung sieht vor, in einem dreistufigen Ausbau bis zum Jahre 1990 Systeme zur Verbesserung der Kommunikation im Gesamtwert von DM 120 Mio. zu beschaffen. Dafür sollen in erster Linie die Büros der Abgeordneten — sowohl in Bonn als auch in ihren Wahlkreisen — mit kleinen Computern ausgestattet werden, die neben einem eigenen Drucker auch über Kommunikationsmöglichkeiten mit Diensten der Deutschen Bundespost, wie Teletex, Bildschirmtext und Telebox, verfügen und deshalb auch zur Abfrage von Datenbanken auf anderen Rechnern geeignet sind. Ende 1986 begann ein Modellversuch, an dem fünfzig Abgeordnete teilnehmen und in den auch zwanzig Arbeitsplätze in der Verwaltung des Deutschen Bundestages einbezogen sind.

Bei technischen Projekten von dieser Größenordnung und Komplexität ist es gerade für die Lösung der Datenschutzprobleme von besonderer Bedeutung, daß eine übergeordnete, leistungsfähige Projektorganisation nicht nur Lieferungen und Installationen der Herstellerfirmen koordiniert, sondern auch das Zusammenwirken der betroffenen Organisationseinheiten des Anwenders sicherstellt — hier: der jeweils für die Teilbereiche zuständigen Referate der Bundestagsverwaltung. Anderenfalls entstehen nach meinem Eindruck Koordinationsprobleme, die leicht zu störenden Verzögerungen führen können. So hatte z. B. die Kommission des Ältestenrates des Deutschen Bundestages für den Einsatz neuer Informations- und Kommunikationstechniken und -medien in ihrem Beschluß vom 13. 10. 1986 dringend empfohlen, „unverzüglich die Erarbeitung eines integrierten Datenschutz- und Datensicherungskonzeptes im Deutschen Bundestag in Angriff zu nehmen und bis zum Ende der 10. Legislaturperiode vorzulegen." Dies ist bis heute nicht geschehen.

Das vom Ältestenrat für PARLAKOM eingesetzte Datenschutzgremium hatte bereits im Dezember 1986 einen Katalog von fünf Schutzmaßnahmen erarbeitet und deren Umsetzung der Verwaltung des Deutschen Bundestages empfohlen. Der Katalog enthält aus meiner Sicht wertvolle Hinweise und Maßnahmen zur Sicherstellung des Datenschutzes. Mir konnte bislang allerdings nicht die Frage beantwortet werden, in welchem Umfange die Verwaltung diesen Empfehlungen bereits nachgekommen ist; schriftliche Dienstanweisungen dazu sind meines Wissens jedenfalls nicht ergangen.

Als Fortschritt aus der Sicht des Datenschutzes ist hingegen die am 19. Mai 1987 zwischen dem Personalrat und der Leitung der Verwaltung des Deutschen Bundestages getroffene „Dienstvereinbarung über den Einsatz von Informations- und Kommunikationstechniken" zu sehen, die auch PARLAKOM umfaßt und in der auch Probleme des Datenschutzes aufgegriffen wurden. So lassen beispielsweise die Regelungen über die automatisierte Telefondatenerfassung die Registrierung der Zielnummer, d. h. der Telefonnummer des Angerufenen, nicht zu. Dies entspricht einer von mir wiederholt erhobenen Forderung, die einer Beeinträchtigung der schutzwürdigen Belange sowohl des Anrufers als auch des Angerufenen entgegenwirken soll.

Die Verwaltung des Deutschen Bundestages hat mich über ihre Absicht informiert, den PARLAKOM-Nutzern aus dem parlamentarischen Bereich im Rahmen der Anwenderberatung auch kurzgefaßte Hinweise zu Fragen des Datenschutzes und der Datensicherung zu geben. Ich habe auch hierzu meine weitere Beratung angeboten.

3.2 Einsichtsrecht in Akten des Petitionsausschusses

Ein Petent hat im Laufe seiner Auseinandersetzungen mit der Arbeitsverwaltung eine Petition an den Deutschen Bundestag gerichtet. Beim Bundesministerium für Arbeit und Sozialordnung (BMA) be-

gehrte er Einsicht in die dort über ihn geführten Personalunterlagen, um feststellen zu können, welche dieser Unterlagen an den Petitionsausschuß weitergegeben wurden. Nach Ablehnung seines Antrages wandte er sich an mich mit der Bitte, ihm entweder Einblick in die über ihn geführten Unterlagen des BMA oder in die Akten des Petitionsausschusses zu verschaffen. Der Beschwerdefall hat sich inzwischen zur Zufriedenheit des Petenten erledigt, nachdem ich die über ihn beim BMA geführten Personalakten eingesehen und keinerlei Anhaltspunkte für die von ihm befürchteten Informationen bzw. deren Übermittlung an den Petitionsausschuß gefunden habe.

Dieser Beschwerdefall gab mir Anlaß, mich mit der geltenden Regelung des Einsichtsrechts in Petitionsakten zu befassen. Nach § 16 der Geschäftsordnung des Deutschen Bundestages ist lediglich Abgeordneten, nicht aber auch dem Petenten die Einsichtnahme in die Petitionsunterlagen gestattet. Ich halte es vor dem Hintergrund der Rechtsprechung des Bundesverfassungsgerichts über das Recht auf informationelle Selbstbestimmung für erwägenswert, in das Gesetz über die Befugnisse des Petitionsausschusses des Deutschen Bundestages vom 19. Juli 1975 (BGBl. I S. 1921) ein Auskunftsrecht des Petenten nach dem Vorbild des § 13 BDSG oder des § 29 VwVfG aufzunehmen. Eine solche Lösung drängt sich auch im Vergleich mit der Verfahrenspraxis im Prozeßwesen auf, derzufolge jede Partei regelmäßig auch die von der Gegenseite in den Prozeß eingebrachten Schriftsätze und sonstigen Unterlagen erhält.

Auf meine entsprechende Anregung hat mir der Vorsitzende des Petitionsausschusses mitgeteilt, er werde die Problematik in die Beratungen des Ausschusses zu den Verfahrensgrundsätzen für die laufende Wahlperiode einbeziehen. Es liege sicherlich auch im Interesse des Petitionsausschusses, seine Verfahren für den Bürger so offen wie möglich zu gestalten, damit dieser, wenn er es wünsche, sich auch selbst von der Ordnungsmäßigkeit des Verfahrens überzeugen könne.

4. Innere Verwaltung

4.1 Asylverfahren

Beim Bundesamt für die Anerkennung ausländischer Flüchtlinge (BAFl) haben meine Mitarbeiter im zurückliegenden Jahr eine datenschutzrechtliche Kontrolle durchgeführt, die erwartungsgemäß ergab, daß der Schwerpunkt der Informationsverarbeitung durch diese Behörde außerhalb von Dateien liegt. Soweit einzelne Dateien existieren, sind einige formale Anforderungen des BDSG, so z. B. bezüglich der Führung einer Übersicht, noch nicht erfüllt; mir wurde zugesagt, daß dies bald nachgeholt wird.

Einem Anliegen des Bundesministers des Innern entsprechend nahm die Nutzung von in Akten enthaltenen personenbezogenen Daten breiten Raum ein. Dabei standen Feststellungen über Informationsbeziehungen zu verschiedenen Stellen außerhalb des BAFl im Vordergrund. Die Erörterung mit dem Bundesminister des Innern hinsichtlich der hieraus zu ziehenden Folgerungen ist noch nicht abgeschlossen. In einer Reihe von Punkten konnte ich bereits technisch-organisatorische Maßnahmen zur Verbesserung der Datensicherheit empfehlen.

Die an anderer Stelle (Nr. 17.2) unter allgemeinen datenschutzrechtlichen Aspekten behandelte AIDS-Problematik spielt auch im Asylverfahren eine Rolle. Hinweisen von Landesbeauftragten für den Datenschutz habe ich entnommen, daß in einigen Bundesländern die Asylbewerber routinemäßig ärztlich untersucht werden. Die Untersuchungen erstrecken sich teilweise auch auf eine HIV-Infektion, werden aber übewiegend auf andere Krankheiten beschränkt.

Von den zuständigen Landesministerien wird als Rechtsgrundlage für diese Untersuchungen auf § 2 Abs. 1 i.V.m. § 10 Abs. 1 Nr. 9 des Ausländergesetzes und zum Teil auf § 10 Abs. 1 und 3 des Bundesseuchengesetzes verwiesen. Die Heranziehung dieser Vorschriften ist problematisch. Der Hinweis auf § 2 Abs. 1 i.V.m. § 10 Abs. 1 Nr. 9 des Ausländergesetzes erscheint nicht zutreffend, weil dort ein Antrag des Ausländers auf eine Aufenthaltserlaubnis vorausgesetzt wird. Asylbewerber stellen jedoch im Regelfall keinen Antrag auf Erteilung einer Aufenthaltserlaubnis; ihnen ist bereits von Gesetzes wegen der Aufenthalt zur Durchführung des Asylverfahrens gestattet (§ 19 Abs. 1 i.V.m. § 20 Abs. 1 Asylverfahrensgesetz). Eine ärztliche Untersuchung nach § 10 Abs. 1 und 3 des Bundesseuchengesetzes ist nur zulässig, wenn im Einzelfall anzunehmen ist, daß Tatsachen vorliegen, die zum Auftreten einer übertragbaren Krankheit führen können. Dies setzt jeweils eine entsprechende Prüfung im Einzelfall voraus. Nicht bei jedem Asylbewerber besteht aber generell ein Anlaß, von einer solchen Gefahr auszugehen.

Auch bezüglich der Möglichkeit, § 20 Abs. 2 Satz 1 des Asylverfahrensgesetzes heranzuziehen, sehe ich enge Grenzen. Nach dieser Vorschrift kann die Aufenthaltsgestattung mit Auflagen versehen werden. Nach meinem Verständnis darf dies nur nach Maßgabe differenzierender Kriterien, jedenfalls nicht allgemein und routinemäßig geschehen. Im übrigen handelt es sich hier um eine nicht hinreichend bestimmte Regelung, die nur in der — hier nicht interessierenden — Weise konkretisiert ist, daß räumliche Beschränkungen auferlegt werden können. Bei der zwangsweisen ärztlichen Untersuchung von Asylbewerbern handelt es sich jedoch um einen so weitgehenden Eingriff in die Persönlichkeitsphäre, daß dafür im Hinblick auf das Gebot der Normenklarheit präzisere Gesetzesvorschriften geschaffen werden sollten, falls seine Erforderlichkeit im überwiegenden Allgemeininteresse bejaht wird.

Ich habe den Bundesminister des Innern und den Bundesminister für Jugend, Familie, Frauen und Gesundheit um eine Stellungnahme gebeten.

4.2 Neue Personalausweise und Pässe

4.2.1 Datensicherung bei der Bundesdruckerei

Seit Inkrafttreten des Gesetzes über Personalausweise am 1. April 1987 werden — schrittweise mit Ablauf gültiger Ausweise — neue fälschungssichere und maschinell lesbare Personalausweise ausgegeben, die bei der Bundesdruckerei hergestellt werden. Entsprechend einer auch von mir gegebenen Anregung (vgl. 9. TB S. 14) wurde das Verfahren der Herstellung im Februar 1987 erprobt. Dabei wurden örtliche Personalausweisbehörden beteiligt. Auch das Verfahren zur Herstellung der neuen Pässe wurde erprobt. Ich habe mich bei der Bundesdruckerei über beide Probebetriebe informiert.

Die Bundesdruckerei ist schon wegen ihrer sonstigen Aufgaben ein Betrieb, der es gewohnt ist, ein hohes Maß an technischen und organisatorischen Maßnahmen zur Datensicherung zu erfüllen. Meine ergänzenden Anregungen zur Verbesserung der Sicherheit bei der Herstellung der Ausweise und der Pässe wurden daher überwiegend akzeptiert und übernommen. In der Bundesdruckerei wurde eine neue Abteilung mit der Aufgabe „Herstellung personalisierter Dokumente" gebildet. Zu dieser Abteilung gehört eine eigene Datenverarbeitung, die ausschließlich der Herstellung der Dokumente (z. Z. Personalausweis und Paß) dient. Ferner wurde in dieser Abteilung eine Gruppe eingerichtet, die die sichere Herstellung der Dokumente kontrolliert und gegebenenfalls verbessert.

Die Bundesdruckerei darf nach § 3 Abs. 3 des Gesetzes über Personalausweise alle Seriennummern zentral speichern. Diese zentrale Sammlung dient ausschließlich zum Nachweise des Verbleibs der Ausweise. Alle übrigen personenbezogenen Angaben der Betroffenen, die die Bundesdruckerei von den Personalausweisbehörden erhält, um die Ausweise produzieren zu können, werden im Anschluß an die Herstellung der Ausweise gelöscht.

4.2.2 Allgemeine Verwaltungsvorschriften

Der Bundesminister des Innern hat mich bei der Vorbereitung von Rechtsvorschriften und allgemeinen Verwaltungsvorschriften zum Paßgesetz beteiligt. Die ursprüngliche Absicht, in den Verwaltungsvorschriften bei Paßbewerbern, die keine Wohnung haben, den Paßeintrag „ohne festen Wohnsitz" vorzusehen, wurde auf Grund meiner Bedenken dahin geändert, daß bei Paßbewerbern ohne Wohnung der derzeitige Aufenthaltsort eingetragen wird. Diese Regelung ist datenschutzfreundlich, weil damit im Paß Personen ohne festen Wohnsitz nicht besonders gekennzeichnet werden.

Hinweise von Bürgern haben gezeigt, daß die Bedeutung der Unterschrift im Antrag auf Ausstellung eines Personalausweises oder Passes nicht immer verstanden wird. Die Unterschrift ist an bestimmter Stelle im sogenannten Grundblankett des Antrages zu leisten. Mit ihr wird aber nicht lediglich die Richtigkeit der Angaben des Antrages bestätigt, sondern sie ist zugleich ein zusätzliches Identitätsmerkmal: Die Bundesdruckerei reproduziert die Unterschrift in das Ausweisdokument. Hinreichende Qualität der Reproduktion vorausgesetzt, ist es daher auch datenschutzrechtlich unproblematisch, daß es sich im Paß und auf dem Personalausweis nicht um die Originalunterschrift handelt, sondern eben nur um deren Reproduktion. Auf meine Anregung hat der Bundesminister des Innern zur Verdeutlichung die Allgemeinen Verwaltungsvorschriften um den Satz „die Unterschrift erfüllt die Funktion eines Identitätsmerkmals" ergänzt.

4.2.3 Mehrfachvergabe der Seriennummer

Im November/Dezember 1987 wurde in den Medien darüber berichtet, daß es bei der Ausgabe der neuen maschinenlesbaren und fälschungssicheren Personalausweise Pannen gegeben habe. Es hat sich herausgestellt, daß ca. 4000 Bürger gültige Personalausweise erhalten haben, deren Seriennummern jedoch schon vergeben waren, also in anderen ebenfalls gültigen Personalausweisen standen. Die Personalausweisbehörden haben diese gültigen und dennoch fehlerhaften Personalausweise zurückgefordert, die Betroffenen mußten erneut einen Ausweis beantragen. Zunächst wurde dafür der Datenschutz verantwortlich gemacht. Dieser Vorwurf trifft nicht zu. Sowohl aus Gründen des Datenschutzes wie auch im Interesse der öffentlichen Sicherheit ist es gerade erforderlich, daß jeder Ausweis mit einer einmaligen Seriennummer versehen wird. Dies wäre besser gewährleistet, wenn die Seriennummer statt durch die örtliche Ausweisbehörde direkt bei der Herstellung des Ausweises durch die Bundesdruckerei zentral vergeben würde. Dagegen könnten aus der Sicht des Datenschutzes schon deshalb keine Bedenken bestehen, weil nach dem Gesetz ohnehin alle vergebenen Seriennummern — ohne sonstige Ausweisdaten — bei der Bundesdruckerei dauerhaft gespeichert werden. Damit habe ich mich schon 1979 ausdrücklich einverstanden erklärt und außerdem in den vergangenen Jahren wiederholt beim Bundesinnenminister Vorkehrungen gegen eine Mehrfachvergabe der Seriennummer gefordert.

Meine sehr ausführlichen und nachdrücklichen Empfehlungen zur Vermeidung der Mehrfachvergabe von Seriennummern habe ich nach meinem ersten Informationsbesuch bei der Bundesdruckerei im September 1985 dem Bundesinnenminister zugeleitet. In diesem Schreiben habe ich mich nach Maßnahmen erkundigt, die bei den rund 4300 Personalausweisbehörden der Länder sicherstellen, daß die Einmaligkeit der Seriennummer von diesen garantiert wird, und empfohlen, bei der Bundesdruckerei Verfahren vorzusehen, die eine Mehrfachvergabe von Seriennummern ausschließen.

Die fortlaufende Vergabe der Seriennummern der Personalausweise ist Aufgabe der Personalausweisbehörden. Das Personalausweisgesetz enthält keine Vorschrift, die einer Kontrolle der korrekten Vergabe der Seriennummern durch die Bundesdruckerei im Wege steht, oder aber sie dazu verpflichtet, eine solche Kontrolle im Rahmen der Herstellung der Ausweise vorzunehmen. Die Bundesdruckerei hat

im übrigen ebenfalls auf die Probleme der Mehrfachvergabe der Seriennummer und deren Bedeutung als wichtiger Garant gegen Verfälschungen aufmerksam gemacht. Da die Bundesdruckerei ohnehin alle die Daten besitzt, die es ihr ermöglichen, festzustellen, ob eine Seriennummer nur einmal vergeben wurde, liegt es nahe, dort ein Verfahren vorzusehen, mit dem sichergestellt wird, daß kein Ausweis mit einer schon einmal vergebenen Seriennummer die Bundesdruckerei verläßt.

Der Bundesminister des Innern hat mir im Dezember 1985 geantwortet, daß die Vorschrift des Personalausweisgesetzes, wonach die Seriennummern *fortlaufend* zu vergeben sind, und die zusätzlichen Durchführungsbestimmungen der Länder gewährleisten, daß eine Seriennummer nicht mehrfach vergeben wird. Das entspreche auch den Sicherungsmaßnahmen für die personenbezogenen Daten auf dem Ausweis. Er hat u. a. festgestellt: „Bei dieser Sachlage wird die Einführung eines zentralen Verfahrens zum Erkennen einer etwaigen Mehrfachvergabe der Seriennummer bei der Bundesdruckerei nicht für erforderlich gehalten. Im übrigen würde ein solches Verfahren Mehrkosten in unvertretbarer Höhe sowie erheblichen Mehrbedarf an Raum und Zeit erfordern".

Da ich weiter auf meinem Anliegen bestand, hat der Bundesinnenminister schließlich doch noch Kontrollmaßnahmen vorgesehen und mir dies im Oktober 1986 mitgeteilt. Danach wird frühestens nach Ablauf von 28 Tagen nach Fakturierung von der Bundesdruckerei die Mehrfachvergabe einer Seriennummer festgestellt. Darüber werden die Innenministerien der Länder und der Bundesinnenminister mit sogenannten Warnlisten informiert. Es liegt dann in der Zuständigkeit der Länder, die Ursache für die Mehrfachvergabe zu ermitteln, den gültigen, aber fehlerhaften Ausweis zurückzufordern und für dessen ordnungsmäßige Vernichtung zu sorgen.

Ich habe ebenfalls im Oktober 1986 dem Bundesinnenminister mitgeteilt, daß mit diesem Verfahren (mit dem eben leider Fehler nur nachträglich entdeckt werden) der datenschutzrechtlichen Mitverantwortung, die der Bund im Hinblick auf die Gewährleistung fortlaufender Vergabe der Seriennummern bzw. die Aufdeckung einer Mehrfachvergabe hat, in angemessener Weise Rechnung getragen wird. Ich habe aber auch darauf hingewiesen, daß es außerhalb meiner Zuständigkeit liegt, zu bewerten, ob die Zeit, die zwischen dem Versand der Personalausweise an die Ausweisbehörde und der Aufdekkung einer Mehrfachvergabe bzw. deren Mitteilung an die zuständige Behörde verstreicht, den Anforderungen der Sicherheitsbehörden genügt.

Aufgrund der nunmehr bekannt gewordenen Fälle und der öffentlichen Diskussion hierzu habe ich dem Bundesinnenminister erneut empfohlen, die Bundesdruckerei anzuweisen, zumindest bei der jetzt anlaufenden Herstellung der Pässe eine Mehrfachvergabe zu unterbinden. Eine endgültige Entscheidung über die bei der Bundesdruckerei zu treffenden Maßnahmen, um vergleichbare Pannen wie beim Personalausweis zu vermeiden, stand zum Zeitpunkt der Erstellung dieses Berichts noch aus.

4.3 Personenstandswesen

Zu dem vom Bundesminister des Innern erarbeiteten Vorentwurf eines Fünften Gesetzes zur Änderung und Ergänzung des Personenstandsgesetzes (5. PStÄndG) habe ich über eine Einzelfrage — nämlich die Erhebung von Daten über den Nachlaß Verstorbener durch den Standesbeamten — bereits in meinem Neunten Tätigkeitsbericht (S. 16 f.) berichtet. Inzwischen habe ich dem Bundesminister des Innern eine umfassende Stellungnahme zu dem Vorentwurf übersandt.

Gegenüber dem geltenden Recht sind deutliche datenschutzrechtliche Verbesserungen zu verzeichnen. Positiv bewerte ich insbesondere die Absicht,

- die Mitteilungspflichten des Standesbeamten gesetzlich zu verankern,
- die Einsicht in die Personenstandsbücher und die Erteilung von Auskünften und Urkunden präziser zu regeln, insbesondere eigenständige Vorschriften über die Auskunft bzw. Einsicht für Zwecke wissenschaftlicher Forschung zu schaffen,
- das öffentliche Aufgebot wegfallen zu lassen (Streichung des geltenden § 3 PStG, Änderung des Ehegesetzes).

Ich habe u. a. empfohlen, auf die Angabe des Berufes in den Personenstandsbüchern zu verzichten. Die Angabe des Berufes ist für die Beurkundung nicht erforderlich. Für Identifizierungszwecke stehen genügend andere Merkmale zur Verfügung. Die Angabe kann zudem rasch veralten und ist wegen ihrer begrifflichen Ungenauigkeit für die Identifizierung auch wenig geeignet. Es bleibt weitgehend dem Betroffenen überlassen, ob er seinen erlernten oder ausgeübten Beruf angibt und welche Bezeichnung er dafür wählt, während die übrigen Eintragungen in die Personenstandsbücher präzise geregelt sind.

Ich habe außerdem Überlegungen des Bundesministers des Innern unterstützt, die Berechtigung von Behörden und bestimmten öffentlichen Stellen, Auskunft und Einsicht in Personenstandseinträge sowie die Erteilung von Personenstandsurkunden zu erhalten, in einer gesonderten Vorschrift zu regeln. Eine „Durchsicht dieser Bücher", wie sie bislang § 61 PStG vorsieht, sollte künftig weder Behörden und bestimmten öffentlichen Stellen noch anderen Personen erlaubt sein.

Auch das Vorhaben, die Gewährung von Informationen zum Zwecke wissenschaftlicher Forschung gesetzlich zu regeln, wird von mir unterstützt. Dabei sollte prinzipiell die Einwilligung der Betroffenen gefordert werden. Auf die Einwilligung könnte ausnahmsweise dann verzichtet werden, wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens das Geheimhaltungsinteresse des

Betroffenen erheblich überwiegt, die Einholung der Einwilligung nicht möglich ist und der Zweck des Forschungsvorhabens auf andere Weise nicht erreicht werden kann. Im Falle der Einwilligung wie auch im Ausnahmefalle bedarf es einer gesetzlichen Bindung der Datenverwendung an den Zweck des im Auskunftsersuchen bestimmten Forschungsvorhabens. Nur bei möglichst konkreter Bestimmung des Forschungsprojekts kann eine rechtsverbindliche Einwilligung zustandekommen; auch im Falle der subsidiär zulässigen Datenweitergabe auf gesetzlicher Grundlage verlangt die dann erforderliche Güterabwägung eine genaue Kenntnis des Forschungszwecks. Soweit zwischen wissenschaftlicher Forschung und Ahnenforschung oder zeitgeschichtlicher Forschung differenziert wird, bedarf es — besonders mit Blick auf erhebliche Abgrenzungsprobleme in der Praxis — näherer Präzisierung.

Für Orts- bzw. Zeitangaben in Urkunden, namentlich in Sterbeurkunden, sollte eine Regelung gefunden werden, durch die Peinlichkeiten für die Betroffenen vermieden werden. Insbesondere sollten Sterbeurkunden so gefaßt werden, daß sie Dritten keinen Anlaß zu Spekulationen über die näheren Umstände des Todes geben. Ich konnte insoweit an frühere Empfehlungen (vgl. 6. TB S. 12f.) anknüpfen.

Neben den Vorschriften über die Informationsgewährung auf Ersuchen durch den Standesbeamten bedarf es präziser Rechtsgrundlagen für seine amtlichen Mitteilungspflichten. Die als Mitteilungsempfänger vorgesehenen Behörden und Stellen sollten im Gesetz abschließend genannt, der Umfang der Mitteilungsinhalte beschrieben und klargestellt werden, daß die Mitteilung der Angaben nur zu einem bestimmten Verwendungszweck erfolgt, der in der Zuständigkeit des Empfängers liegt und gesetzlich bestimmt ist.

Außerdem habe ich darauf hingewiesen, daß die Frage, an welche Meldebehörde die Mitteilung über die Geburt eines Kindes zu richten ist, gesetzlich geklärt werden muß, wenn sich im Zusammenhang mit der Geburt Anhaltspunkte dafür ergeben, daß das Kind für eine Adoptionsvermittlung in Betracht kommt, es also nicht in die Hauptwohnung der leiblichen Eltern bzw. der Mutter aufgenommen, sondern in Adoptionspflege gegeben wird. Da § 1747 Abs. 3 Satz 1 BGB bestimmt, daß die Einwilligung der Eltern bzw. der Mutter eines nichtehelichen Kindes in eine Adoption erst erteilt werden kann, wenn das Kind acht Wochen alt ist, wäre an sich die Geburtsmitteilung an die für die Hauptwohnung der Eltern bzw. der Mutter eines nichtehelichen Kindes zuständige Meldebehörde zu richten. Die Entscheidung, ob die Mitteilung an diese Meldebehörde oder aber an die Meldebehörde der Pflegeeltern erfolgt, sollte jedoch im Falle des Vorliegens derartiger Anhaltspunkte erst getroffen werden, wenn feststeht, ob und ggf. zu wem das Kind in Adoptionspflege gegeben wird.

4.4 Waffengesetz

Nachdem der Entwurf eines Dritten Gesetzes zur Änderung des Waffengesetzes in der 10. Legislaturperiode nicht mehr verabschiedet worden ist, strebt die Bundesregierung eine Novellierung dieses Gesetzes in der 11. Legislaturperiode an. Der Bundesminister des Innern hat mir hierzu einen überarbeiteten Gesetzentwurf zugeleitet, zu dem ich Stellung genommen habe. Ich habe empfohlen, bei der Bearbeitung eines Antrags auf Erteilung einer waffenrechtlichen Erlaubnis Auskünfte bei anderen Behörden nicht — wie vorgesehen — ohne Mitwirkung bzw. Wissen des Antragstellers einzuholen. Ansätze für meine Auffassung sehe ich sowohl in § 31 Bundeszentralregistergesetz als auch in § 93 Abs. 1 Satz 3 Abgabenordnung und nicht zuletzt auch im Beschluß des Bundesgerichtshofs vom 22. Mai 1985 (AnwZ [B] 42/84), in dem es — wenn auch bezogen auf die Zulassung zur Rechtsanwaltschaft — u. a. heißt: „Da der Bewerber ein Selbstbestimmungsrecht insofern hat, als er es in der Hand hat, ob er überhaupt ein Zulassungsgesuch stellt, entspricht es dem Gesamtcharakter des Zulassungsverfahrens besser, ihm auch hinsichtlich seiner Mitwirkung eine Art begrenzte Dispositionsbefugnis einzuräumen, verbunden mit möglichen ihm nachteiligen verfahrensrechtlichen Folgen für den Fall einer Auskunftsverweigerung".

Ferner habe ich Bedenken gegen eine *routinemäßige* Übermittlung personenbezogener Daten zur Unterrichtung der Polizeibehörden über den Erlaß von Waffenbesitzverboten geltend gemacht und vorgeschlagen, dies nur *einzelfallbezogen* zuzulassen.

Ich bedauere, daß der Bundesminister des Innern meine Empfehlungen in den inzwischen durch das Kabinett verabschiedeten Gesetzentwurf nicht aufgenommen hat.

4.5 Selbstschutz-Lehrgänge

Nach § 13 Abs. 2 der Allgemeinen Verwaltungsvorschrift für Aufbau, Förderung und Leitung des Selbstschutzes (Vwv-Selbstschutz) werden Namen und Anschriften der Teilnehmer an Selbstschutz-Lehrgängen des Bundesverbandes für den Selbstschutz (BVS) nach jeder Veranstaltung der Gemeinde mitgeteilt, in der der Teilnehmer seinen Wohnsitz hat. Der Landesbeauftragte für den Datenschutz Nordrhein-Westfalen hat bereits in seinem Achten Tätigkeitsbericht aufgrund einer Eingabe auf die mit diesem Eingriff in das Recht auf informationelle Selbstbestimmung der Lehrgangsteilnehmer verbundenen datenschutzrechtlichen Probleme hingewiesen. Auch ich halte die Mitteilung von Namen und Anschriften der Lehrgangsteilnehmer ohne deren Einwilligung für bedenklich.

Eine gesetzliche Grundlage für die Unterrichtung der Gemeinde über diese Daten der Lehrgangsteilnehmer besteht nicht. Insbesondere kann § 10 BDSG nicht herangezogen werden, wonach die Übermittlung personenbezogener Daten an Behörden oder sonstige öffentliche Stellen u. a. zulässig ist, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit des Empfängers liegenden Aufgaben erforderlich ist. Es trifft zwar zu, daß die Gemeinde darauf

angewiesen ist, für die Durchführung ihrer Selbstschutzaufgaben interessierte und geeignete Bürger zur Mitarbeit zu gewinnen. Diese Bürger werden sich gerade auch im Kreis der Teilnehmer von Lehrgängen des BVS befinden. Für die Gemeinde bedeutet es eine entscheidende und auch unverzichtbare Hilfe, Personen ansprechen zu können, die durch freiwillige Teilnahme an einem solchen Lehrgang ihr Interesse am Selbstschutz bekundet haben.

Die in § 13 Abs. 2 Vwv-Selbstschutz vorgesehene Mitteilung ist dennoch nicht zwingend geboten. Der Zweck dieser Datenweitergabe an die Gemeinde kann auch auf andere, weniger belastende Weise erreicht werden.

Ich habe dem Bundesminister des Innern empfohlen, in Zukunft bereits während der Lehrgänge des BVS mit Informationen an die Teilnehmer heranzutreten, die sie bisher von der Gemeinde erhalten haben, d. h. mit Informationen über weiterführende Lehrgänge und Übungen sowie über die mögliche Übernahme von Funktionen im Selbstschutz. Neben der Verteilung von Informationsmaterial und mündlichen Hinweisen würde dies auch eine gezielte Ansprache durch Vertreter der Gemeinde nicht ausschließen. Eine Weitergabe personenbezogener Daten der Teilnehmer ohne deren Einwilligung sollte jedoch unterbleiben.

Der Bundesminister des Innern ist dieser Empfehlung gefolgt und hat dem BVS gegenüber dargelegt, § 13 Abs. 2 Vwv-Selbstschutz könne von der Zweckbestimmung her nur dahingehend ausgelegt werden, daß die Daten solcher Lehrgangsteilnehmer zu übermitteln sind, die zur Mitarbeit an der gesetzlichen Verpflichtung der Gemeinden zum Aufbau des Selbstschutzes auch bereit sind. Der BVS wurde zugleich gebeten, bei Ausbildungsveranstaltungen entsprechend meiner Empfehlung zu verfahren und die Weitergabe von Daten von Lehrgangsteilnehmern nicht generell und automatisch zu handhaben. Ich begrüße dieses Ergebnis. Bei sich bietender Gelegenheit sollte der Wortlaut des § 13 Abs. 2 Vwv-Selbstschutz entsprechend der getroffenen Regelung präzisiert werden.

4.6 Zivildienst

4.6.1 Aufbewahrung von Anerkennungsunterlagen

Bereits in meinem Neunten Tätigkeitsbericht (S. 18) habe ich auf das Fehlen einer — meines Erachtens gesetzlich zu treffenden — Festlegung hingewiesen, für welchen Zeitraum Anerkennungsunterlagen der Kriegsdienstverweigerer aufzubewahren sind und welche Daten aus diesen Unterlagen für welche Zwecke genutzt werden dürfen. Bisher ist die Aufbewahrung und gegebenenfalls Verwendung der Anerkennungsunterlagen bis zum Ablauf der Zivildienstpflicht des Betroffenen im Verteidigungsfall, d. h. bis zur Vollendung des 60. Lebensjahres, vorgesehen. Mir erscheint nach wie vor zweifelhaft, ob unter Umständen sehr lange zurückliegende Erklärungen, Zeugenaussagen und Verhandlungsprotokolle über die Gewissensgründe noch eine tragfähige Grundlage für eine dann zu treffende Einsatzentscheidung sein können.

Der Bundesminister für Jugend, Familie, Frauen und Gesundheit ist mit dieser Problematik immer noch befaßt; von einem Regelungsvorschlag habe ich bislang nichts erfahren.

4.6.2 Abrechnung von Heilfürsorgemaßnahmen

Das Bundesamt für den Zivildienst (BAZ) ist für die Zivildienstleistenden Träger der Heilfürsorge nach § 35 Abs. 1 Zivildienstgesetz (ZDG). Im Zusammenhang mit der Abrechnung der Heilfürsorgemaßnahmen stellte sich die Frage, ob das BAZ in Ausnahmefällen (z. B. bei besonders hohen Behandlungskosten) unter Berufung auf Vorschriften des Sozialgesetzbuches (SGB) oder der Reichsversicherungsordnung (RVO) von behandelnden Ärzten oder Krankenhäusern Arztberichte anfordern darf.

Gegen ein solches Auskunftsverlangen habe ich rechtliche Bedenken. Eine entsprechende Anforderung gegenüber Ärzten oder Krankenhäusern kann nicht auf § 100 SGB X gestützt werden, da die dort geregelte Auskunftspflicht nur gegenüber einem Leistungsträger im Sinne des Sozialgesetzbuches besteht. Diese Leistungsträger sind nach § 12 SGB I die in den §§ 18 bis 29 SGB I genannten Körperschaften, Anstalten und Behörden, die die in diesem Gesetzbuch vorgesehenen Dienst-, Sach- und Geldleistungen (Sozialleistungen) erbringen (§ 11 SGB I). Weder ist das BAZ danach Leistungsträger, noch sind die vom BAZ im Rahmen der Heilfürsorge nach § 35 Abs. 1 ZDG zu erbringenden Leistungen Sozialleistungen. Ebensowenig können die Vorschriften der RVO über die kassenärztliche Versorgung bei der Gewährung der Heilfürsorge nach § 35 Abs. 1 ZDG unmittelbar Anwendung finden; § 35 ZDG macht die Zivildienstleistenden nicht zu Versicherungspflichtigen nach der RVO. Das BAZ teilt meine Rechtsauffassung und wird Arztberichte zwecks Überprüfung von Abrechnungen nicht anfordern.

4.6.3 Arbeitsberichte von Zivildienstleistenden

Über angestrebte datenschutzrechtliche Verbesserungen in der Gestaltung von Wochenarbeitsberichten der Zivildienstleistenden habe ich schon in meinem letzten Tätigkeitsbericht berichtet (9. TB S. 18f.).

Der Bundesminister für Jugend, Familie, Frauen und Gesundheit hat mir inzwischen den Entwurf einer Dienstanweisung für Zivildienstleistende in der Individuellen Schwerstbehindertenbetreuung zugeleitet. Statt der zunächst vorgesehenen verschlüsselten Angabe der Verrichtungen des Zivildienstleistenden bei der betreuten Person ist nunmehr vorgesehen, im Wochenarbeitsbericht künftig auf Eintragungen über die Tätigkeit zu verzichten. Der Bundesminister für Jugend, Familie, Frauen und Gesundheit hat mich darüber unterrichtet, daß diese Dienstanweisung wegen der noch ausstehenden Abstimmung mit den Wohlfahrtsverbänden noch nicht in Kraft gesetzt worden ist. Gleichzeitig hat er mir

mitgeteilt, er beabsichtige, die Prinzipien der für die Individuelle Schwerstbehindertenbetreuung entworfenen Dienstanweisung auch für den Bereich der Mobilen Sozialen Hilfsdienste zu übernehmen.

Ich halte die vom Bundesminister für Jugend, Familie, Frauen und Gesundheit vorgesehenen Regelungen für eine weitere datenschutzrechtliche Verbesserung.

4.7 Wohnungsbindungsgesetz

Nach § 2 Abs. 1 Wohnungsbindungsgesetz (WoBindG) hat die zuständige Stelle zur Sicherung der Zweckbestimmung alle öffentlich geförderten Wohnungen zu erfassen und die betreffenden Unterlagen auf dem laufenden zu halten. Welche Daten hierbei im einzelnen zu erfassen sind, legt die Vorschrift nicht fest. Dementsprechend verfahren die nach Landesrecht zuständigen bzw. von der Landesregierung bestimmten Stellen in unterschiedlicher Weise. So ist z. B. in Hamburg lediglich die Übermittlung von Meldedaten für diese Zwecke geregelt. Nachdem zwischen dem Hamburgischen Datenschutzbeauftragten und der Baubehörde der Freien und Hansestadt Hamburg längere Zeit der Datenbedarf diskutiert worden ist, wurde dieser in der dortigen neuen Verordnung über regelmäßige Datenübermittlungen aus dem Melderegister von 1986 enger gefaßt.

Die Übermittlung und Verarbeitung personenbezogener Daten im Hinblick auf § 2 Abs. 1 WoBindG kann das Recht auf informationelle Selbstbestimmung der Betroffenen beschränken. Nach dem Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 sind solche Einschränkungen nur in überwiegendem Allgemeininteresse zulässig. Sie bedürfen einer verfassungsmäßigen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muß. Diese Maßstäbe sind auch an das WoBindG anzulegen.

Ich gehe davon aus, daß ein überwiegendes Allgemeininteresse an der Sicherstellung der bestimmungsgemäßen Nutzung von Sozialwohnungen besteht und daß die von § 2 Abs. 1 WoBindG geforderte Erfassung eine geeignete Maßnahme hierzu darstellt. Im Sinne der Normenklarheit muß jedoch der von dieser Vorschrift Betroffene — Verfügungsberechtigter und Mieter — erkennen können, welche Daten zu diesem Zweck bezüglich seiner Person erhoben und in welcher Weise sie verarbeitet werden. Desgleichen muß die Vorschrift ihm verdeutlichen, an welche anderen Stellen Datenübermittlungen erfolgen oder daß Übermittlungen ausgeschlossen sind.

Auf die von mir erhobenen Bedenken hat mir der Bundesminister für Raumordnung, Bauwesen und Städtebau mitgeteilt, daß die aufgeworfenen Fragen auf einer Sitzung der Fachkommission „Wohnungsbindungs- und Berechnungsrecht" der Arbeitsgemeinschaft der für das Bau-, Wohnungs- und Siedlungswesen zuständigen Minister (Senatoren) der Länder — ARGEBAU — erörtert worden sind. Die Fachkommission sei zu dem Ergebnis gekommen, aus § 2 WoBindG in Verbindung mit den übrigen Vorschriften des Gesetzes ergebe sich mit hinreichender Deutlichkeit, daß sowohl die öffentlich geförderten Wohnungen als auch der Verfügungsberechtigte und der jeweilige Wohnungsinhaber erfaßt und daß diese Daten auch verarbeitet und gegebenenfalls an andere mit der Durchführung wohnungsrechtlicher Vorschriften befaßte Stellen weitergeleitet werden dürfen. Man halte aus datenschutzrechtlicher Sicht keine gesetzgeberischen Maßnahmen für erforderlich. Der Bundesminister für Raumordnung, Bauwesen und Städtebau gab jedoch gleichzeitig seine Bereitschaft zu erkennen, § 2 WoBindG anläßlich einer Novelle dieses Gesetzes aus der Sicht des Datenschutzes klarstellend zu ändern. Er weist allerdings darauf hin, daß kurzfristig mit einer solchen Novelle nicht zu rechnen sei. Ich werde die Angelegenheit im Auge behalten.

5. Rechtswesen

5.1 Bundeszentralregister

Ein im Jahre 1987 durchgeführter Informations- und Kontrollbesuch beim Bundeszentralregister hat erneut große Aufgeschlossenheit für den Datenschutz erkennen lassen. Angesichts des täglich zu bewältigenden hohen Arbeitsvolumens gilt es, ein Höchstmaß an Präzision und Zuverlässigkeit zu gewährleisten und Fehleranteile in den einzelnen Arbeitsschritten zu erkennen und möglichst gering zu halten. Anknüpfend an meine schon im Achten Tätigkeitsbericht (S. 11) gemachten Bemerkungen ist in diesem Zusammenhang die Tätigkeit der hausinternen Revisionsgruppe mit ihrer datenschutzrechtlich wichtigen — auch präventiven — Funktion hervorzuheben.

In zwei Fällen der Erteilung unbeschränkter Auskünfte habe ich im Jahre 1987 wegen Nichtbeachtung der in § 41 Abs. 1 Bundeszentralregistergesetz (BZRG) festgelegten Beschränkungen Beanstandungen nach § 20 Abs. 1 Bundesdatenschutzgesetz aussprechen müssen. Dabei handelte es sich um eine unbeschränkte Auskunft an ein Landratsamt „zur Überprüfung der heimrechtlichen Zuverlässigkeit" und um eine unbeschränkte Auskunft an einen Regierungspräsidenten „wegen Entzugs der Erlaubnis als Privatluftfahrzeugführer". In beiden Fällen lagen offensichtlich Versehen des verantwortlichen EDV-Registerführers vor. Wenn auch die Vermutung naheliegt, daß es sich um relativ seltene Einzelfälle handelt, halte ich es für angemessen, es nicht bei entsprechenden Belehrungen der verantwortlichen Mitarbeiter bewenden zu lassen, sondern der Problematik durch ein geeignetes Prüfverfahren nachzugehen. Ein — zunächst zeitlich beschränkter — Lauf eines solchen Verfahrens soll Gewißheit über den Anteil derartiger Vorkommnisse verschaffen und eine verbesserte Grundlage für Entscheidungen über die zu treffenden Maßnahmen bieten. Ziel ist die Feststellung von an Regierungspräsidenten und Kommunalbehörden erteilten unbeschränkten Aus-

künften, die nicht den in § 41 Abs. 1 Nr. 6, 7 und 9 BZRG enumerativ genannten Zwecken dienen. Auszuklammern sind mithin die an Stellen der Justiz gemäß Nr. 1, an oberste Bundes- und Landesbehörden gemäß Nr. 2 sowie an die in Nrn. 3, 4, 5, 8 und 10 genannten Behörden zu erteilenden Auskünfte. Obwohl die Durchführung dieses Prüfverfahrens aufwendig ist, konnte mit dem Bundeszentralregister Einvernehmen über seine Notwendigkeit und Zweckmäßigkeit erzielt werden. Die Vorbereitungen für die Erstellung entsprechender Prüflisten sind bereits abgeschlossen. Außer für meine datenschutzrechtlichen Kontrollen wird das Verfahren aber auch für gezielte Kontrollen durch die Revisionsgruppe des Bundeszentralregisters eingesetzt.

Ich habe wiederholt die Notwendigkeit datenschutzrechtlicher Verbesserungen des Bundeszentralregistergesetzes betont und hierzu dem Bundesminister der Justiz Vorschläge gemacht (s. 8. TB S. 12f., 7. TB S. 13, 6. TB S. 12, 5. TB S. 18). Abgesehen von der Mitteilung, daß der Bundesminister der Justiz einem wesentlichen Teil meiner Überlegungen „nicht ohne Sympathie gegenüberstehe", sind mir bislang weitere Reaktionen nicht zugegangen.

Eingaben von Bürgern haben mich veranlaßt, eines dieser Probleme, nämlich die Suchvermerke und die Auskünfte hierüber, erneut aufzugreifen. Nach § 27 BZRG können Behörden Suchvermerke im Register niederlegen. Der Bundesminister der Justiz vertritt die Auffassung, § 27 BZRG könne „nicht zwingend dahin einschränkend ausgelegt werden, daß Suchvermerke nur zur Erfüllung hoheitlicher Aufgaben im Bundeszentralregister niedergelegt werden können". Wäre diese Auffassung dahin zu verstehen, daß Behörden Suchvermerke für jeden behördlichen Zweck niederlegen können, so bedürfte es keiner Angabe des Niederlegungsgrundes. Mangels Erforderlichkeit wäre dann aber die im Rahmen der Zweiten Allgemeinen Verwaltungsvorschrift zur Durchführung des Bundeszentralregistergesetzes gegebene Anleitung des Bundesministers der Justiz, für die Niederlegung von Suchvermerken ein Formular zu verwenden, das für die Angabe des Niederlegungsgrundes einen Textraum von nicht weniger als 17 Zeilen vorsieht, ebenso zu beanstanden wie auch die hierauf gestützte Eintragungs- und Mitteilungspraxis des Bundeszentralregisters. Der Hinweis des Bundesministers der Justiz, daß dies der Selbstkontrolle der niederlegenden Behörde diene, vermag eine entsprechende Übermittlung personenbezogener Daten von der suchenden Behörde an das BZR sowie die weitere Datenverarbeitung nicht zu rechtfertigen. Auch die Argumentation des Bundesministers der Justiz, die Angabe des Niederlegungsgrundes habe — im Hinblick auf Mitteilungen des BZR an andere Stellen über den Inhalt des Suchvermerks (vgl. besonders § 41 Abs. 1 BZRG) — eine Schutzfunktion für die Person, über die ein Suchvermerk niedergelegt werde, erscheint mir nicht überzeugend: Weder durch Rechtsnorm noch durch Verwaltungsvorschrift wird bislang nämlich z. B. einer Strafverfolgungsbehörde auferlegt anzugeben, ob sie den Betroffenen als Beschuldigten oder als Zeugen sucht. Dementsprechend ist auch das BZR bislang zu einer Differenzierung des Inhalts seiner Datenspeicherung bzw. vom ihm gegebener Mitteilungen nicht verpflichtet.

Meine tatsächlichen Feststellungen beim Bundeszentralregister haben indessen ergeben, daß die niederlegenden Behörden durchweg nur ein bis zwei Zeilen des „Textraumes" füllen. Dabei handelt es sich teilweise lediglich — der Textvorgabe des Musters entsprechend — um selbstverständliche Hinweise auf den Zweck des Suchvermerkes, nämlich „gesucht wegen Aufenthaltsermittlung", teils aber um eingehendere Begründungen wie z. B. „gesucht wegen Ersatzanspruchs des Justizfiskus".

Die festgestellte Uneinheitlichkeit der Mitteilungspraxis und damit auch des Inhalts der Eintragungen im Register sowie des Inhalts von Informationen bzw. Auskünften des BZR über im Register niedergelegte Suchvermerke ist unter datenschutzrechtlichen Gesichtspunkten unbefriedigend. Sie beruht nach meiner Überzeugung aber nicht auf Verfahrensfehlern des Bundeszentralregisters, sondern auf mangelnder Normenklarheit.

Ich habe dem Bundesminister der Justiz daher empfohlen,

a) durch geeignete Formulierungen klarzustellen, daß „Aufenthaltsermittlung" keine hinreichend präzise Zweckangabe für Suchvermerke ist,

b) unter den Gesichtspunkten des überwiegenden Allgemeininteresses und der Verhältnismäßigkeit seine Auffassung zu überprüfen, wonach es sich um eine Suche auch zur Erfüllung nichthoheitlicher Aufgaben handeln kann, und dem Ergebnis dieser Prüfung entsprechend die Vorschriften des BZRG wie auch die Verwaltungsvorschriften zu präzisieren,

c) in Anlehnung an bereits früher gegebene Empfehlungen bezüglich der vom Bundeszentralregister an die suchende Behörde zu gebenden Hinweise differenzierende Regelungen zu schaffen, je nachdem ob es sich um eine unbeschränkt auskunftsberechtigte Behörde handelt oder nicht (Gewährleistung der Auskunftsbeschränkungen des § 41 BZRG),

d) zu überprüfen, welche der bislang auskunftsberechtigten Behörden in welcher Weise durch das BZR über die Gründe der Suche unterrichtet werden sollen. Unter Gesichtspunkten des Informationsbedarfes sowie des Schutzes des Betroffenen halte ich eine differenzierende Auswahl der Behörden wie auch eine differenzierende Bestimmung der Informationsinhalte für unerläßlich.

Ich habe dem Bundesminister der Justiz außerdem nahegelegt, sich bei der Prüfung dieser Vorschläge besonders auch die praktischen Erfahrungen des Bundeszentralregisters nutzbar zu machen.

Auch die Eintragungen wegen Schuldunfähigkeit im Bundeszentralregister sind immer wieder Gegenstand von Bürgereingaben. In letzter Zeit ist diese Problematik in den Medien und im Deutschen Bundestag diskutiert worden. Die Regelung des § 11

Nr. 1 BZRG über die Eintragung von Verfahrenseinstellungen wegen auf Schuldunfähigkeit oder auf Geisteskrankheit beruhender Verhandlungsunfähigkeit sowie die prinzipielle Aufrechterhaltung der Eintragung bis zum neunzigsten Lebensjahr des Betroffenen habe ich schon in meinem Vierten Tätigkeitsbericht (S. 42f.) als datenschutzrechtlich unbefriedigend gekennzeichnet.

Wie mir der Bundesminister der Justiz mitteilte, laufen Bemühungen um eine Regelung, die bezüglich der Erforderlichkeit einer Eintragung nach § 11 Nr. 1 BZRG, ihrer Speicherungsdauer und ihrer Verwendung differenziert. Ich begrüße den Hinweis des Bundesministers der Justiz, es werde geprüft, „ob die Anzahl der Eintragungen nach § 11 BZRG und die Auskunftsmöglichkeiten über solche Eintragungen beschränkt werden können und ob die Entfernung derartiger Eintragungen nach Fristablauf vorgesehen werden kann". Ich habe den Bundesminister der Justiz gebeten, mich über das Ergebnis dieser Prüfung zu unterrichten.

Eine Reihe von Eingaben hat mir allerdings gezeigt, daß zwischenzeitlich noch keine Wege gefunden worden sind um sicherzustellen, daß der Betroffene in jedem Falle von der Eintragung Kenntnis erhält und damit in die Lage versetzt wird, selbst eine Entfernung der Registereintragung nach § 25 BZRG (unter den dort genannten Voraussetzungen durch Anordnung des Generalbundesanwalts) zu betreiben. Nach Auffassung des Bundesministers der Justiz ist der Beschuldigte, wenn das Verfahren wegen Schuldunfähigkeit eingestellt werde, insbesondere dann, wenn er vorher nicht angehört worden sei, nach § 170 Abs. 2 Satz 2 letzte Alternative StPO zu benachrichtigen; die geltende Fassung des § 170 StPO ermögliche diese Benachrichtigung.

Nach den im Volkszählungsurteil des Bundesverfassungsgerichts aufgestellten datenschutzrechtlichen Anforderungen halte ich dies für unzureichend. Dabei geht es mir nicht nur um die Benachrichtigung über die Einstellung, sondern auch um die Benachrichtigung über die Eintragung. Ich habe dem Bundesminister der Justiz daher empfohlen, durch Rechtsnorm (in der Strafprozeßordnung oder im Bundeszentralregistergesetz) sowohl die Verpflichtung als auch den Inhalt der Benachrichtigung des Betroffenen festzulegen. Dabei dürfte — auch aus rechtssystematischen Gründen — weniger eine Benachrichtigung durch das BZR als eine solche durch die Stelle in Betracht kommen, die für die Mitteilung an das BZR verantwortlich ist.

5.2 Strafprozeßordnung

Im Februar 1987 habe ich dem Bundesminister der Justiz den von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Diskussion datenschutzrechtlicher Verbesserungen im Strafverfahren erarbeiteten Katalog von „Überlegungen zu Regelungen der Informationsverarbeitung im Strafverfahren" übersandt (s. auch 9. TB S. 19f.). Es handelt sich dabei um eine Zusammenstellung von Themenbereichen, in denen es sowohl zum Schutz des informationellen Selbstbestimmungsrechts der Betroffenen wie im Interesse wirksamer Aufgabenerfüllung durch die Strafverfolgungsorgane klarer Rechtsgrundlagen bedarf. Dabei geht es um eine Ergänzung der Strafprozeßordnung um Vorschriften, die sowohl die Informationsverarbeitung in Dateien als auch in Akten berücksichtigen. Durch eine deutlichere Abgrenzung zwischen den Befugnissen und Verantwortlichkeiten der Justizverwaltung, der Richter, der Staatsanwaltschaft und der Polizei soll der Datenschutz im Strafverfahren verbessert werden.

Außerdem habe ich im März 1987 eine Stellungnahme zu dem vom Bundesminister der Justiz vorgelegten Arbeitsentwurf eines Gesetzes zur Regelung der rechtlichen Grundlagen für Fahndungsmaßnahmen, Fahndungshilfsmittel und für die Akteneinsicht im Strafverfahren abgegeben. Ich halte es für notwendig, für eine Reihe besonderer Fahndungsmethoden wie die Rasterfahndung, die polizeiliche Beobachtung und die planmäßige Überwachung eigenständige Regelungen zu schaffen und die Zulässigkeit der Maßnahmen jeweils an enumerativ zu bestimmende schwerwiegende Straftaten zu binden, wie dies z. B. in § 163d StPO (Schleppnetzfahndung) geschehen ist. Der Einsatz lesender oder mithörender technischer Geräte und der Einsatz von Bildaufzeichnungen/Video bedarf nicht nur im Hinblick auf besondere Fahndungsmethoden, wie die planmäßige Überwachung, sondern allgemein einer gesetzlich präzisen Regelung. Der Bundesminister der Justiz hat inzwischen mitgeteilt, daß er aufgrund der ihm zugegangenen Stellungnahmen den Arbeitsentwurf überarbeite.

In Ergänzung des Arbeitsentwurfs habe ich ein weiteres Arbeitspapier erhalten, das Vorschläge für „Allgemeine Bestimmungen über die Speicherung, Verwendung und Übermittlung personenbezogener Daten durch die Strafverfolgungsbehörden" enthält. Dabei geht es u. a. um die Befugnisse von Polizeibehörden, personenbezogene Informationen aus einem Strafverfahren entgegen dem eigentlichen Erhebungszweck auch zur Abwehr einer Gefahr für die öffentliche Sicherheit oder Ordnung oder zur Verhütung von Straftaten zu nutzen. Im Zusammenwirken mit den Landesbeauftragten für den Datenschutz bereite ich auch hierzu eine Stellungnahme vor.

5.3 Strafvollzugsgesetz

Schon in meinem Siebenten Tätigkeitsbericht (S. 14f.) habe ich darauf hingewiesen, daß die Rechtsvorschriften des Strafvollzugsgesetzes keine hinreichende Klarheit darüber bieten, ob und welche Einschränkungen des Rechts auf informationelle Selbstbestimmung Bezugspersonen von Strafgefangenen im überwiegenden Allgemeininteresse hinnehmen müssen. Anlaß hierfür waren Hinweise von Landesbeauftragten für den Datenschutz auf ein offensichtlich unterschiedliches Vorgehen von Justizvollzugsanstalten bei der Überprüfung von Urlaubsanschrif-

ten von Strafgefangenen im Zusammenhang mit der Gewährung von Vollzugserleichterungen.

Zwischen den Justizverwaltungen und den Datenschutzbeauftragten besteht Übereinstimmung darin, daß das Strafvollzugsgesetz auf breiterer Basis, insbesondere auch in bezug auf die Erhebung, Aufbewahrung und Verwendung personenbezogener Daten der Gefangenen selbst, datenschutzrechtlicher Ergänzungen bedarf. Auch im Bereich des Strafvollzuges ist es notwendig, Konsequenzen aus dem Volkszählungsurteil des Bundesverfassungsgerichts zu ziehen. Der vom Bundesminister der Justiz im Frühjahr 1987 erstellte Arbeitsentwurf eines Vierten Gesetzes zur Änderung des Strafvollzugsgesetzes — datenschutzrechtliche Ergänzungen — ist eine geeignete Grundlage für weitere Überlegungen und Erörterungen. Meine dem Bundesminister der Justiz hierzu zugeleitete Stellungnahme enthält Vorschläge, durch die dem Recht des Bürgers auf informationelle Selbstbestimmung durch bereichsspezifische Vorschriften auch unter den besonderen Bedingungen des Strafvollzuges Rechnung getragen und zugleich den Strafvollzugsbehörden der Entscheidungsspielraum belassen wird, den sie zur Wahrnehmung ihrer Aufgaben im überwiegenden Allgemeininteresse, aber auch im Interesse der Resozialisierung des Gefangenen, benötigen. Der Bundesminister der Justiz bereitet gegenwärtig auf der Grundlage der ihm zugegangenen Äußerungen eine überarbeitete Fassung seines Entwurfes vor.

In den weiteren Beratungen wird auch die Erhebung von Daten über eine HIV-Infektion und die Verwendung solcher Daten zur Sprache kommen müssen. Damit knüpfe ich an allgemeine datenschutzrechtliche Aspekte der AIDS-Problematik an (s. auch Nr. 17.2). Die in diesem Zusammenhang beim Strafvollzug auftetenden Fragen werden derzeit auf Landesebene geregelt. So heißt es beispielsweise in einem Erlaß des Niedersächsischen Ministers der Justiz vom 12. März 1987:

> Die Tests sind freiwillig. Bei Angehörigen der sog. Risikogruppen ... ist die Untersuchung auf HIV-Antikörper aber dringend geboten. Die Anstaltsärzte werden gebeten, auf diese Gefangenen intensiv einzuwirken, damit sie sich zu dem Test bereiterklären...
>
> Grundsätzlich gilt auch bei HIV-Infektionen die ärztliche Schweigepflicht. Wegen der von HIV-Infizierten ausgehenden Gefahren sind die Anstaltsärzte aber befugt, den Anstaltsleiter zu unterrichten. Ich gehe davon aus, daß die Anstaltsärzte von dieser Befugnis künftig verstärkt Gebrauch machen. Insbesondere bei HIV-infizierten Gefangenen, die zu infektionsgefährlichen Handlungen neigen, wird den Anstaltsärzten empfohlen, eine Rechtsgüterabwägung zugunsten einer Information des Anstaltsleiters zu erwägen.

Nach meiner Einschätzung bedürfen solche Regelungen einer Festlegung in Rechtsnormen. Soweit Rechtsgüterabwägungen in Frage stehen, müssen dafür im Interesse der Infizierten, der Mitgefangenen, der Anstaltsärzte und des übrigen Personals der Justizvollzugsanstalten präzise Kriterien entwickelt werden.

5.4 Justizmitteilungsgesetz

Wie in meinem Neunten Tätigkeitsbericht (S. 19) angekündigt, habe ich in Abstimmung mit den Datenschutzbeauftragten der Länder dem Bundesminister der Justiz zu dem Entwurf eines Gesetzes über Mitteilungen der Justiz von Amts wegen in Zivil- und Strafsachen — Justizmitteilungsgesetz — inzwischen eine eingehende Stellungnahme übersandt. Ich sehe in dem Entwurf einen ersten Schritt auf dem Wege zu einer nach dem Volkszählungsurteil des Bundesverfassungsgerichts unumgänglich gewordenen gesetzlichen Verankerung des Mitteilungswesens im Justizbereich. Für sachgerecht halte ich es auch, daß der Entwurf sich bewußt auf Mitteilungen von Amts wegen an öffentliche Stellen beschränkt, die Aufgaben außerhalb des zugrundeliegenden Verfahrens wahrzunehmen haben. Für Mitteilungen an Verfahrungsbeteiligte sowie für Mitteilungen auf Ersuchen (wegen des Sachzusammenhangs mit dem Akteneinsichtsrecht) wird auf die einzelnen Prozeßordnungen verwiesen. Hier müssen ebenfalls noch die entsprechenden gesetzlichen Grundlagen geschaffen oder in verfassungskonformer Weise ergänzt werden. Bezüglich des Strafverfahrens ist hierzu bereits ein Dialog zwischen den Justizverwaltungen und den Datenschutzbeauftragten im Gange.

Unbefriedigend ist im Hinblick auf das Gebot der Normenklarheit allerdings die geringe Regelungsdichte, die den Entwurf kennzeichnet. Die generalklauselartigen Bestimmungen lassen Anlaß und Umfang der vorgesehenen Datenverarbeitung nicht hinreichend deutlich erkennen und bergen zudem die Gefahr in sich, daß etwaige ergänzende und auf besondere Fallgruppen bezogene Regelungen umgangen werden. In Übereinstimmung mit den Datenschutzbeauftragten der Länder habe ich dem Bundesminister der Justiz empfohlen, darauf hinzuwirken, daß der Bundesgesetzgeber seine Kompetenz voll ausschöpft. Nach meiner Einschätzung bedarf es einer Überarbeitung des Entwurfs, insbesondere einer näheren Konkretisierung der einzelnen Übermittlungstatbestände.

5.5 Zivilprozeßordnung

Die Überprüfung des geltenden Rechts auf seine Vereinbarkeit mit dem Recht auf informationelle Selbstbestimmung ist zwar in den Bereichen besonders dringlich, die sich auf das Strafverfahren beziehen (s. oben Bundeszentralregistergesetz, Strafprozeßordnung, Strafvollzugsgesetz, Justizmitteilungsgesetz). Doch dürfen dabei zivilrechtliche Verfahren nicht außer acht gelassen werden (vgl. auch meine Hinweise im 7. TB S. 16 bezüglich des Grundbuchwesens; zur Sonderproblematik des Schuldnerverzeichnisses s. u. 5.6).

Ein Fragenkreis der Zivilprozeßordnung, zu dem ich mit dem Bundesminister der Justiz im Gespräch bin, betrifft Pfändungs- und Überweisungsbeschlüsse mit einer Mehrzahl von Drittschuldnern. Die §§ 828 ff. Zivilprozeßordnung enthalten keine Regelung über die Pfändung und Überweisung verschiedener Forderungen eines Schuldners gegen mehrere Drittschuldner in ein und demselben Beschluß, verbieten eine solche Zwangsvollstreckungsmaßnahme also nicht ausdrücklich. Rechtsprechung und Schrifttum gehen davon aus, daß der Gläubiger, um keine nichterstattungsfähigen Vollstreckungskosten zu verursachen, im eigenen Interesse grundsätzlich gehalten sei, in einem solchen Falle nur einen Antrag auf die Pfändung mehrerer Forderungen seines Schuldners zu stellen. Dies hat zur Folge, daß die in einem Pfändungs- und Überweisungsbeschluß genannten mehreren Drittschuldner jeweils Kenntnis von den anderen Drittschuldnern und deren Beziehung zu dem Schuldner erhalten. Besonders kritisch ist dies, wenn es sich — wie mir durch Einzelfälle bekannt geworden ist — z. B. um das Verhältnis zwischen einem Arzt als Schuldner und seinen Patienten als Drittschuldnern handelt. Der Bundesminister der Justiz hat mir mitgeteilt, er werde das Problem im Hinblick auf eine gesetzliche Regelung, etwa eine Ergänzung des § 829 Abs. 2 Zivilprozeßordnung, mit den Landesjustizverwaltungen erörtern.

5.6 Schuldnerverzeichnis

Mit dem in § 915 ZPO geregelten Schuldnerverzeichnis befasse ich mich schon seit längerer Zeit und habe in früheren Tätigkeitsberichten (vgl. 8. TB S. 12 f. mit weiteren Hinweisen) gefordert, den Datenschutz bei der Übermittlung von Angaben aus dem Schuldnerverzeichnis zu verbessern, insbesondere den Umfang der Datenübermittlungen zu reduzieren und auch die zugrundeliegende gesetzliche Regelung zu überarbeiten. Zu den letzten mir im August 1987 zugegangenen Entwürfen eines Gesetzes zur Änderung von Vorschriften über das Schuldnerverzeichnis sowie einer Verordnung über die Erteilung von Abdrucken und Listen aus dem Schuldnerverzeichnis habe ich gegenüber dem Bundesminister der Justiz Stellung genommen und dabei folgende datenschutzrechtliche Verbesserungen hervorgehoben:

— die Löschung der Eintragung nach spätestens drei Jahren ohne Antrag des Betroffenen,

— den Wegfall des Einsichtsrechts,

— die Verpflichtung für Bezieher von Abdrucken und Listen, diese unverzüglich in einer Datei zu verarbeiten und die Abdrucke bzw. Listen danach zu vernichten.

Als ein zentrales Problem der vorgesehenen Neuregelung zum Schuldnerverzeichnis sehe ich die Weitergabe von Schuldnerlisten durch die Abdruckempfänger, d. h. die Kammern, an ihre Mitglieder. Dabei kommt es mir auf eine m. E. nur durch eine Eingrenzung des Empfängerkreises erreichbare zweckgerichtete Kontrolle des Verbleibs der Abdrucke bzw. der Listen an und auf die Aktualisierung der darin enthaltenen personenbezogenen Daten. Unter diesem Gesichtspunkt lassen sich gegenüber früheren Vorentwürfen einige deutliche Verbesserungen feststellen:

— Die Entscheidung über den Bezug der Listen wird nicht mehr allein den Kammern und ihren Mitgliedern überlassen; vielmehr ist für den Bezug eine Bewilligung durch die Justizbehörden vorgesehen. Voraussetzung ist, daß dem berechtigten Interesse des Antragstellers durch Einzelauskünfte nicht hinreichend Rechnung getragen werden kann.

— Die Bezieher haben die Listen in einer Datei zu verarbeiten. Hierdurch soll sichergestellt werden, daß die Daten stets übersichtlich geordnet sind und ohne weiteres rechtzeitig gelöscht werden können.

— Es wird die Möglichkeit einer systematischen Datenschutzkontrolle aller Listenempfänger geschaffen.

— Für die Erteilung von Auskünften durch Listenempfänger wird die Zweckbindung verstärkt.

Trotz dieser Verbesserungen habe ich die Sorge, daß in der Praxis eine effektive Kontrolle der Einhaltung der Datenschutzvorschriften, vor allem der Löschung überholter Eintragungen, nicht gewährleistet werden kann. Zwar ist es zu begrüßen, daß bei den Listenbeziehern eine Kontrolle der Einhaltung datenschutzrechtlicher Vorschriften künftig nicht nur aus konkretem Anlaß (§ 30 Abs. 1 BDSG) möglich ist; eine effektive Datenschutzkontrolle setzt aber auch eine personelle Ausstattung der Kontrollbehörden voraus, die sie in die Lage versetzt, auch systematische Überprüfungen mit hinreichender Kontrolldichte durchzuführen. Ich teile die Zweifel meiner Kollegen in den Ländern, ob diese Voraussetzungen bei den Datenschutzkontrollbehörden für den privaten Bereich erfüllt sind.

Ich habe daher zu erwägen gegeben, ob nicht den Interessen der Kammermitglieder dadurch hinreichend Rechnung getragen werden kann, daß die Kammern ihnen die gewünschten Einzelauskünfte erteilen. Dieses Verfahren würde bei den Kammern möglicherweise zusätzliches Personal erfordern; dabei sollte aber berücksichtigt werden, daß damit zugleich der Aufwand für die Verarbeitung der Listen bei einer Vielzahl von Mitgliedern entfallen würde. Nach wie vor scheint mir die Frage offen, ob der Informationsbedarf einzelner Mitglieder wirklich so groß ist, daß er nicht durch einen Auskunftsdienst der Kammern befriedigt werden kann.

Die Entwürfe des Bundesministers der Justiz sehen außerdem vor, anderen Antragstellern als den Kammern den Bezug von Abdrucken zu bewilligen, wenn ihrem berechtigten Interesse durch Einzelauskünfte nicht hinreichend Rechnung getragen werden kann. Der Kreis dieser Antragsteller sollte nach meiner Auffassung schon im Gesetz selbst genannt oder zumindest eingegrenzt, und nicht allein dem Bewilligungsverfahren überlassen werden. Auch wäre zu prüfen, ob und welche Bezugsberechtigte

(etwa Kreditinstitute) neben solchen Stellen in Betracht kommen, die gewerblich Auskünfte an Dritte erteilen (z. B. SCHUFA).

6. Finanzwesen

6.1 Kontrollmitteilungen

Verwaltungsvorschriften zur Bundeshaushaltsordnung (Nr. 5.2 der Anlagen 1—4 zur Vorl. VV Nr. 5.1 zu den §§ 44, 44a BHO) bestimmen, daß Empfänger von Zuwendungen aus dem Bundeshaushalt ihrem Finanzamt Zahlungen mitzuteilen haben, die sie aufgrund von Verträgen (z. B. Dienst- oder Werkverträgen) z. B. an Gutachter, Übersetzer, Unterrichtende, Vortragende oder Sitzungsteilnehmer leisten. Nur in bestimmten näher geregelten Ausnahmefällen können diese Mitteilungen unterbleiben. In den Ländern bestehen in bezug auf Zuwendungen aus den Länderhaushalten vergleichbare Verwaltungsregelungen.

Ich habe erhebliche Zweifel, ob solche Kontrollmitteilungen nach geltendem Recht zulässig sind: Eine Anwendung des § 93 Abgabenordnung (AO) kommt in der Regel schon deshalb nicht in Betracht, weil das in § 93 Abs. 1 Satz 3 AO verankerte Subsidiaritätsprinzip es gebietet, andere Personen oder Stellen erst dann zu Auskünften anzuhalten, wenn die Sachverhaltsaufklärung durch den Steuerpflichtigen selbst nicht zum Ziele führt oder keinen Erfolg verspricht. Auch § 93a AO ist nicht anwendbar, weil diese Vorschrift nur für Behörden gilt und es sich bei den Zuwendungsempfängern gerade nicht um Behörden handelt. Mit der Schaffung des § 93a AO im Rahmen des Steuerbereinigungsgesetzes 1986 wurde aber beispielhaft anerkannt, daß eine derartige Inanspruchnahme Dritter wegen des besonderen Eingriffscharakters gegenüber dem Steuerpflichtigen jedenfalls dann einer spezifischen Regelung bedarf, wenn es sich um eine Verpflichtung zu regelmäßigen Auskünften handelt (vgl. meinen 6. TB S. 15f., 7. TB S. 16, 9. TB S. 20f.).

Insofern begrüße ich die Mitteilung des Bundesministers der Finanzen, daß der Bund/Länder-Arbeitsausschuß „Haushaltsrecht und Haushaltssystematik" zu der Auffassung gelangt ist, eine gesetzliche Regelung der Mitteilungspflicht nicht-öffentlicher Stellen durch Ergänzung des § 93a AO sei unerläßlich. Der BMF will unter diesen Umständen nicht mehr an dem in den zitierten Verwaltungsvorschriften geregelten Verfahren festhalten und hat den Bundesminister des Innern um Überprüfung seiner bisherigen gegenteiligen Rechtsauffassung gebeten.

Zur Sicherung der Besteuerung ermächtigt § 93a AO die Bundesregierung, durch Rechtsverordnung unter den in der Vorschrift näher genannten Voraussetzungen Behörden zu verpflichten, Kontrollmitteilungen an die Finanzbehörden zu richten. Hinweisen von Landesbeauftragten für den Datenschutz habe ich entnommen, daß an dem baldigen Erlaß einer entsprechenden Verordnung auch deshalb ein datenschutzrechtliches Interesse besteht, weil damit eine noch immer ungeregelte und unklare Praxis bereinigt würde. An den hierzu vom Bundesminister der Finanzen aufgenommenen Vorarbeiten bin ich beteiligt. Aufgrund der in meinem Neunten Tätigkeitsbericht (S. 20f.) wiedergegebenen Überlegungen zur Wahrung des Sozialgeheimnisses bei Kontrollmitteilungen ist vorgesehen, Sozialleistungen und personenbezogene Daten, die den Leistungsträgern im Zusammenhang mit der Erfüllung von Aufgaben nach dem Sozialgesetzbuch bekannt sind, nicht an die Finanzbehörden mitzuteilen.

6.2 Steuerdaten-Abruf-Verordnung

Die Regelungen der Abgabenordnung (AO) sind durch das Steuerbereinigungsgesetz 1986 auch zum Schutz des Steuergeheimnisses ergänzt worden. Bisher untersagte das Steuergeheimnis, die in § 30 Abs. 2 Nr. 1 und 2 AO näher bezeichneten Informationen Dritten gegenüber unbefugt zu offenbaren oder sie unbefugt zu verwerten. Nach der Neuregelung ist das Steuergeheimnis für diese Daten erweitert worden, soweit sie in einer Datei gespeichert sind und im automatisierten Verfahren abgerufen werden können. Hiernach verletzt jetzt ein Amtsträger das Steuergeheimnis bereits dann, wenn er solche Daten unbefugt abruft.

Der Bundesminister der Finanzen wurde mit dem Steuerbereinigungsgesetz 1986 zugleich ermächtigt, durch Rechtsverordnung mit Zustimmung des Bundesrates zu bestimmen, welche technischen und organisatorischen Maßnahmen gegen den unbefugten Abruf von Daten zu treffen sind, d. h. insbesondere Regelungen festzulegen über die Art der Daten, deren Abruf zulässig ist, sowie über den Kreis der Amtsträger, die zum Abruf solcher Daten berechtigt sind.

Der Bundesminister der Finanzen hat hierzu einen Entwurf über den Abruf von Daten im automatisierten Verfahren vorgelegt, die „vom Bundesamt für Finanzen oder von einem Finanzamt in einem Verfahren nach der AO oder von einer Gemeinde im Rahmen ihrer Zuständigkeit für Realsteuern oder von einer Stelle für diese Behörden gespeichert worden sind" (Steuerdaten-Abruf-Verordnung). Zum Abruf sollen ausschließlich Amtsträger oder ihnen nach der AO gleichgestellte Personen berechtigt werden, die bei der Durchführung von Verwaltungsverfahren oder gerichtlichen Verfahren in Steuersachen, von Strafverfahren wegen einer Steuerstraftat oder von Bußgeldverfahren wegen einer Steuerordnungswidrigkeit tätig sind. Vergleichbare Regelungen sind für Zahlungen vorgesehen, auf welche die für Steuervergütungen geltenden Vorschriften der AO sowie das Steuergeheimnis entsprechend anzuwenden sind, wenn die Daten von einem Finanzamt oder von einer Stelle für ein Finanzamt gespeichert worden sind.

Ich habe gegenüber dem Entwurf vor allem deshalb Bedenken erhoben, weil m. E. die vorgesehene Kontrolle der Datenabrufe im Stichprobenverfahren unzureichend ist. Hierbei verkenne ich nicht die

Schwierigkeiten des Verordnungsgebers, denn die vorgesehene Verordnung soll Mindestanforderungen an Verfahren regeln, die im einzelnen nicht benannt sind und die wohl auch zum Teil erst noch künftig zu entwickeln sind. Unter diesen Umständen habe ich Verständnis dafür, daß nur solche Anforderungen in der Verordnung festgeschrieben werden können, die als unverzichtbares Minimum für jedes denkbare Verfahren im Bereich der Finanzverwaltung anzusehen sind.

Zum Schutze des Steuergeheimnisses betrachte ich es jedoch als unzureichend, wenn Datenabrufe, die nicht vom zuständigen Bearbeiter, sondern z. B. von seinem Vertreter getätigt werden, nur „unter Berücksichtigung des Schutzbedürfnisses" nach einem Stichprobenverfahren aufgezeichnet werden sollen. Auch ist für Abrufe durch Zugriffsberechtigte anderer Finanzbehörden als der speichernden Stelle lediglich eine Stichprobe von mindestens fünf von Hundert zur Protokollierung vorgesehen. Für beide Fallgestaltungen halte ich eine vollständige Protokollierung der Abrufe für erforderlich, die stichprobenweise durch weitere Aufzeichnungen ergänzt werden sollte.

Die Diskussion mit dem Bundesminister der Finanzen dauert an.

6.3 Abgabenachricht auf Postkarte

Wie mir durch die Eingabe eines Bürgers bekannt wurde, hat ein Hauptzollamt auf einer Postkarte eine Abgabenachricht erteilt, in der vermerkt war, daß das abgegebene Schreiben eine Vollstreckungsmaßnahme gegen einen namentlich genannten Schuldner betraf. Ich begrüße es, daß der Bundesminister der Finanzen auf meine entsprechenden Vorstellungen hin die Dienststellen seines Geschäftsbereichs durch Erlaß angewiesen hat, Postkarten — auch als Abgabenachricht — nicht zu verwenden, wenn sie personenbezogene Daten zum Inhalt haben.

7. Personalwesen

7.1 Personalaktenführung

7.1.1 Neuregelung des Personalaktenrechts

Wie ich in meinem Neunten Tätigkeitsbericht (S. 22) erwähnt habe, nehme ich an den Arbeiten der interministeriellen Arbeitsgruppe zur Neuregelung des Personalaktenrechts beim Bundesminister des Innern in beratender Funktion teil. Die Arbeitsgruppe hat im Frühjahr des Berichtsjahres die Vorarbeiten abgeschlossen. Der Entwurf eines Berichts, der einen ersten Gesetzentwurf für die geplante Regelung enthält, liegt inzwischen vor. Eine weitere Sitzung für die Diskussion dieses Berichts ist für Januar 1988 anberaumt.

Für den Bereich der *konventionellen, d. h. aktenmäßigen Personaldatenverarbeitung* sieht der Entwurf im wesentlichen folgende Regelungen vor:

— Geregelt werden soll die Verpflichtung, daß und von wem eine Personalakte zu führen ist, sowie der wesentliche Inhalt der Personalakte. Der Entwurf hält sich dabei streng an die Rechtsprechung des Bundesverwaltungsgerichts, wonach zur Personalakte alle Vorgänge gehören, die die dienstlichen und persönlichen Verhältnisse des Beamten betreffen, soweit sie mit dem konkreten Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen. Gesetzlich festgelegt wird auch die Forderung, daß die Akte vollständig und lückenlos Aufschluß über den beruflichen Werdegang und insoweit über die Person des Beamten geben muß. Ein Katalog bestimmt die grundsätzlich in die Personalakte aufzunehmenden Unterlagen. Dagegen wird abgegrenzt, was nicht in die Personalakte gehört, nämlich Stellungnahmen und solche Vorgänge, die lediglich der Vorbereitung einer Entscheidung dienen, die Entscheidung aber selbst nicht tragen. Weiter werden die nicht zu den Personalakten zählenden Vorgänge wie Prüfungsakten, Sicherheitsakten, Aufstellungen über Kassenfehlbeträge von Kassenführern, Prozeßakten über Rechtsstreitigkeiten aus dem Dienstverhältnis und Kindergeldakten aufgeführt. Auch zur Zulässigkeit der Personalnebenakten, wenn die personalverwaltende Behörde nicht mit der Beschäftigungsbehörde identisch ist, sowie zur Aufteilung der Personalakte in Grundakten und Teilakten werden Aussagen gemacht.

— Meiner immer wieder vorgetragenen Forderung nach einer gesetzlichen Verankerung des Personalaktengeheimnisses (vgl. 9. TB, S. 22) wird durch eine ausführliche Regelung der Berechtigung zur Einsichtnahme in bzw. Auskunft aus der Personalakte Rechnung getragen. Aus dem Gesetzentwurf geht hervor, daß der Beamte stets, auch nach Beendigung des Beamtenverhältnisses, ein Recht auf Einsicht in seine vollständigen Personalakten hat. Ausgegangen wird hier von dem auch von mir stets vertretenen materiellen Personalaktenbegriff. Darüber hinaus hat ein Bediensteter ein Anhörungsrecht vor Aufnahme von Beschwerden und Behauptungen tatsächlicher Art, die für ihn ungünstig oder ihm nachteilig werden können. Gegebenenfalls ist eine Äußerung des Beamten zu seinen Akten zu nehmen. Neben den ausdrücklich genannten Hinterbliebenen oder Bevollmächtigten eines Beamten kann anderen Personen nur dann Einsicht gewährt werden, wenn dies zur Erfüllung ihnen obliegender gesetzlicher Aufgaben oder im überwiegenden dienstlichen oder öffentlichen Interesse geboten ist.

  Bei der Formulierung „im überwiegenden dienstlichen oder öffentlichen Interesse" handelt es sich um unbestimmte Rechtsbegriffe, die die Gefahr einer übermäßigen Ausdehnung in der Verwaltungspraxis in sich bergen. Bedenken hiergegen können wohl in Anbetracht der bereits jetzt in großem Umfang vorhandenen Rechtsprechung dazu zurückgestellt werden. Dies gilt in gleicher Weise für die Regelung der Vorlage einschließ-

lich der Übersendung der Personalakte an andere Behörden. Sie soll zwar grundsätzlich der Zustimmung des Beamten bedürfen, aber auch ohne diese zulässig sein, wenn „ein berechtigtes Interesse an der Einsichtnahme von seiten der ersuchenden Behörden dargetan ist, schutzwürdige Interessen der Allgemeinheit an der Vorlage überwiegen und berechtigte Belange des Dienstherrn nicht entgegenstehen". Eine zusätzliche Regelung soll für die Erteilung von Auskünften aus der Personalakte an Dritte getroffen werden. Auch sie darf nur stattfinden, wenn der Beamte eingewilligt hat. Sie ist im übrigen zulässig, wenn auch eine Einsichtnahme in die Personalakten zulässig wäre oder die Wahrung einer gesetzlichen Aufgabe, die Abwehr einer Gefahr für die Bundesrepublik Deutschland oder der Schutz berechtigter Interessen eines Dritten dies erfordert. Zusätzlich ist in diesem Falle der Bedienstete über Adressat und Inhalt der Auskunft schriftlich zu unterrichten. Die Durchschrift ist zu den Personalakten zu nehmen.

Ich hätte es begrüßt, wenn im Zusammenhang mit der Auskunftserteilung an Dritte auch eine einschränkende Regelung derart vorgesehen worden wäre, daß der Auskunftserteilung stets der Vorrang vor der Vorlage bzw. Einsichtnahme in die Personalakte zu geben ist, wenn dies für den Antragsteller ausreicht.

— Im Interesse der Bediensteten wird gesetzlich fixiert, welche Vorgänge aus der Personalakte zu entfernen sind. Auch hier wird den Vorgaben der Rechtsprechung im wesentlichen gefolgt, indem auf Antrag Vorgänge in den Personalakten über Beschwerden oder Behauptungen, die sich als unbegründet bzw. als falsch erwiesen haben, aus den Personalakten zu entfernen und zu vernichten sind. § 119 Bundesdisziplinarordnung soll entsprechend gelten für Eintragungen in die Personalakte, die sich auf mißbilligende Äußerungen des Dienstvorgesetzten, Ermahnungen, Rügen oder Abmahnungen beziehen, sofern eine Besserung des Verhaltens oder der Leistung feststellbar ist.

— Besonders hervorgehoben sei die gesetzmäßige Behandlung der bei der Bearbeitung der Beihilfe bekanntgewordenen personenbezogenen Tatsachenfeststellungen (Beihilfedaten). Es ist die Verpflichtung vorgesehen, sie getrennt vom übrigen Inhalt der Personalakten zu führen. Die Verwendung und Weitergabe der Beihilfedaten für andere als für Beihilfezwecke darf stattfinden, wenn und soweit eine Rechtsvorschrift dies zuläßt, der Beihilfeberechtigte im Einzelfall einverstanden ist, die Durchführung eines im Zusammenhang mit dem Beihilfeverfahren bestehenden gerichtlichen Verfahrens einschließlich eines Straf- oder Disziplinar-Verfahrens oder die Abwehr einer Gefahr für die öffentliche Sicherheit oder der Schutz berechtigter Interessen eines Dritten dies erfordern. Soweit die Beihilfedaten für die Festsetzung der Bezüge maßgeblich sind, dürfen sie auch hierfür verwendet und weitergegeben werden. Bei Personalentscheidungen dürfen Beihilfedaten nicht herangezogen werden.

Ich halte es weiterhin für erforderlich, neben der Regelung der getrennten Aktenführung sowie des Verbotes der Heranziehung von Beihilfedaten bei Personalentscheidungen auch eine ausdrückliche Abschottung der Beihilfestellen von der übrigen Personalverwaltung in die gesetzliche Regelung aufzunehmen (vgl. 9. TB S. 22/23).

Für den Bereich der *automatisierten Datenverarbeitung* ist nach diesem Gesetzesentwurf insbesondere folgendes vorgesehen:

— Personenbezogene Daten dürfen mit Mitteln der Informationstechnik nur erhoben und verarbeitet (d. h. gespeichert, verändert, ausgewertet, verknüpft, übermittelt) werden, soweit sie unmittelbar zu bestimmten oder im Zeitpunkt der Erhebung bestimmbaren Zwecken der Begründung, Durchführung und Abwicklung des Dienstverhältnisses erforderlich sind oder eine Rechtsvorschrift dies erlaubt und soweit in der besonderen Verarbeitungsart begründete Gesichtspunkte des Schutzes der Persönlichkeitsrechte nicht entgegenstehen.

— Zu einem bestimmten Zweck erhobene Daten der Beamten dürfen personenbezogen zu einem anderen Zweck nur dann verarbeitet werden, wenn sie auch zu diesem Zweck hätten erhoben werden dürfen.

— Die Verknüpfung personenbezogener Daten zur Herstellung eines Persönlichkeitsprofils, eines vollständigen Abbildes des dienstlichen Arbeitsverhaltens, die lückenlose Kontrolle der Leistung und die heimliche Kontrolle des Beamten mit Mitteln der Informationstechnik sind unzulässig.

— Dienstliche Beurteilungen sowie medizinische und psychologische Befunde dürfen grundsätzlich nicht gespeichert und automatisiert verarbeitet werden.

— Das Ergebnis einer Verarbeitung personenbezogener Daten des Beamten mit Mitteln der Informationstechnik darf nicht allein Grundlage für Personalanentscheidungen sein.

— Art und Umfang der zu erhebenden und zu verarbeitenden Personaldaten sowie die Verarbeitungsverfahren, insbesondere die Verknüpfung, die Auswertung und die Übermittlung einschließlich des jeweiligen Verwendungszwecks und Empfängerkreises sind vom Dienstherrn festzulegen und zu dokumentieren.

— Durch geeignete technische und organisatorische Maßnahmen ist nach dem jeweiligen Stand der Technik sicherzustellen, daß nur der Befugte das System und die Daten nutzen kann und dies auch nur in dem Umfang, wie er es für die Erfüllung der ihm übertragenen Aufgaben benötigt; jede Nutzung muß durch eine Dokumentation kontrollierbar sein.

Diese Regelungen, die sehr viele Detailfragen berühren, werden von mir im einzelnen noch gründlich

zu überprüfen sein. Eine kursorische Bewertung ergibt jedoch, daß zahlreiche meiner Forderungen Eingang in den Gesetzentwurf gefunden haben.

Im Gegensatz zur Neuregelung des Personalaktenrechts sind vergleichbare Fortschritte bei der *bereichsspezifischen Regelung des Arbeitnehmerdatenschutzes* trotz des Auftrages des Deutschen Bundestages an die Bundesregierung, zu Beginn der laufenden Legislaturperiode entsprechende Vorschläge vorzulegen, nicht zu verzeichnen; jedenfalls sind mir entsprechende Entwürfe bisher nicht bekannt geworden. Ich bedauere dies um so mehr, als sich insbesondere im Hinblick auf die zunehmende Automatisierung der Personaldatenverarbeitung und die sich hieraus ergebenden verstärkten Datenschutzprobleme eine bereichsspezifische Regelung des Arbeitnehmerdatenschutzes als immer dringlicher erweist.

7.1.2 Inhalt der Personalakten (Pfändungs- und Überweisungsbeschlüsse)

Im Berichtszeitraum hatte ich mich mit der Frage zu befassen, ob und gegebenenfalls wann eine Besoldungsstelle die allgemeine Personalverwaltung über Vollstreckungsmaßnahmen, wie beispielsweise eine Gehaltspfändung, in Kenntnis setzen muß. Zur Personalakte gehören Vorgänge, die die dienstlichen und persönlichen Verhältnisse des Beamten betreffen, soweit sie mit dem konkreten Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen. Die Besoldungsvorgänge sind somit nach einhelliger Meinung Bestandteil der Personalakte. Da Pfändungs- und Überweisungsbeschlüsse unmittelbaren Einfluß auf die Besoldungsabwicklung haben, zählen sie zu den Personalakten im materiellen Sinne. Dies bedeutet jedoch nicht, daß dem Personenkreis, der mit der allgemeinen Personalverwaltung befaßt ist, auch Einblick in alle zum materiellen Teil der Personalakte zählenden Vorgänge gestattet sein muß. So habe ich immer wieder gefordert, daß durch organisatorische Vorkehrungen besonders sensible Vorgänge gegen unnötige Kenntnisnahme geschützt werden müssen und daher einer besonderen aktenmäßigen Behandlung bedürfen. Ich bin der Auffassung, daß Umstände der privaten Lebensführung nur so weit in Personalentscheidungen der Anstellungsbehörde einfließen dürfen, als sie tatsächlich in den dienstlichen Bereich hineinwirken.

Dies ist nach meiner Auffassung nicht bei jedem einzelnen Pfändungs- und Überweisungsbeschluß der Fall. Erst eine Häufung von Pfändungs- und Überweisungsbeschlüssen bzw. die Pfändung eines überproportional hohen Teiles der Bezüge kann die finanzielle Beweglichkeit eines Bediensteten dermaßen einschränken, daß Auswirkungen in den dienstlichen Bereich hinein zu befürchten sind. Um überflüssige Benachteiligungen eines Bediensteten in seiner Behörde zu vermeiden, sollte zunächst ein Vertreter der die Besoldung anordnenden Stelle mit ihm ein klärendes Gespräch führen. Erst anhand dieses Gesprächsergebnisses ist unter Anwendung des Verhältnismäßigkeitsgrundsatzes zu prüfen, ob und inwieweit eine Datenübermittlung an die allgemeine Personalverwaltung gerechtfertigt ist.

7.1.3 Weitergabe von Personaldaten bzw. Erteilung von Auskünften

Jede Kenntnisnahme Dritter vom Inhalt einer Personalakte ohne Einwilligung des Bediensteten ist ein Eingriff in dessen Recht auf informationelle Selbstbestimmung. Ob ein solcher Eingriff gerechtfertigt ist, bedarf der besonderen Prüfung im Einzelfall. Dabei ist das Geheimhaltungsinteresse des Beamten einerseits gegen etwaige schutzwürdige Interessen der Allgemeinheit oder Dritter andererseits abzuwägen. Das in der Rechtsprechung als besonderes Amtsgeheimnis anerkannte Personalaktengeheimnis verlangt überdies eine besonders strenge Prüfung der Eingriffsvoraussetzungen unter dem Gesichtspunkt der Verhältnismäßigkeit. Diese Problematik stellte sich im Berichtsjahr in zwei Fällen:

— Der Leiter der Vorprüfungsstelle einer obersten Bundesbehörde hatte um Einsichtnahme in die Personalakte von Mitarbeitern vor deren Zuweisung an die Vorprüfungsstelle gebeten. Er berief sich darauf, daß nach Nr. 3.2 der Vorprüfungsordnung für die Bundesverwaltung (VPOB) die Vorprüfungsstelle personell sachgerecht zu besetzen sei. Vor der Zuweisung und Abberufung der Prüfungsbeamten ist der Leiter der Vorprüfungsstelle zu hören (§ 100 Abs. 5 Bundeshaushaltsordnung — BHO —). Der Bundesrechnungshof vertrat in diesem Zusammenhang die Ansicht, daß diese Mitwirkung des Leiters der Vorprüfungsstelle zwangsläufig ein Einsichtsrecht in die Personalakte der Betroffenen — auch ohne deren Zustimmung — impliziere. Diese Auffassung teile ich nicht. Die vorgeschriebene Mitwirkung des Leiters der Vorprüfungsstelle bei der Besetzung der Dienstposten setzt zwar voraus, daß er über die besonderen Qualifikationen der von der Personalstelle vorgeschlagenen Prüfungsbeamten eingehend informiert wird, insbesondere darüber, ob die in den Nrn. 3.3 bis 3.6 VPOB aufgeführten Eignungsvoraussetzungen in deren Person erfüllt sind. Die Informationsverpflichtung der Personalstelle kann jedoch auch ohne Einsichtnahme in die Personalakte durch die Erteilung entsprechender Auskünfte erfüllt werden. Die Weitergabe der Personalakte selbst, in der eine Vielzahl von Vorgängen enthalten ist, die zur Beurteilung der Qualifikation des Bediensteten für eine Tätigkeit in der Vorprüfungsstelle keine Bedeutung haben, wie beispielsweise Religionszugehörigkeit oder Ehe- und Familienverhältnisse, wäre unverhältnismäßig und damit wegen Verstoßes gegen die Vertraulichkeit der Personalakte unzulässig.

  Gleiches gilt auch für die Beurteilung der charakterlichen Eignung eines Bediensteten für die Tätigkeit in der Vorprüfungsstelle. Soweit die dienstlichen Beurteilungen eines Bediensteten darüber überhaupt Aufschluß geben, erscheint es mir unter dem Gesichtspunkt des Personaldatenschutzes als nicht vertretbar, daß der fachliche

Leiter einer oft verhältnismäßig kleinen Einheit Einblick in sämtliche Beurteilungen künftiger Mitarbeiter nehmen kann. Auch hier ist eine zusammenfassende Auskunft der Personalstelle der Behörde, deren Teil die Vorprüfungsstelle ist, ein gleich geeignetes, aber milderes Mittel. Diese Vorgehensweise ermöglicht auch die in § 100 Abs. 5 Satz 2 BHO verlangte Anhörung des Leiters der Vorprüfungsstelle. Ein generelles Einsichtsrecht in die Personalakten eines Bediensteten ohne dessen Zustimmung besteht nach meiner Auffassung jedenfalls zu diesem Zweck nicht.

— Der Petitionsausschuß des Deutschen Bundestages hatte eine oberste Bundesbehörde aufgefordert, die Personal-, Disziplinar- und Sicherheitsakten eines Bediensteten vorzulegen, der nicht selbst Petent war. Auch dazu habe ich Stellung genommen: Die Pflicht zur Geheimhaltung von Personalakten über Dritte gilt grundsätzlich auch gegenüber dem Petitionsausschuß des Deutschen Bundestages (vgl. Maunz Dürig, Kommentar zu § 45c Grundgesetz, Rd. Nr. 23). Zwar gibt Artikel 45c Grundgesetz dem Petitionsausschuß zur Stärkung seiner Funktion direkte Informations- und Sachaufklärungsrechte gegenüber der Verwaltung, jedoch ergibt sich gerade aus § 3 des aufgrund dieser Verfassungsbestimmung erlassenen Gesetzes über die Befugnisse des Petitionsausschusses des Deutschen Bundestages, daß Aktenvorlage, Auskunft sowie der Zutritt zu Einrichtungen verweigert werden dürfen, wenn der Vorgang nach einem Gesetz geheimgehalten werden muß oder sonstige zwingende Geheimhaltungsgründe bestehen. Diese Formulierung entspricht weitgehend dem § 99 Abs. 1 Satz 2 Verwaltungsgerichtsordnung, der die Vorlage und Auskunftspflicht der Behörden im verwaltungsgerichtlichen Verfahren regelt. Das Bundesverwaltungsgericht hat dazu in einer vergleichbaren Fallkonstellation entschieden, daß die Verweigerung der Vorlage von Personalakten eine Ermessensentscheidung darstellt, in deren Rahmen das Geheimhaltungsinteresse des Beamten gegenüber etwaigen schutzwürdigen Interessen der Allgemeinheit oder Dritter abzuwägen ist (vgl. BVerwGE 19, 179 [186]). Diese Interessenabwägung obliegt der die Personalakten führenden Stelle und ist erschöpfend nur anhand der Umstände des Einzelfalles möglich. Die Entscheidung über eine Aktenvorlage hat in diesem Zusammenhang davon auszugehen, daß sich das parlamentarische Informationsrecht des Petitionsausschusses und das aus den Grundrechten der Artikel 1 und 2 Grundgesetz abgeleitete Personalaktengeheimnis prinzipiell gleichrangig gegenüberstehen. Sie müssen, wie das Bundesverfassungsgericht in seiner Entscheidung vom 17. Juli 1984 (BVerfGE 67, 100 ff. [144] — Flickausschuß-Urteil) ausgeführt hat, einander so zugeordnet werden, daß beide soweit wie möglich ihre Wirkung entfalten. Dabei ist auch zu bedenken, daß das Recht auf informationelle Selbstbestimmung grundsätzlich die Einwilligung des Beamten in eine zweckfremde Verwendung seiner Personalakten erfordert. Wird hiervon im überwiegenden Allgemeininteresse abgesehen, so ist im Rahmen der Interessenabwägung stets der Grundsatz der Verhältnismäßigkeit zu berücksichtigen. Demnach werden vollständige Personal- bzw. Disziplinarakten nur dann überlassen werden können, wenn es nicht ausreicht, bestimmte darin enthaltene Teile — möglicherweise nur dem Ausschußvorsitzenden und seinem Stellvertreter — zur Einsicht zur Verfügung zu stellen oder auf konkret formulierte Fragen des Petitionsausschusses hin Auskunft aus den Akten zu erteilen. Dies gilt in gleicher Weise für Sicherheitsakten, soweit diese mit Personalakten inhaltlich übereinstimmen.

Der Petitionsausschuß hat sich demgegenüber auf eine Aussage in dem erwähnten Urteil des Bundesverfassungsgerichts (Flick-Ausschuß-Urteil) berufen, wonach der in dem Verfahren streitige Anspruch auf Aktenvorlage nicht verkürzt werden dürfe, wenn das Parlament Vorkehrungen für den Geheimschutz getroffen habe. Diese Entscheidung läßt sich indessen nicht auf die Befugnisse des Petitionsausschusses übertragen, weil diese — anders als für parlamentarische Untersuchungsausschüsse — ausdrücklich gesetzlich eingeschränkt sind (§ 3 des Gesetzes nach Art. 45c GG).

Ein Hinweis auf die Geheimschutzordnung ist aus folgenden Gründen nicht relevant: Die Geheimschutzordnung des Deutschen Bundestages entspricht inhaltlich der Verschlußsachenanweisung für die Bundesbehörden (VS-Anweisung) und verweist teilweise auf diese. Nach § 5 Abs. 1 der VS-Anweisung ist Verschlußsache alles, was im staatlichen Interesse durch besondere Sicherheitsmaßnahmen vor Unbefugten geheimgehalten werden muß. Daraus ergibt sich, daß die Geheimschutzordnung Vorkehrungen zur Sicherheit des Staates und seiner Einrichtungen zum Gegenstand hat. Diese Vorschriften dienen ausschließlich staatlichen Geheimhaltungsinteressen und nicht Interessen des individuellen Persönlichkeitsschutzes, auch wenn diese in Einzelfällen übereinstimmen mögen. Deshalb werden in der Praxis der Personalverwaltung Personalakten im allgemeinen auch nicht als Verschlußsachen behandelt.

Etwas anderes gilt allerdings dann, wenn ein Bediensteter nicht Dritter eines Petitionsverfahrens ist, sondern sich selbst mit einer seine Dienststellung betreffenden Bitte an den Petitionsausschuß wendet. In einem solchen Fall erfolgt die Weitergabe seiner Personaldaten im Rahmen der Zweckbindung. Hier hielte ich es für sachgerecht, einen Petenten über die beabsichtigte Übersendung seiner Personalakte zu unterrichten und ihm eine Widerspruchsmöglichkeit einzuräumen, sofern seine Einwilligung nicht schon aus der Petition zu entnehmen ist.

7.2 Datenübermittlung an Selbsthilfeeinrichtungen und Gewerkschaften

Mehrere Eingaben warfen die Frage auf, inwieweit die Übermittlung von Mitarbeiterdaten an Gewerkschaften und Versicherungsunternehmen durch Bundesbehörden zulässig ist. Bei einer Prüfung dieses Sachverhalts bin ich zu folgendem Ergebnis gelangt:

Die Übermittlung von Mitarbeiterdaten ist bei verfassungskonformer, restriktiver Interpretation des § 24 Abs. 1 Satz 1 BDSG nur zu Zwecken der Erfüllung des Arbeits- bzw. Dienstverhältnisses (z. B. an die Sozialversicherung) zulässig (vgl. BAG, NJW 87 S. 2459ff.; LAG Mannheim, RDV 86, S. 20, 22). Die Übermittlung zu anderen Zwecken bedarf stets des Einverständnisses der Betroffenen. Das Recht auf informationelle Selbstbestimmung macht es erforderlich, den einzelnen grundsätzlich selbst über die Weitergabe und Verwendung seiner persönlichen Daten bestimmen zu lassen, sofern eine Rechtsgrundlage hierfür nicht existiert.

Dies trifft auf beide in Frage stehenden Übermittlungsvorgänge zu: Die Weitergabe der Mitarbeiterdaten an Selbsthilfeeinrichtungen für den öffentlichen Dienst und Gewerkschaften zu Werbezwecken liegt m. E. nicht im Rahmen der Zweckbestimmung des Dienstverhältnisses; insbesondere scheiden insoweit Fürsorgegesichtspunkte des Dienstherrn aus, auf die zuweilen in diesem Zusammenhang abgestellt wird.

Hinsichtlich der Übermittlung von Personaldaten an Gewerkschaften ergibt sich auch nichts anderes aus der hierzu häufig zitierten Verpflichtung zur Gewährleistung einer koalitionsmäßigen Betätigung durch Werbung neuer und Information schon vorhandener Mitglieder gemäß Artikel 9 Abs. 3 Grundgesetz. Wie das Bundesarbeitsgericht in seinem Urteil vom 23. September 1986 ausgeführt hat, muß dieses Recht dort seine Grenze finden, wo durch diese Betätigung Rechte anderer berührt werden (NJW 1987 S. 2891).

Rechtsgrundlage für die Datenübermittlung kann hier auch nicht § 24 Abs. 2 BDSG sein. Über den dort vorgegebenen Datenumfang hinaus werden bei einer Abgabe an Gewerkschaften und Versicherungsunternehmen weitere, die Mitarbeiter betreffende Angaben übermittelt, auch wenn sie nicht ausdrücklich in der Liste aufgeführt sind; denn aus dem Sachzusammenhang wird deutlich, daß die Betreffenden bei einer bestimmten Dienststelle der Bundesverwaltung beschäftigt sind. Die Übermittlung solcher inhaerenter Merkmale schließt die Anwendung des § 24 Abs. 2 BDSG aus.

Die Weitergabe der Mitarbeiterdaten ist also gemäß § 3 BDSG nur mit deren Einverständnis zulässig. Beim Einholen der Einwilligung ist dem Betroffenen deutlich zu machen, welche Daten an welchen Empfänger zu welchem Zweck übermittelt werden sollen. Der Datenempfänger ist zu verpflichten, die Daten nicht auf Dauer zu speichern, sie nicht weiterzugeben und nur für den vorgegebenen Verwendungszweck (z. B. Werbebrief, nicht aber Vertreterbesuch) zu benutzen.

Während mehrere Bundesbehörden das entsprechende Verfahren bereits an meinen Empfehlungen ausgerichtet haben, hat der Bundesminister für das Post- und Fernmeldewesen meiner Auffassung ausdrücklich widersprochen und angekündigt, das bisher praktizierte Verfahren der Datenübermittlung ohne Einwilligung der Betroffenen fortführen zu wollen.

7.3 Telefondatenverarbeitung

Bei der in den Dienstanschlußvorschriften des Bundesministers der Finanzen vorgesehenen Aufzeichnung von Telefonverbindungsdaten in der Anlage des Anrufers werden auch personenbezogene Daten des Angerufenen gespeichert. Die Aussagefähigkeit dieser Daten ist je nach Dauer und Häufigkeit der Gespräche oder auch je nach Person von Anrufer und Angerufenen, dessen Beziehung zum Anrufer und seiner Funktion von unterschiedlicher Bedeutung. Die Speicherung geht über die bloße Aufzeichnung der Rufnummer hinaus, da sie ein stattgefundenes Gespräch dokumentiert. Der Angerufene kann sich dem Anruf nicht entziehen und hat damit auf die Speicherung und die Art der Verarbeitung seiner Rufnummer keinen Einfluß, häufig wird er von dieser Speicherung auch gar nichts erfahren.

Bei der Beurteilung dieses Verfahrens kommt es darauf an, die Interessen des Anrufers bzw. der Dienststelle (z. B. an einer Kostenkontrolle) gegen eine Beeinträchtigung von Persönlichkeitsrechten auch des Angerufenen abzuwägen. In diesem Zusammenhang haben sich hinsichtlich der Erforderlichkeit der Speicherung der vollständigen Zielnummer in jünger Zeit neue Zweifel ergeben. So sind z. B. in Hessen am 1. April 1986 neue Fernsprechvorschriften erlassen worden, nach denen auf die Speicherung der Zielnummer des angerufenen Teilnehmers völlig verzichtet wird, gleich ob es sich um Dienst- oder Privatgespräche handelt.

Diese Problematik habe ich dem Bundesminister der Finanzen dargelegt und die Auffassung vertreten, Rechtsgrundlage für die Speicherung im Verhältnis zum Angerufenen könne nur § 9 (1) BDSG sein; es komme daher für die Zulässigkeit der Speicherung der vollständigen Zielnummer insoweit entscheidend auf deren Erforderlichkeit für die Aufgabenerfüllung der Behörde an, die sowohl für Dienst-, als auch für Privatgespräche nachzuweisen wäre.

Der Bundesminister der Finanzen hat mir daraufhin mitgeteilt, er werde den Entwurf der Dienstanschlußvorschriften dahingehend ändern, daß die Zielnummer von Privatgesprächen um eine Stelle verkürzt zu speichern sei, bei Dienstgesprächen dagegen solle es bei der Speicherung der vollen Zielnummer aus Gründen der Kontrollierbarkeit und der Rechnungslegung bleiben.

Ich halte meine dargelegten Bedenken dadurch nicht für ausgeräumt und habe dies dem Bundesmi-

nister der Finanzen mitgeteilt: Im Rahmen der datenschutzrechtlichen Beurteilung ist das Interesse der Stelle, von der der Anruf ausgeht, nämlich an der Effektivität der notwendigen Kontrollen und einer ordnungsgemäßen Rechnungslegung, abzuwägen gegen eine Beeinträchtigung von Persönlichkeitsrechten auch des Angerufenen; hierbei spielt, wie schon oben ausgeführt, die Frage der Erforderlichkeit eine wesentliche Rolle. Beispiele aus der Praxis, wie der bereits erwähnte völlige Verzicht im Lande Hessen, zeigen, daß eine ausreichende Kontrolle ohne Speicherung der Zielnummer offenbar möglich ist. So werden auch bei der Verwaltung des Deutschen Bundestages bei „telefongebührenpflichtigen Gesprächen" lediglich „die Nebenstelle und die Summe der Gebühreneinheiten pro Ablesemonat und Nebenstelle automatisch erfaßt" (Dienstvereinbarung vom 19. Mai 1987).

Soweit die Erforderlichkeit nicht zweifelsfrei nachgewiesen werden kann, ist daher ein völliger Verzicht auf Speicherung geboten.

7.4 Personalvertretung

7.4.1 Beratungen

Im abgelaufenen Berichtsjahr haben sich mehrere Personalvertretungen mit der Bitte um Beratung über datenschutzgerechte Lösungen bei der Einführung automatisierter Personaldatenverarbeitung an mich gewandt. Dabei zeigte sich, daß manche Personalvertretungen nicht genug über mögliche Auswirkungen der automatisierten Datenverarbeitung wissen, um feststellen zu können, ob die Persönlichkeitsrechte der Arbeitnehmer und Fragen der Mitbestimmung berührt werden. Bereits in meinem Sechsten und Achten Tätigkeitsbericht habe ich auf die besondere Bedeutung des Mitbestimmungsrechts der Personalvertretungen auch für die Sicherung des Datenschutzes der Arbeitnehmer hingewiesen.

Im Vordergrund der Beratungswünsche standen insbesondere folgenden Themenbereiche:

— Zulässigkeit der Datenverarbeitung

— Einsatz moderner Bürohilfsmittel (Personal Computer)

— Beurteilung von zur Verhaltens- und Leistungskontrolle geeigneter Systeme

— Organisatorische und technische Sicherungsmaßnahmen

— Konkrete Beteiligungs- und Kontrollmöglichkeiten der Personalvertretung.

Dafür, daß Personalvertretungen meine Beratung neben einer solchen durch ihren jeweiligen Dienstherrn in Anspruch nehmen, habe ich wegen der unvermeidlichen Interessengegensätze zwischen Personalvertretung und Behördenleitung (vgl. insbesondere § 68 Abs. 1, Satz 2 BPersVG) – bei aller Würdigung des Grundsatzes der vertrauensvollen Zusammenarbeit – Verständnis.

Ich halte es daher auch für legitim und zulässig, daß Personalvertretungen sich mit Beratungswünschen und Beschwerden ohne Kenntnis des Dienstherrn direkt an mich wenden.

In gleicher Weise sehe ich mich berechtigt, Kontakte zu Personalvertretungen aufzunehmen, ohne die Behördenleitung um Zustimmung bitten zu müssen. Die Auffassung des Bundesministers für das Post- und Fernmeldewesen, der eine solche unmittelbare Kontaktaufnahme für unzulässig hält, habe ich daher zurückgewiesen. Unabhängig hiervon pflege ich aber über Informationsgespräche mit Personalräten, die ich regelmäßig aus Anlaß von Kontrollen der Personaldatenverarbeitung führe, die jeweilige Behördenleitung zu informieren.

Der Befürchtung mancher Personalvertretungen, die Wahrnehmung ihrer gesetzlichen Aufgaben könnte erschwert werden, wenn der Dienstherr von Initiativen des Personalrats zur Kontaktaufnahme mit mir und deren Ergebnis Kenntnis erhält, vermag ich mich nicht zu verschließen. Dasselbe gilt für die Einschätzung, daß bei einer solchen Praxis den Personalvertretungen auch der Zugang zu mir erschwert werden könnte. Ich verfahre deshalb wie folgt: Stelle ich auf Grund solcher Initiativen Verstöße gegen datenschutzrechtliche Vorschriften fest, die eine Beanstandung nach § 20 Abs. 1 BDSG erfordern, ist die Information des Dienstherrn vorgezeichnet; den Hinweisgeber muß die Beanstandung nicht nennen. In allen sonstigen Fällen, in denen eine Benachrichtigung der zuständigen Dienststelle in Betracht kommt, stimme ich mich über mein Vorgehen im einzelnen vorher mit dem betreffenden Personalrat ab. Eine Benachrichtigung der Dienststelle über das Ergebnis der mit dem Personalrat geführten Erörterungen kommt beispielsweise dann in Betracht, wenn die Dienststelle von einer Anfrage des Personalrats an mich oder einem Beratungsersuchen bereits unterrichtet ist oder wenn ich davon ausgehen kann, daß der Personalrat meine Antwort der Dienststelle zur Unterstützung der eigenen Position ohnehin mitteilen wird.

7.4.2 Mitbestimmung als Zulässigkeitsvoraussetzung

Die begrenzte und im einzelnen auch umstrittene Reichweite der Mitbestimmung nach § 75 Abs. 3 Nr. 17 BPersVG – Einführung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen – erhöht mit zunehmender Einführung automatisierter Systeme das Risiko unzulässiger Personaldatenverarbeitung aufgrund fehlender Mitbestimmung. Erhebung, Speicherung und sonstige Verwendung von Personaldaten „in einem Personalabrechnungs- und Informationssystem sind zunächst dann mitbestimmungspflichtig, wenn diese Daten programmgemäß zu Aussagen über Verhalten oder Leistung einzelner Arbeitnehmer verarbeitet werden können" (vgl. BAGE 46, 367; vgl. auch BAG CR6/1987, S. 371).

Das Bundesarbeitsgericht hat die Mitbestimmungsbedürftigkeit inzwischen unter bestimmten Voraussetzungen auch auf Fälle ausgedehnt, in denen le-

diglich auf eine Gruppe von Beschäftigten bezogene Leistungs- und Verhaltensdaten erhoben und verarbeitet werden (vgl. BAG NJW 1986, S. 2070).

Führt eine Dienststelle ein solches Personaldatenverarbeitungssystem ein, so macht die Zustimmung der Personalvertretung die Datenverarbeitung nicht rechtmäßig, wenn sie nach datenschutzrechtlichen Vorschriften unzulässig ist. In Fällen der Mitbestimmungsbedürftigkeit kann dagegen die fehlende Beteiligung des Personalrats zur Unzulässigkeit der Datenverarbeitung gemäß § 3 Satz 1 BDSG führen. So hat das BAG beispielsweise in seinem Urteil vom 22. 10. 1986 (vgl. BAG a. a. O. S. 371) ausgeführt, daß unter Verstoß gegen Mitbestimmungsrechte erhobene Daten nicht gespeichert werden dürfen.

Werden dessen ungeachtet gleichwohl Personaldaten gespeichert und verarbeitet, so können die Betroffenen gegebenenfalls gemäß § 27 Abs. 3 Satz 2 BDSG ihre Löschung verlangen.

In Anbetracht der großen Unsicherheiten bei der richtigen Beurteilung automatisierter Personaldatenverarbeitungssysteme empfiehlt es sich für alle Dienststellen, die die Einführung solcher Systeme erwägen oder planen, so früh wie möglich neben den Datenschutzinstitutionen auch die Personalvertretung zu informieren und zu beteiligen. Dies gilt unabhängig davon, daß der Personalvertretung ohnehin ein erweitertes Informationsrecht zur Überwachung der zugunsten der Bediensteten geltenden Gesetze im Sinne des § 68 Abs. 1 Nr. 2 BPersVG zusteht, zu denen auch das Bundesdatenschutzgesetz zählt (so auch die Bundesregierung in Anlage zu BT-Drs. 10/4594, VI, S. 21). Das möglichst frühzeitige Zusammenwirken von Dienststelle, Personalvertretung und Datenschutzinstanzen empfiehlt sich schon deshalb, weil dadurch möglichen künftigen Unklarheiten, Unstimmigkeiten und Auseinandersetzungen zwischen den Beteiligten von vornherein wirksam vorgebeugt werden kann.

7.4.3 Vereinbarungen zwischen Dienststelle und Personalvertretung über die automatisierte Personaldatenverarbeitung

In meinem Sechsten Tätigkeitsbericht (S. 19) habe ich die umfassende Beteiligung der Personalvertretung schon in der Planungsphase der Einführung automatisierter Personaldatenverarbeitung empfohlen; das Bundesarbeitsgericht hat einen entsprechenden Anspruch der Betriebsräte inzwischen in ständiger Rechtsprechung bestätigt (vgl. BAG 1 ABR 59/85 in RDV 1987, 189, 194). In meinem Zuständigkeitsbereich wurden auch schon Vereinbarungen zwischen Personalvertretungen und Dienststellen über die Einführung und Anwendung von Datenverarbeitungsverfahren für Personaldaten abgeschlossen. Bei weiteren Stellen werden solche zur Zeit vorbereitet. Dies geschieht zum Teil unabhängig von insoweit bestehenden gesetzlichen Verpflichtungen etwa gemäß § 75 Abs. 3 Nr. 17 BPersVG. In diesen Vereinbarungen werden auch die allgemeinen Vorschriften des Bundesdatenschutzgesetzes konkretisiert, das für die Personaldatenverarbeitung keine speziellen Regelungen enthält. Sie sind deshalb besonders geeignet, die Persönlichkeitsrechte der Bediensteten datenschutzrechtlich abzusichern. Durch derartige Vereinbarungen kann auch die Akzeptanz der automatisierten Personaldatenverarbeitung entscheidend erhöht und künftigen Auseinandersetzungen wirksam vorgebeugt werden. Im Rahmen meiner Beratungsauftrages habe ich stets empfohlen, in den Vereinbarungen auch Zweckbestimmung, Inhalt und Ausmaß der automatisierten Personaldatenverarbeitung, Schutz- und Sicherungsvorkehrungen sowie Kontrollen der Maßnahmen präzise zu regeln.

In meinem Sechsten Tätigkeitsbericht (s. o.) bin ich auch auf Einzelfragen eingegangen, die bei der Umstellung auf automatisierte Personaldatenverarbeitung auftreten. In der Zwischenzeit haben sich die technischen Möglichkeiten verändert und die rechtliche Bewertung automatisierter Personaldatenverarbeitung wurde insbesondere aufgrund der Rechtsprechung des Bundesverfassungsgerichts sowie auch des Bundesarbeitsgerichts und des Bundesverwaltungsgerichts fortentwickelt. Aus heutiger Sicht empfehle ich, folgende datenschutzrechtliche Anforderungen zu berücksichtigen, wenn zwischen einer Dienststelle und einer Personalvertretung eine Vereinbarung über die Einführung und Anwendung von automatisierten Verfahren für die Personaldatenverarbeitung abgeschlossen werden soll:

1. Der Zweck der geplanten Personaldatenverarbeitung sollte im einzelnen beschrieben werden, um den unbestimmten Rechtsbegriff „Zweckbestimmung eines Vertragsverhältnisses" (hier: des Dienstverhältnisses) in den §§ 23ff. BDSG so präzise wie möglich auszufüllen.

2. Als Ziel der Vereinbarung sollte der Schutz der Persönlichkeitsrechte der Mitarbeiter und Beschäftigten vor unzulässigen Eingriffen festgelegt werden.

3. Die zugelassenen Daten einschließlich deren Herkunft, Löschungsfristen, Aufgaben, für deren Erfüllung die Speicherung erforderlich ist, und Hinweise auf die Rechtsgrundlagen sollten Bestandteil der Vereinbarung sein. Dabei sollten auch Ausschlüsse bzw. Verwendungsbegrenzungen für bestimmte Datenarten oder Daten (z. B. Beurteilungsnoten, Fehlzeiten oder medizinische und psychologische Daten) formuliert werden. Erweiterungen des Katalogs der Daten sind an die erneute Zustimmung des Personalrats zu binden.

4. Die Auswertungen und Übermittlungen von Personaldaten, die Zugriffe auf Personaldaten und die dazu Berechtigten sollten präzise festgelegt werden. Das Zweckbindungsprinzip ist dabei zu beachten (z. B. durch den Ausschluß freier Abfragesprachen). Auswertungen zum Zwecke lückenloser Leistungs- oder Verhaltenskontrolle sollten grundsätzlich verboten werden, ebenso heimliche Kontrollen mit technischen Hilfsmitteln. Auswertungen und Protokollierungen für Vorprüfungsstellen, für den Bundesrechnungshof oder den internen Datenschutzbeauftragten sollten ebenfalls bestimmt werden.

5. Die verwendete Hardware sollte beschrieben werden.

6. Als Maßnahmen zur Datensicherung sollte festgelegt werden, daß

   — Speicherungen nur in einer aktuellen Datei und in nach Zahl und Rhythmus bestimmten Sicherungskopien erfolgen dürfen,

   — die mit der Verarbeitung betrauten Personen namentlich bestimmt und nach § 5 BDSG verpflichtet werden,

   — die Programmentwicklungen und Tests grundsätzlich nicht mit echten Daten erfolgen.

7. Zur Präzisierung der Forderung nach „angemessenen" Sicherungsmaßnahmen (§ 6 Abs. 1 BDSG) sollten die Vorkehrungen genannt werden, die unter Berücksichtigung der Datenarten und der konkreten Umstände ihrer Verarbeitung zu treffen sind (z. B. in einem Katalog der Sicherungsmaßnahmen). Hierzu sollten zur Absicherung der strikten Zweckbindung Maßnahmen zur Zugriffsberechtigung und -kontrolle vereinbart werden, z. B. sollte

   — die Zugriffskontrolle durch eine Benutzeridentifikation und ein davon getrenntes persönliches Paßwort erfolgen, die vom System miteinander abgeglichen werden,

   — jeder Zugriffsberechtigte namentlich und unter Hinweis auf seine Funktion bestimmt werden,

   — ein Zugriffsberechtigter bei längerer Abwesenheit (z. B. bei Urlaub) die Möglichkeit haben und nutzen, sein Paßwort und seine Benutzeridentifikation zu sperren.

   Darüber hinaus sollten die je nach der Art der verwendeten Zugriffsverfahren zu treffenden weiteren Schutzvorkehrungen bezeichnet und der Umfang der Zugriffsprotokollierung sowie die Bedingungen festgelegt werden, unter denen die Zugriffsprotokolle genutzt werden dürfen.

8. Die Rechte der betroffenen Mitarbeiter sollten ausdrücklich festgehalten werden (z. B. Auskunfts-, Berichtigungs-, Sperrungs- und Löschungsrechte, regelmäßige Informationen über die gespeicherten Daten).

9. Besondere Zuständigkeiten der Personalvertretung und des internen Datenschutzbeauftragten sollten im einzelnen beschrieben werden (z. B. Beteiligung am formalisierten Freigabeverfahren, Einblick in Verfahrensunterlagen, Einsicht in Listen und Protokolle, Schulung).

7.5 Personaldatenverarbeitung auf PC in einem Fernmeldeamt

Bei der Kontrolle eines Fernmeldeamtes habe ich festgestellt, daß dort mit einem Personal-Computer (PC) sowohl Programme zur Personaldatenverarbeitung erstellt als auch die Unterstützung der Dienststellenleitung bei Führungsaufgaben erprobt wird. Die Verfahrensweise stützt sich auf die „Richtlinie für die Organisation der Dienststelle Datenverarbeitung (OrgRichtl. 36 DV)". In dieser Organisationsrichtlinie sind u. a. Aufgaben aufgelistet, die zwangsläufig die Speicherung personenbezogener Daten unumgänglich machen. Zur Erledigung von Personalverwaltungsaufgaben im Bereich dieser Dienststelle wurde eine Datenbank eingerichtet und zunächst mit „Echtdaten" der Bediensteten eröffnet; nachdem Betroffene und die Personalvertretung hieran Anstoß genommen hatten, wurden diese Daten gelöscht und die Dateien mit „Fiktivdaten" beschickt. Diese Verwendung eines PC steht im Gegensatz zu einer früheren Erklärung des Bundesministers für das Post- und Fernmeldewesen, daß ein Einsatz von Personalcomputern zur Verarbeitung von Personaldaten im Bereich der Bundespost nicht vorgesehen sei. Meine grundsätzlichen Bedenken gegen die Verarbeitung personenbezogener Daten mit PC (vgl. auch 8. TB S. 17 und 56 ff.) werden in diesem Fall dadurch verstärkt, daß den Anwendern weitgehend freie Hand bei der Auswahl oder eigenen Erstellung von Programmen gelassen wird, anstatt nach erfolgter Problemanalyse die notwendige Hard- bzw. Software zentral auszuwählen. Nach meiner Erfahrung wird dadurch in der Regel nicht nur ein datenschutzgerechter Einsatz erschwert, sondern auch ein Wildwuchs in der Programmierung und Programmanwendung gefördert, so daß Datenschutz und -sicherheit nicht gewährleistet sind. Maßnahmen, welche die Risiken der Personaldatenverarbeitung unter Verwendung von PC von vornherein ausschließen, wurden ebensowenig getroffen wie eine ausreichende Dokumentation im Sinne des § 15 BDSG bei der Verteilung dieser Geräte an die Fernmeldeämter.

Die Fernmeldeämter haben zwar mit der genannten Organisationsrichtlinie Vorschläge zu den Einsatzmöglichkeiten – u. a. auch für solche mit Personenbezug – erhalten, über die besonderen Risiken des PC-Einsatzes und deren Verminderung wurde jedoch nichts gesagt. Darüber hinaus fehlten Hinweise und Belehrungen hinsichtlich der Einhaltung der Pflichten nach dem BDSG sowie Hilfen zur Erfüllung der Sicherheitsauflagen gemäß § 6 BDSG und der hierzu gehörenden Anlage. Ich habe dieses Verfahren gemäß § 20 Abs. 1 BDSG beanstandet.

In seiner Erwiderung beruft sich der Bundesminister für das Post- und Fernmeldewesen für die Zulässigkeit der Speicherung der personenbezogenen Daten im wesentlichen auf § 23 BDSG. Dessen Voraussetzungen lagen aber nach meinen Feststellungen nicht vor, weil in diesem Dienststellenbereich eine Personaldatenverarbeitung im Rahmen der Zweckbestimmung des Dienstverhältnisses nicht in Betracht kommt. Hinsichtlich der von mir beanstandeten Personaldatenverarbeitung durch PC teilt er u. a. mit, insoweit sei derzeit keine bundesweite Anwendung vorgesehen. Zuletzt habe er am 12. August 1987 in einer Verfügung darauf hingewiesen, daß personenbezogene Daten nicht im Rahmen der individuellen Datenverarbeitung verarbeitet werden dürfen. Im übrigen sei die Verarbeitung personenbezogener

Daten auf PC bei den Behörden der Deutschen Bundespost durch umfangreiche Vorschriften geregelt und nur unter bestimmten Voraussetzungen zugelassen. Die insoweit getroffenen Maßnahmen stellten die Ausführung des BDSG sicher.

Von einer weiteren Speicherung personenbezogener Daten sei inzwischen abgesehen worden.

Damit wird indessen weder die von mir beanstandete unzulässige Personaldatenverarbeitung noch der Vorwurf der unzureichenden verfahrensmäßigen Absicherung der Datenverarbeitung mit PC im Sinne der Anlage zu § 6 BDSG entkräftet. Ich werde die Angelegenheit mit dem Bundesminister für das Post- und Fernmeldewesen weiter erörtern.

8. Post- und Fernmeldewesen

8.1 Datenschutz und Infrastrukturverantwortung der Deutschen Bundespost (DBP)

Erkennbarer Schwerpunkt der Investitionsaktivitäten der Deutschen Bundespost sind sowohl der Ausbau der Telekommunikationsnetze als auch die Erweiterung des Angebotes an Telekommunikationsgeräten und -diensten. Zur Erprobung sogenannter breitbandiger Dienste, wie z. B. des Bildtelefons, ist mit dem Aufbau eines Glasfaserkabel-Netzes begonnen worden. Besonders aber an das sogenannte Integrated Services Digital Network (ISDN) werden hohe Erwartungen hinsichtlich der Vielfalt möglicher technischer Anwendungen, verbesserter Übertragungsqualität sowie höherer Wirtschaftlichkeit geknüpft (s. u. Nr. 8.3.6). Beim Aufbau des ISDN hat die DBP in Europa eine Vorreiterrolle übernommen; bereits im Februar dieses Jahres wurden in Mannheim und Stuttgart im Rahmen eines Pilotprojektes zwei große ISDN-Vermittlungsstellen in Betrieb genommen, Ende 1988 soll in den acht größten Telefon-Ortsnetzen der Bundesrepublik der Anschluß an ISDN möglich sein. Die Umstellung des gesamten bestehenden Telefonnetzes wird in den nächsten 15 bis 20 Jahren im wesentlichen abgeschlossen sein. Diese angesichts der etwa 30 Millionen installierten Telefone sehr rasche Umstellung ist möglich, weil zur Übertragung die bereits verlegten Telefonkabel – wenn auch mit neuer Technik – weiterhin genutzt werden können.

Bereits mit der Ablösung der konventionellen Wähler-Vermittlungsstellen durch digitale Vermittlungscomputer ergeben sich neue Datenschutzprobleme und verschärfen sich bestehende. Der Grund liegt darin, daß – anders als in der herkömmlichen Vermittlungstechnik – für jedes Telefonat zunächst ein kompletter Datensatz angelegt wird, der nicht nur Aussagen über Zeitpunkt und Dauer des Gespräches enthält, sondern auch darüber, zwischen welchen Teilnehmern es geführt wurde (s. u. Nr. 8.3.5).

Wesentliches Kennzeichen eines ISDN-Basisanschlusses ist es, daß an jeder „Telefonsteckdose" nicht nur zwei Kanäle – wahlweise für normales Telefonieren, Text-, Bild- oder Datenübertragung – zur Verfügung stehen, sondern in demselben Kabel auch noch ein sogenannter Zentraler Zeichengabekanal geführt wird. Mit seiner Hilfe wird – ähnlich wie bereits in der digitalen Vermittlungstechnik – für jeden einzelnen Anschluß genau registriert, wann, wielange und mit wem ein Teilnehmer welche Art von Kommunikation durchführt; diese Daten werden bundesweit über das ISDN-Netz übermittelt und gespeichert. Die drei Kanäle können gleichzeitig und auch unterschiedlich genutzt werden.

Die DBP trägt aber nicht nur für die spezifischen Datenschutzrisiken schon angebotener Dienste die Verantwortung. Sie muß sich auch mit den Folgewirkungen der von ihr geschaffenen Infrastruktur auseinandersetzen, die sich in ihrer Gesamtheit noch gar nicht abschätzen lassen, weil die Nutzungsmöglichkeiten kaum voraussehbar sind.

Risiken können nicht nur aus Diensten entstehen, die von der Deutschen Bundespost selbst angeboten werden, sondern beispielsweise auch aus Angeboten privater Unternehmen, die mit Hilfe des ISDN überhaupt erst möglich werden. Auch wegen der Empfehlungen der Regierungskommission Fernmeldewesen, die ihren Bericht im September 1987 vorlegte, kommt diesem Thema besondere Bedeutung zu. Sollte diesen Empfehlungen, z. B. für den Endgerätebereich, Rechnung getragen werden, ist mit einem raschen Anwachsen von privaten Dienstangeboten zu rechnen, die eben nur mit Hilfe der Telekommunikationsdienste der DBP erbracht werden können. Weil kaum damit zu rechnen ist, daß jeder der Anbieter von sich aus den Datenschutz angemessen berücksichtigt, und weil manche Risiken auch nicht durch einzelne Dienste, sondern durch die Gesamtheit aller Kommunikationsdienste entstehen, halte ich es für dringend geboten, daß die DBP rechtzeitig ausreichende rechtliche und tatsächliche Schutzvorkehrungen trifft. Telekommunikationsanwendungen in rechtsfreien Räumen, wie z. B. die sog. „Elektronische Pinwand" im Bildschirmtextdienst, dürfte es dann nicht mehr geben (vgl. unten Nr. 8.4).

Durch die Einführung des ISDN erhöht sich die Übertragungskapazität des vorhandenen Netzes. Wie dargelegt, können über einen Anschluß gleichzeitig mehrere Kommunikationsvorgänge ablaufen. Dies läßt erwarten, daß sich der vermutete Anwendungsstau schnell abbaut und die Datenübertragung – auch bezüglich sensibler Daten – stark zunimmt. Dadurch gewinnt auch eine von mir bereits wiederholt erhobene Forderung an Bedeutung, eine kryptographische Verschlüsselung der zu übertragenden Daten zumindest dann zu ermöglichen, wenn diese besonders schutzbedürftig sind. Die technischen Probleme sind als grundsätzlich gelöst anzusehen.

Ein technisch hochstehendes Telekommunikationsnetz wie das ISDN benötigt zu seinem Betrieb einen komplexen Verbund einer Vielzahl von Rechenanlagen. Die dafür einzusetzende Software umfaßt mehrere Millionen einzelner „Befehle", die sich zum Teil gegenseitig bedingen und aufeinander beziehen. Es gilt heute als gesicherte Erkenntnis, daß solche Systeme nicht fehlerfrei programmiert werden können

und daher möglicherweise zu nachteiligen Wirkungen auch für den Persönlichkeitsschutz der Benutzer führen. Umso wichtiger ist es – auch aus der Sicht des Datenschutzes –, bei der Auswahl der Lieferfirmen sowie der Vertragsgestaltung und -abwicklung darauf zu achten, daß die Softwarequalität möglichst hoch und die Fehlerrate so niedrig wie möglich wird. Besonderes Augenmerk ist dabei auch auf die „Sauberkeit" der Software zu richten: Es sind Fälle bekanntgeworden, in denen in mißbräuchlicher Absicht Befehle in Programme eingebaut wurden, die sich erst zu späteren Zeitpunkten zum erheblichen Schaden des Systembetreibers oder der -anwender auswirkten. Die sich mit solchen Risiken beschäftigenden Berichte über „Computerviren", „Trojanische Pferde" u. ä. mögen gelegentlich übertrieben sein, unbestritten ist es aber möglich, gerade in großen Programmen unerwünschte Befehle zu verstekken. Es kann nicht übersehen werden, daß auch die Post und ihr Kommunikationsnetz für manchen ein reizvolles Ziel für solche schwer aufzudeckende Manipulationen sein könnten.

Wegen der großen Bedeutung zuverlässiger Kommunikationseinrichtungen für unsere Gesellschaft und die Rechte des Bürgers sollte schon die Erstellung der Software den besonderen Sicherheitsbedürfnissen Rechnung tragen. Darüber hinaus müssen Schutzmaßnahmen – wie das „elektronische Versiegeln" – gewährleisten, daß die laufenden Programme, z. B. im Rahmen der Wartung, nicht unzulässig verändert werden. Die DBP könnte als großer Abnehmer solcher Systeme durch Nachfrage nach geeigneten Sicherungsverfahren hier wesentliche Impulse geben, die auch anderen Anwendern, und zwar nicht nur im öffentlichen Bereich, zugute kommen würden.

8.2 Organisation des Datenschutzes bei der DBP

8.2.1 Arbeitskontakte zum Bundesministerium für das Post- und Fernmeldewesen

Nach wie vor besteht ein wesentlicher Teil meiner Arbeit im Bereich des Post- und Fernmeldewesens in der Bearbeitung von Bürgereingaben. Unverändert liegt auch der Schwerpunkt der Anliegen der Bürger im Bereich der Telekommunikation, insbesondere bei den neuen Diensten und Geräten. Bei vielen der mir von den Bürgern vorgetragenen Probleme ist es notwendig, die Deutsche Bundespost um ihre Stellungnahme zum Sachverhalt sowie zur rechtlichen Bewertung zu bitten. Dieses Verfahren erweist sich jedoch als zeitraubend, umständlich und für meine Dienststelle arbeitsintensiv, weil es häufig sehr lange dauert, bis das Ministerium reagiert. Dadurch bedingt ist der Zeitraum bis zur Beantwortung der Eingaben oft für die betroffenen Bürger unverständlich groß, in nicht seltenen Einzelfällen kaum noch zu vertreten.

Beispielhaft für viele steht der Fall des Petenten A. aus Düsseldorf: Eine Dienststelle der Deutschen Bundespost hatte durch einen Bearbeitungsfehler im Bildschirmtextdienst unzulässige Übermittlungen personenbezogener Daten an private Anbieterfirmen vorgenommen; dieser Sachverhalt ist unstreitig. Am 21. Januar 1987 stellte ich dem Bundesminister für das Post- und Fernmeldewesen einige Fragen zur Schadensbegrenzung und -prävention in solchen Fällen und bat um die Übersendung der einschlägigen Regelungen. Dieses Schreiben wurde schriftlich am 26. März, 30. April und 15. Juni, telefonisch am 6. Juli 1987 in Erinnerung gebracht. In einem Zwischenbescheid vom 8. Juli 1987 wurde mir mitgeteilt, die Angelegenheit werde von der zuständigen OPD noch geprüft. Weitere schriftliche Erinnerungen erfolgten am 16. September und 12. Oktober 1987. Mit Schreiben vom 7. Dezember 1987 teilte mir der Bundesminister für das Post- und Fernmeldewesen mit, „daß die bestehenden Regelungen dem Grunde nach ausreichend sind". Zum Inhalt der Regelungen wurden dabei keine Angaben gemacht. Es werden also weitere Bemühungen notwendig sein, um die zu einer abschließenden Beurteilung erforderlichen Informationen zu erhalten. Dieses Verhalten der DBP scheint mir auch nicht mit § 19 Abs. 3 BDSG vereinbar zu sein, wonach die Bundesbehörden verpflichtet sind, mich bei der Erfüllung meiner Aufgaben zu unterstützen und mir Auskunft zu meinen Fragen zu gewähren.

Über einen anderen Fall dieser Art habe ich den Ausschuß für das Post- und Fernmeldewesen des Deutschen Bundestages anläßlich der Beratungen meines Neunten Tätigkeitsberichtes am 4. November 1987 informiert.

8.2.2 Führung der Übersicht und Anmeldung der Dateien

Der Bundesminister für das Post- und Fernmeldewesen hat gemäß § 15 Satz 2 Nr. 1 BDSG in seinem Geschäftsbereich dafür zu sorgen, daß von den speichernden Stellen eine Übersicht geführt wird über die Art der gespeicherten Daten, über die Aufgaben, zu deren Erfüllung die Kenntnis dieser Daten erforderlich ist, sowie über deren regelmäßige Empfänger. Diese Übersicht soll der speichernden Stelle dazu dienen, die Ausführungen der Vorschriften über den Datenschutz, namentlich die Veröffentlichung der Dateien gemäß § 12 und die Meldung zum Register der automatisch betriebenen Dateien gemäß § 19 Abs. 4 BDSG sicherzustellen. Das ist nur möglich, wenn die Übersicht vollständig ist. Bei nahezu allen von mir durchgeführten Datenschutzkontrollen bei Stellen der Deutschen Bundespost hat sich jedoch gezeigt, daß dies nicht der Fall ist: Insbesondere bei den besonders wichtigen neuen Diensten der Telekommunikation fehlten in der Übersicht die entsprechenden Dateien personenbezogener Daten. Demgemäß wurden auch die gesetzlichen Meldepflichten gemäß § 19 nicht erfüllt. Zuletzt wurde dies bei der Kontrolle einer digitalen Ortsvermittlungsstelle festgestellt, in der personenbezogene Daten der Telefonteilnehmer – zum Teil sehr sensibler Art, wie z. B. Daten über den äußeren Ablauf einzelner Telefongespräche – gespeichert werden. Ich habe dem Bundesminister für das Post- und Fernmeldewesen bereits wiederholt mitgeteilt, daß das für den Bereich der DBP praktizierte Verfahren zur Erfas-

sung der Dateien in der Übersicht sowie zur Erfüllung der Meldepflichten zumindest bezüglich neu eingerichteter Verfahren offensichtlich nicht geeignet ist, eine lückenlose Erfassung sicherzustellen. Im Oktober 1987 habe ich schließlich das bei der DBP hierfür eingerichtete Verfahren gemäß § 20 Abs. 1 BDSG beanstandet. Der Bundesminister für das Post- und Fernmeldewesen hat meine Beanstandung zurückgewiesen, die nachgewiesenen Fälle als bedauerliche Einzelfälle bezeichnet und keine Verbesserungen des Verfahrens in Aussicht gestellt. Nach meinen Erfahrungen sind die Unterlassungen gerade bei den neuen Telekommunikationsdiensten aber so häufig, daß ohne eine Änderung der Datenschutzorganisation bei der Deutschen Bundespost weiterhin damit zu rechnen ist, daß die datenverarbeitenden Stellen gesetzlichen Verpflichtungen nicht nachkommen.

8.3 Fernsprechdienst

8.3.1 Beantragung eines Telefonanschlusses

Es steht außer Frage, daß in der heutigen Gesellschaft der Besitz eines Telefonanschlusses für viele Bürger lebenswichtig und unerläßlich geworden ist. Ein Verzicht hierauf ist daher in der Regel keine Alternative und würde in vielen Fällen zu schweren Beeinträchtigungen der privaten sowie beruflichen Verhältnisse führen. Umso wichtiger ist es, daß die Deutsche Bundespost in diesem Zusammenhang nur diejenigen Daten von Bürgern erhebt und verarbeitet, die für die Errichtung und den Betrieb des Telefonanschlusses unerläßlich sind. Aus Sicht des Datenschutzes ist es zu begrüßen, daß die zum 1. Januar 1988 in Kraft tretende Telekommunikationsordnung für die Begründung des Teilnehmerverhältnisses natürlicher Personen lediglich die Erhebung des Namens, der Anschrift und des Geburtsdatums zuläßt (§ 363 Abs. 1 TKO).

Sehr viel weitergehendere Angaben wurden demgegenüber noch bis Mitte dieses Jahres in Fällen verlangt, auf die ich in Eingaben hingewiesen wurde. Sie betrafen Bürger, die einen Antrag auf vorrangige Einrichtung eines Telefonanschlusses deswegen stellten, weil sie z. B. aus gesundheitlichen Gründen darauf besonders dringend angewiesen waren. In dem Antragsvordruck mußte u. a. der behandelnde Arzt des Betreffenden genaue Angaben über Art und Umfang von dessen Erkrankung oder Behinderung machen. Auf meine Initiative hin wird inzwischen darauf verzichtet. Dies ist auch angebracht, weil – ungeachtet der ärztlichen Schweigepflicht – derartige Angaben nicht erforderlich sind, um die heutzutage in der Regel kurzfristig mögliche Herstellung eines Telefonanschlusses zu veranlassen.

8.3.2 Autotelefon

Bereits im Jahre 1950 nahm die DBP die ersten Anlagen des „öffentlich-beweglichen Landfunkdienstes" in Betrieb: Zum ersten Male in der Geschichte des Telefons konnten Privatpersonen aus dem Auto heraus – oder vom Schiff aus – telefonieren. Die Zahl der Teilnehmer hat sich seitdem von etwa 30 im Jahre 1950 auf ungefähr 60.000 erhöht.

Derzeit werden von der DBP zwei Netze betrieben, die sich in ihrer technischen Ausgestaltung unterscheiden, das sogenannte B-Netz und das C-Netz. Für den Anwender unterscheiden sich die beiden Netze vor allem in den verwendeten Autotelefongeräten, wobei die des modernen C-Netzes sich u. a. durch größeren Bedienungskomfort und erhöhte Mißbrauchssicherheit auszeichnen. Das bereits 1972 aufgebaute B-Netz kann aus technischen Gründen nicht mehr als etwa 26.000 Funktelefone aufnehmen. Daher wurde am 1. September 1985 das C-Netz in Betrieb genommen, das bereits etwa 37.000 Teilnehmer versorgt und bis auf mindestens 300.000 Teilnehmern ausgebaut werden kann. Die DBP plant allerdings bereits für das Jahr 1991 die Errichtung eines D-Netzes mit einer Kapazität von 2.000.000 Teilnehmern in der Bundesrepublik Deutschland.

So faszinierend die technischen Möglichkeiten und der Anwendungskomfort auch sein mögen, so knüpfen sich an die im Funktelefondienst vorgenommenen Datenspeicherungen doch häufig Besorgnisse, wie sie mir auch in Eingaben mitgeteilt werden. Besonders durch landespolitische Ereignisse der letzten Zeit ist den Bürgern bewußt geworden, daß – anders als bei „normalen" Telefongesprächen (s. unten Nr. 8.3.5) – zahlreiche weitere Datenverarbeitungen in Rechnern der DBP erfolgen.

Entsprechend der Zweckbestimmung können die Daten dabei nach Bestands-, Verbindungs- und Gebührendaten unterschieden werden. Als Bestandsdaten werden Angaben zur Person des Teilnehmers sowie zu dem verwendeten Autotelefongerät gespeichert, die der „Verwaltung" des Teilnehmers sowie der ihm für die Benutzung des C-Netzes, auf das sich die weitere Darstellung bezieht, übergebenen „Berechtigungskarte" dienen. Diese Berechtigungskarte speichert auf einem Magnetstreifen u. a. einige den Inhaber identifizierende Angaben und muß zur Inbetriebnahme in das Autotelefon eingeschoben werden.

Bei der Benutzung des Autotelefons im C-Netz werden ständig umfangreiche Speicherungen für das Herstellen gewünschter Verbindungen vorgehalten: Unabhängig von seinem momentanen Standort ist ein Autotelefon stets über die gleiche Vorwahl (0161) erreichbar. Damit dies gewährleistet ist, muß das System zu jedem Zeitpunkt den Aufenthalt des Fahrzeuges kennen. Zu diesem Zweck meldet jedes *betriebsbereite* Autotelefon automatisch in kurzen Zeitabständen seinen Aufenthaltsort – gekennzeichnet durch die jeweilige „Funkzone", in der sich das Fahrzeug gerade befindet – und die Nummer der Berechtigungskarte, mit der es gerade aktiviert ist, an die ortsfeste Funkstation, und zwar auch dann, wenn das Autotelefon nicht benutzt wird. Nach meinen Informationen erfolgen diese Speicherungen jedoch nur vorübergehend, nämlich nur für die Aufenthaltsdauer in der jeweiligen Funkzone. Abhängig von den geographischen Gegebenheiten haben diese Funkzonen Durchmesser von ca. 4 bis 50 km.

Baut ein Telefonteilnehmer von seinem Fahrzeug aus eine Gesprächsverbindung auf, so entsteht im Verlauf des Gespräches ein Datensatz, der neben der Kennung der Berechtigungskarte und den Angaben zum Zeitpunkt, zur Dauer und zu den aufgekommenen Gebühren der Gesprächsverbindung auch die angewählte Telefonnummer sowie die Nummern der Funkzonen enthält, in denen das Gespräch begonnen und beendet wurde. In der entgegengesetzten Gesprächsrichtung – also bei Anruf eines Fahrzeuges vom „normalen" Telefon aus – entsteht ein ähnlicher Datensatz, der allerdings die Telefonnummer des Anrufers nicht enthält. Bezüglich der Aufbewahrungsdauer dieser Einzelgesprächsdaten hat mir die Deutsche Bundespost mitgeteilt, daß die Gesprächsdatensätze regelmäßig am 80. Tag nach Absendung der Fernmelderechnung automatisch gelöscht werden. Unter Berücksichtigung der Verarbeitungsdauer bleiben somit in der Praxis die Einzelgesprächsdaten eines Funktelefonates, das am ersten Tag des Erfassungszeitraumes – etwa vier Wochen – geführt wurde, bis zu 120 Tagen gespeichert.

Auf die datenschutzrechtlichen Probleme im Zusammenhang mit der Registrierung von Einzelgesprächsdaten im Funkfernsprechdienst der Deutschen Bundespost habe ich wiederholt hingewiesen. So habe ich unter Bezug auf eine im April 1984 vorgenommene Datenschutzkontrolle bereits in meinem Siebenten Tätigkeitsbericht (S. 25 f.) dieses Thema aufgegriffen und die Speicherungen der Einzelgesprächsdaten unter Gesichtspunkten des Datenschutzes für bedenklich erklärt; die Bundespost ist meinen Bedenken aber nicht gefolgt. In meinem Neunten Tätigkeitsbericht (S. 31) habe ich dieses Thema erneut angesprochen und im Zusammenhang mit der Verabschiedung der neuen Telekommunikationsordnung darauf hingewiesen, daß die Speicherung der Einzelgesprächsdaten – wenn die Deutsche Bundespost aus betrieblichen Gründen hieran festhalten will – einer ausdrücklichen und transparenten Regelung in der Telekommunikationsordnung bedarf. Auch meine Bemühungen, die Post zu veranlassen, durch Merkblätter, in der Bedienungsanleitung oder auf andere Weise die Betroffenen auf die Speicherung hinzuweisen, blieben bisher ohne den gewünschten Erfolg.

Es kann kein Zweifel bestehen, daß die oben beschriebenen Einzelgesprächsdaten dem Schutz des Fernmeldegeheimnisses aus Artikel 10 GG unterliegen. Dies kommt auch in § 10 Abs. 1 Satz 3 des Fernmeldeanlagengesetzes zum Ausdruck, nach dem sich dieser Schutz „auch auf die näheren Umstände des Fernmeldeverkehrs, insbesondere darauf, ob und zwischen welchen Personen ein Fernmeldeverkehr stattgefunden hat", erstreckt.

Nach Auffassung der Deutschen Bundespost darf jedoch über die Einzelgesprächsdaten – unabhängig vom Anlaß ihrer Speicherung – Auskunft gemäß § 12 des Fernmeldeanlagengesetzes erteilt werden. Nach dieser Vorschrift kann „in strafgerichtlichen Untersuchungen ... der Richter und bei Gefahr im Verzuge auch die Staatsanwaltschaft Auskunft über den Fernmeldeverkehr verlangen, wenn die Mitteilungen an den Beschuldigten gerichtet waren oder wenn Tatsachen vorliegen, aus denen zu schließen ist, daß die Mitteilungen von dem Beschuldigten herrührten oder für ihn bestimmt waren und daß die Auskunft für die Untersuchung Bedeutung hat."

Anders als die §§ 100 a und 100 b der Strafprozeßordnung, die eine Durchbrechung des Fernmeldegeheimnisses nur für einen abschließenden Katalog besonders schwerwiegender Straftaten vorsehen, könnte demnach bei Anwendung von § 12 des Fernmeldeanlagengesetzes der Autotelefonverkehr eines Beschuldigten in allen Fällen strafrechtlicher Ermittlungen offengelegt werden. Dieser erhebliche Unterschied dürfte daran liegen, daß diese Vorschrift im wesentlichen unverändert aus der Fassung des Gesetzes vom 14. Januar 1928 übernommen worden ist. Betroffen waren damals lediglich die manuellen Aufschreibungen des „Fräuleins vom Amt" bei Ferngesprächen; automatisierte Aufzeichnungen existierten nicht. Angesichts der vollständigen und umfassenden Aufzeichnungen in modernen Kommunikationsnetzen wie dem C-Netz des Funktelefondienstes erscheint daher heute die Frage berechtigt, ob und in welchem Umfange die Vorschrift des § 12 Fernmeldeanlagengesetz zu einer Offenlegung der Telekommunikation des Betroffenen noch herangezogen werden kann.

8.3.3 Kartentelefon

Die Benutzung eines öffentlichen Münzfernsprechers ist wegen der erforderlichen Münzen oftmals unbequem; außerdem werden die Geräte – wie die Schadensstatistiken der DBP belegen – häufig manipuliert oder ausgeraubt. Die DBP hat daher einen Betriebsversuch mit sogenannten Kartentelefonen aufgenommen. Anstelle von Münzen werden dabei in den Telefonapparat Kunststoffkarten eingeführt, in die eine miniaturisierte elektronische Schaltung, ein Chip, integriert ist. Dabei sind zwei Arten von Karten zu unterscheiden: Die „Guthabenkarte" kann am Postschalter zu einem Preis gekauft werden, der sich aus ihrem Gebührenwert und einem gewissen Aufschlag zusammensetzt. Während des Telefonates „verbraucht" sich dieses Guthaben in Abhängigkeit von der entstandenen Anzahl von Telefon-Gebühreneinheiten. Personenbezogene Daten werden dabei nicht gespeichert. Als Alternative wird die sog. Buchungskarte angeboten; sie erhält ein Telefonanschlußinhaber auf Antrag von seinem Fernmeldeamt. Die bei ihrer Benutzung entstehenden Gebühren werden seiner Telefonrechnung zugeschlagen. Das Verfahren sowohl der Verarbeitung der Stammdaten dieses Telefonteilnehmers als auch der bei der Benutzung der Buchungskarte anfallenden Einzelgesprächsdaten habe ich kontrolliert.

Auch bezüglich dieser Dateien war die DBP ihren Pflichten zur Veröffentlichung gemäß § 12 BDSG und zur Meldung der Dateien zum Register der automatisch betriebenen Dateien gemäß § 19 Abs. 4 BDSG nicht nachgekommen (s. oben Nr. 8.2.2).

Zentrales Anliegen der Kontrolle war die Speicherung und Verarbeitung der Gesprächsdatensätze, die am Ende eines gebührenpflichtigen Gesprächs erzeugt und zunächst auf der Karte selbst gespei-

chert werden. In dem derzeit angewandten Verfahren enthält dieser Datensatz jedoch in der Regel die Gebührensumme mehrerer Gespräche, deren Gebühreneinheiten im Speicher der Karte aufsummiert werden. In unregelmäßigen zeitlichen Abständen werden diese Gebührensummen automatisch und vom Karteninhaber unbemerkt aus Anlaß eines Telefongesprächs von einem zentralen Rechner abgerufen und zu der dort bereits vorhandenen Summe hinzuaddiert. Dadurch ist weder erkennbar, von welchem Kartentelefon aus ein bestimmtes Telefonat geführt wurde, noch zu welchem Zeitpunkt es erfolgte oder wieviel Gebühreneinheiten entstanden sind. Die DBP hat mir bestätigt, daß auch die Telefonnummer des angerufenen Teilnehmers nicht registriert wird.

Der BMP hat mich jedoch über seine Absicht informiert, in Zukunft auf der Karte nicht nur den Standort des Kartentelefones zu registrieren, von dem aus ein Gespräch geführt wurde, sondern auch die Einzelgesprächsdaten, insbesondere die angewählte Rufnummer. Unter Datenschutzgesichtspunkten werfen solche Registrierungen der dem Fernmeldegeheimnis unterliegenden und daher sehr schutzbedürftigen Gesprächsdaten erhebliche Probleme auf. Sorgfältiger Untersuchung bedarf dabei die Frage, ob schutzwürdige Belange des *Angerufenen* dadurch beeinträchtigt werden können, daß ohne seine Einwilligung nicht nur registriert wird, daß, zu welchem Zeitpunkt und mit welcher Dauer sein Anschluß benutzt wurde, sondern – sofern es sich um ein ISDN-Anschluß handelt – auch, ob telefoniert oder welche andere Kommunikationsform genutzt wurde.

Entscheidet sich die DBP für die Speicherung der Verbindungsdaten, ist in jedem Fall zu fordern, daß der jeweilige Benutzer der Buchungskarte über diese Art der Registrierung präzise informiert wird. Ihm muß auch verdeutlicht werden, daß die Speicherung nicht nur die Auswertung der Datensätze durch die DBP ermöglicht, sondern daß über sie bei Vorliegen der Voraussetzungen des § 12 Fernmeldeanlagengesetz auch Auskünfte in einem Strafverfahren erteilt werden (s. dazu Nr. 8.3.2). Auch für den angerufenen Partner muß die Speicherung und ihre mögliche Verwertung transparent sein.

Die Datenübertragungen zwischen den einzelnen Komponenten des Kartentelefonsystems (Kartentelefon, Vermittlungsstelle, zentraler Rechner) erfolgen im öffentlichen Datexnetz, das jedermann zugänglich ist. Es muß daher auch die Frage geklärt werden, ob die in diesem Netz erzielbare Sicherheit gegen unbefugten Zugriff der Schutzbedürftigkeit der Daten entspricht. In diesem Zusammenhang ist auf die sich in jüngster Zeit häufenden Berichte über Aktivitäten von „Hackern" zu verweisen, insbesondere auf das Anfang September 1987 gelungene Eindringen in ein weltweites amerikanisches Datennetz.

Auch die zur Sicherstellung des Datenschutzes getroffenen technischen und organisatorischen Maßnahmen nach § 6 Abs. 1 Satz 1 BDSG waren teilweise unzureichend. So war der Systemzugang an den Bildschirm-Bedienungsplätzen nur durch einen einfachen Schlüsselschalter geschützt; eine Paßwortprozedur war nicht vorgesehen (s. auch Nr. 8.3.5). So konnte jeder Bedienstete, der den Schlüssel benutzen darf, unabhängig von seiner Aufgabenstellung nicht nur alle Dateien einsehen, sondern auch alle personenbezogenen Daten verändern und löschen. Eine nachträgliche Mißbrauchsaufklärung wäre im Bedarfsfall schon deswegen nicht möglich gewesen, weil keinerlei Protokollierungen der Benutzeraktivitäten erfolgten.

Ich habe den Bundesminister für das Post- und Fernmeldewesen um Stellungnahme zu den angesprochenen Problemen gebeten; sie stand bei Erstellung dieses Berichts noch aus.

8.3.4 Mithören von Telefonaten durch Dritte

Ein Petent hatte mich darauf aufmerksam gemacht, daß die von Telefonapparaten einer bestimmten Ausführung aus geführten Telefonate im Langwellenbereich eines Rundfunkempfängers abzuhören sind. Dies ist bis zu einer Entfernung von ca. 2 Metern – auch durch Wände hindurch – beobachtet worden. Bei den betroffenen Telefonapparaten handelt es sich um solche mit Gebührenanzeiger in konventioneller Ausführung; die moderneren sogenannten Komforttelefone weisen den Effekt nicht auf. Die Deutsche Bundespost hat mir nach entsprechenden Untersuchungen diesen Sachverhalt bestätigt, einen generellen Austausch der Geräte jedoch abgelehnt. Angesichts der begrenzten Gefährdung erscheint mir dies vertretbar. Sehr bedauert habe ich jedoch, daß meine Empfehlung, die betroffenen Teilnehmer in geeigneter Weise zumindest auf das Problem hinzuweisen, abgelehnt wurde.

Nicht nur bei Telefonapparaten, sondern bei Telekommunikationsgeräten aller Art treten „kompromittierende Strahlungen" auf; ich habe hierüber auch in meinem Neunten Tätigkeitsbericht (S. 74f.) berichtet. Die DBP sollte den vorliegenden Fall zum Anlaß nehmen, ihre Anforderungen an Telefonapparate und andere Telekommunikationsendgeräte hinsichtlich unzulässiger Abstrahlungen zu überprüfen und zu verschärfen.

Ebenfalls durch Eingaben wurde ich auf die Möglichkeit unbefugten Mithörens bei „teilgesperrten" Anschlüssen hingewiesen. Die Teilsperre eines Anschlusses wird entweder von Amts wegen – z. B. wegen nicht bezahlter Gebühren – oder aber auch auf Antrag des Teilnehmers durchgeführt. Von dem betroffenen Apparat aus können dann keine Telefonate mehr geführt, jedoch Anrufe entgegengenommen werden. Wird bei einem solchen Apparat der Hörer nicht oder nicht richtig aufgelegt, so erhält ein Anrufer nicht etwa – wie normalerweise – das Besetztzeichen, vielmehr wird die Verbindung unmittelbar hergestellt und der Anrufer kann – ohne daß dies von dem Betroffenen bemerkt wird – etwa Gespräche mithören, die in der Nähe des Telefonapparates geführt werden, er lauscht quasi in der Wohnung des Angerufenen. Auch hier wäre es m. E. geboten, die Betroffenen zumindest in geeigneter Weise über diese Möglichkeit aufzuklären. Auch wenn eine Rechts-

verpflichtung hierfür möglicherweise nicht besteht, so könnte dies doch aus Gründen der Kundenfreundlichkeit erfolgen. Um so mehr ist es zu bedauern, daß der Bundesminister für das Post- und Fernmeldewesen es abgelehnt hat, etwa im Rahmen der bei einer Teilsperrung ohnehin anfallenden Kundenkontakte eine solche Information zu geben.

8.3.5 Digitale Fernsprech-Vermittlungstechnik

Der Leitungsweg einer Telefonverbindung im Postnetz besteht aus mehreren Leitungsstücken. Diese Leitungsabschnitte werden – gesteuert von der Wählscheibe, die der Telefonteilnehmer an seinem Apparat betätigt – in den Vermittlungsstellen der DBP durch elektrische Schalter (Wähler) miteinander verbunden. Für die Dauer des Telefonates bleiben die Wähler in der durch die Ziffernwahl bestimmten Stellung, nach Auflegen des Hörers gehen sie in ihre Ausgangsstellung zurück; der Leitungsweg zerfällt wieder in Teilstücke. Ausgehend von diesen Gegebenheiten der konventionellen Fernsprech-Vermittlungstechnik konnte der Telefonteilnehmer daher bislang im allgemeinen davon ausgehen, daß sein Gespräch nach der Beendigung keine Spuren hinterläßt. Weil die Technik es nicht erlaubte, wurde an keiner Stelle des Telefonnetzes festgehalten, wer mit wem zu welcher Zeit telefoniert hatte. Sollte das ausnahmsweise trotzdem registriert werden, so waren dafür zusätzliche, besonders anzubringende Geräte erforderlich. Dies änderte sich bereits im Jahre 1978, als die DBP begann, die konventionelle Wählertechnik in den Vermittlungsstellen durch das Elektronische Wählsystem (EWS) zu ersetzen. Gleichzeitig wurde damit begonnen, die Verbindungsdaten – Zeitpunkt, Dauer, aufgekommene Gebühren und angewählte Telefonnummer – aller Ferngespräche zu registrieren, die ein bestimmtes Gebührenaufkommen überschritten. Nicht zuletzt wegen meiner unverzüglichen und nachdrücklichen Einwände wurde diese Vollspeicherung jedoch bald eingestellt (vgl. 3. TB S. 31). Die EWS-Technik war im übrigen bereits bei ihrer Einführung technisch überholt; seit 1985 werden stattdessen Ortsvermittlungsstellen in digitaler Vermittlungs-Technik (DIV-Technik) errichtet; derzeit sind es nahezu zwanzig. Anders als bei den früheren EWS-Vermittlungsstellen handelt es sich hierbei um Rechner, deren hohe Leistungsfähigkeit auch einen dementsprechenden Bedarf an Sicherheitsvorkehrungen bedingt.

Im Oktober des Berichtsjahres kontrollierten meine Mitarbeiter erstmals eine DIV-Vermittlungsstelle. Sie gewannen dabei den Eindruck, daß das technisch-organisatorische Konzept zum Betrieb der DIV-Vermittlungsstellen noch nicht in ausreichendem Maße den Unterschieden zur herkömmlichen Wählertechnik Rechnung trägt. Dies wird deutlich am Beispiel der Bildschirmterminals, mit deren Hilfe die technischen Einrichtungen betrieben, aber auch die Teilnehmerbestands- und Verbindungsdaten verwaltet werden. So können einige Bedienungsfunktionen – z. B. die Sperrung des Anschlusses – unmittelbar zu einer Beeinträchtigung der schutzwürdigen Belange von Betroffenen führen. Dies gilt auch für Bedienungsvorgänge, die den Zugriff auf solche Daten umfassen, die dem Schutz des Fernmeldegeheimnisses unterliegen, so z. B. beim befristeten Zählvergleich (BZV) und der Fangschaltung. In konventionellen (Wähler-)Vermittlungsstellen bestehen technisch bedingte Hemmnisse dagegen, daß solche Maßnahmen versehentlich oder mißbräuchlich, jedenfalls ohne dienstliche Veranlassung, vorgenommen werden. Diese Hemmnisse gibt es bei digitalisierten Vermittlungsstellen nicht: Maßnahmen der genannten Art können von einer Person allein durch ein einfaches Kommando am Bildschirm bewirkt werden, was technisch nur sehr schwer verhindert werden kann. Große Bedeutung kommt daher solchen technischen und organisatorischen Maßnahmen zu, die einerseits das Verfahren gegen die Benutzung durch Unbefugte sichern, andererseits aber auch eine zweifelsfreie nachträgliche Aufklärung gestatten.

Zur Sicherstellung einer wirksamen Eingabe- und Speicherkontrolle wird in solchen Fällen üblicherweise – neben anderen technisch-organisatorischen Maßnahmen – auch ein Paßwortsystem eingesetzt. Hierbei erhält jeder Bedienstete ein individuelles Paßwort, mit dessen Hilfe er einerseits überhaupt erst Systemzugang erhält, andererseits jedoch nur solche Bedienungsvorgänge ausführen kann, die seiner geschäftsplanmäßigen Aufgabenzuweisung entsprechen. Durch Protokollierungen lassen sich Stichprobenkontrollen, aber auch nachträgliche Aufklärungen eventueller Unstimmigkeiten ermöglichen.

Aufgrund meiner Feststellungen in der kontrollierten Ortsvermittlungsstelle habe ich dem Bundesminister für das Post- und Fernmeldewesen dringend empfohlen, die technischen Einrichtungen und die entsprechenden Arbeitsanweisungen zu ergänzen.

Ich gehe im übrigen davon aus, daß die festgestellten Mängel nicht aufgetreten wären, wenn bereits frühzeitig die für den Datenschutz bei der DBP zuständigen Stellen bei der Entwicklung des Betriebskonzeptes beteiligt worden wären. Dies gilt auch für das Unterlassen der gesetzlich vorgeschriebenen Veröffentlichung und Registermeldung (s. oben Nr. 8.2.2).

8.3.6 Leistungsmerkmale künftiger ISDN-Telefone

Bereits mit Inkrafttreten der neuen Telefonkommunikationsordnung zum 1. 1. 1988 wird die Deutsche Bundespost zwischen zwei Arten von Telefonanschlüssen unterscheiden, dem „normalen" Anschluß in der alten, analogen Technik und dem „Universalanschluß" in der ISDN-Technik (siehe auch 8.1). Universalanschlüsse ermöglichen nicht nur – wie bereits dargelegt – zwei gleichzeitige Kommunikationsvorgänge, sondern bieten darüber hinaus neue Leistungsmerkmale, die indes aus der Sicht des Datenschutzes auch Probleme aufwerfen.

Die neuen ISDN-Telefonapparate, die bereits jetzt in vielen hausinternen Telefonanlagen Verwendung finden, weisen ein kleines Anzeigefeld (Display) auf. Auf diesem kann z. B. die Telefonnummer eines An-

rufers angezeigt werden. Auch wenn dies oftmals wünschenswert erscheint, so ist jedoch für eine Reihe besonderer Anwendungen – wie z. B. die Telefonseelsorge oder Gesundheitsberatung – die Anonymität des Anrufers unerläßlich. Die hier zu erwartenden Konflikte lassen sich m. E. am besten dadurch lösen, daß der Anrufende von Fall zu Fall entscheiden und entsprechend steuern kann, ob seine Telefonnummer angezeigt wird oder nicht, und der Angerufene dann entscheidet, ob er den jeweiligen Anruf annimmt. Ob dieses Leistungsmerkmal wirklich so kundenfreundlich realisiert werden soll, ist mir bisher nicht bekannt.

Auch die besondere Betriebsmöglichkeit „Anrufumleitung" bzw. „Anrufweiterleitung" ist sicherlich in vielen Situationen eine Hilfe: Sie ermöglicht es einem Telefonteilnehmer, einen von ihm erwarteten, wichtigen Anruf z. B. in der Wohnung von Bekannten entgegenzunehmen, während er sich dort aufhält. Hierbei wird die DBP jedoch Vorkehrungen zu treffen haben, die eine mißbräuchliche Einrichtung einer solchen Anrufumleitung bzw. -weiterschaltung – etwa zu Lasten eines unbeteiligten Dritten – verhindern.

Künftig soll sich durch das sog. „Anklopfen" ein Anrufer auch dann bei einem Telefonteilnehmer bemerkbar machen können, wenn dieser bereits ein Telefonat führt: Während des Gesprächs hört der Angerufene ein besonderes Signal, gleichzeitig erscheint die Telefonnummer des Anrufers auf dem Display seines Apparates. Auch wenn dies bei beruflicher Nutzung des Telefones mitunter wünschenswert erscheint, so könnte es zumindest im privaten Bereich als Störung oder gar als Belästigung empfunden werden. Hier sollte jedem Teilnehmer die Möglichkeit gegeben werden, sich gegen solches „Anklopfen" auf Wunsch zu schützen.

Der Bundesminister für das Post- und Fernmeldewesen hat bereits zu einigen Aspekten der neuen Leistungsmerkmale der ISDN-Telefone meine Beratung in Anspruch genommen. Ich gehe davon aus, daß er dies auch weiterhin tun wird.

8.3.7 Meinungsumfragen bei Telefonteilnehmern

Seit September 1985 können sich Telefonteilnehmer zusätzlich zu ihrem „normalen" Apparat von der DBP das schnurlose Telefon „SINUS" anschließen lassen. Die Verbindungsschnur zwischen Telefonapparat und Hörer wird dabei durch eine Funkverbindung ersetzt; der Telefonteilnehmer kann sich beim Telefonieren bis zu 200 Meter vom Apparat entfernen. Zur Erforschung der Akzeptanz dieses schnurlosen Telefons erteilte der Bundesminister für das Post- und Fernmeldewesen einem privaten Marktforschungsinstitut einen entsprechenden Auftrag und übermittelte ihm in diesem Zusammenhang die Namen und Anschriften von 7.150 „SINUS"-Besitzern, aus denen dann 500 private Nutzer für Befragungen ausgewählt wurden.

Bürger beschwerten sich bei mir nicht nur darüber, daß ohne ihre Einwilligung Dritte über ihre Anschrift und die Tatsache, daß sie ein solches Funktelefon besitzen, informiert wurden. Die Beschwerden betrafen auch die Art und Weise, in der Beauftragte des Marktforschungsinstitutes an die zu Befragenden herangetreten sind. Durch die Vorlage einer mit dem Siegel des Bundesministers für das Post- und Fernmeldewesen versehenen „Unbedenklichkeitsbescheinigung" entstand dabei oft der irrige Eindruck, die Befragten seien zur Beantwortung der gestellten Fragen verpflichtet. Dies wurde besonders deswegen als belastend empfunden, weil einigen Fragen weit in die private Lebenssphäre hineinreichten. So wurde u. a. nicht nur nach den familiären Verhältnissen und dem Alter gefragt, sondern auch nach dem Schulabschluß der „SINUS"-Besitzer.

Ich habe dem Bundesminister für das Post- und Fernmeldewesen meine Auffassung dargelegt, daß eine solche Befragung – da sie weder zur Errichtung noch zum Betrieb des Telefonanschlusses erforderlich ist – nur auf freiwilliger Basis, also mit Einwilligung der Betroffenen durchgeführt werden darf. Entsprechend ist auch die Einwilligung der Betroffenen notwendig, wenn die Deutsche Bundespost ihre Anschriften an das Marktforschungsinstitut weitergibt. Demgegenüber vertritt der Bundesminister für das Post- und Fernmeldewesen die Meinung, das Erforschen der Marktakzeptanz eines Telefones werde von dem der DBP gesetzlich zugewiesenen Aufgabenbereich „Fernsprechdienst" mit umfaßt, die Übermittlung der Anschriften der „SINUS"-Besitzer sei daher zur rechtmäßigen Erfüllung der in der Zuständigkeit der DBP liegenden Aufgaben erforderlich und somit gemäß § 11 Satz 1 BDSG auch zulässig. Ich habe dieser Auffassung mit Nachdruck widersprochen und betont, daß die Übermittlung von Teilnehmerdaten durch die Deutsche Bundespost an Dritte für Marktforschungszwecke ohne Einwilligung der Betroffenen auf durchgreifende rechtliche Bedenken stößt. Ich habe daher empfohlen, in solchen Fällen künftig Verfahren vorzusehen, die eine Einwilligung – sowohl in die Übermittlung der Anschriften als auch in die Teilnahme an der Befragung selbst – zweifelsfrei sicherstellen.

8.4 Bildschirmtext

Ein Btx-Teilnehmer sah seine schutzwürdigen Belange dadurch beeinträchtigt, daß von einem Btx-Dienstanschluß einer Postdienststelle aus unter seiner Identität im System Aktivitäten vorgenommen und dabei auch Anbietervergütungen verursacht worden sind. Da ein solches Fehlverhalten nie völlig auszuschließen ist, halte ich es für geboten, durch geeignete technisch-organisatorische Maßnahmen sowohl die Mißbrauchsmöglichkeit der Dienstanschlüsse zu begrenzen, als auch allgemein für Störungsfälle aller Art unverzüglich Maßnahmen zu ergreifen, die es ermöglichen, den Verursacher festzustellen oder zumindest den Kreis der in Frage kommenden Personen einzugrenzen. Da dies im vorliegenden Fall nicht geschehen war und m. E. auch die bestehenden Regelungen für solche Fälle nicht ausreichen, habe ich das Verhalten der DBP gemäß § 20 BDSG beanstandet. Der BMP hat jedoch die erhobe-

nen Vorwürfe zurückgewiesen und es abgelehnt, weitergehende als die bereits getroffenen – und im angesprochenen Fall unwirksamen – Maßnahmen vorzusehen.

Ein Großteil der Btx-Seiten ist nur vergütungspflichtig abrufbar; das Inkasso übernimmt die DBP. Weigert sich der Teilnehmer, die Vergütung zu bezahlen, teilt die DBP dies – im Einklang mit den Regelungen der Fernmeldeordnung – den betroffenen Anbietern mit, zusammen mit der Höhe der ihnen zustehenden Vergütungen. In mehreren mir mitgeteilten Fällen ist jedoch durch Bearbeitungsfehler bei der DBP fälschlich der Eindruck der Zahlungsverweigerung entstanden; entsprechend erfolgte eine unzutreffende – und auch unzulässige – Benachrichtigung der Informationsanbieter (vgl. oben Nr. 8.2.1). Ich habe den BMP aufgefordert, die Arbeitsvorgänge und Organisationsabläufe in diesem Zusammenhang zu überprüfen und Vorkehrungen zu treffen, um eine Wiederholung zu vermeiden.

Besonders betroffen gemacht hat mich folgender Fall: Einzelne Btx-Anbieter stellen – unter verschiedenen Bezeichnungen – eine „Elektronische Pinwand" zur Verfügung. Hiervon wird ein Btx-Teilnehmer möglicherweise dann Gebrauch machen, wenn er eine Mitteilung einem größeren Personenkreis zugänglich machen will, wie etwa eine Wohnungs- oder Verkaufsanzeige. Zu diesem Zweck muß er über Bildschirmtext in Kontakt mit dem privaten Anbieter der „Pinwand" treten und ihm den Text der Anzeige elektronisch zusenden. Dabei gibt es für ihn keine technische Notwendigkeit, etwa seinen Namen und seine Anschrift mitzusenden, so daß er auch anonyme Anzeigen oder aber auch solche unter fremdem Namen aufgeben kann. Wie bei einem „Schwarzen Brett" kann nun jeder Btx-Teilnehmer auch diese Anzeige lesen.

In den mir mitgeteilten Fällen hatte ein Unbekannter vorsätzlich Telefonanrufe belästigender und beleidigender Art bei Frauen ausgelöst, die im übrigen nicht einmal Btx-Teilnehmerinnen waren. Er hatte dazu unter mißbräuchlicher Verwendung ihrer Namen „Kontaktanzeigen" zweideutigen Inhaltes an die „Elektronische Pinwand" geheftet. Eine der Frauen hat mir berichtet, sie habe nach vielen belästigenden Anrufen die Polizei um Hilfe gebeten. Von dieser sei sie zunächst an die Post und von dort wiederum an die Btx-Zentrale in Duisburg verwiesen worden. Dort habe man ihr den Rat gegeben, sich selbst an den Anbieter der „Elektronischen Pinwand" zu wenden, „da man nichts machen könne". Auf ihre Bitte, ihr die Anschrift dieses Anbieters mitzuteilen, riet man ihr, doch im Btx-Verzeichnis nachzuschlagen – das sie aber gar nicht besitzt.

Die DBP hat sich auch mir gegenüber zutreffend darauf berufen, daß sie grundsätzlich den Inhalt der über Btx ausgetauschten Mitteilungen nicht zur Kenntnis nimmt und etwa beleidigenden oder zu Belästigungen führenden Inhalt deshalb auch nicht als solchen erkennen kann. Sie lehnt daher jede – auch datenschutzrechtliche – Verantwortung ab. Ich habe dies der genannten Petentin mitgeteilt und sie im übrigen an den für die Datenverarbeitung des Anbieters der „Elektronischen Pinwand" zuständigen Landesbeauftragten für den Datenschutz verwiesen. Der von der DBP vertretene Standpunkt führt aber letztlich dazu, daß durch die technischen Gegebenheiten des von ihr konzipierten und betriebenen Systems nicht nur eine Beeinträchtigung schutzwürdiger Belange ermöglicht wird, sondern auch der Verursacher der Beeinträchtigung nicht erkannt werden kann. Dies kann jedoch unter den Gesichtspunkten des Datenschutzes und des allgemeinen Persönlichkeitsrechts so nicht hingenommen werden: Die Infrastrukturverantwortung der Deutschen Bundespost für die von ihr zur Verfügung gestellten Netze und Dienstleistungen verpflichtet dazu, die verwendete Technik sowie die Benutzungsbedingungen so zu gestalten, daß elementare Bürgerrechte dabei respektiert werden (siehe oben Nr. 8.1). Dies gilt zumindest für die Netze und Dienstleistungen, die allein von der DBP als Monopolträger zur Verfügung gestellt werden.

Bezüglich Btx ist daher zu fordern, daß entweder durch geeignete technische und organisatorische Vorkehrungen „anonyme Anzeigen" verhindert werden, oder aber daß zumindest der verursachende Btx-Anschluß ermittelt und dem Betroffenen benannt werden kann, damit diesem ermöglicht wird, seine Rechte wahrzunehmen. Die dafür notwendigen Aufwendungen müssen geleistet und auch die daraus eventuell für die Post und die Anbieter entstehenden Einnahmeminderungen hingenommen werden, wenn es anders nicht möglich ist, Unbeteiligte vor beleidigenden Angriffen und schamlosen Belästigungen zu schützen.

8.5 Fernwirkdienst TEMEX

Mit TEMEX stellt die Deutsche Bundespost einen Telekommunikationsdienst zur Verfügung, der es gestattet, Signale und Meßwerte z. B. aus den Wohnungen der „TEMEX-Nutzer" zur Leitstelle eines „TEMEX-Anbieters" zu übertragen. Dafür wird das vorhandene Telefon-Leitungsnetz benutzt, wobei die Signalübertragung für TEMEX unabhängig davon erfolgt, ob über die betreffende Leitung gerade ein Telefongespräch geführt wird oder nicht. Die Infrastruktur für einen flächendeckenden Einsatz ist somit schon vorhanden. Mit dem Beginn erster Systemversuche Ende 1985 konnten zunächst nur einwertige Meldungen, wie z. B. das Auslösen eines Notsignals durch eine hilfsbedürftige Person bei der Leitstelle einer Hilfsorganisation, übertragen werden. Im Juli des Berichtsjahres nahm die DBP in elf Städten der Bundesrepublik Betriebsversuche auf, die über die einwertige Signalübertragung hinaus beispielsweise auch das Fernablesen der Verbrauchszähler und die automatische Übertragung der Meßwerte an die Energieversorgungsunternehmen ermöglicht.

TEMEX kann schon bald ein sehr hilfreicher Dienst werden. Allerdings kann mit TEMEX auch eine Vielzahl von Informationen aus dem geschützten Bereich des privaten Wohnumfeldes in die Zentralen der Energieversorgungsunternehmen, der sozialen

Hilfsdienste, der Wachunternehmen und anderer Stellen übertragen und miteinander verknüpft werden – ohne daß der Bürger dies bemerkt, geschweige denn, sich dagegen wehren kann.

Derzeit befindet sich erst eine geringe Anzahl von TEMEX-Anlagen in Betrieb. Dabei handelt es sich nach meinen Informationen ausschließlich um Anwendungen, in denen einfache Signale übertragen werden und diese somit unter Datenschutzaspekten weniger relevant sind. Sensiblere Anwendungen, die etwa die Übertragung von Verbrauchsmeßdaten gestatten, sind – abgesehen von den laufenden Betriebsversuchen – erst in der Vorbereitung.

Rechtsgrundlage der Datenverarbeitung der Deutschen Bundespost bei TEMEX ist die Fernmeldeordnung, die bezüglich TEMEX am 1. Juni 1986 ergänzt worden ist. Die einschlägigen Vorschriften lassen das Bemühen um eine datenschutzgerechte Gestaltung des Dienstes erkennen. So wird ausdrücklich festgelegt, daß TEMEX-Daten durch die DBP nur ausnahmsweise und unter speziellen, einschränkenden Voraussetzungen gespeichert und nach vier Wochen gelöscht werden. Auch eine etwa zu Datensicherungszwecken darüber hinausgehende Speicherung ist damit ausgeschlossen.

Bei der Beratung der datenschutzrelevanten Vorschriften für TEMEX hat mich der Bundesminister für das Post- und Fernmeldewesen bereits frühzeitig beteiligt. Ich habe dabei darauf hingewiesen, daß die TEMEX betreffenden Vorschriften in der Fernmeldeordnung nicht in einem Abschnitt zusammengefaßt sind und darunter die Lesbarkeit und das Verständnis diese Vorschriften litten. Leider hat sich dies bei der Umsetzung der einschlägigen Vorschriften in die zum 1. Januar 1988 in Kraft tretende Telekommunikationsordnung nicht geändert, möglicherweise sogar verschlechtert: Wer sich bezüglich TEMEX „über die Bedingungen und Gebühren für die Benutzung der Einrichtungen des Post- und Fernmeldewesens" informieren will, muß dafür insgesamt *achtzehn* einzelne Vorschriften der TKO heranziehen.

Ich gehe davon aus, daß es Ziel der erwähnten TEMEX-Betriebsversuche ist, Erfahrungen zu gewinnen, die u. a. auch noch offene Datenschutzprobleme erkennen lassen. Solche Probleme könnten sich z. B. daraus ergeben, daß Versorgungsunternehmen für ihre Planungen mehr über die Verbrauchsgewohnheiten erfassen und speichern wollen, als die betroffenen Bürger über ihr Privatleben preisgeben möchten.

Nach Vorliegen der Erfahrungen wird erneut zu prüfen sein, ob die von der DBP bislang getroffenen Datenschutzregelungen den Anforderungen entsprechen. Zu hoffen ist auch, daß bis dahin von den zuständigen Stellen die Frage abschließend geklärt worden ist, ob die Verordnungsermächtigung des § 14 Postverwaltungsgesetz auch eine ausreichende Rechtsgrundlage für die Einführung völlig neuartiger Dienste bietet, die – wie auch TEMEX – die Kommunikationsbeziehungen der Bürger wesentlich verändern können.

8.6 Postgirodienst

8.6.1 Kontrolle eines Postgiroamtes

Im Rahmen einer datenschutzrechtlichen Kontrolle eines Postgiroamtes habe ich die Verarbeitung personenbezogener Daten von Postgirokunden geprüft. Einen Schwerpunkt bildete hierbei die Verarbeitung der Klarschriftlese-Belege, die ich von der Einzahlung am Schalter eines Postamtes bis zur abschließenden Verarbeitung beim Postgiroamt verfolgt habe. Ich habe mich davon überzeugen können, daß die für alle Postgiroämter geltenden Vorschriften über die Behandlung der Klarschriftlese-Belege den Schutz der zu verarbeitenden personenbezogenen Daten ausreichend sichern.

8.6.2 Sperrdatei für den Postgirodienst

Die Deutsche Bundespost führt im Postgirodienst eine sog. Sperrdatei. In sie werden ehemalige Postgirokunden aufgenommen, die nicht mehr zum Postgirodienst zuzulassen sind. Im Zusammenhang mit der Sperrdatei gehen mir immer wieder Eingaben von Bürgern zu, die durchweg selbst Teilnehmer am Postgirodienst sind bzw. waren. Die Fragen und Besorgnisse betreffen nicht nur die Gründe, die zu einer Eintragung führen, und die Art und Dauer einer Eintragung, sondern insbesondere auch die Konsequenzen, die eine Eintragung für den Betroffenen hat. Anlaß für eine Speicherung in dieser Datei ist im allgemeinen eine mißbräuchliche Benutzung des Postgirokontos. Unter diesem Gesichtspunkt sind nach meiner Einschätzung der Betrieb und die Anwendung der Sperrdatei nicht nur zweckmäßig, sondern durchaus auch erforderlich, um die Deutsche Bundespost vor Vermögensschäden zu schützen.

Als Rechtsgrundlage für die Sperrdatei betrachtet die Deutsche Bundespost § 9 Abs. 1 BDSG. Dazu habe ich dem Bundesminister für das Post- und Fernmeldewesen folgendes zu bedenken gegeben: Die Eintragung in die Sperrdatei hat für den Betroffenen erhebliche Nachteile zur Folge und bedeutet einen Eingriff in sein Recht auf informationelle Selbstbestimmung. Angesichts dieses besonderen Eingriffscharakters der Sperrdatei sowie der Übermittlung und Verwendung von personenbezogenen Daten hieraus stellen die allgemeinen Vorschriften des Bundesdatenschutzgesetzes meines Erachtens keine hinreichend präzise und für den Betroffenen transparente Rechtsgrundlage für die Speicherung dar. Auch § 9 Abs. 3 Nr. 1 der Postgiroordnung, nach der Postgirokonten wegen mißbräuchlicher Benutzung von Amts wegen gelöscht werden können, reicht meines Erachtens als Rechtsgrundlage nicht aus. Diese Vorschrift entspricht schon deshalb nicht den Anforderungen der Normenklarheit, weil sie von Löschung spricht, nicht aber von der Schaffung einer Datei, die den Betroffenen die Einrichtung eines neuen Postgirokontos unmöglich macht.

Es bedarf vielmehr klarer Festlegungen der Voraussetzungen und der näheren Umstände der Eintragung in die Sperrdatei wie auch der zulässigen Verwendung der Daten, des Kreises der Verwendungsberechtigten und der Speicherungsdauer.

Um diese Transparenz bzw. Normenklarheit herzustellen, habe ich dem Bundesminister für das Post- und Fernmeldewesen empfohlen, ergänzende Rechtsvorschriften in der Postgiroordnung zu schaffen. Es könnte auch erwogen werden, den künftigen Postgirokunden bei der Begründung des Postgiroverhältnisses – entsprechend den bei Banken üblichen SCHUFA-Hinweisen (SCHUFA-Merkblatt) – über Sinn und Zweck der Sperrdatei eingehend aufzuklären. Wenn er dann ein Benutzungsverhältnis unter diesen Voraussetzungen eingeht, könnte von seiner Einwilligung ausgegangen werden. Diese Lösung bietet sich an, wenn man die Deutsche Bundespost im Hinblick auf den Postgirodienst als ein Unternehmen ansieht, das am Wettbewerb teilnimmt und somit unter den Dritten Abschnitt des Bundesdatenschutzgesetzes fällt. Der Bundesminister für das Post- und Fernmeldewesen ist wegen des inzwischen vorliegenden Berichts der mit der Neustrukturierung des Post- und Fernmeldewesens befaßten Regierungskommission, deren Vorschläge er hinsichtlich des Postgirodienstes zunächst umfassend prüfen will, bisher noch nicht auf meine Vorschläge eingegangen. Ich hoffe aber, daß es bald zu einem weiterführenden Dialog kommt.

8.6.3 Übermittlung einer Kontoverbindung durch ein Postgiroamt an Dritte

In Bürgereingaben werde ich immer wieder gefragt, ob und unter welchen Voraussetzungen ein Postgiroamt Dritten gegenüber Angaben darüber machen darf, ob eine bestimmte Person ein Postgirokonto besitzt und wie die Kontonummer lautet. Grundsätzlich gehe ich davon aus, daß das Postscheck- und Postsparkassengeheimnis, so wie es im Gesetz über das Postwesen geregelt ist, keine Angaben über den jeweiligen Kontostand und über die ihn beeinflussenden Bewegungen zuläßt.

Die Postgiroordnung ermächtigt aber die Postgiroämter, Dritten Auskunft über die Kontonummer und die Kontobezeichnung der Postgirokunden zu erteilen, soweit dem kontoführenden Postgiroamt eine gegenteilige Erklärung des Kontoinhabers nicht vorliegt. Diese Regelung halte ich für sachgerecht. Ihr liegt die Überlegung zugrunde, daß der Postgiroteilnehmer mit der Einrichtung eines Postgirokontos in aller Regel die Bereitschaft verbindet, Überweisungen zu empfangen, und demnach auch davon ausgeht, daß seine Kontonummer und seine Kontobezeichnung Dritten zugänglich gemacht werden.

Schwieriger ist jedoch eine andere Frage zu beurteilen, mit der ich mich auch aufgrund von Eingaben wiederholt befassen mußte. Es geht darum, ob nach Zustellung eines Pfändungsbeschlusses das Postgiroamt als Drittschuldner im Rahmen seiner Erklärungspflicht nach § 840 ZPO gegenüber dem pfändenden Gläubiger zu einer Angabe über die Kontonummer selbst dann verpflichtet ist, wenn eine Widerspruchserklärung des Kontoinhabers im oben geschilderten Sinne vorliegt. Da es sich bei dem Vollstreckungsverfahren um das von der Rechtsordnung vorgesehene äußerste Mittel zur Durchsetzung von Forderungen unter Zuhilfenahme staatlichen Zwanges handelt, halte ich eine solche Auskunft des Postgiroamtes auch dann für unbedenklich, wenn der Kontoinhaber von der Möglichkeit einer Auskunftssperre Gebrauch gemacht hat. In der Angabe der Kontonummer sehe ich eine notwendige Information zur Bestimmung der Forderung, über die sich der Drittschuldner im Rahmen seiner Erklärungspflicht zu äußern hat. Eine nach der Postgiroordnung erklärte Sperre des Kontoinhabers darf nicht dazu führen, daß sein Postgirokonto faktisch zu einem „Geheimkonto" und damit einer Pfändung unzugänglich wird.

8.7 Rentenrechnungsdienst

Im Mai/Juni des Berichtsjahres erhielt ich zahlreiche Eingaben, die sich auf die den Beschwerdeführern zugegangene „Mitteilung zur Leistung aus der gesetzlichen Unfallversicherung" bezogen. Den Empfängern war mit den für sie bestimmten Leistungsbescheiden gleichzeitig jeweils ein für einen anderen Rentenempfänger bestimmter Bescheid zugestellt worden. Es handelte sich um eine fehlerhafte Kuvertierung, die nur bei einer Rentenrechnungsstelle vorgekommen ist, dort allerdings in einer großen Zahl von Fällen. Ich habe diese Rentenrechnungsstelle kontrolliert und u. a. festgestellt, daß es zu diesem Bearbeitungsfehler gekommen ist, weil die auf Endlosformular gedruckten Rentenbescheide nicht in der vorgesehenen Weise auseinandergeschnitten worden waren. Der Fehler hätte sich vermeiden lassen, wenn im Arbeitsablauf alle üblichen Anforderungen an eine ordnungsgemäße Datenverarbeitung beachtet worden wären. Ich habe dem Bundesminister für das Post- und Fernmeldewesen eine Reihe von Empfehlungen gegeben, wie zukünftig verhindert werden kann, daß ein solcher Fehler entsteht.

Der fehlerhafte Versand der Rentenbescheide stellt eine unbefugte Offenbarung von Sozialdaten dar (§ 35 SGB I i. V. m. § 67 SGB X). Das Sozialgeheimnis nach § 35 SGB I verpflichtet die Stellen, die es zu beachten haben – und hierzu gehören die Rentenrechnungsstellen der Deutschen Bundespost – alle Maßnahmen zu treffen, die geeignet und erforderlich sind, um zu verhindern, daß Sozialdaten in die Hände Unbefugter gelangen.

Die bei der kontrollierten Rentenrechnungsstelle getroffenen Maßnahmen waren nicht ausreichend, um die Versendung der Leistungsbescheide im Sinne des § 6 Abs. 1 BDSG und der dazugehörigen Anlage angemessen zu sichern. Ich habe den Verstoß gegen das Sozialgeheimnis nach § 20 BDSG beanstandet. Der Bundesminister für das Post- und Fernmeldewesen hat mir nach schriftlicher und telefonischer Mahnung im Dezember 1987 mitgeteilt, daß die Arbeitsabläufe, nach denen die Arbeiten durchgeführt werden, überprüft und sicherer gestaltet wurden. Wegen weitergehender Maßnahmen zur Vermeidung von Fehlkuvertierungen sind noch Untersuchungen im Gange. Der Bundesminister für das Post- und Fernmeldewesen ist in seiner kurzen Antwort auf meine Beanstandung weder auf meine Empfeh-

lungen eingegangen noch hat er die Maßnahmen dargestellt, die er aufgrund meiner Beanstandung getroffen hat, wozu er nach § 20 Abs. 4 BDSG verpflichtet gewesen wäre.

9. Verkehrswesen

Schwerpunkte meiner Kontroll- und Beratungstätigkeit auf dem Gebiet des Verkehrswesens bezogen sich im Berichtsjahr auf

— das Kraftfahrt-Bundesamt (KBA),

— die Zentrale Militärkraftfahrtstelle (s. 9.4.2) sowie

— die Deutsche Bundesbahn (s. 9.5).

Einige Probleme, die sich bei der Kontrolle und Beratung des KBA ergeben haben, sowie meine Bewertungen hierzu stelle ich weiter unten in anderem Zusammenhang dar (s. 9.1, 9.3).

Ein weiteres Problem, das einer Lösung bedarf, ist die Erstellung von Statistiken durch das KBA. Meiner Auffassung nach sind auch diese Statistiken unter Beachtung des § 16 des Bundesstatistikgesetzes so aufzubereiten, daß Einzelangaben über persönliche und sachliche Verhältnisse einem Betroffenen nicht zuzuordnen sind. Die Möglichkeit, in diesem Sinne einen Personenbezug herzustellen, ist zur Zeit nicht völlig auszuschließen. Ich strebe mit dem KBA daher eine Lösung an, die sowohl die Interessen der Statistiknutzer berücksichtigt als auch eine Beeinträchtigung schutzwürdiger Belange der Betroffenen ausschließt.

Weiterhin habe ich mich im KBA über die aus Sicherheitsgründen durchgeführte Auslagerung der Magnetbandkopien informiert. Das bisher in diesem Zusammenhang praktizierte Verfahren ist aus meiner Sicht verbesserungsbedürftig und sollte im Rahmen eines Gesamtplanes neu geregelt werden.

Außerdem habe ich im abgelaufenen Jahr den Bundesminister für Verkehr bei der Erarbeitung der Fahrzeugregisterverordnung (s. 9.1) beraten.

9.1 Fahrzeugregisterverordnung (ZEVIS)

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

Einzelheiten der

— Erhebung und Speicherung von Fahrzeug- und Halterdaten,

— regelmäßigen Übermittlung von Fahrzeug- und Halterdaten aus den Fahrzeugregistern,

— Übermittlung durch Abruf im automatisierten Verfahren und

— Übermittlungssperren sowie Löschung der Daten

werden in einer vom Bundesminister für Verkehr mit Zustimmung des Bundesrates erlassenen Fahrzeugregisterverordnung (FRV) geregelt, die am 29. Oktober 1987 in Kraft getreten ist.

An den Beratungen über den Verordnungsentwurf wurde ich bereits in einem frühen Stadium beteiligt, so daß ich rechtzeitig auf Unklarheiten und Unstimmigkeiten im Entwurfstext hinweisen konnte. Als mißlich habe ich es empfunden, daß wegen des Zeitdrucks und der Abstimmungsschwierigkeiten innerhalb der Bundesregierung eine vorherige Beratung mit den Landesbeauftragten für den Datenschutz nicht möglich war.

Die Verordnung konnte allerdings nicht bis zum Inkrafttreten des Gesetzes zur Änderung des StVG erlassen werden. Daher war auch nach dem 15. Februar 1987 die Rechtsgrundlage für die Einrichtung und den Betrieb des Zentralen Verkehrsinformationssystems (ZEVIS) – wegen deren Fehlens ich 1983 den Betrieb von ZEVIS beanstandet hatte – noch nicht vorhanden. Trotz des Zeitdrucks, unter dem die parlamentarische Beratung des Gesetzes zur Änderung des StVG aus übergeordneten Gründen (Terrorismusbekämpfung) stand, änderte sich die Rechtslage hinsichtlich des Abrufs im automatisierten Verfahren bis zum Inkrafttreten der FRV nicht. Meine bei der parlamentarischen Beratung des Gesetzes dargelegte Auffassung, daß die Bekämpfung des Terrorismus durch datenschutzrechtliche Hemmnisse beim Zugang zu Daten der Kraftfahrzeugzulassung bisher nicht behindert worden sei und dies daher kein Grund für die Eilbedürftigkeit der Gesetzesberatung sein könne (s. auch 9. TB S. 35), wurde durch die zeitliche Verzögerung des Inkrafttretens der FRV im nachhinein bestätigt.

Bei der Beratung der Fahrzeugregisterverordnung habe ich insbesondere zu folgenden Punkten (vgl. nachstehend 9.1.1 – 9.1.3) datenschutzrechtliche Bedenken und Anregungen vorgebracht:

9.1.1 Umfang der Datenübermittlung im automatisierten Verfahren

Eine Datenübermittlung darf grundsätzlich nur insoweit erfolgen, als die Daten zur Aufgabenerfüllung des Empfängers erforderlich sind. Diesem Grundsatz wird das in der Verordnung festgelegte Verfahren, nämlich Übermittlung umfassender Datensätze für nur wenige vorgegebene Anfragetypen, nicht in allen Situationen gerecht. Es fehlt z. B. eine „Unbedenklichkeitsanfrage" für Kontrollen des laufenden Verkehrs (mögliche Auskunft: „Fahrzeug ist zugelassen, negative Erkenntnisse liegen nicht vor"). Die Folge hiervon ist, daß bei Routinekontrollen stets ein ganzer Datensatz übermittelt werden muß, obwohl hierfür personenbezogene Angaben im Regelfall nicht erforderlich sind. Es stellt sich darüber hinaus die Frage, ob überhaupt vorgefertigte Aus-

kunftstypen bereitgehalten werden müssen und ob nicht eine Abstufung nach Name, Vorname und Anschrift einerseits und – für jeweilige Auskunftsarten unterschiedlich zusammengestellt – den übrigen Daten andererseits genügt.

Die in der Fahrzeugregisterverordnung festgelegte Datenübermittlungsregelung wurde wegen des nach Verkündung des Gesetzes zur Änderung des StVG entstandenen Zeitdrucks als Kompromiß akzeptiert. Ich werde jedoch im Rahmen meiner Mitwirkung an dem dem Deutschen Bundestag zu erstattenden ZEVIS-Bericht (s. zu 9.1.4) erneut zur Frage der Erforderlichkeit und der Verhältnismäßigkeit der Datenübermittlung Stellung nehmen.

9.1.2 Maßnahmen der Datensicherung

Die vorgesehenen Regelungen entsprechen im wesentlichen dem Stand der Technik. Folgende Verbesserungen sollten aus meiner Sicht jedoch in Aussicht genommen werden:

— Die Kennung der abrufberechtigten Dienststelle sollte in einem Rhythmus von höchstens 12 Monaten geändert werden anstelle der geltenden 18-Monatsregelung (Sicherheitsgewinn).

— Die Kennung sollte von der abrufberechtigten Dienststelle selbst und nicht – wie vorgesehen – von der übermittelnden Stelle vergeben werden.

— Bei jeder erfolgreichen Verbindungsaufnahme zu ZEVIS sollte die abrufberechtigte Dienststelle über vorangegangene Fehlversuche (z. B. bei Eingabe einer falschen Kennung) informiert werden, um deren Ursache aufdecken zu können.

9.1.3 Umfang und Ausgestaltung der Auswahlprotokollierungen

Die Regelung des § 14 FRV über die Aufzeichnung der Abrufe stellt grundsätzlich einen tragfähigen Kompromiß zwischen Aufwand und Kontrollierbarkeit dar. Aus datenschutzrechtlicher Sicht wäre es zwar wünschenswert gewesen,

— eine konkretere Angabe des Anlasses der Abrufe vorzusehen – die Detaillierung über die im Gesetz genannten Gründe hinaus ist nicht sehr tief – sowie

— eine Regelung zu finden, die die Zuordnung der Abfragen zu dem konkreten Abfragegrund (Ermittlung als Verdächtiger, Geschädigter, möglicher Zeuge, Störer etc.) ermöglicht.

Ich verkenne jedoch nicht, daß eine weitere Konkretisierung im Hinblick auf den damit verbundenen Aufwand schwierig ist.

In den Erörterungen zu § 14 Abs. 2 FRV (Angabe des Anlasses eines Abrufs) wurde davon ausgegangen, daß bei Verwendung der Schlüsselzahl 4 (Fahndung, Grenzfahndung, Kontrollstelle) regelmäßig ein Aktenzeichen oder eine Tagebuch-Nummer vorhanden und daher auch zusätzlich anzugeben ist. Diese Prämisse wird im Verordnungstext jedoch nicht konsequent durchgehalten. Die Formulierung ermöglicht es den Anfragenden, die Angaben ohne Schwierigkeiten zu unterlassen. Meine diesbezüglichen Bedenken sind nicht berücksichtigt worden.

Bei einer Kontrolle des KBA habe ich u. a. festgestellt, daß im Rahmen der Auswahlprotokollierung nach § 36 Abs. 7 StVG zwar maschinell geprüft wird, ob die Felder „Schlüsselzahl" und „Zusatzangaben" (s. § 14 Abs. 2 FRV) jeweils tatsächlich belegt sind; eine Prüfung, ob eine Dienststelle zu der angegebenen Abfrageart überhaupt berechtigt ist, findet jedoch nicht statt. Es können daher sowohl unzutreffende Schlüsselzahlen als auch unsinnige Begründungen angegeben werden. Die Zulässigkeit eines Abrufes kann somit erst im nachhinein anhand vorhandener Unterlagen überprüft werden. Ich habe Zweifel, ob dieses Verfahren bei der Vielzahl der zu erwartenden Abrufe geeignet ist, unrechtmäßige Abrufe zu verhindern. Insofern bedarf es noch eingehender Erörterungen, in welcher Weise das Verfahren verbessert werden kann.

In § 14 Abs. 4 FRV ist eine Stichprobenquote von nur 2 Prozent vorgesehen. Ich bin der Auffassung, daß eine Zweckmäßigkeitskontrolle des Abfrageverhaltens durch die Fachaufsicht und eine Kontrolle der Zulässigkeit der Abrufe sowohl durch die Fachaufsicht als auch durch die Datenschutzbeauftragten nur mit einer hinreichend dichten Stichprobe zu erreichen ist. Dafür wäre 10 Prozent ein angemessener und geeigneter Satz. Die Festlegung einer Quote von 5 Prozent ist meines Erachtens das Minimum dessen, was zur Erfüllung des gesetzlichen Auftrages gerade noch ausreichen würde. Auch hier konnte ich mich mit meinen Vorstellungen nicht durchsetzen. In dem vorzulegenden Erfahrungsbericht werde ich darlegen können, ob sich meine Besorgnisse bestätigt haben.

9.1.4 Kontrolle der Rechtmäßigkeit der Abrufe

Die Zulässigkeit der Übermittlung im automatisierten Verfahren wird, wie im vorangegangenen Abschnitt dargelegt, lediglich im Rahmen einer rein formalen Plausibilitätskontrolle geprüft. Die nach § 36 Abs. 6 und 7 StVG zu fertigenden Aufzeichnungen dienen daher ausschließlich der nachträglichen Kontrolle der Zulässigkeit der Abrufe. Es wird aus diesem Grunde in erster Linie die Aufgabe der abrufberechtigten Dienststellen selbst und deren Aufsichtsbehörden sein, dafür zu sorgen, daß Abrufe nur für die gesetzlich vorgesehenen Zwecke vorgenommen werden, daß die Einhaltung dieser Voraussetzung in regelmäßigen Zeitabständen überprüft und hierzu auch die Unterstützung des KBA und der Zulassungsstellen durch Anforderung von Protokollauswertungen gemäß § 14 Abs. 6 FRV in Anspruch genommen wird. Die Personalkapazitäten der Datenschutzbeauftragten des Bundes und der Länder lassen demgegenüber nur begrenzt Kontrollen der abrufberechtigten Dienststellen zu.

Meine Mitwirkung an dem dem Deutschen Bundestag zu erstattenden ZEVIS-Bericht wird jedoch in

der nächsten Zeit verstärkte Kontrollen der ZEVIS-Abrufe auch durch meine Dienststelle erfordern. Dieser Bericht soll sich nach der Entschließung des Deutschen Bundestages darauf erstrecken, welche Erfahrungen in einem Zeitraum von 4 Jahren nach Inkrafttreten des Gesetzes zur Änderung des Straßenverkehrsgesetzes mit dem automatisierten Abrufverfahren, mit der Aufzeichnungspflicht, mit der Anfrage unter Verwendung von Personalien (P-Anfrage) und mit der Einsichtnahme in die örtlichen Fahrzeugregister gemacht worden sind. Dabei ist ausdrücklich gewünscht, daß ich an der Erstellung des Berichtes mitwirke.

9.2 Verkehrszentralregister

9.2.1 Stand der Gesetzesvorbereitung

Der Bundesminister für Verkehr ist nunmehr bereit, die Vorbereitungsarbeiten für eine normenklare gesetzliche Regelung hinsichtlich der Erhebung, Speicherung und Übermittlung von Daten des Verkehrszentralregisters verstärkt in Angriff zu nehmen. Auch das Problem der Konkurrenz zwischen § 29 StVG (Verwertungsverbot nach Tilgung einer Eintragung) und § 52 Abs. 2 des Bundeszentralregistergesetzes (Aufhebung des Verwertungsverbots im Rahmen der Erteilung oder Entziehung von Fahrerlaubnissen) soll in diesem Zusammenhang gelöst werden.

Erste Überlegungen sind mit mir erörtert worden. Sollte der Deutsche Bundestag ein entsprechendes Änderungsgesetz noch in der laufenden Legislaturperiode verabschieden – wie vom Bundesminister für Verkehr angestrebt –, wären die in meinem Neunten Tätigkeitsbericht (S. 36 f.) vorgebrachten Bedenken, auch soweit sie den Übergangsbonus betreffen, ausgeräumt.

9.2.2 Auskunftserteilung nach § 30 StVG (Vollauskunft)

Bei der Vorbereitung bereichsspezifischer Gesetzesregelungen für die personenbezogene Datenverarbeitung im Verkehrszentralregister (VZR) stehen Überlegungen über mögliche Teilauskunftsregelungen im Vordergrund, die sowohl dem Datenschutz als auch den Aufgaben des Registers gerecht werden. Mit einer derartigen Regelung würde meinem Anliegen, daß Auskünfte über eine Person nur in dem tatsächlich erforderlichem Umfang zu erteilen sind, Rechnung getragen (vgl. 7. TB S. 31, 9. TB S. 37). Möglicherweise kann in bestimmten Fällen auf eine VZR-Auskunft völlig verzichtet und statt dessen etwa ein Führungszeugnis aus dem Bundeszentralregister eingeholt werden. Erste Vorstellungen hat der Bundesminister für Verkehr mit mir erörtert.

Die Auskunftserteilung aus dem VZR an Verwaltungsbehörden dient in erster Linie der Sicherheit des Straßenverkehrs. Wenn es darum geht, habe ich gegen eine Vollauskunft keine Einwände. Hierzu gehören wohl auch die Fälle, in denen von Behörden die Zuverlässigkeit eines Antragsstellers oder Erlaubnisinhabers unter dem Gesichtspunkt der Verkehrssicherheit geprüft werden muß. Anders verhält es sich aber, wenn eine derartige Prüfung entbehrlich ist. Hat ein Führerscheininhaber z. B. seine Fahrerlaubnis verloren, ist eine Vollauskunft aus dem VZR vor Ausfertigung eines Ersatzführerscheins nicht erforderlich; hier könnte das KBA eine beschränkte Auskunft erteilen.

Die VZR-Auskünfte werden jedoch auch bei nur mittelbar mit dem Straßenverkehr im Zusammenhang stehenden Verwaltungsmaßnahmen genutzt, um die Zuverlässigkeit von Bewerbern/Antragstellern zu prüfen, insbesondere bei

- Erteilung, Rücknahme und Widerruf einer Anerkennung als Sehteststelle,
- Anerkennung der Eignung einer „anderen Stelle" für die Unterweisung in Sofortmaßnahmen am Unfallort oder über die Ausbildung in Erster Hilfe,
- Anerkennung von Kraftfahrzeugwerkstätten, Bremsendiensten und Betrieben für die Eigenüberwachung,
- Anerkennung von Kraftfahrzeugwerkstätten zur Durchführung von Abgassonderuntersuchungen.

In diesen Fällen ist sogar fraglich, ob bei einer zukünftigen Regelung überhaupt eine VZR-Auskunft zugelassen werden sollte.

Ich werde die Frage der Erforderlichkeit der Auskunftserteilung aus dem VZR mit dem Bundesminister für Verkehr noch eingehend erörtern. Erfreulich ist, daß der Bundesminister beabsichtigt, für einige Auskunftszwecke bereits vor einer gesetzlichen Regelung mit den Bundesländern pragmatische Auskunftsregelungen zu vereinbaren.

9.3 Datenübermittlungen an die Automobilindustrie

Eine Übermittlung von Fahrzeug- und Halterdaten an die Automobilindustrie ist nach § 35 Abs. 2 Nr. 1 StVG nur zulässig für Rückrufmaßnahmen zur Beseitigung von erheblichen Mängeln für die Verkehrssicherheit an bereits ausgelieferten Fahrzeugen. Die Automobilindustrie ist jedoch daran interessiert, den Zeitpunkt der Zulassung ausgelieferter Fahrzeuge zu erfahren, und zwar bezogen auf den einzelnen Händlerbezirk, um den Anteil der zugelassenen Fahrzeuge am Gesamtbestand feststellen und darüber hinaus ihr Vertriebssystem optimieren zu können. Der überwiegende Teil der Automobilhersteller und -importeure hat daher vertragliche Vereinbarungen mit dem Kraftfahrt-Bundesamt (KBA) über die Übermittlung von Zulassungsdaten abgeschlossen.

Bei einer Kontrolle des KBA sind mir die Grundzüge dieser Verträge sowie das Verfahren wie folgt beschrieben worden:

Zur Feststellung der Zulassung eines Fahrzeugs übermitteln zunächst die Hersteller und Importeure dem KBA für die an ihre Händler ausgelieferten Fahrzeuge je einen Datensatz, der u. a. die ungekürz-

te Fahrzeugidentifizierungsnummer, eine Händlernummer sowie Monat und Jahr der Auslieferung enthält. Durch einen Abgleich dieser Daten mit den beim KBA gespeicherten monatlichen Neuzulassungen wird vom KBA ermittelt, ob diese Fahrzeuge inzwischen zugelassen worden sind.

Im Trefferfalle wird dem Hersteller oder Importeur vom KBA die Zulassung je Fahrzeug mit einem neu erzeugten Datensatz mitgeteilt, der u. a. folgende Daten enthält:

Fahrzeugidentifizierungsnummer (gekürzt um die Zählziffer), Tag, Monat und Jahr der Erstzulassung, Ortsteil der Gemeinde, in dem der Halter bei der Zulassung seinen Wohnsitz hatte, Händler-Nr., Monat und Jahr der Auslieferung.

Das KBA ist sich dessen bewußt, daß eine fahrzeug- oder personenbezogene Datenübermittlung an die Automobilindustrie zu den oben bezeichneten Zwecken nach dem Straßenverkehrsgesetz nicht zulässig ist. Es war aber bisher der Auffassung, daß es lediglich anonymisierte Daten liefere, da es den Empfängern aufgrund der Kürzung der Fahrzeugidentifizierungsnummer um die Zählziffer nicht möglich sei, den Bezug zu einem einzelnen Fahrzeug (Unikat) herzustellen.

Von einer solchen Annahme kann indessen nicht mehr ausgegangen werden. Aufgrund meiner Bitte hat das KBA inzwischen ermittelt, daß die Automobilhersteller und -importeure in 85 bis 100 Prozent der Fälle aus dem übermittelten Datensatz den Rückschluß auf ein einzelnes Fahrzeug ziehen können. Damit handelt es sich um eine – durch § 35 Abs. 2 Nr. 1 StVG nicht gedeckte – Übermittlung von Fahrzeugdaten. Die Datenübermittlung ist auch nicht durch § 45 StVG gerechtfertigt. Diese Vorschrift deckt nur den Umgang mit Daten ab, die keinen Bezug zu einer bestimmten oder bestimmbaren Person ermöglichen. Die Automobilindustrie ist aber durch die im Datensatz enthaltene Händlernummer und die ihr vorliegenden Verkaufsinformationen – zum Teil werden automatisierte Verkaufsinformationssysteme geführt – ohne Schwierigkeiten in der Lage, den jeweiligen Erwerber eines ausgelieferten Fahrzeuges festzustellen. Da die Erwerber in aller Regel die Fahrzeuge auf ihren Namen zulassen, kann auch auf die Halter geschlossen werden. Damit bedeutet die Praxis des KBA zugleich auch eine Übermittlung von Halterdaten; auch dies ist durch § 35 StVG nicht abgedeckt.

Die Hersteller und Importeure können mit Hilfe des für jedes Fahrzeug übermittelten Datensatzes nicht nur Rückschlüsse darauf ziehen, wie hoch der Anteil der zugelassenen Fahrzeuge an den ausgelieferten bzw. veräußerten Fahrzeugen eines Händlers ist. Sie können auch feststellen, ob eventuell vertraglich ausgeschlossene Verkäufe in andere Händlerbezirke hinein erfolgt sind. Schließlich ist zu berücksichtigen, daß anonymisierte, kleinräumig gegliederte und herstellerbezogene Zulassungsdaten vom KBA ebenfalls an den Verband der Automobilindustrie (VDA) übermittelt werden. Diese Daten bilden die Grundlage für statistische Aufbereitungen durch den VDA. Mit Hilfe dieser Statistik und mit zusätzlicher Kenntnis der händlerbezogenen Informationen können die Hersteller und Importeure den Verkaufsanteil eines Händlers je Typ/Klasse im Verhältnis zu anderen Herstellern/Typen, und zwar bezogen auf einzelne Gemeindeteile, feststellen. Diese Kenntnisse können auch zu verkaufs- und marktpolitischen Maßnahmen genutzt werden.

Es kann nicht Aufgabe staatlicher Stellen sein, bestimmten Wirtschaftszweigen Informationen über die von den Fahrzeughaltern im Rahmen des Zulassungsverfahrens faktisch unter Zwang erhobenen Daten (ohne Angabe personenbezogener Daten keine Zulassung) zukommen zu lassen, die es u. a. ermöglichen, Leistungskontrollen durchzuführen und die Vertragstreue ihrer Partner zu überprüfen.

Ich habe die dem § 35 StVG zuwiderlaufende Datenübermittlung gegenüber dem Bundesminister für Verkehr beanstandet und diesen gebeten, das KBA anzuweisen, die Datenübermittlung an die Automobilindustrie unverzüglich auszusetzen. Anfang 1988 werde ich gemeinsam mit dem Bundesminister für Verkehr prüfen, in welcher Weise der Umfang der an die Industrie gelangenden Daten auf das zulässige Maß eingegrenzt werden kann.

Das KBA ist sich darüber hinaus bewußt, daß durch den übermittelten Datensatz auch personenbezogene Daten der in den Abgleich einbezogenen Automobilhändler verwertet werden. Deshalb läßt es sich von den Automobilherstellern und -importeuren versichern, daß die Händler in die Verarbeitung ihrer personenbezogenen Daten eingewilligt haben. Aus den mir vorgelegten Mustern der Einwilligungserklärungen geht allerdings weder der genaue Inhalt noch der Umfang der Datenübermittlungen noch deren Nutzung klar und unmißverständlich hervor. Ich habe daher Zweifel, ob die Betroffenen danach die Konsequenzen ihrer Einwilligung überblicken können. Außerdem sind nach den mir zugegangenen Unterlagen in einer Reihe von Fällen die Formerfordernisse des § 3 BDSG nicht erfüllt (gesonderte schriftliche Einwilligungserklärung bzw. besonderer schriftlicher Hinweis hierauf, wenn sie zusammen mit anderen Erklärungen erteilt wird). Die Verarbeitung der personenbezogenen Daten der Händler durch das KBA könnte daher wegen der unzureichenden Einwilligungserklärungen zumindest teilweise nicht durch § 3 BDSG gedeckt sein. Ich werde beim KBA darauf hinwirken, daß die Mindestanforderungen an eine Einwilligung im Sinne des § 3 BDSG erfüllt werden.

9.4 Fahrerlaubnisdaten

9.4.1 Gesetzliche Regelungen

Der Bundesminister für Verkehr hat mir mitgeteilt, daß er bis zum Ende der laufenden Legislaturperiode eine bereichsspezifische gesetzliche Regelung für die Erhebung, Speicherung, Übermittlung und Löschung personenbezogener Fahrerlaubnisdaten anstrebt.

Ich begrüße diese Initiative, zumal die gegenwärtige unzureichende gesetzliche Regelung oft Grund für

auftretende Unsicherheiten über den Umfang der zulässigen Datenspeicherungen durch die Fahrerlaubnisbehörden ist. In diesem Zusammenhang sollten u. a. auch die Informationsbeziehungen zwischen den örtlichen Fahrerlaubnisbehörden und den Sonderfahrerlaubnisbehörden (Dienststellen der Bundeswehr, der Deutschen Bundesbahn, der Deutschen Bundespost, des Bundesgrenzschutzes und der Polizei) klar und umfassend geregelt und die Voraussetzungen für eine Einsichtnahme in die Führerscheinakten eindeutig festgelegt werden.

9.4.2 Zentrale Militärkraftfahrtstelle

Eine Eingabe war für mich Anlaß, bei der Zentralen Militärkraftfahrtstelle (ZMK) der Bundeswehr die Einhaltung von Datenschutzvorschriften zu kontrollieren. Die ZMK ist eine Sonderfahrerlaubnisbehörde gemäß § 14 Abs. 1 StVZO und in dieser Eigenschaft u. a. Zulassungsstelle für Bundeswehrfahrzeuge, zentrale Erfassungsstelle der Fahrlehrerlaubnisse und der Fahrerlaubnisse sämtlicher Angehöriger der Bundeswehr, Vermittler zwischen den Bundeswehreinheiten und dem KBA für die Einholung von Auskünften aus dem Verkehrszentralregister vor Erteilung einer Fahrerlaubnis und zuständige Behörde für die Erteilung von Fahrverboten sowie für die Entziehung von Fahrerlaubnissen.

Ich habe mich davon überzeugen können, daß die ZMK verantwortungsbewußt mit den personenbezogenen Daten der Soldaten umgeht. Der Bundesminister der Verteidigung hat mir inzwischen mitgeteilt, daß eine Reihe von zum Teil von mir angeregten Verfahrensänderungen umgesetzt worden ist.

Hierzu gehört vor allem eine Reduzierung des Datenumfangs bei Mitteilungen an das KBA. Ferner sind militärische Dienstvorschriften dahingehend geändert worden, daß die Vernichtung von Fahrerlaubnisunterlagen nach einer dritten negativen Prüfung früher als bisher erfolgt.

Ich begrüße die Bereitschaft des Bundesministers der Verteidigung, Verfahrensabläufe unter datenschutzrechtlichen Gesichtspunkten kritisch zu überdenken und – soweit möglich – zu ändern. Die von mir für notwendig angesehenen Änderungen der Verfahren hinsichtlich

— der automatisierten VZR-Auskunft zur Beurteilung der Kraftfahrverwendungsfähigkeit der Wehrpflichtigen durch ihre zukünftigen militärischen Einheiten und

— der statistischen Auswertung von Unfallmeldungen

erfordern noch einen längerfristig angelegten Entscheidungsprozeß innerhalb der Bundeswehr, so daß ihre Umsetzung erst zu einem späteren Zeitpunkt erfolgen kann.

9.5 Deutsche Bundesbahn (DB)

Meine Kontrollen bei der Deutschen Bundesbahn haben sich im Berichtsjahr vorwiegend auf die nachstehend erläuterten Bereiche erstreckt.

9.5.1 Datenschutzrechtliche Verantwortung der Zentrale der DB

Dateien im Verantwortungsbereich der Deutschen Bundesbahn wurden bisher dezentral nach den fachlichen Erfordernissen und technischen Möglichkeiten eingerichtet. Zwar haben die nach § 16 BDSG vom Vorstand der DB erlassenen allgemeinen Verwaltungsvorschriften „den Dienststellen" der DB die Wahrnehmung der Aufgaben des Datenschutzes übertragen; hierzu ist eine ausführende Datenschutzvorschrift erlassen worden. In der Praxis hat sich jedoch herausgestellt, daß manche nachgeordneten Stellen bereits bei der Beurteilung der Frage, welche Daten als personenbezogene Daten im Sinne des Bundesdatenschutzgesetzes zu werten sind, überfordert waren. Nicht zuletzt auch aus diesem Grunde hat die Deutsche Bundesbahn ihre oben genannte Datenschutzvorschrift dahin geändert, daß Dateien mit personenbezogenen Daten, die in automatisierten Verfahren betrieben werden, ausschließlich von der Zentrale der DB angeordnet oder genehmigt werden. Dabei hat die Zentrale u. a. zu prüfen, ob für die neu einzurichtenden Dateien eine fachliche Notwendigkeit besteht, ob die Speicherung und Verwendung zulässig und die vorgesehenen Schutzmaßnahmen angemessen sind. Ich begrüße diese neue Regelung, an deren Konzeption ich mitgewirkt habe, und die dort enthaltenen Datenschutz- und Datensicherungsbestimmungen.

Für die Beachtung der technischen und organisatorischen Maßnahmen zum Datenschutz ist nach der genannten Datenschutzvorschrift der jeweilige Fachdienst verantwortlich, in dessen Bereich die Dateien genutzt werden. Deshalb bedarf es m. E. im Hinblick auf die einzelnen Anwendungsbereiche noch besonderer Handlungsanweisungen durch die jeweiligen Fachdienste, um die Anwendungspraxis den jeweiligen Bedürfnissen anzupassen. Außerdem sollten die einzelnen Dienststellen in regelmäßigen Zeitabständen an die Einhaltung der Datenschutzbestimmungen erinnert und gleichzeitig aufgefordert werden, die Notwendigkeit zur Weiterführung bestehender Dateien in der ursprünglich konzipierten Form zu prüfen.

Ich werde die Deutsche Bundesbahn bitten, in diesem Sinne an die Fachdienste heranzutreten. Daß derartige organisatorische Maßnahmen erforderlich und nützlich sein können, habe ich bei meiner Kontrolle des ehemaligens Ressorts Absatz der Zentrale der Deutschen Bundesbahn festgestellt, von dem für gleichartige Aufgaben unterschiedliche Dateimeldungen zu meinem Register erfolgten, obwohl es sich nach Darstellung der Deutschen Bundesbahn lediglich um unterschiedliche Anwendungen einzelner Dateien handelte.

9.5.2 Videoüberwachung

Eine Videoüberwachung mit Fertigung von Aufzeichnungen erfolgt

— durch den Fahndungsdienst als verdeckte Observation,

— in Einzelfällen durch den Betriebsdienst der Deutschen Bundesbahn zur Feststellung von Betriebsstörungen an Halbschrankenanlagen und

— zu Dokumentationszwecken.

Aufgabe des Fahndungsdienstes der DB ist die Aufklärung von Straftaten (überwiegend Eigentumsdelikte), die im Bereich der Anlagen der Bundesbahn begangen wurden. Zu diesem Zweck erfolgt u. a. auch eine verdeckte Videoüberwachung bestimmter Orte (z. B. Stückgutabfertigung, Lagerhallen), wenn wegen der örtlichen Gegebenheiten oder bei angeordneten Dauerobservationen eine Überwachung durch Fahndungsbeamte nicht möglich ist. Verwertbare Aufzeichnungen können als Hilfsmittel zur Beweissicherung oder als Beweismittel bei Strafanzeigen genutzt werden. Meine Kontrollbesuche bei einigen Bundesbahndirektionen haben ergeben, daß die Deutsche Bundesbahn mit den Aufzeichnungen verantwortungsbewußt umgeht und angemessene Löschungsfristen eingehalten werden.

Bei den Aufzeichnungen zur Feststellung von Betriebsstörungen an Halbschrankenanlagen können auch Bahnbedienstete erfaßt werden, die den Bahnübergang während der Betriebsstörungen sichern. Es ist nicht auszuschließen, daß hierbei Personen zwar nicht unmittelbar, aber mit Hilfe besonderen Zusatzwissens identifiziert werden können. Die Aufzeichnung von Mitarbeitern der Deutschen Bundesbahn könnte daher nach dem Personalvertretungsrecht unter dem Gesichtspunkt der Verhaltens- und Leistungskontrolle mitbestimmungspflichtig sein. Mir wurde bisher lediglich von einer Bundesbahndirektion bestätigt, daß vor Einführung einer Videoüberwachung die Zustimmung des Personalrats eingeholt worden ist. Ich habe die Deutsche Bundesbahn gebeten, der Mitbestimmungsfrage nachzugehen.

Die Videoüberwachungen mittels Monitor ohne Aufzeichnungen dienen grundsätzlich der Observationshilfe zur Sicherung von Anlagen, Frachtgut und zur Aufrechterhaltung der Sicherheit und Ordnung auf dem Bahngelände. Gegen diese Überwachungsmaßnahmen habe ich keine Bedenken, da die Kameras nicht verdeckt angebracht, die Maßnahmen verhältnismäßig sind und eine Beeinträchtigung des informationellen Selbstbestimmungsrechts des betroffenen Personenkreises durch die Bahnbediensteten nicht zu befürchten ist.

Auf einem Bahnhof habe ich festgestellt, daß unmittelbar nach begangener strafbarer Handlung festgenommene Personen bis zur Übergabe an die allgemeine Polizei vorübergehend in Arrestzellen der Bahnpolizei untergebracht werden. Diese Räume sind zur Beobachtung der Arrestanten jeweils mit einer Videokamera ausgestattet. Der Monitor befindet sich in der Hauptwache; die in den Zellen befindlichen Personen können von dem wachhabenden Polizeibeamten ständig optisch und akustisch überwacht werden. Ich habe gegenüber der Deutschen Bundesbahn meine Zweifel geäußert, ob die Überwachung – auch unter dem Gesichtspunkt des Eigenschutzes der betroffenen Personen – von strafprozessualen oder sonstigen Rechtsvorschriften gedeckt sei, dem Grundsatz der Verhältnismäßigkeit entspreche bzw. unter den gegebenen Umständen (Schock, fehlende Zurechnungsfähigkeit Angetrunkener u. a.) von einer rechtswirksamen Einwilligung ausgegangen werden könne. Diese Bedenken werden inzwischen auch von der Deutschen Bundesbahn geteilt. Sie wird daher die zuständige Bundesbahndirektion anweisen, die Überwachung so zu gestalten, daß nur eine zeitweise Beobachtung möglich ist und die einsitzende Person dies auch erkennen kann.

9.5.3 Schwarzfahrerdatei

In den einzelnen Bundesbahndirektionen werden sogenannte Schwarzfahrerdateien geführt, wobei es unterschiedliche Verfahren (manuell und automatisiert) mit unterschiedlichen Ausgestaltungen gibt. Die Deutsche Bundesbahn beabsichtigt deshalb, automatisierte Dateien einzuführen, die für den gesamten Bundesbahnbereich nach einheitlichem Muster betrieben werden. Diese Dateien sollen bei den jeweiligen Fahrkartenausgabestellen am Sitz der einzelnen Bundesbahndirektionen geführt werden, jedoch getrennt für den eigentlichen Bahn-Bereich und die Verkehrsverbünde. Ein gegenseitiger Datenaustausch zwischen diesen Bereichen soll nicht stattfinden.

Ich begrüße dieses Vorhaben, das zu Beginn des Jahres 1988 realisiert werden soll, da hierdurch die Zuständigkeiten klar abgegrenzt, einheitliche Löschungsregelungen eingeführt und klare Regelungen zur Entscheidung von Kulanzfällen vorgegeben werden können.

Die vorgesehenen Löschungsregelungen halte ich für angemessen. Danach beträgt die Speicherungsdauer grundsätzlich nur einen Monat nach Zahlungsabwicklung. Wurde eine Mahnung erforderlich, verbleibt der Datensatz zur Feststellung von Wiederholungstätern vom Ende des Monats nach Zahlungseingang noch ein Jahr, bei erneuter Auffälligkeit jedoch unabhängig von der Zahl der Wiederholungen noch drei Jahre im Datenbestand.

Die personenbezogenen Daten strafunmündiger Kinder sollen, soweit die Schwarzfahrt im reinen DB-Verkehr stattfand, nach Zahlung des erhöhten Beförderungsentgelts grundsätzlich nur bis zum Schluß des betreffenden Kalendermonats gespeichert werden. Diese Regelung halte ich für angemessen, da Grund für die Speicherung der Daten strafunmündiger Kinder nur die Beitreibung des genannten Beförderungsentgelts sein kann; ein Verfahren nach § 265 a StGB entfällt bei diesem Personenkreis.

Im Gegensatz hierzu ist für den Verbundverkehr vorgesehen, daß die Daten strafunmündiger Kinder unabhängig von der Begleichung des erhöhten Be-

förderungsentgelts ein Jahr lang gespeichert werden. Diese Maßnahme soll der Erkennung von Mehrfachtätern dienen. Meiner Auffassung nach ist eine solche Speicherung nach Zahlung des besonderen Beförderungsentgelts nicht mehr gerechtfertigt, da – wie dargelegt – aus dieser Erkenntnis keine zivil- und strafrechtlichen Konsequenzen gezogen werden können. Ich habe die Deutsche Bundesbahn hierauf hingewiesen. Sie hält gleichwohl an einer längerfristigen Speicherung fest, um u. a. die Aufsichtspflichtigen über mehrfach begangene Schwarzfahrten ihrer strafunmündigen Kinder unterrichten zu können. Ich habe der Deutschen Bundesbahn mitgeteilt, daß erwünschte erzieherische Maßnahmen nicht Grundlage für Datenspeicherungen sein können, und gebeten, von einer Speicherung der Daten strafunmündiger Kinder nach Zahlung des erhöhten Beförderungsentgelts auch im Verbundverkehr abzusehen.

9.5.4 Fahndungsdienst der Deutschen Bundesbahn

Nach den mir zugegangenen Informationen werden die Beamten des Fahndungsdienstes der Deutschen Bundesbahn im Rahmen der Aufklärung von Straftaten, die auf dem Gelände der Deutschen Bundesbahn begangen worden sind (vorwiegend Eigentumsdelikte), aufgrund des § 152 Gerichtsverfassungsgesetz (GVG) in Verbindung mit den Beschlüssen des AK II der Innenministerkonferenz von 1952 und 1954 als Hilfsbeamte der Staatsanwaltschaft tätig. Eine gesetzliche Aufgabenzuweisung ist bisher nicht erfolgt. Der Fahndungsdienst ist vielmehr mit Organisationserlaß des Vorstandes der Deutschen Bundesbahn eingerichtet worden.

Ich werde mit dem Bundesminister für Verkehr erörtern, ob eine bereichsspezifische Rechtsgrundlage für den Fahndungsdienst der Deutschen Bundesbahn geschaffen werden muß, sofern – wie der Presse zu entnehmen war – dieser Fahndungsdienst nicht demnächst aufgelöst wird.

9.5.5 Deutsche Bundesbahn als Teilnehmer an Verkehrsverbünden

Über einen Teilbereich der Datenverarbeitung des Verkehrs- und Tarifverbundes Stuttgart GmbH (VVS), an dem die Deutsche Bundesbahn als Gesellschafter beteiligt ist, habe ich in meinem Neunten Tätigkeitsbericht (S. 40f.) berichtet. Hierbei ging es um die Aufteilung der Einnahmen aus einem besonderen Verbundtarif auf die mit dem VVS kooperierenden Verkehrsunternehmen. In diesem Zusammenhang habe ich die Frage gestellt, ob mit Hilfe der Verbundpaßnummer, die u. a. in diesem ansonsten anonymen Abrechnungsverfahren erhoben wird, auf die personenbezogenen Daten der Verkehrsteilnehmer in den Verbundpaßanträgen zurückgegriffen werden kann und somit sämtliche im Rahmen des Abrechnungsverfahrens erhobenen Daten (u. a. genaue Fahrtrouten des Hin- und Rückweges) personenbeziehbar gemacht werden können. Nur unter diesen Voraussetzungen ist der Datenschutz berührt. Außerdem war noch nicht geklärt, ob für die korrekte Aufteilung der Verbundeinnahmen überhaupt die Kenntnis der Verbundpaßnummer erforderlich ist.

Ich habe inzwischen festgestellt, daß

— sowohl die Sammlung der Verbundpaßanträge und die der Erhebungsbögen, die u. a. zur Übermittlung an Dritte bestimmt sind, als auch die Erfassung der Daten aus den Erhebungsbögen auf elektronischen Datenträgern Dateien im Sinne des § 2 Abs. 3 Nr. 3 BDSG sind und

— es sich bei den Angaben in den Erhebungsbögen um personenbezogene Daten gemäß § 2 Abs. 1 BDSG handelt, da über die Verbundpaßnummer unter Zuhilfenahme der Verbundpaßanträge ein Personenbezug hergestellt werden kann.

Rechtswirksame Einwilligungserklärungen der Betroffenen zur Verarbeitung ihrer personenbezogenen Daten liegen nicht vor. Die Zulässigkeit der Speicherung solcher Daten durch den VVS richtet sich deshalb danach, ob die Datenspeicherung zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist und ob kein Grund zur Annahme besteht, daß dadurch schutzwürdige Belange der Betroffenen beeinträchtigt werden (vgl. § 23 Satz 1 BDSG).

Durch mögliche Verknüpfungen der für Abrechnungszwecke gespeicherten Daten über die Verbundpaßnummer mit den personenbezogenen Daten in den Verbundpaßanträgen können die Fahrgewohnheiten bestimmter Personen, und zwar über einen Zeitraum von 5 Jahren (Dauer der Aufbewahrung der Datenträger), festgestellt werden. Bereits eine summarische Prüfung führt also zu der Feststellung, daß das gewählte Abrechnungsverfahren schutzwürdige Belange der Betroffenen beeinträchtigen kann.

Außerdem kann meines Erachtens durch organisatorische und verfahrensmäßige Änderungen des Abrechnungsverfahrens auf eine Verarbeitung personenbezogener Daten ganz verzichtet werden, z. B. durch Weglassen der Zählziffern bei der Erfassung der Verbundpaßnummern. Darauf habe ich die Deutsche Bundesbahn hingewiesen. Das durch den Verkehrs- und Tarifverbund Stuttgart GmbH praktizierte Abrechnungsverfahren ist daher nicht erforderlich im Sinne des § 23 Satz 1 BDSG.

Ich habe die Deutsche Bundesbahn gebeten, durch Wahrnehmung ihrer Gesellschafterrechte im Verkehrsverbund auf ein Abrechnungsverfahren hinzuwirken, das auf die Erhebung und Speicherung personenbezogener Daten verzichtet.

Welche datenschutzrechtlichen Folgerungen die zuständige Aufsichtsbehörde für den nicht-öffentlichen Bereich, die meine Rechtsauffassung teilt, gegenüber dem Verkehrsverbund ziehen wird, ist mir nicht bekannt.

10. Statistik

10.1 Volkszählung 1987

10.1.1

Die Vorbereitungen für die Volkszählung 1987 nahmen mich bereits zu Beginn des abgelaufenen Berichtsjahres zunehmend in Anspruch. So war sehr bald deutlich geworden, daß sich viele Bürger Gedanken über die *Verfassungsmäßigkeit* der Volkszählung selbst machten. Ich habe daher in einem Informationspapier die wesentlichen Aspekte der Volkszählung erläutert und hierbei deutlich gemacht, daß nach meiner Auffassung der Bundesgesetzgeber im Volkszählungsgesetz 1987 (VZG) alle verfassungsrechtlichen und datenschutzrechtlichen Vorgaben des Volkszählungsurteils des Bundesverfassungsgerichts erfüllt hat. Dieses Papier ist zahlreichen anfragenden Bürgern zugesandt worden.

10.1.2

Auch die Volkszählungsunterlagen selbst bedurften der Ergänzung. Nach Fertigstellung der Begleitpapiere, die der Unterrichtung der Bürger dienen sollten, war im Januar 1987 ein *neues Bundesstatistikgesetz* in Kraft getreten; die Volkszählungsunterlagen nahmen aber noch auf das bis dahin geltende Statistikgesetz von 1980 Bezug. Das Bundesministerium des Innern hat gemeinsam mit mir ein ergänzendes Informationsblatt erarbeitet, das über die Bedeutung der Gesetzesänderung unterrichtete sowie die sog. Hilfsmerkmale aufzählte, die nach dem VZG gesondert aufzubewahren und zum frühestmöglichen Zeitpunkt zu vernichten sind.

Wichtig erschien mir, bereits im Vorfeld der Volkszählung eine Klärung herbeizuführen, in welchem Verhältnis die Vorschriften des VZG zu möglicherweise schärferen Bestimmungen des neuen Bundesstatistikgesetzes stehen. Beide Gesetze enthalten u. a. unterschiedliche Trennungs- und Löschungsregelungen für erhobene Daten, unterschiedliche Ausgestaltungen der Auskunftspflicht und unterschiedliche Formulierungen des Reidentifizierungsverbotes mit Auswirkungen auf die entsprechenden Strafvorschriften. Fraglich war in dieser Situation, ob das neue Bundesstatistikgesetz mit seinen Regelungen für alle Bundesstatistiken auch entgegenstehende Einzelbestimmungen des – früher erlassenen – VZG verdrängt oder ob das VZG seinerseits als lex specialis den konkurrierenden Bestimmungen des späteren Bundesstatistikgesetzes vorgehen soll. Aus dem Bundesstatistikgesetz ergibt sich zu dieser Frage nichts. Meine Befürchtung war daher, daß Verwaltungsstellen und Verwaltungsgerichte möglicherweise im späteren Verlauf des Volkszählungsverfahrens auf im Einzelfall schärfere Bestimmungen des Bundesstatistikgesetzes zurückgreifen würden, obwohl die Auskunftspflichtigen darauf vertrauten, daß es sich bei dem in ihren Unterlagen abgedruckten VZG um eine insoweit abgeschlossene Regelung handele. Um diese Unsicherheit zu beenden, habe ich im Januar 1987 das Bundesministerium des Innern gedrängt, eine Klärung vorzunehmen und die Öffentlichkeit hierüber zu unterrichten. Dies ist recht bald in Abstimmung mit mir dahingehend geschehen, daß im wesentlichen das VZG die speziellere Rechtsgrundlage darstelle. Eine Zusammenstellung der für die Volkszählung nicht anwendbaren Vorschriften des Bundesstatistikgesetzes wurde in Form einer Bekanntmachung des Bundesministeriums des Innern vom 25. März 1987 im Gemeinsamen Ministerialblatt 1987 S. 163 veröffentlicht.

10.1.3

Zweifelsfragen bei der Durchführung der Volkszählung standen auch im Mittelpunkt der *Konferenzen der Datenschutzbeauftragten* des Bundes und der Länder im Februar und Mai 1987. Gemeinsam wurde eine Klärung zahlreicher bis dahin aufgetretener Fragen herbeigeführt.

Im April 1987 haben sich meine Mitarbeiter im *Statistischen Bundesamt* über den Inhalt der für die statistische Auswertung bestimmten Datensätze unterrichten lassen. Dabei haben sie sich insbesondere über Möglichkeiten informiert, die Datensätze nach bestimmten Merkmalen auszuwerten. Die Beschreibung des für die späteren Auswertungen vorgesehenen Datensatzes selbst konnte mir allerdings zu diesem Zeitpunkt noch nicht zur Verfügung gestellt werden. Sie ist mir erst im Spätsommer des Berichtsjahres zugeleitet worden.

10.1.4

Mit dem Näherrücken des Zählungsstichtages nahm die Zahl der Anfragen zur *Zählergewinnung* durch die kommunalen Erhebungsstellen zu. So bin ich gefragt worden, ob es zulässig sei, daß eine Dienststelle die Adressen aller ihrer Bediensteten der Erhebungsstelle meldet, auch wenn nur eine geringere Zahl als Zähler benötigt werde. Ich habe hierzu die Auffassung vertreten, daß eine derartige Übermittlung nicht zu beanstanden sei, weil nach dem Gesetzeswortlaut die Auswahl der Zähler nicht durch die Dienststelle, sondern durch die Erhebungsstelle erfolgen muß. Eine Vorauswahl durch eine Dienststelle widerspräche diesem Grundsatz. Eine Ausnahme ist nur insoweit zulässig, als diejenigen Personen, die nicht in der betreffenden Gemeinde wohnen oder die lebenswichtige Aufgaben erfüllen, nicht gemeldet zu werden brauchen, da insofern eine Zählerbestellung von vornherein ausscheidet.

Besorgnisse sind auch im Hinblick auf den Umfang der Daten geäußert worden, die den Erhebungsstellen zum Zwecke der Zählerbestellung übermittelt werden dürfen. Dienststellen haben sich im allgemeinen auf die Weitergabe von Name und Anschrift ihrer Bediensteten beschränkt. Soweit darüber hinaus von einzelnen Behörden auch weitere Angaben wie Dienstbezeichnungen, Funktionen und Geburtsdaten an die Erhebungsstellen übermittelt worden sind, war dies für deren Aufgabe, Zähler auszuwählen und zu bestellen, keineswegs erforderlich; hierauf habe ich die betreffenden Stellen hingewiesen.

In einem gravierenderen Fall war ich allerdings zu einer förmlichen Beanstandung gezwungen. Nach

Aufforderung einer örtlichen Erhebungsstelle zur Benennung von geeigneten Zählern hat ein Arbeitsamt die Namen und Anschriften von zwanzig arbeitslosen Angestellten übermittelt. Die Bundesanstalt für Arbeit hat argumentiert, daß die Weitergabe von Adreßdaten zur Zählergewinnung der Erfüllung einer gesetzlichen Aufgabe nach dem Arbeitsförderungsgesetz diene. Diese Ansicht verkennt, daß es sich bei der Tätigkeit als Zähler im Sinne des VZG um ein gemeindliches Ehrenamt handelt, für das eine steuerfreie Aufwandsentschädigung vorgesehen ist. Die Aktivität des Arbeitsamtes diente damit keinesfalls einer Arbeitsvermittlung im Sinne des § 13 Arbeitsförderungsgesetz oder einer Vermittlung in andere Erwerbstätigkeiten. Die Betroffenen hatten weder der Offenbarung ihrer Daten an die Erhebungsstelle zugestimmt noch bestand eine gesetzliche Offenbarungsbefugnis nach dem Sozialgesetzbuch. Daher stellte die Weitergabe der Namensliste durch das Arbeitsamt einen Verstoß gegen das Sozialgeheimnis (§ 35 Abs. 1 Satz 1 SGB I) dar, den ich gegenüber der Bundesanstalt für Arbeit beanstandet habe. Auch ich halte es unter sozialen Gesichtspunkten für sinnvoll, Arbeitslose bei der Zählerwerbung bevorzugt zu berücksichtigen. Unter dem Aspekt des Sozialdatenschutzes ist der einzig gangbare Weg jedoch der, daß die Arbeitsämter die Betroffenen in geeigneter Weise auf die Möglichkeit hinweisen, sich bei den Erhebungsstellen als Zähler zu bewerben.

Ich habe erfahren, daß auch ein Sozialamt von einer Erhebungsstelle aufgefordert worden ist, alle dort bekannten Sozialhilfeempfänger zum Zwecke der Zählerbestellung mitzuteilen. Wäre dies geschehen, wäre auch insoweit das Sozialgeheimnis verletzt worden, ein Tatbestand, den der zuständige Landesbeauftragte für den Datenschutz hätte rügen müssen.

10.1.5

Einen Rechtsverstoß hätte auch die Verwirklichung des mir bekanntgewordenen Ansinnens einer Erhebungsstelle gegenüber einer Ersatzkasse bedeutet, einen Auszug mit Firmennamen und Anschriften der bei ihr gemeldeten Arbeitgeber zum Zwecke der Arbeitsstättenzählung zu übermitteln. Ich sehe § 11 Abs. 3 VZG als abschließende Regelung für die Übermittlung der *Adressen von Arbeitsstätten* an die Erhebungsstellen an; danach sind nur die für die Entgegennahme von Gewerbeanzeigen zuständigen Stellen der Gemeinden zur Bekanntgabe der Arbeitsstätten befugt. Die Übermittlung solcher Anschriften durch Industrie- und Handelskammern, Ärztekammern und Krankenkassen halte ich für unzulässig. Das gleiche gilt für Angaben aus nicht allgemein zugänglichen Registern und Verzeichnissen wie dem Grundbuch, der Handwerksrolle und Schuldnerverzeichnissen sowie Adreßdateien der Statistischen Ämter. Allenfalls können allgemein zugängliche Quellen wie Adreßbücher und Branchenverzeichnisse genutzt werden.

10.1.6

In den Wochen vor dem Zählungsstichtag häuften sich auch die Beschwerden gegen die *Besetzung der Erhebungsstellen*. Es wurde bemängelt, daß dort Bedienstete eingesetzt sind, bei denen aufgrund ihrer bisherigen oder noch nebenher ausgeübten Tätigkeit insbesondere im Einwohnermelde-, Sozial-, Steuer- oder Ordnungsamt nicht auszuschließen sei, daß sie bei der Volkszählung gewonnene Erkenntnisse auch für andere Aufgaben verwenden. Zum Teil wurde berichtet, daß die Leiter der genannten Ämter gleichzeitig zu Leitern der Erhebungsstellen bestellt worden seien.

Das VZG enthält zwar im auffälligen Gegensatz zu den Vorschriften über die Zählerbestimmung keine Einzelheiten über die Auswahl der Mitarbeiter der Erhebungsstellen. Insofern obliegt es nach dem VZG den Ländern, das Nähere zu regeln. Es ist jedoch evident, daß für die Bediensteten in den Erhebungsstellen zumindest die gleichen Kriterien gelten müssen wie für die Auswahl der Zähler, die im Gegensatz zu jenen nur einen Bruchteil der bei den Auskunftspflichtigen erhobenen Daten zu Gesicht bekommen. Es dürfen deshalb nur solche Personen in den Erhebungsstellen eingesetzt werden, bei denen Interessenkonflikte aufgrund ihrer sonstigen Tätigkeit eindeutig ausgeschlossen sind. Insofern hat die zugrunde liegende Norm des § 9 Abs. 1 Satz 2 VZG Doppelcharakter: Einerseits soll der auskunftgebende Bürger aufgrund seiner Angaben weder unmittelbare noch mittelbare Nachteile durch die Verwaltung befürchten müssen; andererseits sollen die Bediensteten vor dem – durch strafbewehrte Verwendungsverbote nicht zu lösenden – Konflikt bewahrt werden, latent vorhandene Informationen, die sie in ihrer zeitlich befristeten Tätigkeit in der Erhebungsstelle gewonnen haben, bei der Erfüllung ihrer Hauptaufgabe vollständig verdrängen zu müssen. Die insofern zuständigen Landesbeauftragten für den Datenschutz hatten auf den Ausschluß solcher Mitarbeiter in den Erhebungsstellen hinzuwirken, bei denen aufgrund ihrer sonstigen Tätigkeit die Gefahr bestand, daß Volkszählungsinformationen in belastende Verwaltungsentscheidungen einfließen könnten.

Schließlich sind mir bereits vor der Volkszählung Absichten von Erhebungsstellen bekannt geworden, Gemeindebedienstete aus dem Sozialamt oder der Wohngeldstelle als *Zähler* zu verpflichten. In solchen Fällen wäre mit Recht zu besorgen, daß Erkenntnisse aus der Zählertätigkeit zu Lasten der Auskunftspflichtigen genutzt werden könnten; denn gegenüber als Zähler eingesetzten Gemeindebediensteten, die sonst Anträge auf Sozialhilfe oder Wohngeld bearbeiten, müssen nach § 10 Abs. 7 VZG auf Verlangen Angaben u. a. über die Zahl der Personen im Haushalt und die Zahl der Haushalte im Gebäude gemacht werden. Der Einsatz solcher Personen als Zähler wäre deshalb ein Verstoß gegen § 10 Abs. 5 VZG.

10.1.7

Um weiteren Verstößen gegen Vorschriften des VZG durch örtliche Erhebungsstellen vorzubeugen, erschien mir wichtig, daß von zentraler Stelle eindeutige *Anweisungen über eine gesetzeskonforme Praxis* formuliert würden. Ich habe daher Anfang

März 1987 die mir bis dahin bekannten Einzelfälle einschließlich einer rechtlichen Bewertung dem Bundesministerium des Innern mitgeteilt; zugleich habe ich empfohlen, die Statistischen Landesämter über das für die Koordinierung der Zählung zuständige Statistische Bundesamt zu bitten, den Erhebungsstellen eindeutige Anweisungen über die Anwendung der einschlägigen Vorschriften des VZG zu erteilen. Der Bundesminister des Innern und das Statistische Bundesamt haben in allen Fällen meine Rechtsauffassung bestätigt. Das Statistische Bundesamt hat die Statistischen Landesämter mit Schreiben vom 10. März 1987 auf diese gemeinsame Rechtsauffassung hingewiesen und insbesondere die große Bedeutung der einwandfreien personellen Besetzung der Erhebungsstellen für das Gelingen der Zählung betont.

10.1.8

In der Presse wurde geargwöhnt, die Behörden für *Verfassungsschutz* speicherten systematisch die personenbezogenen Angaben von Volkszählungsgegnern. Im Rahmen meiner Kontrollzuständigkeit habe ich beim Bundesamt für Verfassungsschutz eine Stichprobe durchgeführt. Dabei ergaben sich keine Anhaltspunkte dafür, daß Personen durch das Bundesamt für Verfassungsschutz allein deswegen erfaßt werden, weil sie gegen die Volkszählung eingetreten sind (vgl. auch Antwort des Parlamentarischen Staatssekretärs Spranger auf eine Frage des Abgeordneten Wüppesahl vom 15. 10. 1987, BT-Drucksache 11/978 S. 6).

Allerdings stellt das Bundeskriminalamt – Abteilung Staatsschutz – Daten direkt in das nachrichtendienstliche Informationssystem *NADIS* ein (was ich aus verschiedenen Gründen beanstandet habe, vgl. näher unter 19.2). Dazu können auch Fälle des „harten Volkszählungsboykotts" zählen, d. h. Aktionen, in denen die Strafverfolgungsbehörde eine strafbare Handlung erblickt. Dies betrifft nach Auffassung einiger Strafverfolgungsbehörden bekanntlich bereits die Aufforderung zum Abschneiden der Seriennummer von den Erhebungsbögen. Eine höchstrichterliche Bewertung solchen Verhaltens steht noch aus (s. auch 19.2.1).

10.1.9

Die nach dem Zählungsstichtag an mich gerichteten Fragen bezogen sich im wesentlichen auf die – offenbar erst jetzt zur Kenntnis genommene – Ausgestaltung der Volkszählungsbogen. Im Vordergrund standen dabei Befürchtungen, der gegenüber den Bürgern versprochene Schutz vor einer *Reidentifizierung* sei nicht gewährleistet. Insbesondere galt dies für diejenigen selbständig tätigen Auskunftspflichtigen, die bei der Beantwortung der Frage 12 des Personenbogens, nämlich der Frage nach Name und Anschrift der Arbeitsstätte, ihren eigenen Namen angeben mußten oder deren eigene Anschrift sich mit ihrer Arbeitsstätte deckte; diese Personen bezweifelten ihre Verpflichtung, auch die Frage 12 des Personenbogens zu beantworten.

In diesem Bereich hat sich gezeigt, daß die in der Öffentlichkeit verbreitete Versicherung, eine spätere (Re-)Identifizierung der Auskunftspflichtigen sei so gut wie ausgeschlossen, in dieser Form nicht zutraf. Dies ergibt sich eindeutig aus der Regelung, daß die kommunalen Erhebungsstellen ebenso wie die Statistischen Ämter der Länder zu Plausibilitätskontrollen und gegebenenfalls zu Rückfragen bei den Bürgern verpflichtet sind. So ist in § 15 Abs. 1 VZG ausdrücklich davon die Rede, daß die dort vorgesehene Trennung von Hilfs- und Erhebungsmerkmalen nach Durchführung der Eingangskontrollen bei den Statistischen Landesämtern vorzunehmen ist. Dies bedeutet in der Praxis, daß es selbstverständlich den Bediensteten der örtlichen Erhebungsstellen und zunächst auch der Statistischen Ämter der Länder möglich ist, auf die Auskunftspflichtigen zurückzuschließen, da in diesen Stellen alle Daten gemeinsam mit Namen und Anschriften der Bürger ungetrennt vorhanden sind. Dies ist konsequent, denn wenn das Gesetz die Einrichtung von Kontrollinstanzen vorsieht, müssen die dort tätigen Bediensteten diejenigen kennen, bei denen Rückfragen erforderlich sind. Eine Trennung der Haushaltsmantelbögen von den übrigen Volkszählungsunterlagen hat der Gesetzgeber bis zu dieser Phase der Erhebung nicht vorgeschrieben, weil er den Arbeitsaufwand für eine Zusammenführung jeweils im Fall einer Kontrolle offensichtlich als unverhältnismäßig angesehen hat.

Aber auch nach der Trennung und gesonderten Aufbewahrung von Hilfs- und Erhebungsmerkmalen ist die Reidentifizierbarkeit lediglich erschwert, keineswegs aber ausgeschlossen. Ähnliches gilt nach Vernichtung der Erhebungsbögen in den Statistischen Landesämtern, wenn die Volkszählungsdaten nur noch auf maschinell lesbaren Datenträgern gespeichert sind, die die Namen der Betroffenen und – in einem späteren Stadium – auch die Angaben über Straße und Hausnummer nicht mehr enthalten. Die dann gespeicherten Daten lassen eine Identifizierung der Betroffenen etwa bei seltenen Berufsangaben („Ministerpräsident", „Landesbeauftragter für den Datenschutz") durchaus noch zu. Auch mit Hilfe spezieller Programme wäre es möglich, in den Statistischen Landesämtern Reidentifizierungen vorzunehmen. All dies ist im VZG angelegt und mit ihm vereinbar. Das – notwendige – Korrektiv ist die Strafbarkeit einer Reidentifizierung durch Zusammenführung von Volkszählungsdaten mit anderen statistischen Daten (§ 18 VZG) sowie die Verpflichtung der Mitarbeiter in den Erhebungsstellen und den Landesämtern auf das Statistikgeheimnis (§ 9 Abs. 2 VZG bzw. § 16 BStatG), dessen unbefugte Offenbarung eine strafbare Handlung im Sinne von § 203 Abs. 2 StGB darstellt.

Aus den vorstehenden Überlegungen ergibt sich auch die Antwort auf die in der Frage 12 des Personenbogens enthaltene Problematik. Wahrscheinlich hat der Gesetzgeber nicht bedacht, daß eine nicht unerhebliche Zahl selbständig tätiger Personen (freie Berufe, Landwirte) bei der Beantwortung dieser Frage ihre eigene Identität preisgibt, weil ihr eigener Name und ihre eigene Anschrift an dieser

Stelle angegeben werden müssen. Der Gesetzgeber hat sich jedenfalls nicht veranlaßt gesehen, für die Beantwortung der Frage nach Name und Anschrift der Arbeitsstätte einen eigenen Erhebungsbogen vorzuschreiben oder durch andere Maßnahmen den in Rede stehenden Personenkreis besonders gegen eine Deanonymisierung zu schützen. Nach meiner Ansicht ist diese Unterlassung indessen unschädlich, da man darauf vertrauen kann, daß auch insoweit die Schutzmaßnahmen, insbesondere die Strafsanktionen bei Verletzung des Statistikgeheimnisses, ausreichen, um eine genügende Sicherheit der Angaben zu gewährleisten. Ich habe deshalb allen anfragenden Bürgern geraten, auch die Frage 12 des Personenbogens zu beantworten.

10.1.10

Im übrigen war inhaltlicher Schwerpunkt der nach dem Zählungsstichtag an mich gerichteten Eingaben der *Einsatz der Zähler*. Gerade in diesem Bereich sind viele Fehler gemacht worden. Überwiegend handelt es sich um Fälle, in denen Zähler

- eingesetzt wurden, die in unmittelbarer Nachbarschaft der Auskunftspflichtigen wohnten;
- eingesetzt wurden, bei denen zu besorgen war, daß sie die gewonnenen Erkenntnisse zu Lasten der Auskunftspflichtigen nutzen könnten, z. B. als Polizei- oder Steuerbeamte oder Bedienstete in örtlichen Einwohnermelde-, Wohnungs- oder Sozialämtern;
- ausgefüllte Erhebungsbögen oder die ihnen überlassenen Begehungslisten verloren haben;
- ihre gesetzlich festgelegten Kompetenzen gegenüber den Auskunftspflichtigen überschritten haben;
- von Nachbarn Informationen eingeholt haben, wenn die Auskunftspflichtigen nicht in ihren eigenen Wohnungen angetroffen werden konnten.

Die hierin liegenden Verstöße gegen Bestimmungen des VZG sind von den Datenschutzbeauftragten der Länder beanstandet worden, die in diesen Wochen durch eine Flut von Bürgeranfragen bis aufs äußerste beansprucht waren. Viele solcher Einzelfälle wurden in der Presse behandelt, was bedauerlicherweise dazu beitrug, daß das Vertrauen in die gesetzlich vorgesehenen datenschutzrechtlichen Gewährleistungen immer wieder erschüttert wurde.

10.1.11

Zum Jahresende 1987 ist die Zahl der wegen der Volkszählung an mich gerichteten Anfragen erheblich zurückgegangen. Die Auseinandersetzung über die Rechtmäßigkeit der Volkszählung verlagert sich nunmehr zu den Verwaltungsgerichten. Auch das *Bundesverfassungsgericht* ist bereits in mehreren Beschwerdeverfahren mit Problemen der Volkszählung befaßt worden. Möglicherweise wird das Gericht seine früheren Ausführungen im Volkszählungsurteil angesichts der durch das Bundesstatistikgesetz von 1987 und das VZG geänderten Rechtslage weiter präzisieren können; ich würde dies begrüßen.

Nachdem das Bundesverfassungsgericht bisher eine Reihe von Verfassungsbeschwerden wegen mangelnder Erfolgsaussicht nicht zur Entscheidung angenommen hatte, hat es mir in zwei Beschwerdeverfahren Gelegenheit zu einer Stellungnahme gegeben. In der einen Sache (1 BvR 1043/87) geht es u. a. um die Frage, welche Eintragungen in den den Zählern ausgehändigten Begehungslisten vorgenommen werden dürfen. Ich habe hierzu die Auffassung vertreten, daß der Zähler persönliche Daten – auch gegen den Willen des Auskunftspflichtigen und ohne dessen Mitwirkung – bereits im Vorfeld der Zählung von seiner Erhebungsstelle erhalten darf, aber nur insoweit, als diese für die organisatorische Durchführung der Erhebung zwingend erforderlich sind. Dies sind diejenigen Daten, die gemäß § 13 Abs. 5 VZG auch zwangsweise erhoben werden können, nämlich im wesentlichen die Angaben über die Zahl der Personen im Haushalt, die Zahl der Haushalte in der Wohnung, das Leerstehen der Wohnung und Name und Anschrift des Haushaltsmitglieder. Für alle übrigen Daten gilt uneingeschränkt der Grundsatz des § 13 Abs. 2 VZG, wonach jeder Bürger das essentielle Recht hat, die in den Erhebungsvordrucken enthaltenen Fragen mündlich gegenüber dem Zähler oder schriftlich gegenüber der Erhebungsstelle zu beantworten. Dieses Recht würde unterlaufen, wenn auch insoweit in den Begehungslisten bereits Eintragungen vorgenommen würden.

Das andere Verfassungsbeschwerdeverfahren (1 BvR 962/87) berührte das Problem, ob die Beantwortung der Frage 12 des Personenbogens in den oben diskutierten Fällen mit dem Gebot einer möglichst frühzeitigen Anonymisierung und der Verpflichtung zur Trennung der Identifikations- von den Erhebungsmerkmalen vereinbar ist. Hierzu habe ich ausgeführt, daß ich es nicht für erforderlich halte, die Informationen über Name und Anschrift der Arbeitsstätte auch nach Abschluß der Kontrollen in den Statistischen Landesämtern noch länger auf dem Personenbogen bis zu dessen Vernichtung (vgl. § 15 Abs. 2 VZG) zu belassen. Da nämlich der Name der Arbeitsstätte lediglich der Richtigkeitskontrolle der Angabe zum Wirtschaftszweig (Frage 16 des Personenbogens) dient, kann mit der Signierung des Wirtschaftszweiges der Name der Arbeitsstätte auf dem Personenbogen geschwärzt oder auf andere Weise unkenntlich gemacht werden; seine maschinelle Speicherung ist nach dem VZG ohnehin nicht zulässig. Und da weiterhin mit Hilfe der Anschrift der Arbeitsstätte lediglich die Pendlerbewegungen zwischen Wohnung und Arbeitsplatz ermittelt werden sollen, solche aber in den hier vorliegenden Fällen überhaupt nicht stattfinden, kann die Anschrift in gleicher Weise unkenntlich gemacht werden. Die Information, daß ein Pendlerstrom nicht vorhanden ist, kann aus dem Fehlen der Anschrift auf dem für die weitere Auswertung bestimmten Datenträger entnommen werden. Sie ergibt sich ferner aus der An-

gabe zur Frage 14 (Zeit des Weges zur Arbeitsstätte) des Personenbogens. Außerdem würde die dauerhafte Speicherung der Anschriften mit dem Löschungsgebot für Straße und Hausnummer nach § 15 Abs. 4 VZG kollidieren. Darüber hinaus könnten die gespeicherten Anschriften als Verknüpfungsmerkmal für gesetzlich unzulässige Zusammenführungen mit anderen auf Arbeitsstätten bezogenen Statistikdaten dienen und einen Mißbrauch erleichtern; der Datensatz könnte auch für sonstige Aufbereitungen kombinierter Art genutzt werden. Ich habe deshalb dem Bundesverfassungsgericht mitgeteilt, daß ich den inzwischen von einzelnen Statistischen Landesämtern beabsichtigten Verzicht auf die maschinelle Speicherung der Anschrift der Arbeits- oder Ausbildungsstätte zum Schutz der Betroffenen für geboten erachte. Diese Auffassung hat das Bundesverfassungsgericht in seinem unmittelbar vor Fertigstellung dieses Berichts ergangenen Beschluß vom 18. Dezember 1987 bestätigt.

10.1.12

Gegen Ende des Berichtsjahres ist mit der *Wiederholungsbefragung* begonnen worden. Sie ist für etwa 60.000 Bürger vorgesehen, die aufgrund ihrer Zugehörigkeit zu bestimmten, nach einem Zufallsverfahren ermittelten Zählbezirken der Volkszählung ausgewählt wurden. Diese Erhebung, die sich auf wenige Merkmale des Haupterhebungsprogrammes beschränkt, verfolgt das Ziel, die Vollständigkeit und Qualität der Volkszählungsangaben abschätzen zu können.

Das ursprünglich vorgesehene Konzept der Wiederholungsbefragung wurde den datenschutzrechtlichen Anforderungen an statistische Erhebungen nicht gerecht. Ich habe daher in einer schriftlichen Stellungnahme an den Bundesminister des Innern auf meine Bedenken und klärungsbedürftige Fragen hingewiesen und deren eingehende Erörterung angeregt. In einer gemeinsamen Besprechung, an der ferner das Statistische Bundesamt, einige Statistische Landesämter, ein Landesbeauftragter sowie der Vorsitzende des Wissenschaftlichen Beirats für Mikrozensus und Volkszählung teilnahmen, konnte Einigung über ein verändertes Verfahren erzielt werden, das nach meiner Einschätzung eine hinreichend aussagefähige Wiederholungsbefragung ermöglicht, bei der die Rechte der von der Erhebung betroffenen Bürger ausreichend berücksichtigt werden.

Die erzielten Verbesserungen betrafen insbesondere den Inhalt und die frühzeitige Anonymisierung des Auswertungsdatensatzes, die Rechtsfolgen für die Befragten bei Feststellung von abweichenden Angaben bei der Haupt- und der Wiederholungsbefragung sowie den Text der den Befragten vor der Erhebung überreichten „Informationen zur Wiederholungsbefragung".

Wesentlich ist die Gewähr, daß keine Bußgeldverfahren durchgeführt werden, wenn unrichtige Angaben bei der Haupterhebung durch abweichende Angaben bei der Wiederholungsbefragung entdeckt werden. Wäre dies nicht sichergestellt worden, hätte die wahrheitsgemäße Angabe bei der Wiederholungsbefragung dazu geführt, daß sich einzelne Auskunftspflichtige selbst einer Ordnungswidrigkeit wegen unrichtiger Angaben bei der Haupterhebung bezichtigt hätten. Es war meines Erachtens zu befürchten, daß die Betroffenen zur Vermeidung eines Bußgeldes bemüht gewesen wären, unabhängig vom Wahrheitsgehalt dieselben Angaben wie bei der Haupterhebung zu machen. Damit wäre aber auch der Zweck der Wiederholungsbefragung verfehlt worden.

10.1.13

Im gegenwärtigen Zeitpunkt kann noch nicht beurteilt werden, ob die Volkszählung ausreichendes und verläßliches Datenmaterial erbracht hat. Dies liegt zum Teil auch daran, daß weit mehr Auskunftspflichtige als ursprünglich angenommen für die Abgabe der Erhebungsbögen den Postweg gewählt haben. Dies führte vielfach auch deshalb zu unrichtigen Angaben, weil die Beratung und Hilfe des Zählers fehlte.

10.1.14

Auch nach Zuleitung der Volkszählungsbögen an die Statistischen Ämter der Länder bleibt es meine Aufgabe, für die weitere datenschutzrechtlich korrekte *Behandlung der gewonnenen Daten* Sorge zu tragen. Dabei wird ein Schwerpunkt meiner Tätigkeit sein zu prüfen, ob die Übermittlung von Einzelangaben für Zusatzaufbereitungen für Bundeszwekke durch die Statistischen Landesämter an das Statistische Bundesamt den Voraussetzungen des VZG entspricht (vgl. § 14 Abs. 6 VZG). Daneben werde ich mein Augenmerk auf das vom Statistischen Bundesamt in Zusammenarbeit mit den Statistischen Ämtern der Länder zu erstellende Konzept der Übermittlung und Veröffentlichung der Volkszählungsdaten richten. Hierbei handelt es sich um Einzelangaben auf der Grundlage von Blockseiten für statistische Ämter von Gemeinden, um anonymisierte Einzelangaben, die jedermann, insbesondere auch der Wissenschaft, zur Verfügung gestellt werden können, und um die Ausgestaltung der zur Veröffentlichung bestimmten Tabellen. Ich werde mich zu gegebener Zeit im Statistischen Bundesamt über den Sachstand informieren und dafür Sorge tragen, daß im Rahmen solcher Datenübermittlungen dem Datenschutz hinreichend Rechnung getragen wird.

10.2 Straßenverkehrsunfallstatistik

10.2.1 Novellierung des Straßenverkehrsunfallstatistikgesetzes

Im Zuge der Anpassung von einzelstatistischen Rechtsgrundlagen an die Anforderungen des Volkszählungsurteils des Bundesverfassungsgerichts hat der Bundesminister für Verkehr den Entwurf eines neuen Straßenverkehrsunfallstatistikgesetzes vorgelegt.

Der Entwurf, der unter meiner Beteiligung in zwei Ressortbesprechungen erörtert wurde, führt insbesondere durch die präzisere Formulierung der für die Statistik zu erhebenden Angaben im Vergleich zum derzeit geltenden Gesetz zu größerer Normenklarheit. Gleichzeitig wirft er aber Probleme grundsätzlicher Natur auf, die noch einer eingehenden Erörterung bedürfen.

So hat sich bei der Diskussion des Entwurfs herausgestellt, daß die für statistische Zwecke zu erhebenden Angaben gleichzeitig wesentlicher Bestandteil der empirischen Grundlagen der Unfallforschung der Bundesanstalt für Straßenwesen (BASt) sind. Bei einigen Merkmalen ist sogar zu vermuten, daß sie nur deshalb mit dem vorgesehenen Detaillierungsgrad erhoben werden sollen, damit der Datenbedarf der BASt befriedigt werden kann.

Es steht außer Zweifel, daß der Straßenverkehrsunfallforschung ein hoher Stellenwert zukommt und daß den damit betrauten Stellen das dafür erforderliche Datenmaterial zur Verfügung gestellt werden muß. Andererseits müssen bei der Anordnung von Datenerhebungen für bundesstatistische Zwecke die von der Verfassung vorgegebenen und vom Bundesverfassungsgericht in seinem Volkszählungsurteil konkretisierten Rahmenbedingungen für die Bundesstatistik beachtet werden.

Zu den Voraussetzungen einer verfassungskonformen Rechtsgrundlage für eine Bundesstatistik gehört danach die Erforderlichkeit der zu erhebenden Merkmale für bundesstatistische Zwecke. Ein Forschungszweck der BASt würde demgemäß als Legitimation eines Informationseingriffs der Bundesstatistik allein nicht ausreichen.

Weiterhin verlangt der vom Bundesverfassungsgericht betonte Grundsatz der Trennung von Statistik und Verwaltung, daß personenbezogene Statistikdaten nur zum Zweck statistischer Aufbereitungen an andere Behörden übermittelt werden dürfen. Die Weitergabe von Daten, die keinen Personenbezug mehr aufweisen, ist hingegen ohne Einschränkung zulässig.

Zur Erfüllung ihres Forschungszweckes benötigt die BASt sehr detaillierte Informationen u. a. über den Ort und die Zeit eines Unfalls sowie die einzelnen Unfallbeteiligten. Darüber hinaus müssen für die Aufgaben der BASt die Daten über einen Unfall in einer Weise individualisierbar sein, die eine Ergänzung um zusätzliche, für den einzelnen Unfall relevante Angaben aus anderen der BASt zugänglichen Quellen ermöglicht. Dadurch tritt im Hinblick auf die Anonymität der Unfalldaten ein schwer zu lösender Konflikt ein. Je konkreter die Umstände eines Unfalls umschrieben werden und je mehr Verknüpfungsmerkmale ein Unfalldatensatz aufweist, desto weniger ist das Unerkanntbleiben der durch den Unfall Betroffenen gewährleistet. Nach meiner Einschätzung wäre die BASt im Falle des Inkrafttretens des Entwurfs aufgrund des ihr zur Verfügung stehenden Zusatzwissens in vielen Fällen in der Lage, die von einem Unfall betroffenen Personen zu identifizieren.

Um einerseits der BASt die notwendige Forschungstätigkeit zu ermöglichen, ohne andererseits die Wahrung statistischer Rechtsgrundsätze zu gefährden, habe ich angeregt, bei den weiteren Beratungen auch die Möglichkeit zu prüfen, die Erhebungsgrundlagen der Straßenverkehrsunfallstatistik und der Unfallforschung in zwei getrennten Rechtsgrundlagen zu regeln.

10.2.2 Übermittlung von Einzelangaben des Jahres 1985 an die Bundesanstalt für Straßenwesen (BASt)

Vor Inkrafttreten des 2. Statistikbereinigungsgesetzes im Dezember 1986 enthielt das Straßenverkehrsunfallstatistikgesetz eine Regelung, die die Übermittlung von Einzelangaben dieser Statistik u. a. an die BASt erlaubte. Auf der Grundlage dieser unter Berücksichtigung der Ausführungen des Volkszählungsurteils über die Trennung von Statistik und Verwaltung verfassungskonform ausgelegten Vorschrift hat das Statistische Bundesamt der BASt aus dem Berichtsjahr 1985 erstmals nur „faktisch anonyme" Unfalldaten übermittelt. Zu diesem Zweck hatte das Bundesamt den Umfang der in früheren Jahren übermittelten Unfalldatensätze um drei Merkmale reduziert, ohne deren Kenntnis ihm die Herstellung eines Personenbezuges zu Unfallbeteiligten nicht mehr möglich erschien.

Die BASt hat sich mit der Verringerung des Umfangs der übermittelten Daten nicht einverstanden erklärt. Der Bundesminister für Verkehr und der Bundesminister des Innern haben hierzu die Auffassung vertreten, daß die Verkürzung der Datensätze durch das Statistische Bundesamt rechtlich nicht geboten gewesen sei.

Nach meiner Überzeugung war sowohl die Beurteilung der Rechtslage durch das Statistische Bundesamt als auch dessen Einschätzung der faktischen Möglichkeiten einer Identifizierung von Unfallbeteiligten zutreffend. Diese Auffassung habe ich allen Beteiligten mitgeteilt.

Ungeachtet dieses Sachverhalts hat das Statistische Bundesamt der BASt nachträglich doch noch die gewünschten Daten in ungekürzter Form geliefert. Ich habe mich daher veranlaßt gesehen, diese unzulässige Datenübermittlung gegenüber dem fachlich zuständigen Bundesminister für Verkehr förmlich zu beanstanden. Dazu bestand nach meiner Auffassung um so mehr Anlaß, als die Datenübermittlung zu einem Zeitpunkt erfolgte, zu dem deren Rechtsgrundlage bereits außer Kraft getreten war.

10.3 Agrarberichterstattung

Im Frühjahr 1987 hat die Agrarberichterstattung, eine statistische Erhebung über die Struktur von etwa 100.000 landwirtschaftlichen Betrieben, stattgefunden.

Nachdem ich mich bereits im vorausgegangenen Jahr im Rahmen der Beurteilung der Agrarberichterstattung-Zusatzprogrammverordnung zu den da-

tenschutzrechtlichen Problemen der geplanten Erhebung geäußert hatte (vgl. hierzu 9. TB S. 46), habe ich rechtzeitig vor ihrer Durchführung in einem Schreiben an den Bundesminister für Ernährung, Landwirtschaft und Forsten zu den verwendeten Erhebungsunterlagen Stellung genommen. Zu meinem Bedauern hat der Bundesminister auf die darin enthaltenen Fragen und Bedenken erst geantwortet, nachdem die Erhebung bereits – unverändert – durchgeführt worden war. Auch unter Berücksichtigung seines Antwortschreibens bin ich zu dem Ergebnis gekommen, daß bei der Agrarberichterstattung 1987 die datenschutzrechtlichen Anforderungen an eine Bundesstatistik in zwei Punkten nicht erfüllt waren.

Zum ersten hätten bei der Befragung keine Personen für die Erhebung eingesetzt werden dürfen, die in der Nachbarschaft der zu Befragenden wohnen. Der in dieser Frage einschlägige § 14 Abs. 1 Satz 2 Bundesstatistikgesetz spricht zwar für diesen Fall ein solches Verbot nicht ausdrücklich aus. Nach meiner Ansicht stellt aber die Nachbarschaft zum Befragten einen „anderen Grund" im Sinne dieser Regelung dar, der den Einsatz als Erhebungsbeauftragter ausschließt. Diese Auslegung wird auch durch die Begründung der Vorschrift nahegelegt, in der es heißt, daß hiermit die Auflagen des Volkszählungsurteils berücksichtigt werden sollen. Das Volkszählungsurteil sieht es nämlich nicht als ausreichend an, daß den zu Befragenden die Möglichkeit eingeräumt wird, ihre Auskunft schriftlich – ohne Kenntnisnahme des Erhebers – zu erteilen. Es hält vielmehr „als weitere Maßnahme" ausdrücklich eine Vorschrift für geboten, daß Zähler nicht in der unmittelbaren Nähe ihrer Wohnung eingesetzt werden sollen (BVerfGE 65, 1, 60).

Zum zweiten war zwar die vorgenommene Erhebung der außerbetrieblichen Einkommen der Betriebsinhaber und deren Ehegatten rechtlich abgedeckt, nicht aber die der Einkünfte der auf dem Betrieb lebenden Familienangehörigen, Verwandten und Verschwägerten einschließlich deren Kinder. Der Bundesminister hat das Fehlen einer Rechtsgrundlage für diese Fragen nicht bestritten, die Befragung aber damit zu rechtfertigen versucht, daß „diese Informationen für die Beurteilung der Struktur des landwirtschaftlichen Betriebes relevant sind".

Ich halte die Erhebung dieser Merkmale deshalb für besonders bedenklich, weil der Bundesrat selbst der Erhebung der außerbetrieblichen Einkommen der im Betrieb beschäftigten Familienangehörigen, die im Entwurf der Agrarberichterstattung-Zusatzprogrammverordnung des Bundesministers für Ernährung, Landwirtschaft und Forsten noch ausdrücklich vorgesehen gewesen war, seine Zustimmung versagt hatte (vgl. 9. TB S. 46). Der Bundesrat hatte damit einerseits meinen datenschutzrechtlichen Bedenken Rechnung tragen wollen. Er hatte seine Ablehnung andererseits auch mit fachlichen Gesichtspunkten begründet: „Erhebungen über das außerbetriebliche Einkommen auch der im Betrieb beschäftigten Familienangehörigen gewährleisten keine verbesserte Darstellung der wirtschaftlichen Situation landwirtschaftlicher Betriebe. Sie lassen auch keine zusätzlichen Informationen über die Voraussetzung zur Fortführung des Betriebes zu, weil die finanzielle und soziale Bindung der im Betrieb beschäftigten Familienangehörigen sehr unterschiedlich ist." Diese Gründe gelten verständlicherweise erst recht für Familienangehörige, Verwandte und Verschwägerte, die lediglich auf dem Betrieb wohnen, ohne dort beschäftigt zu sein.

An einer förmlichen Beanstandung dieser Verstöße gegen Datenschutzbestimmungen gegenüber dem Bundesminister für Ernährung, Landwirtschaft und Forsten war ich aus Rechtsgründen gehindert, da die Durchführung der Agrarberichterstattung nicht durch das Statistische Bundesamt, sondern die Statistischen Landesämter erfolgt ist. Die Verarbeitung personenbezogener Daten durch diese Stellen kann nur von den Landesbeauftragten für den Datenschutz bzw. der Datenschutzkommission Rheinland-Pfalz beanstandet werden. Diesen habe ich meine Rechtsauffassung mitgeteilt.

11. Bundesarchivgesetz

Mit dem Bundesarchivgesetz ist nunmehr erstmalig die gesamte Materie des Archivwesens bundesrechtlich geregelt worden, nachdem bereits Baden-Württemberg im Juli 1987 ein eigenes Landesarchivgesetz verabschiedet hatte. Auf die Notwendigkeit einer derartigen bundesrechtlichen Regelung habe ich bereits in früheren Tätigkeitsberichten hingewiesen (2. TB S. 14f., 4. TB S. 50f.).

Der Gesetzentwurf war schon in der vergangenen Legislaturperiode beraten worden (vgl. 7. TB S. 37); es hat auch eine öffentliche Anhörung vor dem Innenausschuß des Deutschen Bundestages stattgefunden (vgl. 8. TB S. 26f.). Aus Zeitgründen kam es jedoch nicht mehr zu einer Verabschiedung. Zu Beginn der laufenden Legislaturperiode ist der Entwurf unverändert wieder eingebracht worden.

An den Beratungen des Gesetzentwurfes im Innenausschuß sowie im Arbeits- und Sozialausschuß des Deutschen Bundestages habe ich teilgenommen. In einer schriftlichen Stellungnahme gegenüber dem federführenden Innenausschuß habe ich meine Vorstellungen verdeutlicht und Änderungsvorschläge gemacht. Es ist gelungen, in einem wichtigen Punkt Verbesserungen gegenüber dem ursprünglichen Entwurf zu erzielen; nicht alle meine Vorstellungen finden sich allerdings in der endgültigen Fassung des Gesetzes wieder.

Ich begrüße es, daß die im Entwurf enthaltene Bestimmung gestrichen worden ist, wonach die Anbietungspflicht gegenüber dem Bundesarchiv auch Unterlagen umfaßt, die nach Rechtsvorschriften des Bundes der Vernichtung unterliegen. Nunmehr steht fest – auch durch eine zusätzliche deklaratorische Bestimmung –, daß alle Rechtsvorschriften über die Vernichtung und Löschung von Unterlagen vom Bundesarchivgesetz unberührt bleiben. Damit ist einem wichtigen datenschutzrechtlichen Anliegen Rechnung getragen worden.

Die Anbietungspflicht gegenüber dem Bundesarchiv umfaßt dagegen – insofern unverändert gegenüber den bisherigen Entwürfen – gemäß § 2 Abs. 4 auch Unterlagen, die Rechtsvorschriften des Bundes über Geheimhaltung unterliegen. Dies konnte akzeptiert werden (vgl. 7. TB S. 37), solange in den Entwurfsfassungen die Übergabe an das Archiv an die Voraussetzung geknüpft war, daß zuvor schutzwürdige Belange Betroffener durch Anonymisierung oder durch andere Maßnahmen angemessen zu berücksichtigen waren. Danach hätte die abgebende Behörde in jedem Einzelfalle eine Interessenabwägung zwischen den Erfordernissen der Archivierung und den Belangen Betroffener vorzunehmen gehabt. Eine derartige Regelung wäre auch deshalb konsequent gewesen, weil die abgebende Stelle für diese Abwägung über das Problembewußtsein und die speziellen Fachkenntnisse verfügt. Ich hatte deshalb zuletzt noch um eine Formulierung gebeten, wonach die abgebende Stelle und das Bundesarchiv – also beide gemeinsam – vor Übergabe der den Geheimhaltungsbestimmungen unterliegenden Unterlagen die schutzwürdigen Belange der Betroffenen durch geeignete Maßnahmen zu berücksichtigen haben.

Diese Regelung, der der Arbeits- und Sozialausschuß des Deutschen Bundestages zugestimmt hat, ist jedoch nicht in das Gesetz übernommen worden. Insbesondere hat der Innenausschuß des Bundestages befürchtet, damit praktische Schwierigkeiten bis zu einem Verweigerungsrecht der zur Abgabe verpflichteten Behörde hervorzurufen; auch sollten jegliche Veränderungen am Archivgut unterbleiben.

Die jetzt gefundene Regelung bedeutet, daß das Bundesarchiv Material erhält, ohne daß datenschutzrechtlich an sich gebotene Maßnahmen – wie Zusammenfassung, Veränderung, Vergröberung, Kürzung oder Weglassung einzelner sensitiver Daten oder Verknüpfungsmerkmale – getroffen werden oder die Einwilligung Betroffener eingeholt wird.

In diesem Zusammenhang ist es zu begrüßen, daß auf meinen Wunsch an dieser Stelle als Minimalsicherung des Schutzes der Persönlichkeitsrechte der betroffenen Bürger eine Bestimmung eingefügt wurde (§ 2 Abs. 4 Satz 2), wonach das Bundesarchiv bei der Erfüllung seiner Aufgaben hinsichtlich solcher Unterlagen, die Geheimhaltungsvorschriften unterliegen, diejenigen Vorschriften über die Verarbeitung und Sicherung zu beachten hat, die für die abgebende Stelle gelten. Eine derartige Vorschrift habe ich zur Klarstellung dessen für erforderlich gehalten, daß auch das Bundesarchiv selbst für seine eigenen Aufgaben (vgl. § 1 des Gesetzes) die notwendigen bereichsspezifischen Verarbeitungsbeschränkungen und Datensicherungsbestimmungen einzuhalten hat. Bei den übrigen im Gesetz geregelten Benutzungsbeschränkungen, insbesondere hinsichtlich der Verknüpfung personenbezogener Daten (§ 5 Abs. 9), handelt es sich um Teilregelungen, die sich zudem in erster Linie auf die Benutzer beziehen und hinsichtlich derer sich nicht mit der erforderlichen Deutlichkeit aus dem Gesetzeszusammenhang ergibt, daß sich auch die Mitarbeiter des Archivs selbst daran zu halten haben.

Ich gehe bei dieser Rechtslage davon aus, daß sich das Bundesarchiv, um die Anforderungen der eingefügten Vorschrift des § 2 Abs. 4 Satz 2 zu erfüllen, mit der Stelle in Verbindung setzen wird, von der das abgegebene Archivgut stammt. Insofern ist eine gewisse Berücksichtigung schutzwürdiger Belange Betroffener zwar nicht bei der Übergabe, aber bei der Nutzung des Materials gesetzlich vorgegeben.

Mit meinem Anliegen, alle speziellen Geheimhaltungspflichten, die durch die Übergabepflicht an das Bundesarchiv durchbrochen werden, im Gesetz aufzuzählen, konnte ich mich nicht durchsetzen. Nach meiner Auffassung hätte es sich empfohlen, durch eindeutige Aussagen für jeden Normbereich – und nicht lediglich für die in § 2 Abs. 4 Nr. 1 des Gesetzes genannten Bereiche – zum Ausdruck zu bringen, welche Geheimhaltungsbestimmungen durch das Bundesarchivgesetz verdrängt werden sollen. Dies sollte insbesondere für die durch § 203 StGB geschützten Geheimnisse (so auch Baden-Württemberg) und für das Statistikgeheimnis (§ 16 Bundesstatistikgesetz) gelten. Zumindest hätte klargestellt werden können, daß es sich bei den ausdrücklich genannten Geheimhaltungsvorschriften um keine abschließende Aufzählung handelt. Die Bundesregierung hat dagegen an ihrer Auffassung festgehalten, daß eine Auflistung der Geheimhaltungsvorschriften wegen ihrer großen Zahl und der Schwierigkeit bei häufigen Gesetzesänderungen gesetzestechnisch nicht opportun sei. Dem ist der Deutsche Bundestag gefolgt.

Bedauerlicherweise ist auch das Verhältnis zwischen § 5 Abs. 3 und § 5 Abs. 6 Nr. 5 des Gesetzes unklar geblieben. Die erstgenannte Bestimmung erweckt den Eindruck, nach Ablauf der dort genannten Benutzungssperrfrist von 80 Jahren könne jedermann sein Benutzungsrecht ausüben. Diese Regelung wird jedoch offenbar durch Absatz 6 Nr. 5 dieser Vorschrift verdrängt, wonach die Benutzung der von Rechtsvorschriften des Bundes über Geheimhaltung betroffenen Unterlagen durch Dritte auch nach Ablauf jeglicher Sperrfrist ausgeschlossen ist. Um irreführende Umkehrschlüsse zu vermeiden, hätte die Vorrangigkeit der – datenschutzrechtlich voll befriedigenden – Ausschlußlösung des Absatzes 6 deutlicher zum Ausdruck gebracht werden müssen. Das ist jedoch nicht geschehen.

Die Regelung über die Auskunftserteilung und die Folgen bei Unrichtigkeit von Daten (vgl. § 4) stellt eine bereichsspezifische Abweichung von Rechten Betroffener gegenüber dem Bundesdatenschutzgesetz dar. Weil sich hier das Interesse des Bundesarchivs durchgesetzt hat, das Archivgut frei von jeglicher Veränderung, etwa durch Anonymisierung, zu halten, sind die Rechte der Betroffenen geringfügig reduziert. So gibt es bei feststehender Unrichtigkeit personenbezogener Angaben keinen Berichtigungsanspruch, sondern nur die Möglichkeit, die Unrichtigkeit in den Unterlagen zu vermerken. Ein Auskunftsrecht des Betroffenen besteht nur dann, wenn das Archivgut durch den Namen seiner Person erschlossen wird. Darüber hinaus kann das Bundesarchiv anstelle einer Auskunft Akteneinsicht gewähren; bei dann erforderlichen weiten Anreisen ist es

denkbar, daß der Betroffene auf dieses Recht verzichtet. In allen Fällen hätte ich mir eine Regelung vorstellen können, die sich näher am Bundesdatenschutzgesetz orientiert.

Aus meiner Sicht zufriedenstellend ist die Fassung des § 11, der sich mit dem Übergabeverfahren in den Ländern gegenüber Landesarchiven befaßt. Auf meinen Vorschlag wird in dieser Bestimmung umfassend auf die vorangehenden Regelungen über die Berücksichtigung schutzwürdiger Belange Betroffener Bezug genommen. Insofern gibt es im Länderbereich keine Schlechterstellung gegenüber der Bundesregelung.

Ich werde in der nächsten Zeit beobachten, wie sich die dem Gesetz zugrunde liegende Konzeption in der Praxis bewährt.

12. Wissenschaft und Forschung

12.1 Datenübermittlung zu Forschungszwecken

Die Datenverarbeitung für wissenschaftliche Zwekke ist seit dem Volkszählungsurteil von Rechtsunsicherheit sowohl auf der Seite der Forschung als auch auf der Seite der über die erforderlichen Informationen verfügenden Stellen gekennzeichnet. Diese Unsicherheit ist darauf zurückzuführen, daß in weiten Bereichen, in denen wissenschaftliche Forschung betrieben wird, bislang keine bereichsspezifischen Regelungen vorliegen über die Modalitäten der Informationsbereitstellung und die Rechtspositionen der an einem Forschungsvorhaben beteiligten Stellen und Personen – einschließlich der Bürger, deren Daten ausgewertet werden sollen. Soweit einzelne Gesetze, wie z. B. das Bundeszentralregistergesetz, Wissenschaftsklauseln enthalten, muß noch abschließend geprüft werden, ob diese in vollem Umfang dem Volkszählungsurteil entsprechen. Bis zu einer speziellen gesetzlichen Regelung muß daher bei jedem Forschungsvorhaben in einem schwierigen und teilweise langwierigen Prozeß nach Wegen gesucht werden, wie den Wissenschaftlern – auch im Hinblick auf die grundgesetzlich verbürgte Forschungsfreiheit – Zugang zu den erforderlichen Daten gewährt werden kann, ohne dabei das informationelle Selbstbestimmungsrecht der Betroffenen, das ebenfalls Verfassungsrang einnimmt, zu verletzen.

Soweit ich mit diesen Fragen befaßt war, haben sich kriminologische Forschungsvorhaben als besonders problematisch erwiesen, da diese regelmäßig nur auf der Grundlage von – z. B. in Strafakten enthaltenen – Informationen höchster Sensitivität durchgeführt werden können, die darüber hinaus häufig als „Längsschnittdaten" eines größeren Zeitraums zur Verfügung stehen müssen.

Für die absehbare Zukunft verspreche ich mir allerdings mehr Rechtsklarheit in diesem Bereich, da diese Problematik zunehmend auch die Aufmerksamkeit des Bundesgesetzgebers gewinnt. Nachdem die Datenverarbeitung für wissenschaftliche Zwecke zunächst im neuen Hessischen Datenschutzgesetz entsprechend den verfassungsgerichtlichen Vorgaben geregelt wurde, liegt mit Inkrafttreten des Bundesstatistikgesetzes nunmehr die erste – bereichsspezifische – Wissenschaftsklausel auf Bundesebene vor (vgl. 9. TB S. 43). Ich würde es sehr begrüßen, wenn weitere sektorale Regelungen noch in dieser Legislaturperiode folgen würden. Die zuständigen Ressorts haben bereits mit der Vorbereitung entsprechender Bestimmungen für die Geltungsbereiche der Strafprozeßordnung, des Strafvollzugsgesetzes und des Personenstandsgesetzes begonnen. Diese Bemühungen sollten nach meiner Auffassung auch nicht durch die Beratungen des Entwurfs eines Bundesdatenschutzgesetzes aufgehalten werden. Die in diesen Gesetzentwurf aufgenommene – allgemeine – Wissenschaftsklausel kann nur als Auffangregelung verstanden werden, durch die speziellere Regelungen in Fachgesetzen nicht obsolet werden.

Da die Beratungen der genannten Gesetzgebungsvorhaben noch am Anfang stehen, habe ich dazu noch keine abschließende Stellungnahme abgeben können. Ich gehe aber davon aus, daß ich im weiteren Verfahren dazu noch rechtzeitig Gelegenheit erhalten werde.

Bereits heute kann ich feststellen, daß die Wissenschaftsklausel im Entwurf eines Bundesdatenschutzgesetzes noch einer eingehenden Erörterung bedarf. Sie weicht deutlich ab sowohl von den erwähnten Bestimmungen im Hessischen Datenschutzgesetz und im Bundesstatistikgesetz als auch von ihrem Vorläufer, dem Artikel 1 Nr. 5 (§ 3 a) des in der vergangenen Legislaturperiode nicht mehr verabschiedeten Entwurfs eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze. Insbesondere werden diese Abweichungen zu diskutieren sein, die auch die Frage betreffen, unter welchen Voraussetzungen auf die Einwilligung des Betroffenen in die Übermittlung seiner Daten zu Forschungszwecken verzichtet werden darf. Im Vordergrund der anstehenden Diskussion sollte auch die Frage stehen, wie eine stärkere Gleichbehandlung von öffentlicher und privater Forschung im Hinblick auf den Datenzugang und die für die Verarbeitung geltenden Schutzvorschriften erreicht werden kann. Ferner halte ich eine Verstärkung der Zweckbindung der benötigten Daten – insbesondere durch die grundsätzliche Beschränkung ihrer Nutzung auf ein bestimmtes Forschungsvorhaben – und die Verbesserung der Transparenz der Datenflüsse – u. a. durch Begründung von Anzeige- und Protokollierungspflichten – für erforderlich. Darüber hinaus sehe ich es als wesentlich an, daß der Kreis der privilegierten Datenempfänger auf die „unabhängige" wissenschaftliche Forschung beschränkt wird.

12.2 Gentechnologie

Die Enquête-Kommission „Chancen und Risiken der Gentechnologie" hat in ihrem Bericht an den Deutschen Bundestag (Drucksache 10/6775) mehrfach und unter verschiedenen Aspekten auf Probleme des Datenschutzes hingewiesen, die bei der Anwendung

der Gentechnologie entstehen können. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, die in dem Bericht der Enquête-Kommission auch direkt angesprochen wird, hat im Berichtsjahr eine Arbeitsgruppe Gentechnologie gebildet, deren Vorsitz von mir wahrgenommen wird.

Die Arbeitsgruppe beabsichtigt, zu folgenden Themen des Berichts der Enquête-Kommission Arbeitspapiere zu erstellen, die dazu beitragen sollen, auf die insoweit auftretenden datenschutzrechtlichen Fragen Antworten zu finden:

— Genomanalyse im Strafverfahren

— Genomanalyse an Arbeitnehmern

— Genomanalyse für Versicherungen

— Menschliche Sicherheit im Arbeitsverhältnis

— Genetische Beratung und pränatale Diagnostik

— Neugeborenen-Screening

Ich habe einige Ausschüsse des Deutschen Bundestages, in denen der Bericht der Enquête-Kommission behandelt wird, gebeten, mich über ihre Beratungsergebnisse zu informieren oder zu beteiligen, wenn Fragen des Datenschutzes zu den oben genannten Themen beraten werden. Ich rechne damit, daß die Erörterung dieser sehr schwierigen Materie in der Arbeitsgruppe noch geraume Zeit in Anspruch nehmen wird, bis sich Ergebnisse abzeichnen.

13. Sozialwesen – Allgemeines

13.1 Innerbehördliche Schweigepflicht bei Berufsgeheimnissen

Die Frage, welche Wirkungen die Schweigepflicht beamteter oder angestellter Träger von Berufsgeheimnissen im Sinne des § 203 Abs. 1 StGB (z. B. Ärzte, Psychologen, Erziehungsberater, Sozialarbeiter) im innerdienstlichen Verkehr hat, ist immer wieder Gegenstand datenschutzrechtlicher Erörterungen. Die Reichweite der „innerbehördlichen Schweigepflicht" bei Berufsgeheimnissen ist umstritten.

Einen wesentlichen Beitrag zur Klärung dieser Fragen hat das Bundesarbeitsgericht mit seinem Urteil vom 13. Januar 1987 (1 AZR 267/85) geleistet, in dem festgestellt wird, „daß der beklagte Landkreis nicht berechtigt ist, bei den von den Nebenstellen der Beratungsstelle für Erwachsene, Kinder und Jugendliche ausgehenden dienstlichen Telefongesprächen die vollständige Rufnummer des Gesprächspartners zu erfassen, soweit der Kläger in seiner Eigenschaft als Berufspsychologe/Berater Klienten anruft." Zur Begründung hat das BAG u. a. ausgeführt: „Eine fachgerechte psychologische Beratung und Behandlung, die Aussicht auf Erfolg haben soll, setzt ein Vertrauensverhältnis zwischen der zu betreuenden Person und dem Psychologen voraus, dessen Entstehen wesentlich dadurch bedingt ist, daß die Beratung und Behandlung vertraulich bleibt, d. h. anderen Personen nicht bekannt wird. Davon, daß die psychologische Beratung und Behandlung von Personen eine solche Vertraulichkeit erfordert und daß die behandelte Person gegen den Psychologen einen Anspruch auf Wahrung dieser Vertraulichkeit hat, geht § 203 Abs. 1 Nr. 2 und 4 StGB aus. Nach dieser Vorschrift macht sich strafbar, wer als Berufspsychologe mit staatlich anerkannter wissenschaftlicher Abschlußprüfung oder als Ehe-, Erziehungs- oder Jugendberater sowie Berater in Suchtfragen in einer öffentlichen oder öffentlich anerkannten Beratungsstelle ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis unbefugt offenbart. Schon die Tatsache, daß jemand die Beratung oder Behandlung des Klägers in seiner Eigenschaft als Berufspsychologe in Anspruch nimmt, ist ein solches Geheimnis im Sinne von § 203 StGB und nicht erst das Problem oder die Krankheit, die Anlaß für die Inanspruchnahme des Berufspsychologen ist. Dieses Geheimnis zu wahren, ist der angestellte Berufspsychologe auch gegenüber seinem Arbeitgeber verpflichtet. ... Er (der Arbeitgeber) darf vom angestellten Diplom-Psychologen nicht Auskunft darüber verlangen, wer ihn in seiner Eigenschaft als Berater in Anspruch genommen hat."

Diese deutlichen Hinweise auf den hohen Stellenwert der Berufsgeheimnisse auch im innerdienstlichen Verkehr ist zu begrüßen. Wenn danach schon die Bekanntgabe der Rufnummer des Klienten an den Arbeitgeber bzw. Dienstherrn unbefugt ist, weil damit sein Name festgestellt werden kann, so ist m. E. erst recht die Offenbarung personenbezogener Daten bzw. die Überlassung nicht anonymisierter Unterlagen z. B. an vorgesetzte Personen oder Stellen zum Zwecke der Dienst- oder Fachaufsicht oder etwa zur Einleitung oder Durchführung von Verwaltungsmaßnahmen unbefugt, soweit nicht im Einzelfall ein konkreter Rechtfertigungsgrund (Einwilligung, gesetzliche Mitteilungspflicht, rechtfertigende Interessenabwägung gemäß § 34 StGB) vorliegt. Eine generelle Pflicht oder ein allgemeines Recht zur Mitteilung geheimer Tatsachen oder zur Vorlage entsprechender Vorgänge läßt sich mit diesen Rechtfertigungsgründen jedoch nicht begründen. Auch Dienstanweisungen, Verwaltungsvorschriften oder sonstige allgemeine interne Regelungen sowie dienst- oder arbeitsvertragliche Regelungen reichen als Rechtfertigung von Offenbarungen nicht aus.

13.2 Sozialdatengeheimnis und Rechnungsprüfung

Der Bundesrechnungshof hatte im Rahmen einer Prüfung der Einziehung der im Lohnabzugsverfahren entrichteten Beiträge zur Rentenversicherung der Arbeiter, die bei der Landesversicherungsanstalt Oldenburg-Bremen stattfand, einigen Krankenkassen (Einzugsstellen gemäß § 1399 RVO) eine örtliche Prüfung der Einziehung und Abführung der Rentenversicherungsbeiträge sowie ihrer Verwaltung und Abrechnung angekündigt. Die beteiligten Krankenkassen haben zunächst datenschutzrechtliche Bedenken gegen eine solche Prüfung durch den Bundesrechnungshof geäußert. Nach ihrer Auffassung stehe der Schutz der Sozialdaten und die Pflicht zur Wahrung des Sozialgeheimnisses (§ 35 SGB I) der

Prüfung und der damit verbundenen Offenbarung von Sozialdaten entgegen.

Der Bundesrechnungshof hat dem entgegengehalten, daß sein Recht, die Haushalts- und Wirtschaftsführung des Bundes zu prüfen, durch Artikel 114 GG verfassungsrechtlich abgesichert sei. Nach dieser Vorschrift gebe es keine prüfungsfreien Räume mehr. Dieser Grundsatz werde auch nicht unter dem Gesichtspunkt des Datenschutzes oder des Steuergeheimnisses eingeschränkt. Im übrigen seien die rechnungsprüfungsberechtigten Behörden in § 35 Abs. 1 SGB I ausdrücklich als Adressat des Geheimhaltungsanspruchs genannt. Vom Wortsinn und vom logischen Handlungsablauf sei aber ein solcher Anspruch gegen den Bundesrechnungshof nur denkbar, wenn dieser zuvor überhaupt die Möglichkeit habe, im Rahmen einer Prüfung von etwaigen personenbezogenen Daten Kenntnis zu nehmen. Bei dieser Rechtslage erübrige sich ein Rückgriff auf die Offenbarungsvorschriften (§§ 67 bis 77 SGB X).

In einer auf Bitten der Krankenkassen abgegebenen Stellungnahme habe ich zu der hier streitigen Frage, ob Krankenkassen gegenüber dem Bundesrechnungshof im Rahmen einer Prüfung gemäß § 112 Bundeshaushaltsordnung Sozialdaten offenbaren dürfen, folgende Auffassung vertreten:

Einzelangaben über die persönlichen und sachlichen Verhältnisse des einzelnen (personenbezogene Daten) sind von den in § 35 Abs. 1 SGB I genannten Stellen als Sozialgeheimnis zu wahren und dürfen von diesen Stellen nicht unbefugt offenbart werden. Eine Offenbarung ist nur unter den Voraussetzungen der §§ 67 bis 77 SGB X zulässig (§ 35 Abs. 2 SGB I).

Es wäre irrig, aus der Aufzählung der zur Wahrung des Sozialgeheimnisses verpflichteten Stellen in Absatz 1 den Schluß zu ziehen, daß bereits deswegen eine Offenbarung von Sozialdaten innerhalb des Kreises dieser Stellen ohne weitere Voraussetzungen bzw. Beschränkungen zulässig sei. Dem steht einmal der eindeutige Wortlaut des Absatzes 2 entgegen und zum anderen hätte es dann der Vorschrift des § 69 Abs. 1 Nr. 1 SGB X nicht bedurft. Es ist deshalb und aufgrund der vom Gesetzgeber gewählten Systematik – Normierung des Sozialgeheimnisses im Ersten Buch und Regelung des Datenverkehrs der wahrungspflichtigen Behörden und Stellen untereinander und mit Dritten im Zehnten Buch – m. E. nicht statthaft, der Aufzählung der Stellen in § 35 Abs. 1 SGB I eine weitergehende Bedeutung und Funktion als die Bestimmung des Anwendungsbereichs beizumessen.

Den Datenverkehr der in § 35 SGB I genannten Stellen untereinander regelt § 69 Abs. 1 Nr. 1 SGB X. Danach ist eine Offenbarung personenbezogener Daten zulässig, soweit sie für die Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch erforderlich ist.

Die Prüfung der Haushalts- und Wirtschaftsführung durch den Bundesrechnungshof ist indes unter keinem Gesichtspunkt eine Aufgabe nach dem Sozialgesetzbuch. Eine Befugnis zur Offenbarung von Sozialdaten an den Rechnungshof kann daher aus dieser Vorschrift nicht abgeleitet werden.

Andererseits wurde bei der parlamentarischen Beratung des Sozialgesetzbuchs auf Vorschlag des Vermittlungsausschusses die Aufzählung in § 35 Abs. 1 SGB I um die „rechnungsprüfungsberechtigten Behörden" ergänzt, um klarzustellen, „daß durch die Datenschutzvorschriften das Recht der Rechnungshöfe nicht beeinträchtigt wird" (Bericht über die 491. Sitzung des Bundesrats vom 18. Juli 1980 – Beratung des Antrags des Vermittlungsausschusses, Drucks. 421/80). Die „Klarstellung", daß das Recht der Rechnungshöfe nicht „beeinträchtigt" wird, hat nach meinem Verständnis in diesem Zusammenhang die Bedeutung eines Hinweises auf einen bestehenden Rechtszustand, der keiner neuerlichen gesetzlichen Regelung mehr bedarf. Der Gesetzgeber hat damit seine Auffassung bekundet, daß der verfassungsmäßige Prüfungsauftrag des Bundesrechnungshofes (Artikel 114 GG) das notwendige Zugriffsrecht auch auf Vorgänge und Daten umfaßt, die einer besonderen Geheimhaltung unterliegen, und daher die Offenbarung solcher Vorgänge und Daten an den Bundesrechnungshof einer einfachgesetzlichen Regelung im Sozialgesetzbuch entzogen ist.

Unter diesem Gesichtspunkt besteht für die Stellen, die das Sozialgeheimnis zu wahren haben, eine gleichsam „übergesetzliche" Offenbarungsbefugnis an den Bundesrechnungshof, soweit diese Stellen der Prüfung durch den Bundesrechnungshof unterliegen.

Im vorliegenden Fall beabsichtigte der Bundesrechnungshof auf der Grundlage des § 112 Abs. 1 Satz 1 BHO i. V. m. § 111 BHO die Haushalts- und Wirtschaftsführung der Landesversicherungsanstalt Oldenburg-Bremen, insbesondere die Einziehung der im Lohnabzugsverfahren entrichteten Beiträge zur Rentenversicherung der Arbeiter, örtlich zu prüfen. Der Beitragseinzug wird von der Landesversicherungsanstalt nicht selbst durchgeführt. Diese Beiträge werden vielmehr von den Trägern der gesetzlichen Krankenversicherung (Einzugsstellen) eingezogen. Insoweit handeln die Einzugsstellen auf der Grundlage eines gesetzlichen Auftrags im Sinne des § 93 SGB X für den Rentenversicherungsträger. Wie sich auch aus § 1437 RVO und § 89 Abs. 3 i. V. m. § 93 SGB X ergibt, hat der Rentenversicherungsträger als Auftraggeber Verfügungsmacht über die durch den auftragsgemäßen Einzug der Beiträge zur gesetzlichen Rentenversicherung entstandenen Unterlagen und Daten. Insoweit bezieht sich die Offenbarungsbefugnis des Rentenversicherungsträgers gegenüber dem Bundesrechnungshof auch auf diese Unterlagen. Als Auftragnehmer sind die Einzugsstellen berechtigt, die dem Rentenversicherungsträger zukommenden Befugnisse – in dessen Namen und auf dessen Veranlassung – auszuüben.

Eine Offenbarungsbefugnis der Landesversicherungsanstalt gegenüber dem Bundesrechnungshof erstreckt sich demzufolge auch auf die Einzugsstellen, soweit die Landesversicherungsanstalt entsprechende Weisungen erteilt. Unter dieser Voraussetzung sind die Einzugsstellen berechtigt und ver-

pflichtet, dem Bundesrechnungshof die von diesem für die Durchführung seines Prüfungsauftrags (bei der Landesversicherungsanstalt) für erforderlich gehaltenen Unterlagen (§ 95 Abs. 1 BHO) über die Einziehung der Rentenversicherungsbeiträge und ihre Abführung an die Landesversicherungsanstalt vorzulegen.

13.3 Sozialgeheimnis und Staatsanwaltschaft

„Seitdem sich Ermittlungsverfahren gegen Ärzte häufen, kann beobachtet werden, wie patientenbezogene Daten aus Krankenkassen und anderen Körperschaften öffentlichen Rechts, Staatsanwaltschaften ohne richterlichen Beschluß, offenbar im Wege sog. Amtshilfe, zur Verfügung gestellt werden. Ebenso erfolgt die Weitergabe bei Anzeigen zur Einleitung von Ermittlungsverfahren. Krankenkassen und andere begründen dieses Verfahren mit der Verpflichtung zum Schutze der Versichertengemeinschaft, hinter deren Interessen das Interesse der Patienten an der Geheimhaltung ihrer Daten zurückzutreten habe."

Diese Feststellung ist mir von Ärzten zur Stellungnahme vorgelegt worden. Mit der darin enthaltenen Fragestellung, inwieweit und unter welchen Voraussetzungen eine Offenbarung von Sozialdaten im Zusammenhang mit staatsanwaltschaftlichen Ermittlungsverfahren ohne richterliche Anordnung zulässig ist, hatte ich mich aus gegebenen Anlässen bereits mehrfach zu befassen. Ich vertrete dazu folgende Auffassung:

Einzelangaben über die persönlichen und sachlichen Verhältnisse (personenbezogene Daten) von Patienten unterliegen bei den gesetzlichen Krankenkassen und den Kassenärztlichen Vereinigungen dem besonderen Schutz des Sozialgeheimnisses gemäß § 35 SGB I. Eine Offenbarung ist nur unter den Voraussetzungen der §§ 67 bis 77 SGB X zulässig.

Abgesehen von der Einwilligung des Betroffenen (§ 67 Ziffer 1 SGB X) kommt im vorliegenden Zusammenhang eine Offenbarung nach § 69 Abs. 1 Nr. 1 SGB X in Betracht. Danach ist eine Offenbarung personenbezogener Daten zulässig, soweit sie für die Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch (einschließlich seiner besonderen Teile) durch die Krankenkasse bzw. die Kassenärztliche Vereinigung oder für die Durchführung eines damit zusammenhängenden gerichtlichen Verfahrens einschließlich eines Strafverfahrens erforderlich ist.

Nach meiner Auffassung, die sich auf vergleichbare Vorschriften des Sozialgesetzbuches stützt, hat die Staatsanwaltschaft nach dem Wortlaut des § 69 Abs. 1 Nr. 1 SGB X keinen Auskunftsanspruch, da ausdrücklich nur „gerichtliche" Verfahren genannt sind. Im Verhältnis Staatsanwaltschaft und Sozialleistungsträger kommt jedoch während des staatsanwaltschaftlichen Ermittlungsverfahrens eine Offenbarungsbefugnis nach der 1. Alternative der Vorschrift in Betracht. Danach hat die Krankenkasse bzw. die Kassenärztliche Vereinigung in eigener Entscheidungskompetenz zu prüfen, ob die Offenbarung für die eigene Aufgabenerfüllung erforderlich ist. Entsprechende Aufgaben ergeben sich im vorliegenden Zusammenhang aus den Vorschriften über die kassenärztliche Versorgung, die angemessene Vergütung ärztlicher Leistungen und die rechtmäßige Verwendung der Mittel; dazu gehört nach herrschender Meinung auch eine Strafanzeige oder die Unterstützung entsprechender Ermittlungen im erforderlichen Umfang, wenn der Verdacht oder Anhaltspunkte für strafrechtlich relevante Abrechnungsmanipulationen bestehen.

Die Vorschrift des § 76 Abs. 1 SGB X, die grundsätzlich die Wahrung des Patientengeheimnisses auch nach einer befugten Offenbarung durch den Arzt an die dem Sozialgeheimnis unterliegenden Stellen gewährleisten soll, steht einer Offenbarung gegenüber der Staatsanwaltschaft insoweit nicht entgegen. Die vorzunehmende Rechtsgüterabwägung, die nach dem Zweck dieser Vorschrift auf die Interessen der offenbarenden Stelle abzustellen ist, ergibt m. E., daß das Interesse an der strafrechtlichen Verfolgung von Abrechnungsmanipulationen als Aufgabe der Krankenkasse bzw. der Kassenärztlichen Vereinigung das Interesse des einzelnen an der Geheimhaltung seiner Daten überwiegt.

Aus den dargelegten Gründen halte ich die Offenbarung personenbezogener Daten einschließlich der von einem Arzt zugänglich gemachten Daten an Strafverfolgungsbehörden durch die Krankenkasse bzw. die Kassenärztliche Vereinigung im Rahmen der Erfüllung eigener Aufgaben ohne richterliche Anordnung für zulässig. Allerdings ist gerade in diesen Fällen die Erforderlichkeit und Verhältnismäßigkeit der Offenbarung personenbezogener Daten besonders sorgfältig zu prüfen.

13.4 Datenerhebung für statistische Zwecke

Wer Leistungen nach dem Bundesausbildungsförderungsgesetz (BAföG) beantragt oder erhält, hat nach § 60 Abs. 1 Nr. 1 SGB I alle Tatsachen anzugeben, die für die Leistung erheblich sind. Die zur Feststellung des Anspruchs erforderlichen Tatsachen sind auf den Formblättern anzugeben, die der Bundesminister für Bildung und Wissenschaft durch allgemeine Verwaltungsvorschrift bestimmt hat. die Mitwirkungspflicht gemäß § 60 SGB I gilt auch für die Eltern und den Ehegatten des Auszubildenden (§ 47 Abs. 4 BAföG).

Aufgrund dieser Vorschriften haben der Auszubildende und gegebenenfalls der Ehegatte und die Eltern bei der Beantragung von Ausbildungsförderung verschiedene Formblätter auszufüllen und dabei die in den Formblättern festgelegten Angaben über ihre persönlichen und sachlichen Verhältnisse (personenbezogene Daten) zu machen, die für die beantragte Leistung erheblich sind.

Darüber hinaus werden mit diesen Formblättern aber auch personenbezogene Daten erhoben, die für die Leistungsgewährung nicht erforderlich sind (z. B. Berufstätigkeit oder Art der Ausbildung des

Ehegatten, Familienstand und Berufstätigkeit der Eltern). In einem „Hinweisblatt" werden diese zusätzlichen Angaben als erforderlich „für Statistik, Planung und Weiterentwicklung der Ausbildungsförderung (§ 55 BAFöG)" bezeichnet. Nach Auffassung des Bundesministers für Bildung und Wissenschaft sind solche Angaben deshalb erforderlich, weil die Vorschriften über den Förderungsbereich des Gesetzes zunächst nur teilweise in Kraft gesetzt wurden. Der Gesetzgeber habe sich selbst zur Weiterentwicklung der Ausbildungsförderung verpflichtet. Dafür seien Erkenntnisse über die soziale Wirksamkeit der Ausbildungsförderung notwendig.

Diesem Zweck dient offensichtlich die nach § 55 BAFöG jährlich durchzuführende Bundesstatistik. Über die in Absatz 2 a. a. O. aufgeführten Daten sind die Ämter für Ausbildungsförderung auskunftspflichtig (Abs. 3 a. a. O.).

Bei § 55 BAFöG handelt es sich um die Anordnung einer Sekundärstatistik. Es gehört zum Wesen einer Sekundärstatistik, daß die auskunftgebenden Stellen den Statistischen Ämtern Angaben machen, die bei ihrer eigenen Aufgabenerfüllung angefallen sind. Eine Ermächtigung der auskunftgebenden Stellen, ihrerseits bei den Betroffenen Daten nur für statistische Zwecke zu erheben, ist damit nicht verbunden. Im vorliegenden Fall kann also die Erhebung von Daten bei den Betroffenen nicht darauf gestützt werden, daß diese für Zwecke der BAFöG-Statistik erforderlich sind. § 10 Bundesstatistikgesetz kommt nicht als Ermächtigungsgrundlage für eine Erhebung in Betracht. Diese Vorschrift besagt nur, daß bei statistischen Erhebungen grundsätzlich Auskunftsverpflichtung für den Kreis der zu Befragenden besteht, es sei denn, die Auskunftserteilung ist ausdrücklich freigestellt. Die Vorschrift setzt also voraus, daß an anderer Stelle der Kreis der zu Befragenden für eine bestimmte Statistik festgelegt ist (vgl. §§ 6 Abs. 1 i. V. m. 7 Abs. 1 Bundesstatistikgesetz). Im vorliegenden Fall sind aber in § 55 Abs. 3 BAFöG nur die Ämter für Ausbildungsförderung genannt. Die Auskunftspflicht (§ 46 Abs. 3 BAFöG) und die Mitwirkungspflicht der Eltern und des Ehegatten (§ 60 SGB I i. V. m. § 47 Abs. 4 BAFöG) sind ausdrücklich auf diejenigen Angaben beschränkt, die für die Feststellung des Anspruchs erforderlich bzw. für die Leistung erheblich sind. Die Angaben, die allein für statistische Zwecke benötigt werden, dürfen auch nicht auf freiwilliger Basis bei den Betroffenen erhoben werden, da gemäß § 5 Abs. 1 i. V. m. § 9 Abs. 1 Bundesstatistikgesetz auch „freiwillige" Bundesstatistiken – d. h. Statistiken ohne Auskunftspflicht – unter Gesetzesvorbehalt stehen und die zu erhebenden Merkmale in dieser Rechtsvorschrift bestimmt werden müssen.

Als Ergebnis bleibt somit festzuhalten, daß über § 55 BAFöG nur diejenigen Daten erfragt werden dürfen, die aufgrund der Verwaltungstätigkeit der Förderungsämter bei diesen anfallen. Für rein statistische Zwecke dürfen Daten durch die Förderungsämter weder aufgrund vermeintlicher Auskunftsverpflichtung der Betroffenen noch auf freiwilliger Basis erhoben werden. Die Datenerhebung entbehrt somit einer rechtlichen Grundlage. Soweit die im Verwaltungsvollzug angefallenen Daten für statistische Zwecke nicht ausreichen, hat der Gesetzgeber zu entscheiden, ob eine (zusätzliche) Primärerhebung bei den Betroffenen anzuordnen ist.

14. Arbeitsverwaltung

Im Laufe des Berichtsjahres habe ich zahlreiche Beratungsgespräche mit Vertretern der Bundesanstalt für Arbeit sowohl auf regionaler Ebene bei Arbeitsämtern wie auch in der Hauptstelle in Nürnberg geführt. Dabei ging es im wesentlichen um den Umgang mit Sozialdaten und die zugrunde liegenden innerdienstlichen Vorschriften. In einer Reihe von Fragen sind daraufhin wichtige Veränderungen angekündigt oder bereits eingeführt worden.

Nachstehend werden dafür einige ausgewählte Beispiele dargestellt:

14.1 Weitergabe von Bewerbungsunterlagen

Die Frage der *Weitergabe von Bewerbungsunterlagen* durch das Arbeitsamt an potentielle Arbeitgeber, mit der ich mich sowohl in meinem Achten (S. 30) wie auch meinem Neunten Tätigkeitsbericht (S. 48) auseinandergesetzt habe, kann nunmehr als gelöst betrachtet werden.

Im Zusammenhang mit der Einführung eines computerunterstützten Arbeitsvermittlungsverfahrens (coArb), das bereits in einigen Arbeitsämtern im Einsatz ist und bis zum Jahresende 1989 allgemein eingeführt sein wird, hat die Bundesanstalt für Arbeit eine Regelung getroffen, die meinen Anforderungen gerecht wird. Das Verfahren coArb sieht vor, daß ein Arbeitssuchender, der zum ersten Mal Kontakt mit der Arbeitsvermittlung aufnimmt, einen Erhebungsbogen ausfüllt, dem ein Blatt mit Hinweisen zum Ausfüllen der Beratungs- und Vermittlungsunterlagen beigefügt ist. Auf diesem Blatt befindet sich der folgende Satz: „Durch eine unmittelbare Vorlage Ihrer Bewerbungsunterlagen bei Auftraggebern kann das Vermittlungsverfahren beschleunigt werden. Sofern Sie damit nicht einverstanden sind, vermerken Sie dies bitte in der letzten Zeile des Anmeldebogens." Die Entscheidung über die Weitergabe der Bewerbungsunterlagen wird also jetzt dem Betroffenen überlassen und in der Datenverarbeitungsanlage gespeichert. Der dieses Verfahren regelnde Runderlaß 8/87 ist zwischenzeitlich in Kraft und entfaltet damit auch Wirkungen auf das bisherige konventionelle Vermittlungsverfahren. Diese Lösung wird von mir als geeignete Maßnahme zur Wahrung der Belange der Arbeitssuchenden angesehen.

14.2 Gewährung von Arbeitslosenhilfe

Die Problematik des Verfahrens der Bundesanstalt für Arbeit bei der Gewährung von Arbeitslosenhilfe

beschäftigte mich auch im Berichtszeitraum aufgrund von verschiedenen Eingaben.

— Unterhaltspflichtige beschwerten sich, daß auf den Arbeitslosenhilfebescheiden ihr Einkommen entsprechend der Berechnung des anrechnungsfähigen Betrages aufgeschlüsselt dargestellt wird. Aus zahlreichen Gesprächen mit Vertretern der Arbeitsverwaltung – sowohl der Hauptstelle der Bundesanstalt wie auch regionaler Arbeitsämter – wurde mir bekannt, daß das derzeitige Verfahren auch dort nicht für erforderlich gehalten wird. Es handelt sich um die Übermittlung sensibler Daten der betroffenen Unterhaltspflichtigen an Unterhaltsberechtigte, deren Bekanntgabe im Stadium der Bescheidung keine unmittelbaren Auswirkungen hat. Es wäre daher ausreichend, wenn den Unterhaltsberechtigten nach einem Widerspruch gegen den Bescheid die Einkommensverhältnisse des Unterhaltspflichtigen offenbart würden. Ich hätte es begrüßt, wenn der Bundesminister für Arbeit und Sozialordnung seinen Entwurf zur 8. Novelle zum Arbeitsförderungsgesetz zum Anlaß genommen hätte, eine dem § 50 Abs. 2 Satz 2 Bundesausbildungsförderungsgesetz (BAFöG) entsprechende Regelung vorzusehen, wie dies von mir wiederholt angeregt worden ist (vgl. u. a. 9. TB S. 49).

— Mehrere Eingaben betrafen die Datenerhebung im Zusammenhang mit der Feststellung des Einkommens bzw. der Unterhaltspflicht bei der Gewährung von Arbeitslosenhilfe. Die Bundesanstalt für Arbeit ermittelt den als Einkommen bzw. Unterhaltsanspruch anzurechnenden Betrag auf der Grundlage des Nettoeinkommens des Antragstellers bzw. des Unterhaltspflichtigen. Der Auskunftspflichtige muß in dem Antragsformular auf Arbeitslosenhilfe bzw. in dem für Unterhaltspflichtige bestimmten Formular die Beträge eintragen, die zu seinem Einkommen zählen. Hierzu gehören beispielsweise auch Einnahmen aus Miet-, Pacht- oder Patentnutzungsverträgen. Die Bundesanstalt für Arbeit nimmt derartige Vertragsunterlagen in Kopie zu den Leistungsakten des Arbeitslosenhilfeempfängers.

  Meine Bedenken richten sich nicht gegen die Tatsache der Einsichtnahme der Bundesanstalt in diese Verträge, aus denen dem Antragsteller oder Angehörigen Einkommen erwächst. Ich halte es aber für ausreichend, wenn in diesen Fällen durch die Leistungsabteilung überprüft wird, ob der in dem Vertrag genannte Betrag mit der Eintragung in dem jeweiligen Antragsformular übereinstimmt, und die Verträge im Anschluß daran dem Antragsteller oder dessen unterhaltspflichtigen Angehörigen wieder zurückgegeben werden. Eine Vorhaltung dieser Unterlagen in den Akten halte ich unter Aspekten des Sozialdatenschutzes für bedenklich. Ich habe daher der Bundesanstalt für Arbeit empfohlen, die Verfahrensweise der Leistungsverwaltung in diesem Punkte, möglicherweise auch im Einvernehmen mit dem Bundesrechnungshof zu ändern.

14.3 Ärztlicher und Psychologischer Dienst

14.3.1

Im Bereich des *Ärztlichen Dienstes* der Bundesanstalt für Arbeit konnte ich nach eingehenden Gesprächen einige wesentliche Verbesserungen des Sozialdatenschutzes erreichen.

— Zur Frage der Verwertung von *Vorgutachten* hat sich die Bundesanstalt für Arbeit nunmehr insoweit festgelegt, als vorhandene Vorgutachten, die älter als ein halbes Jahr sind, grundsätzlich nicht mehr Grundlage für ein Gutachten nach Aktenlage sein dürfen. So wird in dem internen „Informationsblatt für Ärzte" ausgeführt: „Im allgemeinen wird man sich aus Gründen der ärztlichen Gewissenhaftigkeit zu einer Begutachtung mit Untersuchung und Erhebung neuer Befunde entschließen, wenn das Vorgutachten älter als ein halbes Jahr ist." Diese Regelung soll bei nächster Gelegenheit in einen neu zu fassenden Runderlaß aufgenommen werden. Dabei werde ich allerdings auf eine Präzisierung hinwirken.

— Auch meine Forderung, in Zukunft in den Fällen, in denen Arbeits- oder Ratsuchende anläßlich einer Untersuchung einer *Familieanamnese* unterzogen werden, darauf hinzuweisen, daß die Angaben zu Familienangehörigen freiwillig sind und nicht der Mitwirkungspflicht der §§ 60 ff. Sozialgesetzbuch I unterliegen, ist aufgegriffen worden. In die allgemeinen Weisungen der Arbeitsamtsärzte, die sog. „Gutachterfibel", wird ein entsprechender Hinweis aufgenommen werden.

— Von Arbeitssuchenden selbst eingereichte Atteste und Gutachten, die über eine Attestierung der bloßen Verwendungsfähigkeit hinausgehen, werden in Zukunft beim Ärztlichen Dienst und nicht in der Datei der Arbeitsvermittlung verwahrt.

— Es ist nunmehr allgemeine Praxis der Arbeitsverwaltung, daß der Ärztliche Dienst des jeweiligen Arbeitsamtes für den Fall der Beiziehung von Gutachten die Einwilligung des Betroffenen einholt. Diese soll neben der Befreiung des behandelnden Arztes von der ärztlichen Schweigepflicht auch das Einverständnis mit der Übersendung medizinischer Befundunterlagen durch einen Rententräger, ein Versorgungsamt oder den Vertrauensärztlichen Dienst etc. einschließlich der Angabe des Zweckes der Datenverwendung enthalten. Entsprechendes gilt für die Weiterleitung durch den Arbeitsamtsärztlichen Dienst. In den „Informationen des Ärztlichen Dienstes" ist dieses Verfahren beschrieben; insbesondere wird darauf hingewiesen, daß pauschale Erklärungen rechtsunwirksam sind.

14.3.2

Ich habe festgestellt, daß Gutachten *Psychologischer Dienste* der Arbeitsverwaltung teilweise offen

in der Vermittlungsdatei enthalten sind. Da die psychologischen Gutachten im Gegensatz zu den ärztlichen Gutachten, die auf das für die Arbeitsvermittlung ausschließlich notwendige Maß reduziert sind, meist einen umfassenden und den Intimbereich der Betroffenen stark berührenden Inhalt haben, habe ich vorgeschlagen, diese Gutachten in Zukunft in der Vermittlungsdatei in verschlossenen Umschlägen aufzubewahren, deren Öffnung zu protokollieren ist. Die Bundesanstalt für Arbeit ist meinem Vorschlag in diesem Punkte zu meinem Bedauern nicht gefolgt. Nachdem der Bundesminister der Verteidigung in einem durchaus vergleichbaren Zusammenhang eine solche Lösung akzeptiert und umgesetzt hat (vgl. 9. TB S. 65f.), werde ich mein Anliegen bei der Bundesanstalt weiterverfolgen.

Allerdings hat die Bundesanstalt meine Empfehlung im Neunten Tätigkeitsbericht (S. 50) aufgegriffen und veranlaßt, daß Teamberatungsprotokolle in Zukunft keine gutachterlichen Äußerungen von Psychologen mehr enthalten werden.

14.4 Rehabilitationsverfahren

Im Rehabilitationsverfahren der Bundesanstalt für Arbeit werden die wesentlichen Daten eines Betroffenen in zwei Berichten zusammengefaßt. Zum einen handelt es sich um den sog. Eingliederungsvorschlag, der aufgrund von ärztlichen Zeugnissen über die Verwendungsfähigkeit sowie auf der Grundlage einer Zusammenstellung der Vorbildung eines Rehabilitanten vor Beginn der Maßnahme angefertigt wird. Zum anderen ist es ein Ergebnisbericht über die Rehabilitationsmaßnahme, der auch die Befundunterlagen, die während der Rehabilitation entstanden sind, einschließt.

— Der Eingliederungsvorschlag sowie die begründenden Unterlagen haben zwei Adressaten, den Maßnahmeträger und den Kostenträger. Eine weitere Streuung kann sich unter arbeitsmarktpolitischen Gesichtspunkten ergeben, wenn die Arbeitsvermittlung die voraussichtlichen Beschäftigungsmöglichkeiten in dem vorgeschlagenen Beruf begutachten muß.

  Die Rehabilitanten werden in allen Fällen auf die vorgesehene Versendung hingewiesen und ihre Einwilligung wird schriftlich eingeholt. Insgesamt gesehen habe ich daher gegen dieses Verfahren keine Bedenken.

— Nach Abschluß der Rehabilitationsmaßnahmen bei dem Maßnahmeträger erstellt dieser einen Ergebnisbericht, dem er die in der Maßnahme entstandenen Befundunterlagen beifügt. Ich habe festgestellt, daß die Befundunterlagen nur an den Ärztlichen bzw. Psychologischen Dienst des zuständigen Arbeitsamtes gesandt werden. Den Ergebnisbericht selbst erhält das Sachgebiet Rehabilitation des jeweiligen Arbeitsamtes. Der Kostenträger erhält nur im Falle seiner Vorleistung ein Exemplar des Ergebnisberichts nebst gutachterlicher Beurteilung der Verwendungsfähigkeit.

  Innerhalb des Arbeitsamtes werden Ergebnisbericht und Gutachten ausschließlich im Abschnitt Rehabilitation bearbeitet. Arbeitsvermitltung und Arbeitsberatung haben darauf keinen Zugriff. Die Übermittlungen bewegen sich nach meinen Feststellungen hier in dem notwendigen Rahmen, datenschutzrechtliche Bedenken bestehen nicht.

  Allerdings habe ich festgestellt, daß der Ergebnisbericht bei Maßnahmen der Berufsfindung und Arbeitserprobung teilweise sehr detaillierte Angaben – insbesondere zum medizinischen und psychologischen Bereich – enthält. Ich habe Zweifel, ob eine so umfassende Informationsweitergabe an Arbeitsämter und andere Leistungsträger tatsächlich für eine sachgerechte Aufgabenwahrnehmung notwendig ist. Ich habe daher angeregt, den Maßnahmeträgern aufzugeben, die Ergebnisberichte im Hinblick auf den Sozialdatenschutz zu straffen. Daraufhin hat sich die Bundesanstalt für Arbeit an die Arbeitsgemeinschaft Deutscher Berufsförderungswerke gewandt und darauf hingewirkt, daß die Form der Ergebnisaufbereitung meinen Forderungen angepaßt wird. Im Bereich der Bundesarbeitsgemeinschaft der Berufsbildungswerke sollen meine Forderungen im Rahmen eines Forschungsprojektes „Revision, Entwicklung und Erprobung von Ausgaben-, Beobachtungs- und Beurteilungssystemen für die Berufsfindung/Arbeitserprobung in Berufsbildungswerken" Berücksichtigung finden.

  Ich betrachte dies als einen ersten Schritt, den Umfang psychologischer und ärztlicher Daten eines Rehabilitanten bei der Weitergabe durch die Rehabilitationsträger zu begrenzen.

14.5 Sozialdatenschutz in Selbstverwaltungsgremien der Bundesanstalt für Arbeit

Durch Presseberichte wurde im Januar 1987 bekannt, daß in den damals laufenden Tarifverhandlungen für die Metallarbeitnehmer in Württemberg Detailangaben aus der örtlichen Arbeitslosenkartei von zwei Arbeitsämtern in die Diskussion gebracht worden waren, und zwar von einem Funktionär des Verbandes der Metallindustrie Süd-Württemberg-Hohenzollern (VMI), der zugleich Vorsitzender des Verwaltungsausschusses des einen Arbeitsamtes ist.

Die von mir vorgenommene Prüfung der Angelegenheit bei diesem Arbeitsamt hat folgendes ergeben:

Im Dezember 1986 hat auf Wunsch des erwähnten Funktionärs und Vorsitzenden des Verwaltungsausschusses dieses Arbeitsamtes ein Informationsgespräch mit drei Mitarbeitern des Arbeitsamtes über „Struktur der Arbeitslosigkeit bei Metallarbeitern und etwa bestehende Vermittlungshemmnisse" stattgefunden. Bei dem Gespräch hat der zuständige Arbeitsvermittler anhand der Karteikarten für jeden einzelnen Fall ein „Arbeitslosenprofil" vorgetragen, etwa nach folgendem Muster: „Ein dreißigjähriger

gelernter Mechaniker, arbeitslos seit einem Jahr, zuvor in verschiedenen Betrieben beschäftigt, zweimal wegen Alkoholgenusses während der Arbeitszeit entlassen, Verbüßung einer halbjährigen Haftstrafe, mehrere Vermittlungsversuche sind gescheitert, u. a. wegen einer Alkoholfahne beim Vorstellungsgespräch".

Bei dem anderen Arbeitsamt, dessen Verwaltungsausschuß der Funktionär nicht angehört, hat er entsprechende Informationen erhalten. Insoweit haben meine Mitarbeiter keine weitergehenden Feststellungen getroffen.

In einer Sitzung der Tarifverhandlungen hat der Funktionär diese Profile vorgetragen und dabei davon gesprochen, „ein Großteil der fünfundzwanzig Arbeitslosen seien Kriminelle, Alkoholiker und Psychopathen".

Für die datenschutzrechtliche Bewertung ist entscheidend, ob es sich bei den vom Arbeitsamt gegebenen Informationen über Arbeitslose um personenbezogene Daten im Sinne des § 35 SGB I handelt, d. h. ob die mitgeteilten Einzelangaben einer bestimmten Person zugeordnet werden können. Es unterliegt m. E. keinem Zweifel, daß die „Profile" jeweils eine bestimmte, unverwechselbare Person betreffen, deren Identität lediglich zunächst nicht bekannt ist. Um eine „bestimmte" Person handelt es sich auch dann, wenn diese z. B. durch eine Kombination von Informationen, die eine Kennzeichnung ergeben, identifiziert werden kann; diese Identifikationsinformationen sind dabei ebenfalls personenbezogene Informationen, die dem Sozialdatenschutz unterliegen. Auch eine namentliche Identifizierung ist auf der Grundlage der bekanntgegebenen Identifikationsinformationen in den fraglichen Einzelfällen nicht auszuschließen, zumal der in Betracht kommende Personenkreis relativ klein ist. Von Bedeutung ist in diesem Zusammenhang, daß unter den jeweils ausdrücklich oder implizit genannten Daten solche sind, die eine eindeutige und enge Eingrenzung von vornherein erlauben, wie z. B. die Zugehörigkeit zu einem ganz bestimmten Metallverarbeitungsberuf. Mit Hilfe weniger weiterer Informationen lassen sich die einzelnen Betroffenen identifizieren. Es ist nach der Lebenserfahrung jedenfalls nicht auszuschließen, daß ein Interessent von dieser Möglichkeit Gebrauch machen wird. Insbesondere unter ehemaligen Arbeitskollegen und Nachbarn, ebenso aber auch bei potentiellen künftigen Arbeitgebern dürfte ein relativ hohes Interesse daran bestehen festzustellen, welcher arbeitslose Mechaniker Alkoholiker, Psychopath oder Vorbestrafter ist. Der Aufwand, mit dem das für eine Identifizierung erforderliche Zusatzwissen beschafft werden könnte, ist im Falle der drei genannten Interessengruppen möglicherweise unterschiedlich, aber relativ gering.

Die vom Arbeitsamt vorgetragenen „Profile" unterliegen deshalb als personenbezogene Sozialdaten dem Schutz nach § 35 SGB I.

Adressat des Geheimhaltungsanspruchs und des Offenbarungsverbots gemäß § 35 SGB I sind die Leistungsträger, soweit sie Aufgaben nach dem Sozialgesetzbuch einschließlich seiner besonderen Teile wahrnehmen. Für die Aufgaben nach dem Arbeitsförderungsgesetz ist Leistungsträger die Bundesanstalt für Arbeit in ihrer Gesamtheit. Zu dieser Gesamtheit gehören die Verwaltung und die Selbstverwaltungsorgane. Innerhalb des Leistungsträgers findet begrifflich eine Offenbarung nicht statt. Auch bei einer internen Weitergabe von Sozialdaten ist jedoch die allgemeine funktionale Einschränkung zu beachten, d. h. Sozialdaten dürfen nur weitergegeben werden, wenn dies im Rahmen des Aufgabenbereichs des Empfängers liegt (vgl. auch das Verbot der unbefugten Weitergabe von Daten, § 5 BDSG). Nach der Satzung der Bundesanstalt haben die Verwaltungsausschüsse die Aufgabe, die Situation der Arbeitnehmergruppen, die schwer zu vermitteln sind, mit der Verwaltung zu erörtern. Die für die Beratungen erforderlichen schriftlichen Unterlagen stellt die Verwaltung zur Verfügung. Die Leiter der Dienststellen haben zu gewährleisten, daß die Mitglieder der Organe auch außerhalb von Organsitzungen die zur Erfüllung ihrer Aufgaben erforderlichen Auskünfte erhalten.

Wenn danach durch das Arbeitsamt weder eine Offenbarung noch eine unzulässige interne Weitergabe von Sozialdaten an den Vorsitzenden des Verwaltungsausschusses stattgefunden hat, so hat aber jedenfalls der Vorsitzende des Verwaltungsausschusses, der seinerseits dem Geheimhaltungsgebot des § 35 SGB I unterliegt, gegen die Verpflichtung zur Wahrung des Sozialgeheimnisses und gegen das Verbot der unbefugten Offenbarung von Sozialdaten verstoßen, indem er die „Profile" an die Teilnehmer der Tarifverhandlungen bekanntgegeben hat.

Ebenso hat das andere Arbeitsamt gegen das Offenbarungsverbot des § 35 SGB I verstoßen, als es dem erwähnten Funktionär des VMI entsprechende Informationen gab, da eine der in § 67 SGB X genannten Voraussetzungen nicht vorgelegen hat.

Ich habe diese Verstöße gemäß § 20 Abs. 1 BDSG gegenüber dem Vorstand der Bundesanstalt beanstandet und gemäß § 20 Abs. 3 BDSG empfohlen, die Mitglieder der Selbstverwaltungsorgane – künftig bereits bei ihrer Bestellung – ausdrücklich auf ihre Geheimhaltungspflicht gemäß § 35 SGB und gegebenenfalls gemäß § 78 SGB X hinzuweisen.

Der Vorstand der Bundesanstalt hat der Beanstandung widersprochen, weil es sich nach seiner Auffassung bei den „Profilen" nicht um personenbezogene Daten – Einzelangaben über die persönlichen und sachlichen Verhältnisse einer bestimmten oder bestimmbaren Person – handelt.

Unabhängig davon hat der Vorstand der Bundesanstalt für Arbeit mir inzwischen mitgeteilt, daß die „Hinweise des Vorstands der Bundesanstalt für Arbeit zu den Aufgaben der Verwaltungsausschüsse bei den Landesarbeitsämtern und Arbeitsämtern" bezüglich der Aussagen über die Einhaltung des Sozialgeheimnisses und der Amtsverschwiegenheit überarbeitet bzw. Begriffe und Verpflichtungen noch näher erläutert werden.

14.6 Bundeskindergeldgesetz

Die Durchführung des automatisierten Datenabgleichs mit den Finanzbehörden für die Kindergeldberechnung, wie ich sie in meinem Siebenten Tätigkeitsbericht (S. 43) dargestellt habe, hat im Berichtszeitraum erneut zu Beschwerden betroffener Bürger geführt. Auf meine Initiative hin war im Jahre 1985 der Erfassungsbogen des Kindergeldantrags um ein Datenfeld ergänzt worden, in dem nach der Zustimmung zur Einbeziehung in den Datenabgleich gefragt wird (vgl. 8. TB S. 30). Da der Datenabgleich nach meiner Auffassung jedoch weit überwiegend in Fällen stattfindet, in denen die dafür erforderlichen Daten bereits vor Ergänzung des Erfassungsbogens erfaßt und gespeichert worden sind, habe ich die Bundesanstalt für Arbeit um Auskunft gebeten, ob die gespeicherten Altfälle im Hinblick auf die erforderliche Zustimmung überprüft worden sind. Mir wurde daraufhin mitgeteilt, daß nach Feststellungen der Landesarbeitsämter in dreizehn Arbeitsämtern Fehler in größerem Umfange vorgekommen sind. Für diese Arbeitsämter wurde eine Überprüfung aller in Betracht kommenden Fälle angeordnet; es handelte sich um rd. 21.000 Fälle. Zur stichprobenweisen Überprüfung wurden weitere 31.000 Fälle ausgewählt. Nach dem Ergebnis dieser Überprüfung, die unter Aufsicht der Landesarbeitsämter stattfand, wurden noch bei fünf weiteren Arbeitsämtern Bearbeitungsfehler vermutet; auch für diese fünf Arbeitsämter wurden totale Überprüfungen angeordnet, die rd. 7.000 Fälle umfaßten. Demnach wurden nachträglich noch rd. 60.000 Altfälle auf Mängel in der Sachbearbeitung überprüft.

Ich gehe nunmehr davon aus, daß das Verfahren des automatisierten Datenabgleichs, das den betroffenen Bürgern die jährliche Vorlage von Fragebögen und Einkommensnachweisen erspart, in Zukunft keine generellen Probleme mehr aufwerfen wird.

15. Krankenversicherung

15.1 Kontrolle bei der Hanseatischen Ersatzkasse

Bei der Hanseatischen Ersatzkasse (HEK) habe ich erstmals eine sog. Querschnittsprüfung unter datenschutzrechtlichen Gesichtspunkten durchgeführt. Schwerpunkte waren dabei die Organisation des Datenschutzes in der Kasse und die Kontrolle der Einhaltung der Datenschutzvorschriften sowie die zur Gewährleistung des Datenschutzes getroffenen Maßnahmen in einigen ausgewählten Bereichen.

Bemerkenswert war, daß die Bestellung des internen Datenschutzbeauftragten auf Vorschlag des Hauptpersonalrats erfolgte.

Meine Feststellungen gaben keinen Anlaß für eine Beanstandung. Gleichwohl zeigte sich, daß in einigen Bereichen der Schutz personenbezogener Daten der Versicherten und der Mitarbeiter der Kasse noch zu verbessern war. Dies betraf insbesondere die Aufgabenzuweisung und die Stellung des internen Datenschutzbeauftragten, die Transparenz der Datenverarbeitung, einige Datensicherungsmaßnahmen (Anlage zu § 6 Abs. 1 BDSG) bei der automatisierten Datenverarbeitung, die Datenverarbeitung im Auftrag der Kasse durch externe Stellen sowie die Organisation der Datenverarbeitung für die Mitarbeiter der Kasse (Personalaktenführung, Beihilfeverfahren, Mitarbeiter-Leistungsverwaltung). Nachdem schon die Kontrolle selbst aufgrund der Aufgeschlossenheit der Leitung und der Mitarbeiter der Kasse sehr positiv verlief, ist die Kasse auch auf meine Vorschläge und Anregungen zur Verbesserung des Datenschutzes bereitwillig eingegangen. Alle aufgetretenen Fragen konnten inzwischen zufriedenstellend gelöst werden.

Hervorzuheben ist in diesem Zusammenhang die auch hier festgestellte Praxis, daß die Kasse von Kur-, Reha- und anderen Kliniken umfangreiche und ausführliche Entlassungsberichte mit Informationen über Anamnese, Verwandtenanamnese, Beschwerden, Aufnahmebefunde, Laborbefunde, Diagnosen einschließlich Erläuterungen und über die Behandlung und den Verlauf des Heilverfahrens erhält. In den Gesprächen mit der Kasse und ihrem beratenden Arzt konnte geklärt werden, daß die Entlassungsberichte in dieser ausführlichen Form, wenn überhaupt, dann nur vom beratenden Arzt von Fall zu Fall benötigt werden, um beurteilen zu können, ob die ärztliche Behandlung sinnvoll war und die Kur- bzw. Krankenanstalt auch für weitere Behandlungsfälle geeignet erscheint. Für die sonstige gesetzliche Aufgabenerfüllung benötigt die Kasse nur die Diagnoseangaben. Die vollständigen Entlassungsberichte werden in den jeweiligen Geschäftsstellen fünf Jahre lang aufbewahrt.

Dies erscheint unter datenschutzrechtlichen Gesichtspunkten problematisch, da die vollständigen Berichte für die Aufgabenerfüllung der Kasse nicht bzw. nicht mehr erforderlich sind. Angesichts der hohen Sensibilität dieser Daten, die teilweise in den Kernbereich der Persönlichkeit des Mitglieds und seiner Angehörigen fallen, hat die Kasse zugesagt, aus umfangreichen Entlassungsberichten künftig nur noch die wesentlichen Daten auf einen Vordruck zu übertragen. Dieser Vordruck enthält außer dem Namen des Versicherten nur noch Angaben über den Maßnahmeträger, die Kosten und die antragsauslösenden Diagnosen. Die Berichte sollen dann entweder an den Hausarzt weitergeleitet oder – falls er bereits einen Bericht erhalten hat – vernichtet werden. Unter Hinweis auf meine ausführlichen Darlegungen zum Problem der ärztlichen Entlassungsberichte in meinem Achten Tätigkeitsbericht (S. 32f.) habe ich die Kasse darauf hingewiesen, daß die Übersendung des Entlassungsberichts an den behandelnden Hausarzt stets das Einverständnis des Patienten im Einzelfall erfordert und dabei insbesondere zu beachten ist, daß eine rechtswirksame Einwilligung die Kenntnis dessen voraussetzt, was offenbart werden soll. Eine etwa bei Kurantritt regelmäßig abverlangte Einwilligung ohne Kenntnis vom Inhalt des Entlassungsberichts kann dem nicht genügen. Die Kasse will diesen Empfehlungen folgen.

15.2 Mitgliederwerbung durch die Krankenkassen

Über datenschutzrechtliche Aspekte und Probleme im Zusammenhang mit Werbemaßnahmen von Krankenkassen habe ich in meinem Neunten Tätigkeitsbericht (S. 54) berichtet. In einem Teilbereich konnte inzwischen Einvernehmen mit dem Bundesminister für Arbeit und Sozialordnung, dem Bundesversicherungsamt und den Aufsichtsbehörden der Länder erzielt werden:

Der Arbeitgeber darf nach geltendem Recht Anschriftenlisten von Arbeitnehmern an RVO- und Ersatzkassen zu deren Werbezwecken nicht ohne Einwilligung des Arbeitnehmers überlassen. Das folgt aus seiner Pflicht zur Verschwiegenheit und gilt auch für künftig Einzustellende. Soweit die Kenntnisse eines Arbeitnehmers über andere Arbeitnehmer auf Umständen beruhen, die eine Verschwiegenheitspflicht des Arbeitnehmers auslösen (z. B. Personalsachbearbeitung oder Tätigkeit bei der Datenverarbeitung), darf er gleichfalls Adreßdaten anderer Arbeitnehmer nicht der Krankenkasse zu Werbezwecken mitteilen. Die Krankenkasse darf Adreßmaterial für Aufklärung und Werbung nicht verwenden, wenn die Möglichkeit besteht, daß es unter Verstoß gegen Datenschutzbestimmungen erlangt oder an sie weitergegeben wurde. Ist der Übersender einer Adresse ein Arbeitgeber oder ein zur Verschwiegenheit über Personaldaten Verpflichteter, hat sie deshalb vor einer Werbung stets die Erklärung des Übersenders einzuholen, daß der Betroffene schriftlich in die Verwendung seiner Daten zu Werbezwecken der Krankenkasse eingewilligt hat. Die Einhaltung dieser Grundsätze soll im Wege der Rechtsaufsicht einheitlich gegenüber den gesetzlichen Krankenkassen und den Ersatzkassen durchgesetzt werden.

Eine Ersatzkasse, der ich diese Grundsätze aus gegebenem Anlaß mitteilte, hat mir daraufhin erwidert, die Ersatzkassen könnten diese Auffassung nicht teilen, da sonst ihre existentiellen Interessen beeinträchtigt würden. Sie habe daher einen Rechtswissenschaftler gebeten, die Problematik im Rahmen einer wissenschaftlichen Arbeit zu bewerten. Erst nach Eingang dieses Gutachtens werde sie ihre Entscheidung treffen.

15.3 Einzelfälle

Einer Mitarbeiterin wurde von ihrem Arbeitgeber wegen längerer und wiederholter Krankheit gekündigt. Die Krankenkasse hatte dem Arbeitgeber die Auskunft gegeben, daß ein Ende der Arbeitsunfähigkeit der Betroffenen nicht abzusehen sei.

Die Feststellungen in diesem Fall haben ergeben, daß die betreffende *Betriebskrankenkasse* dem Arbeitgeber folgendes mitgeteilt hatte:

„Wir nehmen Bezug auf Ihre Anfrage und bestätigen, daß die ab 28. Mai 1986 bestehende Arbeitsunfähigkeit der Vorgenannten noch andauert. Eine sozialmedizinische Begutachtung hat zuletzt am 4. Juli 1986 stattgefunden. Danach war Frau V. als Serviererin zunächst noch arbeitsunfähig. Die weitere Abheilung sollte abgewartet werden. Wir bestätigen, insbesondere auch aufgrund der Vorerkrankung, daß mit der Arbeitsaufnahme von Frau V. vorerst nicht zu rechnen ist."

Die Krankenkasse vertrat die Auffassung, mit dieser Auskunft nicht gegen Vorschriften des Datenschutzes verstoßen zu haben. Frau V. habe bereits selbst gegenüber ihrem Arbeitgeber erklärt, daß sie noch längere Zeit arbeitsunfähig sein würde; die Krankenkasse habe dies lediglich bestätigt. Welche personellen Konsequenzen die Firma anschließend treffen würde, hätte die Kasse nicht voraussehen können und dies entziehe sich auch ihrer Einflußnahme. Arbeitnehmer seien aus gutem Grunde verpflichtet, Arbeitgeber über ihre Nichteinsatzfähigkeit selbst in Kenntnis zu setzen. Die entsprechende Nachweispflicht diene nicht allein dazu, die Ansprüche auf Lohnfortzahlung prüfen und erfüllen zu können, sondern auch und insbesondere, die Dispositionsfähigkeit des Arbeitgebers für die Besetzung des Arbeitsplatzes zu erhalten. Die Dauer der voraussichtlichen krankheitsbedingten Arbeitsverhinderung könne demnach kein schützenswerter Tatbestand sein.

Demgegenüber ist aus datenschutzrechtlicher Sicht festzustellen:

Der Anspruch des Betroffenen auf Wahrung des Sozialgeheimnisses erstreckt sich auf alle Einzelangaben über die persönlichen und sachlichen Verhältnisse (§ 35 Abs. 1 SGB I). Für eine Differenzierung nach mehr oder weniger schützenswerten Tatbeständen besteht kein Ermessensspielraum. Eine Offenbarung ist nur unter den Voraussetzungen der §§ 67 bis 77 SGB X zulässig (§ 35 Abs. 2 SGB I).

Eine Einwilligung der Betroffenen gemäß § 67 SGB X in die Offenbarung von Einzelangaben über ihre persönlichen und sachlichen Verhältnisse an ihren Arbeitgeber lag nicht vor. Nach der hier als gesetzliche Offenbarungsbefugnis allein in Betracht kommenden Vorschrift des § 69 Abs. 1 Nr. 1 SGB X ist eine Offenbarung nur zulässig, soweit sie für die Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch durch die Betriebskrankenkasse erforderlich ist. Diese Voraussetzung war nicht gegeben. Es ist keine gesetzliche Aufgabe der Krankenkasse ersichtlich, die es erforderlich macht, den Arbeitgeber darüber zu informieren, daß eine bestehende Arbeitsunfähigkeit noch andauert, daß nach der stattgefundenen sozialmedizinischen Begutachtung die weitere Abheilung abgewartet werden sollte und daß aufgrund der Vorerkrankungen mit einer Arbeitsaufnahme vorerst nicht zu rechnen sei. Im übrigen besteht ungeachtet der fehlenden Informationspflicht bzw. Offenbarungsbefugnis der Krankenkasse aus der Sicht des Arbeitgebers auch keine Notwendigkeit für eine derartige Information, denn die für den Arbeitgeber allein relevante voraussichtliche Dauer der Arbeitsunfähigkeit ergibt sich aus der entsprechenden Bescheinigung des behandelnden Arztes.

Das Schreiben der Betriebskrankenkasse an die Firma stellt danach eine unbefugte Offenbarung perso-

nenbezogener Daten dar und verstößt somit gegen § 35 Abs. 2 SGB I. Diesen Verstoß habe ich gemäß § 20 Abs. 1 BDSG beanstandet.

— Ein Arzt hat sich geweigert, einer Patientin für die zuständige Betriebskrankenkasse die verlangte „ärztliche Bescheingiung zur Erlangung von Krankengeld" mit Angabe der Diagnose auszustellen. Da diese Bescheinigung im Personalbüro abgegeben werden mußte, war er der Auffassung, daß er damit der ärztlichen Schweigepflicht unterliegende Angaben dem Arbeitgeber seiner Patientin unbefugt offenbaren und sich möglicherweise strafbar machen würde.

  Die Nachprüfung hat ergeben, daß die BKK bei einzelnen Zweigniederlassungen des Unternehmens sogenannte Zahlstellen eingerichtet hatte, in denen Mitarbeiter beschäftigt sind, die die Zahlstellentätigkeit neben Aufgaben des Personalbereichs der Trägerfirma wahrnehmen.

  Die Einrichtung solcher Mischarbeitsplätze ist grundsätzlich unvereinbar mit den Vorschriften über die Wahrung des Sozialgeheimnisses und den Schutz der Sozialdaten gemäß § 35 SGB I. Das Bundesversicherungsamt hatte bereits anläßlich einer Aufsichtsprüfung im Mai 1982 insoweit einen datenschutzrechtlichen Organisationsmangel festgestellt und die BKK aufgefordert, die Zahlstellen-Mitarbeiter künftig ausschließlich mit der Erledigung von BKK-Aufgaben zu befassen. Die notwendige Organisationsänderung war jedoch bis zum Zeitpunkt meiner Intervention noch nicht durchgeführt. Es bedurfte noch mehrfachen Schriftwechsels – unter Einschaltung des Bundesversicherungsamtes – bis mir die BKK am 15. September 1987 mitteilte, daß die Zahlstellen in den Zweigniederlassungen des Unternehmens geschlossen worden sind.

— Ein Versicherter einer gesetzlichen Krankenkasse hatte sich 1984 bei mir über eine Verletzung des Sozialgeheimnisses durch eine Kasse beklagt.

  Der Versicherte war infolge einer tätlichen Auseinandersetzung arbeitsunfähig krank und es war zu klären, ob der auf die Krankenkasse übergegangene Entgeltfortzahlungsanspruch beim Arbeitgeber des Versicherten geltend gemacht werden konnte. In diesem Zusammenhang hatte die Kasse dem Arbeitgeber eine Kopie des Gerichtsurteils, das wegen der tätlichen Auseinandersetzung ergangen war, übersandt.

  Um diese Übersendung zu rechtfertigen, legte mir die Kasse mit einer Stellungnahme eine Kopie des Urteils vor, in der die Diagnosen unkenntlich gemacht worden waren. Ich war daraufhin zu dem Ergebnis gekommen, die Offenbarung der Sozialdaten (Übersendung des Urteils ohne Diagnosen) an den Arbeitgeber sei von Art und Umfang her im Rahmen des § 69 SGB X zulässig. Im Berichtsjahr wandte sich der Versicherte erneut an mich. Bei einer Personalakteneinsicht im Januar 1987 hatte er festgestellt, daß in der dort vorhandenen Urteilskopie die Diagnosen *nicht* unkenntlich gemacht waren. Die Kasse räumte jetzt ein, daß sie eine Ausfertigung des Urteils mit Diagnosen an den Arbeitgeber übersandt hatte. Diese Offenbarung war nicht erforderlich; sie stellt eine Verletzung des Sozialgeheimnisses dar, die ich gemäß § 20 Abs. 1 BDSG beanstandet habe.

  Dieser Verstoß wiegt umso schwerer, als die Kasse mir gegenüber zunächst den Eindruck erweckt hatte, Diagnosen seien nicht offenbart worden, obwohl das Gegenteil der Fall war.

15.4 Betriebskrankenkasse

In meinem Neunten Tätigkeitsbericht (S. 52) habe ich über allgemeine Datenschutzprobleme berichtet, die sich u. a. aus der personellen Verpflechtung der Organe von Betriebskrankenkasse und Unternehmensleitung ergeben. Der Bundesverband der Betriebskrankenkassen (BdB) hat diese Bemerkungen aufgegriffen und zum Anlaß genommen, die Problematik mit mir zu erörtern. In mehreren offenen und konstruktiven Gesprächen wurden gemeinsame Lösungsmöglichkeiten gesucht und diskutiert. Die Gespräche werden fortgesetzt.

Inzwischen hat der Bundestags-Ausschuß für Arbeit und Sozialordnung diese Fragen bei der Beratung meines Neunten Tätigkeitsberichts ebenfalls aufgegriffen und erklärt, „daß bei allen Sozialversicherungsträgern im Rahmen einer Tätigkeit in den Selbstverwaltungsorganen und besonderen Ausschüssen weder dem Arbeitgeber selbst noch einem anderen Vorgesetzten noch einem Angehörigen der Personalverwaltung Kenntnis von personenbezogenen Daten eines Betriebsangehörigen offenbart werden dürfen, die dem Sozialgeheimnis unterliegen. Die Bundesregierung wird daher um Prüfung gebeten, wie sichergestellt werden kann, daß diese Personen bei der Einsichtnahme in Daten von Betriebsangehörigen, die dem Sozialgeheimnis unterliegen, und bei deren Erörterung nicht mitwirken und durch andere Personen vertreten werden. Darüber hinaus sollte sichergestellt werden, daß der Arbeitgeber nicht Personen zur Führung der Geschäfte der Betriebskrankenkasse bestellt, die befugt sind, gleichzeitig Aufgaben im Personalbereich des Betriebes oder Dienstbetriebes wahrzunehmen".

Ich gehe davon aus, daß dieser Beschluß zu (gesetzlichen) Maßnahmen führen wird, die eine dauerhafte Lösung der Datenschutzprobleme in diesem Bereich ermöglichen.

16. Unfallversicherung

16.1 Datenschutzkontrolle bei der Berufsgenossenschaft der Keramischen und Glas-Industrie

Im Berichtsjahr habe ich eine Kontrolle bei einer Berufsgenossenschaft (BG) und bei einer BG-eigenen Klinik für Berufskrankheiten durchgeführt. Schwer-

punkte waren die Erhebung, Verarbeitung und sonstige Verwendung medizinischer Daten.

Die allgemeine Organisation und Durchführung des Datenschutzes gaben keinen Anlaß für eine förmliche Beanstandung. Einige Anregungen zur Verbesserung des Datenschutzes bei der Datenerhebung, bei den Formalitäten der Patientenaufnahme sowie zur Konkretisierung der „Dienstweisung Datenschutz" wurden von der BG aufgegriffen und werden schrittweise in die Praxis umgesetzt. Drei Feststellungen sind m. E. von allgemeinem Interesse:

— Der interne Datenschutzbeauftragte der BG ist zugleich Geschäftsführer einer ihrer Bezirksverwaltungen. Diese Doppelfunktion kann m. E. zu Konflikten und Interessenkollisionen führen. Der Geschäftsführer einer Bezirksverwaltung ist z. B. naturgemäß primär daran interessiert, daß seine Mitarbeiter die Informationen bekommen, verarbeiten und weitergeben können, die eine optimale und möglichst reibungslose Erfüllung ihrer Aufgaben ermöglichen. In seiner Funktion als Datenschutzbeauftragter muß er dagegen, will er dieser Funktion gerecht werden, mit aller Entschiedenheit auf die strikte Einhaltung der gesetzlich definierten Verarbeitungsgrenzen bestehen. Die BG hat demgegenüber darauf hingewiesen, daß nach ihrer Auffassung mit der Besetzung der Funktion des Datenschutzbeauftragten durch den Geschäftsführer einer Bezirksverwaltung den Datenschutzinteressen gerade ein besonders hoher Rang eingeräumt werde. Der Geschäftsführer einer Bezirksverwaltung sei nämlich in der Amtshierarchie der BG im oberen Bereich angesiedelt, was ihm auch entsprechende Durchsetzungsbefugnisse einräume, die anderen Bediensteten keineswegs in diesem Umfang zustünden.

  Konkrete Erfahrungen aus meiner Kontrolltätigkeit liegen mir insofern nicht vor. Ich halte es daher für erforderlich, die Auswirkungen dieser Doppelfunktion über einen gewissen Zeitraum zu beobachten.

— Der Chefarzt der Klinik für Berufskrankheiten wird im Rahmen genehmigter Nebentätigkeit als freiberuflicher Gutachter bei der Beurteilung und Anerkennung von Berufskrankheiten tätig. Die sogenannten Gutachtenpatienten werden in der Regel für zwei Tage in die Klinik aufgenommen. Pflegekosten und Nebenkosten, mit Ausnahme des Gutachterhonorars, werden von der Klinik dem Auftraggeber direkt in Rechnung gestellt. Die Verwaltungsunterlagen über die Gutachtenpatienten unterliegen daher notwendigerweise und zweifelsfrei der Obhut und Verantwortung sowie dem Zugriff der Klinikverwaltung. Die Unterlagen, die unmittelbar mit der Erstellung des Gutachtens zusammenhängen (Entwürfe, Durchschriften, Befunde, Laborergebnisse) unterliegen dagegen ebenso zweifelsfrei ausschließlich der Verantwortung und dem Zugriff des Gutachters. Aufgrund der ärztlichen Schweigepflicht ist eine Offenbarung dieser Unterlagen nur gegenüber dem Auftraggeber im Rahmen des Gutachtenauftrages zulässig. Ansonsten sind die Gutachtenunterlagen m. E. Eigentum des Gutachters, d. h. sie sind wie Unterlagen und Aufzeichnungen eines niedergelassenen Arztes zu behandeln. Dies bedeutet, daß der Arzt dafür Sorge tragen muß, daß diese Unterlagen nach Beendigung der Nebentätigkeit bzw. nach seinem Ausscheiden aus dem Dienst der Berufsgenossenschaft „in gehörige Obhut" gegeben werden (§ 11 Abs. 4 der Ärztlichen Berufsordnung). Ebenso wie der niedergelassene Arzt bei Praxisaufgabe darf der Chefarzt seine Unterlagen aus freiberuflicher Nebentätigkeit bei seinem Ausscheiden nicht ohne weiteres seinem Nachfolger oder der Klinik überlassen.

  Nach Auffassung der BG ist der Sachverhalt nur bedingt vergleichbar. Während beim niedergelassenen Arzt, der seine Praxis aufgibt, ein echter „Unternehmerwechsel" stattfinde und beim Ausscheiden eines beamteten Arztes dessen Unterlagen aus freiberuflicher Nebentätigkeit vom Dienstherrn zur eigenen Aufgabenerfüllung nicht benötigt würden, sei die BG im präventiven Bereich wie im Heilverfahren auf dem besonderen Gebiet des Berufskrankheitenrechts gerade zur Berücksichtigung der vorliegenden Gutachten verpflichtet.

  Ich habe mich dieser Argumentation in diesem speziellen Fall im Ergebnis angeschlossen, insbesondere im Hinblick darauf, daß die fachliche Seite der Gutachtentätigkeit nahezu in allen Fällen identisch ist mit der Behandlung durch die Klinik, und daß die Gutachtertätigkeit zwar auf eigene Rechnung, aber im Grunde genommen vom *jeweiligen* Chefarzt im Auftrag der Klinik ausgeübt wird.

— Ebenso wie bei Gutachtenpatienten werden auch die ärztlichen Unterlagen und die Verwaltungsunterlagen der Behandlungspatienten zusammen in einer Akte geführt und aufbewahrt. Dies widerspricht grundsätzlich dem allgemeinen Trennungsgebot zwischen ärztlichem Bereich und Verwaltungsbereich in einer Klinik.

  Die ärztliche Schweigepflicht gilt auch gegenüber der Krankenhausverwaltung. Der ärztlichen Schweigepflicht unterliegt der gesamte ärztliche Schriftwechsel, den Krankenhausärzte führen. Dieser Schriftwechsel darf von der Verwaltung nicht eingesehen werden. Der Patient will aufgrund der besonderen Vertrauensbeziehung zum Arzt über seine Erkrankung nur ihm, nicht aber der Institution Krankenhaus Mitteilung machen. Deshalb ist z. B. eine Postverteilung im Krankenhaus, die auf diese besondere Vertrauensbeziehung zwischen Arzt und Patient keine Rücksicht nimmt, sondern der Verwaltung den gesamten – auch ärztlichen – Schriftwechsel zur Einsichtnahme zuleitet, unzulässig. Diese Grundsätze lassen sich allerdings in kleineren Kliniken nicht strikt durchhalten. Wenn in diesen Fällen dem ärztlichen Bereich kein eigener Schreibdienst/Postdienst/Registraturdienst zur Verfügung stehen kann, muß zwangsläufig die Verwaltung diese

Dienste für den ärztlichen Bereich mit übernehmen. Insoweit ist das Verwaltungspersonal der ärztlichen Schweigepflicht unterworfen wie „berufsmäßig tätige Gehilfen" im Sinne § 203 Abs. 3 StGB, zu denen nach herrschender Meinung z. B. auch Sekretärinnen des Arztes gehören. Es ist aber sicherzustellen, daß diesem „Ärztlichen Hilfsdienst" ärztliche Geheimnisse nur in dem notwendigen Umfang zur Kenntnis gelangen. Deshalb dürfen z. B. die Verwaltungsangehörigen keinen uneingeschränkten Zugang zum Krankenarchiv haben.

16.2 Datenerhebung ohne Auskunftspflicht

In der gesetzlichen Unfallversicherung hat der Unternehmer den Gegenstand des Unternehmens anzuzeigen, ferner die Zahl der Versicherten, den Eröffnungstag oder den Tag der Aufnahme der vorbereitenden Arbeiten für das Unternehmen (§ 661 RVO) sowie den Wechsel einer Person, für deren Rechnung das Unternehmen geführt wird (§ 665 RVO) und Unternehmensänderungen, die für die Zugehörigkeit zu einer Berufsgenossenschaft wichtig sind (§ 666 RVO); insoweit besteht eine gesetzliche Auskunftspflicht des Unternehmers gegenüber dem Träger der gesetzlichen Unfallversicherung.

In vielen Fällen reichen jedoch diese Angaben zur Feststellung des zuständigen Versicherungsträgers und/oder der Beitragspflicht nicht aus. Insbesondere bei sogenannten Eigenbauunternehmern, das sind Bauherren, die Bautätigkeiten in eigener Regie ausführen und/oder bei der Ausführung öffentlich geförderter oder steuerbegünstigter Bauvorhaben im Rahmen der Selbsthilfe tätig werden, sind dafür weitere Angaben erforderlich. Insoweit besteht jedoch nach geltendem Recht weder eine Auskunfts- noch eine Mitwirkungspflicht des Unternehmers. Eine entsprechende Datenerhebung auf freiwilliger Grundlage reicht nicht aus, da solche Angaben für die Durchführung der Versicherung zweifellos notwendig sind. Ich halte es daher im Hinblick auf die vom Bundesverfassungsgericht entwickelten Grundsätze zur Gewährleistung des Rechts auf informationelle Selbstbestimmung für unvermeidlich, im Dritten Buch der RVO (Unfallversicherung) eine einerseits generelle, andererseits aber möglichst konkrete gesetzliche Vorschrift zu schaffen, die den Betroffenen zur Angabe aller für die Durchführung der Versicherung erforderlichen Angaben über seine persönlichen und sachlichen Verhältnisse und die der versicherten Personen verpflichtet.

17. Gesundheitswesen

17.1 Bundesgesundheitsamt (BGA)

Beim BGA wurde eine weitere Kontrolle durchgeführt (vgl. 7. TB S. 54/55), die Datenschutzfragen bei folgenden Vorhaben und Verfahren betraf:

- Erkennung und Bewertung von Vergiftungsfällen
- Pseudokrupp-Studie
- Hepatitis- und Influenza-Forschung
- AIDS-Erhebung (vgl. 17.2.1)
- Parasitologische und bakteriologische Forschung
- Deutsche Herz-Kreislauf-Präventions-Studie
- Meldeverfahren nach dem Bundesseuchengesetz
- Erfassung unerwünschter Arzneimittelnebenwirkungen.

Keine Probleme ergaben sich bei der Pseudokrupp- und der Herz-Kreislauf-Präventions-Studie. Die in den übrigen Bereichen aufgetretenen Fragen bedürfen teilweise noch weiterer Erörterungen. Überwiegend liegen die datenschutzrechtlichen Probleme weniger in der eigentlichen Datenverarbeitung im BGA, als vielmehr in der Beschaffung der Daten, insbesondere deren Übermittlung durch Dritte (Behörden und andere Stellen) an das BGA und der Zulässigkeit ihrer weiteren Verwendung.

Erst kurz vor Abschluß dieses Berichts habe ich eine umfangreiche Stellungnahme des BGA zu den aufgeworfenen Fragen erhalten. Ich werde darauf im nächsten Tätigkeitsbericht eingehen.

Darüber hinaus hatte ich mich erneut mit dem Problem der *Abschottung der Beihilfestelle* zu befassen.

In meinem Siebenten Tätigkeitsbericht (17.1, S. 55) habe ich darüber berichtet, daß im Bundesgesundheitsamt bei der Führung und Verwaltung der Beihilfeunterlagen eine unter datenschutzrechtlichen Aspekten beispielhafte Abschottung sensibler Mitarbeiterdaten praktiziert wird. Nach der dort zunächst getroffenen Regelung sollten nur die für die Bearbeitung von Beihilfen zuständigen Sachbearbeiter Zugriff zu den Beihilfeakten haben. Später wurde jedoch auch für die Vorgesetzten der Beihilfesachbearbeiter ein Zugriffsrecht geschaffen, um die notwendige Fachaufsicht zu gewährleisten. Gegen diese Regelung habe ich Bedenken erhoben, weil die betroffenen Vorgesetzten der Beihilfesachbearbeiter zugleich Leitungsfunktionen im Personalbereich wahrnehmen.

Im Zuge einer Organisationsprüfung der Zentralabteilung des Bundesgesundheitsamtes durch den Bundesrechnungshof wurden die Möglichkeiten einer konsequenten datenschutzgerechten Trennung der Fach- und Dienstaufsicht in Beihilfeangelegenheiten, die gleichzeitig den haushaltsrechtlichen Erfordernissen gerecht werden sollte, mit den betroffenen Behörden unter meiner Beteiligung erörtert. Das Bundesgesundheitsamt hat mir inzwischen mitgeteilt, daß nach der mit Wirkung vom 1. Januar 1988 vorgesehene Neuorganisation der Zentralabteilung das Personalreferat zukünftig über drei Gruppen verfügen werde. Die Gruppe I werde voraussichtlich für die Personalbetreuung- und Verwaltung, die Gruppe 2 für Besoldungs- und Vergütungsangele-

genheiten und die Gruppe 3 für besoldungsrechtliche Nebengebiete sowie Serviceleistungen zuständig sein. In der Gruppe 3 würden im wesentlichen Dienstreiseangelegenheiten, Nebentätigkeiten, Kommissionsbetreuungen und Beihilfen abgewikkelt. Alle drei Gruppen verfügten über eine/n Gruppenleiter/in. Die Fachaufsicht für Beihilfesachen werde vom Leiter der Gruppe 3, nicht jedoch vom Leiter des Personalreferats wahrgenommen. Die rechtliche Beratung der Beihilfesachbearbeiter wie auch die Prozeßführung solle – auch nach den Vorstellungen des Bundesrechnungshofes – dem Rechtsreferat übertragen werden.

Ich halte diese Lösung für eine unter Datenschutzaspekten geeignete und angemessene Organisationsform der Beihilfesachbearbeitung, die als Vorbild für andere Behörden dienen kann.

17.2 AIDS

AIDS ist innerhalb weniger Jahre zu einem zentralen gesundheits-, gesellschafts- und forschungspolitischen Problem geworden. Zahlreiche öffentliche und private Institutionen und Aktivitäten befassen sich mit der Erforschung und den Möglichkeiten, diese noch unheilbare Krankheit aufzuhalten, einzudämmen und zu besiegen. Angesichts dieser großen Herausforderung mögen Gesichtspunkte des Datenschutzes vordergründig nur eine Nebenrolle spielen. Manche meinen, sie seien gänzlich zu vernachlässigen oder dürften die Lösung der Probleme jedenfalls nicht behindern. Wer jedoch den grundrechtlichen Anspruch des einzelnen, auch des Infizierten und Kranken, auf Achtung der Menschenwürde und auf Wahrung des Persönlichkeitsrechts – also seines Rechts auf informationelle Selbstbestimmung – als Teil unserer Verfassung ernst nimmt, muß sich auch mit den Fragen der Erfassung, Speicherung, Verwendung und Weitergabe von Daten im Zusammenhang mit AIDS befassen. Dies ist auch deshalb unverzichtbar, weil einerseits das Bekanntwerden einer AIDS-Infektion oder AIDS-Erkrankung geeignet ist, den Betroffenen wie bei keiner anderen Krankheit ins soziale Abseits zu stellen, andererseits aber auch dem Schutz gesunder Menschen vor einer Infektion ein hoher Stellenwert zukommt. Beide Gesichtspunkte haben eine wesentliche datenschutzrechtliche Bedeutung.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat aus diesen Gründen einen eigenen Arbeitskreis AIDS eingerichtet, der die mannigfachen datenschutzrechtlichen Fragen im Zusammenhang mit AIDS aufgreifen, bewerten und möglichst einer verfassungskonformen Lösung zuführen soll. Unabhängig davon war ich in letzter Zeit in verschiedenen Teilbereichen prüfend und beratend tätig, und zwar hinsichtlich der Verarbeitung von „AIDS-Daten" bei der Polizei (vgl. Nr. 19.3), im Strafvollzug (vgl. Nr. 5.3) und bei Asylbewerbern (vgl. Nr. 4.1).

17.2.1 Fallberichtsbogen

Das Bundesgesundheitsamt hat etwa im April 1983 damit begonnen, Fälle von AIDS-Erkrankungen zu erfassen. Es hat dafür einen Fragebogen (Fallberichtsbogen) entwickelt, der den Ärzten und Krankenhäusern zur Verfügung gestellt wurde. Die Rücksendung der ausgefüllten Fragebogen ist in die Entscheidungsfreiheit des Arztes gestellt; eine Pflicht zur Abgabe des AIDS-Fallberichts besteht nicht. Die Einwilligung des Betroffenen liegt in aller Regel nicht vor. Daher ist mangels gesetzlicher Grundlagen eine Meldung von AIDS-Erkrankungen an das Bundesgesundheitsamt nur in anonymisierter Form zulässig.

Aufgrund der von verschiedenen Seiten geltend gemachten Bedenken wurde der Fragebogen mehrfach geändert, um die Anonymität der Betroffenen (besser) zu wahren. Die geltende Fassung wurde im Frühsommer 1986 an die obersten Landesgesundheitsbehörden und an zahlreiche Verbände und Institutionen zur Verteilung an Ärzte und Krankenhäuser übersandt. Dieser Fragebogen enthält folgende Angaben zur Person des Betroffenen:

— Vom Familien- und Vornamen jeweils der dritte Buchstabe und die Anzahl der Buchstaben

— Geschlecht

— Geburtsjahr

— Staatsangehörigkeit

— Bundesland und die zwei ersten Ziffern der Postleitzahl

— Gegebenenfalls Monat und Jahr des Todes.

Die Frage der Anonymisierung der Angaben zur Person des Betroffenen wird unterschiedlich beurteilt. Von einer absoluten Anonymisierung kann m. E. nicht ausgegangen werden, da mit entsprechendem Zusatzwissen oder auch über den meldenden Arzt der Betroffene identifiziert werden kann. Dabei ist andererseits zu berücksichtigen, daß die Angaben einer bestimmten Person möglicherweise „nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft zugeordnet werden können" (analog § 16 Abs. 6 Bundesstatistikgesetz) bzw. daß eine Identifizierung über den meldenden Arzt nur unter Verletzung der ärztlichen Schweigepflicht möglich wäre. Es wird deshalb überwiegend von einer ausreichenden Anonymisierung der Angaben zur Person in dem AIDS-Fallberichtsbogen ausgegangen. Dieser Auffassung habe ich mich angeschlossen.

17.2.2 Laborberichtsverordnung

Im Juli 1987 übersandte mir der Bundesminister für Jugend, Familie, Frauen und Gesundheit den Entwurf einer „Verordnung über die Berichtspflicht für positive HIV-Bestätigungstests (Laborberichtsverordnung)" zur Stellungnahme unter datenschutzrechtlichen Gesichtspunkten. Die Laborberichtsver-

ordnung hat den Zweck, alle Personen und Stellen, die Bestätigungstests zum Nachweis von Antikörpern gegen HIV, also einer AIDS-Infektion, durchführen, zu verpflichten, positive Ergebnisse dem (neu errichteten) zentralen AIDS-Infektionsregister beim Bundesgesundheitsamt in Form eines anonymen Berichts zu melden.

Zur datenschutzrechtlichen Bewertung des vorgesehenen Berichtsverfahrens habe ich mich mit dem Leiter des Robert-Koch-Instituts beim Bundesgesundheitsamt in Verbindung gesetzt und mit ihm die Fragen der Erfassung, Verarbeitung und Verwendung der notwendigen Daten erörtert. Durch von mir angeregte Änderungen und Ergänzungen des Verordnungsentwurfs ist nunmehr insbesondere sichergestellt, daß mit den gemeldeten Daten eine Identifizierung der untersuchten Person ausgeschlossen ist; die Berichte über positive Ergebnisse sind dem Bundesgesundheitsamt auf einem einheitlichen Vordruck ohne Angabe des Namens der Person, ohne Namensbestandteile oder eines alphanumerischen Schlüssels zur Kennzeichnung der Person zu melden. Eine Verknüpfung der gemeldeten Daten mit den Daten des AIDS-Fallregisters (vgl. oben Nr. 17.2.1) findet nicht statt.

Die aufgrund des § 7 Abs. 1 und 2 des Bundesseuchengesetzes vom Bundesminister für Jugend, Familie, Frauen und Gesundheit erlassenen Verordnung ist inzwischen am 1. Oktober 1987 mit einer Geltungsdauer von drei Monaten in Kraft getreten (BGBl. I S. 2141). Sie ist mit Wirkung vom 1. Januar 1988 durch eine mit Zustimmung des Bundesrats erlassene Rechtsverordnung gleichen Inhalts abgelöst worden.

17.3 Auskunftsverweigerung gegenüber dem Betroffenen

Ein Petent hat sich mit der Bitte um Unterstützung seines Anspruchs auf Auskunft gemäß § 13 BDSG an mich gewandt. Er vermutet, daß das Bundesministerium für Jugend, Familie, Frauen und Gesundheit (BMJFFG) personenbezogene Daten über ihn in einer Datei gespeichert hat. Diese Vermutung hat er auch schlüssig begründet, ohne hierzu verpflichtet zu sein. Denn selbst wenn keine Datenspeicherung in Dateien vorliegt, umfaßt der Auskunftsanspruch das Recht, gerade dies zu erfahren.

Das BMJFFG hat bisher weder meine mehrfachen Bitten um Stellungnahme beantwortet, noch dem Petenten die erwünschte Auskunft erteilt. Ich habe diesen Verstoß gegen §§ 13 und 19 Abs. 3 Satz 1 BDSG gemäß § 20 Abs. 1 BDSG beanstandet.

18 Sicherheitsbereich – Übergeordnete Probleme

18.1 Probleme der Kontrollpraxis

Die Anwendung automatisierter Systeme zur Verarbeitung personenbezogener Daten im Sicherheitsbereich ist im Berichtsjahr zügig ausgebaut worden. Dies belegen nicht nur die nachfolgend exemplarisch dargestellten Problembereiche (s. u. Nr. 19 bis 24), sondern auch folgende Zahlen. Im vergangenen Jahr haben mich erreicht:

10 Errichtungsanordnungen für Dateien des Bundeskriminalamts (BKA)

20 Dateimeldungen des BKA zum besonderen Register nach § 19 Abs. 4 Satz 5 BDSG

5 Mitteilungen über geplante bzw. neu eingerichtete Dateien/Verfahren beim Bundesamt für Verfassungsschutz.

Abgesehen davon, daß mir die Errichtungsanordnungen oft erst geraume Zeit nach dem Beginn der Datenverarbeitung zugehen, ist es mir aus Kapazitätsgründen nicht möglich, jede neue Datenverarbeitung auch nur aktenmäßig – d. h. ohne praktische Stichproben – zu überprüfen. Es liegt aber auf der Hand und wird durch viele in meinen Tätigkeitsberichten niedergelegte Beispiele belegt, daß zahlreiche Eingriffe in die Selbstbestimmung der Betroffenen vermeidbar gewesen wären, wenn unterbliebene oder erst später durchgeführte Kontrollen rechtzeitig stattgefunden hätten. Deshalb liegt mir viel daran, bessere Möglichkeiten zu erhalten, den Datenschutz so früh wie möglich zur Geltung zu bringen. Dies entspräche auch den Vorstellungen des Bundesverfassungsgerichts im Volkszählungsurteil, wonach „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 Rechtsschutzes durch rechtzeitige Vorkehrungen ... die Beteiligung unabhängiger Datenschutzbeauftragter von erheblicher Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung (ist)" (BVerfGE 65, 1 [46]). „Rechtzeitige Vorkehrungen" im Sinne dieser Aussage sehe ich u. a. dann nicht als gewährleistet an, wenn der Datenschutzkontrolle die Informationen fehlen, die für eine zeitnahe Analyse der eingesetzten Verarbeitungssysteme erforderlich sind.

Ich bin der Meinung, daß eine kontinuierliche und zeitnahe Begleitung durch den Datenschutz auch im Sinne der Sicherheitsbehörden liegen muß, da sie den Weg dazu öffnet, Probleme früher zu erkennen und durch Beratung mit weit weniger Aufwand und Reibungsverlusten zu lösen, als dies bei einer Kritik an einer schon fest eingeführten Praxis zwangsläufig der Fall ist. Dieser Erkenntnis entspricht auch die Empfehlung des Deutschen Bundestages an die Bundesregierung, den Bundesbeauftragten nicht nur bei Gesetzesvorhaben, sondern auch bei der Vorbereitung von Verwaltungsvorschriften möglichst frühzeitig zu beteiligen (Beschlußempfehlung und Bericht zum 6. und 7. TB, Drucksache 10/6583 S. 3 Nr. 3).

Auch die Erschwerungen meiner Kontrolltätigkeit durch Auseinandersetzungen über die Reichweite meiner Prüfungsbefugnisse dauern an. Zwar ist die Frage meiner Befugnis zur Einsicht in Unterlagen, die im Zusammenhang mit der Speicherung personenbezogener Daten stehen, in dieser Form nicht

wieder aufgeworfen worden, nachdem sich der Bundestag damit befaßt hatte (vgl. unten Nr. 20). Jedoch ist im Verhältnis zum Bundesminister des Innern eine Meinungsverschiedenheit darüber aufgetreten, ob eine dort vorhandene Informationssammlung den Dateibegriff erfüllt. Zugrunde liegt folgende Fragestellung:

Im September 1986 hatte sich ein Bürger durch seinen Rechtsanwalt an mich gewandt, weil er glaubte, durch die Weitergabe ihn betreffender unrichtiger Angaben an die überregionale Presse in seinen Rechten verletzt worden zu sein. Meine daraufhin an den Bundesminister des Innern gerichtete Anfrage wurde erst nach mehrfacher Erinnerung beantwortet, nachdem ich eine Beanstandung wegen Verletzung der Mitwirkungspflicht nach § 19 Abs. 3 BDSG in Aussicht gestellt hatte. Die Auskünfte des Bundesministers des Innern blieben jedoch trotz Nachfragen unergiebig. Er teilte zwar mit, daß Angaben des Petenten in einem Bericht vom Februar 1985 über extremistische Aktivitäten eines bestimmten Personenkreises enthalten sind, beschränkte sich jedoch hinsichtlich der entscheidenden Frage, an wen dieser Bericht weitergegeben worden ist, auf die Aussage, er sei „nur im zulässigen Rahmen umgesetzt" worden. Eine Einsicht in Informationssammlungen und Unterlagen des Fachreferats des Ministeriums ergab, daß der Bericht Angaben über zwei Straftaten und eine Verurteilung enthielt, obwohl die Täterschaft nicht nachgewiesen und die Verurteilung rechtskräftig aufgehoben worden war. Ich habe beanstandet, daß Kopien des Berichts mit diesen unrichtigen Angaben an mehrere Außenstehende übermittelt worden sind, und um Darlegung gebeten, wie künftig sichergestellt werden soll, daß keine überholten oder sonst unrichtigen Angaben weitergegeben werden (§ 20 Abs. 4 BDSG).

Der Bundesminister des Innern verweist hinsichtlich der Unrichtigkeit auf einen in dem Bericht gegebenen Quellenhinweis, der den Sinn eines Vorbehalts habe, und ist der Auffassung, daß den Individualinteressen angemessen Rechnung getragen worden sei. Im übrigen hat er die Beanstandung zurückgewiesen, seine Auskunftspflicht nach § 19 Abs. 3 BDSG verneint und dementsprechend weitere Auskünfte abgelehnt, weil es sich bei der Informationssammlung, aus der der Bericht gespeist worden ist, nicht um eine Datei im Sinne des BDSG handele.

Diese Position ist nicht überzeugend. Die betreffende Informationssammlung besteht aus mehreren nach verschiedenen Merkmalen sortierten Listen, so daß alle Auswertungsmöglichkeiten, die eine Informationssammlung zur Datei qualifizieren, gegeben sind. Jedenfalls müssen die Datenschutzvorschriften entsprechend angewendet werden, wenn man die leichte Auswertbarkeit und Verfügbarkeit der Daten berücksichtigt und das Gebot beachtet, das einfache Recht verfassungskonform auszulegen. In diesem Sinne bin ich im September 1987 erneut an den Bundesminister des Innern herangetreten. Die mir zum Jahresende zugegangene Antwort führt in der Sache nicht weiter und enthält keine für den Datenschutz positiven Ansätze.

Ich befürchte, daß es auch künftig immer wieder zu Auseinandersetzungen dieser Art kommen wird, nachdem auch der mir vorliegende Entwurf zur Neufassung des BDSG in der hier streitigen Rechtsfrage keine Änderung vorsieht.

18.2 Zeitpunkt meiner Beteiligung an den Gesetzgebungsvorhaben

Über meine Mitwirkung an den Gesetzgebungsvorhaben der Bundesregierung auf dem Gebiet der Datenverarbeitung bei den Sicherheitsbehörden kann ich – vom Projekt eines Geheimschutzgesetzes abgesehen (vgl. dazu unter 18.3) – wenig berichten, weil mir bislang lediglich der Entwurf für ein neues Bundesverfassungsschutzgesetz vor kurzem „zur Kenntnisnahme" zugesandt wurde, also ohne Einbeziehung in die Erörterungen. Nicht erhalten habe ich bislang Entwürfe für die Zusammenarbeit der Staatsschutzbehörden (Zusammenarbeitsgesetz), für ein MAD-Gesetz, für die Datenverarbeitung der Polizeibehörden des Bundes sowie des Bundesnachrichtendienstes. Der Bundesminister der Finanzen hat mir mitgeteilt, er werde das „neue Polizeigesetz des Bundes" abwarten und danach prüfen, ob die Abgabenordnung geändert werden müsse. Es kann danach also nicht davon die Rede sein, ich sei an den Gesetzesvorhaben zur Datenverarbeitung bei den Sicherheitsbehörden des Bundes bisher beteiligt gewesen. Zwar kann ich datenschutzrechtliche Gesichtspunkte auch noch im Rahmen der parlamentarischen Beratung geltend machen, eine frühere Beteiligung könnte aber die parlamentarische Arbeit entlasten.

18.3 Entwurf eines Geheimschutzgesetzes

Das Bundeskabinett hat neue Sicherheitsüberprüfungsrichtlinien verabschiedet (vgl. 9. TB S. 56 f.). Sie enthalten eine Reihe bemerkenswerter datenschutzrechtlicher Fortschritte, auch wenn nicht alle meine Vorstellungen berücksichtigt wurden.

Nunmehr kommt es darauf an, das Sicherheitsüberprüfungsverfahren durch Gesetz einwandfrei zu regeln. Eine steigende Zahl von Eingaben belegt die bei den Betroffenen wachsenden Zweifel an der Tragfähigkeit der bislang herangezogenen Rechtsgrundlagen. Auch die Gerichte müssen immer häufiger der Frage nachgehen, ob diese Grundlagen nach dem Volkszählungsurteil noch ausreichen und wie lange ein etwaiger Übergangsbonus noch in Anspruch genommen werden kann. Der Bundesminister des Innern hat mich frühzeitig an den Vorüberlegungen für das zu schaffende Geheimschutzgesetz beteiligt. In mehreren Gesprächsrunden habe ich datenschutzrechtliche Gesichtspunkte, die bei der Formulierung dieses Gesetzes nach meiner Auffassung zu berücksichtigen sind, geltend gemacht, wobei sich die Erfahrungen aus der Kontrolle der Abteilung V des Bundesamtes für Verfassungsschutz als wertvoll erwiesen. Aus meiner Sicht kommt es be-

sonders darauf an, den Kreis der in eine Sicherheitsüberprüfung einzubeziehenden Personen auf das erforderliche Maß zu begrenzen. Eine solche Begrenzung würde es auch erleichtern, stärker nach dem Grundsatz „Qualität geht vor Quantität" vorzugehen. Außerdem muß der Gesetzgeber so präzise wie möglich regeln, welche Daten im Rahmen einer Sicherheitsüberprüfung bei wem erhoben werden und in welcher Form und wie lange sie anschließend gespeichert bleiben dürfen. Darüber hinaus erscheint es mir wichtig, daß die für die Zwecke der Sicherheitsüberprüfung erhobenen Daten auch nach der Überprüfung nicht für alle möglichen Zwecke, etwa für die gesamte Aufgabenerfüllung der Verfassungsschutzbehörden und anderer Sicherheitsbehörden, verwendet werden.

18.4 Sicherheitsüberprüfungen von in Privatunternehmen Beschäftigten

Durch Presseberichte wurde bekannt, daß alle Beschäftigten eines größeren Bereichs eines süddeutschen Großunternehmens durch den Verfassungsschutz sicherheitsüberprüft worden sind. Um die Rechtmäßigkeit und Angemessenheit dieser Maßnahme hat sich eine öffentliche Diskussion entwikkelt. Auch die Gerichte wurden mit der Angelegenheit befaßt.

Die Sicherheitsüberprüfung der Beschäftigten in der Privatwirtschaft ist im Handbuch für den Geheimschutz in der Wirtschaft geregelt. Zuständig ist der Bundesminister für Wirtschaft, der über die Erteilung oder Versagung der Ermächtigung zum Umgang mit Verschlußsachen entscheidet. Die Überprüfung selbst wird vom BfV durchgeführt.

Meine Bemühungen, die Beteiligung von Bundesbehörden an den Überprüfungen in dem eingangs genannten Fall festzustellen, um sie datenschutzrechtlich bewerten zu können, sind noch nicht abgeschlossen. Der Bundesminister für Wirtschaft hat mir mitgeteilt, daß es sich nicht um Maßnahmen im Rahmen des Geheimschutzes in der Wirtschaft handelt, sondern um die Überprüfung von Personen, die an sicherheitsempfindlichen Stellen von lebens- und verteidigungswichtigen Einrichtungen beschäftigt sind oder beschäftigt werden sollen (vorbeugender personeller Sabotageschutz, § 3 Abs. 2 Ziffer 2 Bundesverfassungsschutzgesetz), für die er nicht zuständig ist. Der Bundesminister für das Post- und Fernmeldewesen hat auf eine Kleine Anfrage der Fraktion DIE GRÜNEN geantwortet, daß die Sicherheitsüberprüfungen nicht auf seine Veranlassung durchgeführt werden und daß er das betreffende Unternehmen auf Anfrage an die zuständige oberste Landesbehörde verwiesen habe, um prüfen zu lassen, in welchen Bereichen Sicherheitsüberprüfungen erforderlich sind (Drucksache 11/504 S. 2). Weiterhin hat er erklärt, das Bundesamt für Verfassungsschutz wirke bei solchen Überprüfungen nicht mit (Drucksache 11/503 S. 28).

Ich habe den Bundesminister für das Post- und Fernmeldewesen darüber hinaus um Mitteilung gebeten, ob es sich bei dem betroffenen Unternehmenszweig um einen sicherheitsempfindlichen Bereich handelt, ob die Fertigung ausschließlich ziviler Telefonanlagen die Einstufung als sicherheitsempfindlich rechtfertigt und welche Gründe hierfür maßgebend sind. Er hat darauf geantwortet, daß meine Anfrage in keinem Zusammenhang mit der Verarbeitung personenbezogener Daten in Dateien bei Behörden der Deutschen Bundespost stehe und im übrigen nur darauf verwiesen, daß das Ministerium mit der Angelegenheit nicht weiter befaßt gewesen sei. Weitergehende Auskünfte zur Sache habe ich auch nach Hinweis auf die Verpflichtung aller Bundesbehörden, den Bundesbeauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen (§ 19 Abs. 3 BDSG), nicht erhalten. Meine im Oktober an den Bundesminister des Innern gerichtete Anfrage, die mir weiteren Aufschluß über die Beteiligung des Bundesamtes für Verfassungsschutz bringen soll, wurde noch nicht beantwortet.

Eine datenschutzrechtliche Bewertung ist mir daher noch nicht möglich. Ich gehe allerdings davon aus, daß das mit dem Entwurf eines Sicherheitsüberprüfungsgesetzes verfolgte Ziel „Qualität vor Quantität" uneingeschränkt auch für den hier angesprochenen Bereich von Überprüfungen im Rahmen des vorbeugenden personellen Sabotageschutzes gelten muß und daß es klarer Grenzziehungen bedarf, damit ein Verdacht, Überprüfungen durch Verfassungsschutzbehörden würden mißbräuchlich eingesetzt, möglichst gar nicht entsteht.

18.5 Auskunft an Betroffene

Nach § 13 Abs. 2 BDSG sind die Nachrichtendienste, die Steuerbehörden sowie die Polizeibehörden von der Verpflichtung zur Auskunftserteilung an Betroffene freigestellt. Während die Polizeibehörden in den Richtlinien über kriminalpolizeiliche personenbezogene Sammlungen sowie in den Dateienrichtlinien sich weitgehend zur Auskunftserteilung verpflichtet haben, verhalten sich die Nachrichtendienste sowie die Finanzbehörden gegenüber Auskunftsersuchen nach wie vor restriktiv. In der Rechtsprechung hat sich mehr und mehr die Auffassung durchgesetzt, daß die Behörden auch im Rahmen von § 13 Abs. 2 BDSG die Auskunft nicht schlechthin verweigern können, sondern nach pflichtgemäßem Ermessen über die Erteilung von Auskünften an Betroffene zu entscheiden haben. Das Oberverwaltungsgericht Bremen hat in seinem Urteil vom 24. Februar 1987 – OVG I BA 50/86 – darüber hinaus betont, daß die ablehnende Entscheidung über ein Auskunftsersuchen die im Einzelfall maßgeblichen Gründe für die Ermessensentscheidung erkennen lassen muß. In der Praxis werden die Begründungen für die Verweigerung der Auskunft diesen Anforderungen häufig nicht gerecht.

So hatte sich beispielsweise ein Bürger an mich gewandt, gegen den beim Grenzübertritt ein Ermittlungsverfahren wegen einer Steuerordnungswidrigkeit eingeleitet worden war. Er hatte versäumt, anmeldepflichtige Waren im Wert von 100 DM bei der

Zollkontrolle anzumelden. Zum Zeitpunkt seiner Eingabe wußte der Petent bereits, daß das zuständige Zollfahndungsamt aufgrund dieses Vorgangs eine Speicherung seiner Daten in der Datei veranlaßt hatte. Ich konnte zwar erreichen, daß die Speicherdauer von zehn auf drei Jahre herabgesetzt wurde. Einer Auskunft an den Petenten aber wollte der Bundesminister der Finanzen nicht zustimmen. Er machte geltend, daß der Petent allenfalls unbefugt Kenntnis von seiner Speicherung erlangt haben könnte. Sein Vater habe sich nämlich die Informationen als angeblicher Kriminalbeamter beim zuständigen Zollfahndungsamt verschafft (dem Umstand, daß hier möglicherweise leichtfertig Daten übermittelt wurden, gehe ich noch gesondert nach). Erst nach einer Beanstandung war der Bundesminister der Finanzen bereit, „wegen der Geringfügigkeit des begangenen Steuerdelikts und unter besonderer Berücksichtigung des Umstandes, daß der Petent – wenn auch unbefugt – von der Speicherung und dem Anlaß hierzu Kenntnis" hatte, Auskunft zu erteilen. Wenn der Auskunftssuchende ohnehin weiß, daß ein Ermittlungsverfahren gegen ihn eingeleitet worden ist, kann nach meiner Auffassung grundsätzlich kein öffentliches Interesse gegen die Auskunftserteilung sprechen, wie auch die Praxis im Polizeibereich bestätigt.

In einem anderen Fall wurde ein Bürger mehrfach intensiven Grenzkontrollen unterzogen. Er vermutete nicht zu Unrecht, daß dem eine Speicherung in einer Datei der Zollbehörden zugrunde lag. Gleichwohl hat der Bundesminister der Finanzen sich geweigert, dem Betreffenden Auskunft zu erteilen. Ich habe dies beanstandet, weil ich die Ermessensentscheidung für fehlerhaft halte. Es hätte berücksichtigt werden müssen, daß der Betroffene mit hoher Wahrscheinlichkeit davon ausgehen konnte, daß über ihn Daten bei den Zollbehörden gespeichert sind. Der Bundesminister der Finanzen hat nunmehr „im Hinblick auf das ... Urteil des Oberverwaltungsgerichts Bremen" der Auskunftserteilung zugestimmt.

Problematisch ist auch weiterhin das Auskunftsverhalten der Nachrichtendienste. Im Regelfall wird lediglich Auskunft erteilt, wenn Daten des Betroffenen im Rahmen einer Sicherheitsüberprüfung gespeichert worden sind. In diesem Falle kann ohnehin davon ausgegangen werden, daß er die Speicherung seiner Daten vermutet. In fast allen übrigen Fällen wird die Auskunft zumeist unter pauschaler Berufung auf die gesetzliche Regelung verweigert, ohne daß die Ermessensausübung erkennbar bzw. nachvollziehbar wäre.

19 Bundeskriminalamt

19.1 Die Dateien GEAK und FAMAL – Massendatenverarbeitung zur Abwehr arabischer Terroristen

Im Berichtsjahr wurde öffentlich bekannt, daß das Bundeskriminalamt die von der Grenze gemeldeten Ein- und Ausreisen von Staatsangehörigen bestimmter arabischer Staaten sowie Nachweise über Sichtvermerksanträge von Angehörigen eines arabischen Staates verarbeitet. Die Thematik hat auch den Innenausschuß des Deutschen Bundestages beschäftigt. Ich habe die Datenverarbeitung, an der verschiedene Bundes- und auch Landesbehörden beteiligt sind, in einigen Punkten beanstandet, die im folgenden noch dargestellt werden. Der Bundesminister des Innern hat mir darauf mitgeteilt, daß die Organisation und die Konzeption der Datei FAMAL grundlegend verändert werden sollen und daß die Datei GEAK eingestellt worden ist. Die allgemeine Fragestellung, welche Behörden im Rahmen welcher Aufgaben Dateien über sehr große Personenkreise anlegen dürfen, um im Falle eines terroristischen Anschlages Anknüpfungspunkte für Ermittlungen oder zur Gefahrenabwehr zu besitzen, ist damit freilich nicht geklärt und kann jederzeit wieder auftreten, auch in bezug auf ganz anders geschnittene Personengruppen. Unter diesem Aspekt erscheint es notwendig, die Problematik im Auge zu behalten, wobei die Vorgänge des Jahres 1987 als Modellfall gelten können.

Ich werde bei dieser Frage weiter von folgenden Grundsätzen ausgehen: Die polizeilichen Maßnahmen der Gefahrenabwehr und der vorbeugenden Verbrechensbekämpfung müssen sich auch auf dem Gebiet der Verarbeitung personenbezogener Daten nach der Schwere der Gefahr richten. Es unterliegt in erster Linie der fachlichen Verantwortung der Sicherheitsorgane, welche Maßnahmen geeignet und erfolgversprechend sind. Auf der anderen Seite muß von seiten des Datenschutzes darauf geachtet werden, daß das aus dem Recht auf informationelle Selbstbestimmung folgende Verbot der Sammlung personenbezogener Daten auf Vorrat beachtet wird, und zwar auch bei der Bekämpfung terroristischer Gefahren. Ich betrachte insoweit die systematische Speicherung aller Grenzübertritte der Angehörigen einer Vielzahl arabischer Länder (Datei GEAK) jedenfalls als einen Grenzfall, weil die gespeicherten Tatbestände nur einen sehr entfernten Bezug zu den Erkenntnissen über drohende Gefahren aufwiesen; allerdings ist anzuerkennen, daß die Belastung der Betroffenen relativ gering war, weil die Speicherdauer der Einzeldaten auf sechs Monate beschränkt und auch die Maßnahme im ganzen von vornherein befristet angesetzt war.

Der Bundesminister des Innern sieht die Rechtsgrundlage der Speicherung in den §§ 1 Nr. 1, 2 Nr. 2 und 10 des Bundesgrenzschutzgesetzes, die nach seiner Auffassung bis zur Schaffung bereichsspezifischer Regelungen ausreichend seien. Mir erscheint allerdings zweifelhaft, ob die Generalklausel des § 10, die dem Grenzschutz erlaubt, die nach pflichtgemäßem Ermessen notwendigen Maßnahmen zu treffen, auch dazu berechtigt, Datenspeicherungen in großem Umfange nach formalen Abgrenzungskriterien durchzuführen und insofern Maßnahmen gegen Personen zu ergreifen, bei denen nicht ersichtlich ist, daß von ihnen eine Gefahr ausgehen könnte.

Was die Organisation der Datenverarbeitung betrifft, können aus den Vorgängen um diese beiden

Dateien nach meiner Auffassung unmittelbare Lehren gezogen werden.

Bei beiden Dateien sind zwischen den unmittelbar beteiligten Behörden (Bundeskriminalamt, Bundesgrenzschutz, Bundesverwaltungsamt), dem Bundesminister des Innern und mir Meinungsverschiedenheiten entstanden, wer eigentlich die speichernde Stelle im Sinne des Bundesdatenschutzgesetzes und damit auch für die Beachtung des Datenschutzes verantwortlich ist. Bei der Datei FAMAL ist durch Zusammenfassung verschiedener Datenarten und Zwecksetzungen – ermittlungsverfahrensbezogene Daten einerseits, Sichtvermerksangaben sowie Ein- und Ausreisen aller libyschen Staatsangehörigen zu weitergehenden Zwecken andererseits – eine Gemengelage entstanden. Der Bundesminister des Innern hat dazu nunmehr erklärt, die Datei sei zum einen Teil vom Bundeskriminalamt zur Erfüllung eigener Aufgaben, zum anderen Teil in Erledigung eines Datenverarbeitungsauftrages des Bundesverwaltungsamtes geführt worden. Einen entsprechenden Auftrag konnte ich allerdings nicht feststellen. Gerade bei einer solchen Vermischung ist es unerläßlich, durch sehr klare Vorgaben (Registermeldungen und Errichtungsanordnungen) sicherzustellen, daß klare Schnittstellen bestehen und daß jeder Beteiligte seine Rechte und Pflichten genau kennt. Ich empfehle jedoch, solche Mischgebilde möglichst zu vermeiden, da sie Mißverständnisse, Reibereien und Pannen geradezu herausfordern.

Bei der Datei GEAK war ich nach Studium der Aktenlage und Verarbeitungspraxis beim Bundesgrenzschutz und beim Bundeskriminalamt zu dem Ergebnis gelangt, daß das Bundeskriminalamt die Datei als eigene Aufgabe betreibt. Denn dieses hatte die Registermeldung verfaßt, wobei es in einer ersten Meldung sich selbst, in einer zweiten, vom April 1987 datierenden Meldung die Grenzschutzdirektion als speichernde Stelle eingesetzt hatte. Das BKA hatte die Daten auch mehrfach ohne Rückfrage beim Bundesgrenzschutz ausgewertet und zum Teil auch übermittelt, während der Bundesgrenzschutz sein grenzpolizeiliches Desinteresse bekundet hatte, nachdem sich die Einrichtung eines direkten Anschlusses als technisch nicht machbar erwiesen hatte. Demgegenüber hat mir der Bundesminister des Innern mitgeteilt, daß durch eine Dienstbesprechung mit den beteiligten Behörden sowie eine fernschriftliche Anweisung an die Grenzschutzdirektion, den Entwurf einer Errichtungsanordnung in Fühlungnahme mit dem BKA zu erstellen, ein Auftragsverhältnis zustande gekommen sei. Wenn sich allerdings im folgenden die Grenzschutzbehörden nur wie Datenlieferanten und das Bundeskriminalamt wie der Datenherr verhalten haben, so bestärkt dies die Zweifel, ob die Aufgabe der Datenspeicherung dem Bundesgrenzschutz richtig zugeordnet wurde; zugleich wird dadurch belegt, daß es verstärkter Durchführungsmaßnahmen nach § 6 BDSG bedarf, um im Sinne von Nr. 8 der Anlage zu § 6 zu gewährleisten, daß im Auftrag zu verarbeitende Daten nur entsprechend den Weisungen des Auftraggebers verarbeitet werden (Auftragskontrolle).

19.2 Die Systeme APIS und NADIS

Ich hatte darüber berichtet, daß im Januar 1986, nachdem die systemtechnischen Voraussetzungen geschaffen waren, die Arbeitsdatei PIOS-Innere Sicherheit (APIS) in Betrieb genommen wurde (vgl. 9. TB S. 60 ff.). In APIS sind nebeneinander Daten über strafrechtliche Verurteilungen, eingeleitete Ermittlungsverfahren, bloße Verdachtsfälle, Daten über Personen, die weder Beschuldigte noch Verdächtige sind, und Daten zum Zwecke der Gefahrenabwehr gespeichert. Es handelt sich also um eine Mischung aus Daten zum Zwecke der Strafverfolgung, der vorbeugenden Straftatenbekämpfung und der Gefahrenabwehr. Gemeinsam ist ihnen lediglich der Staatsschutzbezug.

APIS wird als Verbundsystem von Bund und Ländern gemeinsam betrieben mit der Maßgabe, daß alle bei den Teilnehmern vorhandenen Informationen zu einer Person zusammengefügt werden und daß jeder Mitbesitzer berechtigt ist, die Daten der anderen nicht nur zu lesen, sondern auch zu ergänzen und sogar zu verändern. Neue Datenbankstrukturen und komfortable Auswertungsprogramme machen das System überaus effektiv. Der Übergang von der bisherigen Datenverarbeitung im Staatsschutz auf APIS bedeutet einen außerordentlichen Qualitätssprung.

Ich bin der Auffassung, daß derartige qualitative Veränderungen der Datenverarbeitung bei der Polizei nur eingeführt werden können, wenn hierfür einwandfreie Rechtsgrundlagen vorliegen. Die Neueinführung einer Datei vom Zuschnitt der APIS kann nicht lediglich auf den „Übergangsbonus" gestützt werden, da dieser bis zur Schaffung der notwendigen Rechtsvorschriften lediglich die Fortführung unerläßlicher Maßnahmen gestattet.

Nunmehr werden vollendete Tatsachen auch bei der Frage des Informationsaustausches zwischen Polizei und Verfassungsschutz geschaffen. Wie bereits im Neunten Tätigkeitsbericht (S. 61 f.) dargestellt, speicherte die Abteilung Staatsschutz des BKA bislang Daten im nachrichtendienstlichen Informationssystem NADIS der Verfassungsschutzbehörden, da sie über kein eigenes Aktennachweissystem verfügte. Seit Januar 1986 steht für diesen Zweck APIS zur Verfügung. Gleichwohl speichert das BKA auch weiterhin Daten in NADIS, zusätzlich zur Erfassung in APIS.

Nachdem der ursprüngliche Speicherungszweck weggefallen ist, erfolgt die Erfassung in NADIS nunmehr nur noch zum Zwecke der Datenübermittlung an die Verfassungsschutzbehörden. Noch bevor der Gesetzgeber über die besonders schwierige Ausgestaltung der Informationsbeziehungen zwischen Polizei und Verfassungsschutz entschieden hat, erfolgt in Form der NADIS-Speicherung durch das Bundeskriminalamt eine ständige automatisierte Übermittlung der Daten über Verdächtige und Beschuldigte im Rahmen von Staatsschutzermittlungsverfahren an die Verfassungsschutzbehörden. Die meisten dieser Daten stammen von den Ländern. Sie werden von den Landeskriminalämtern an das Bundeskrimi-

nalamt gemeldet, dort unmittelbar im NADIS der Verfassungsschutzbehörden gespeichert und können von den Verfassungsschutzbehörden des Bundes und der Länder direkt, vom Militärischen Abschirmdienst und vom Bundesnachrichtendienst im Wege des regelmäßigen Bandabgleichs, abgerufen werden. Mir erscheint fraglich, ob der Gesetzgeber einem so umfassenden Datenverbund je zustimmen wird.

Ich habe gegenüber dem Bundesminister des Innern die Speicherung von Personendaten durch das Bundeskriminalamt in NADIS beanstandet. Diese Beanstandung wurde zurückgewiesen und der Verbund fortgeführt.

Der Bundesminister des Innern macht im wesentlichen geltend, alle vom Bundeskriminalamt in NADIS gespeicherten Fälle seien von Relevanz für die Verfassungsschutzbehörden. Deshalb könne es keinen „durchgreifenden datenschutzrechtlichen Bedenken unterliegen, daß die Relevanzprüfung und die Datenpflege durch das in Staatsschutzangelegenheiten erfahrene Bundeskriminalamt vorgenommen werden". Auch vermöge er „nicht zu sehen, worin eine datenschutzrechtliche Gefährdung liegen soll, wenn dem Bundeskriminalamt bei der Abfrage der eigenen Fundstelle in NADIS mitgeteilt wird, daß eine Verfassungsschutzbehörde ebenfalls über Erkenntnisse zu der Person verfügt ...". NADIS-PZD sei außerdem keine „Belastetendatei", so daß sich aus dem gespeicherten Aktenzeichen keine den Betroffenen belastenden inhaltlichen Rückschlüsse auf die beim Bundesamt für Verfassungsschutz vorliegenden Informationen ziehen lassen.

Ich halte diese Argumentation des Bundesministers des Innern für nicht überzeugend. Sie ist primär an Zweckmäßigkeitsgesichtspunkten aus der Perspektive der beteiligten Sicherheitsbehörden orientiert. Die Verarbeitung personenbezogener Daten muß sich aber gerade auch im Sicherheitsbereich streng und bis in die Details an Recht und Gesetz orientieren. Ich bleibe deswegen bei meiner Bewertung, daß die Beteiligung des Bundeskriminalamts am nachrichtendienstlichen Informationssystem NADIS dem geltenden Recht widerspricht.

19.2.1 Daten von Volkszählungsgegnern in APIS

Kurz vor Drucklegung dieses Berichts begann eine öffentliche Diskussion darüber, ob es gerechtfertigt sei, Daten von Volkszählungsgegnern in APIS zu speichern (s. auch 10.1.8). Hierzu ist folgendes zu bemerken:

In der Dateierrichtungsanordnung für APIS wird als Zweck für dieses System auf Staatsschutzdelikte abgestellt. Ich kann nicht erkennen, daß jemand, der im Zusammenhang mit der Volkszählung möglicherweise eine strafbare Handlung wie z. B. Beschädigung eines Volkszählungsbogens begeht, sich als Verfassungsfeind qualifiziert hat. Dabei ist vor allem auch zu bedenken, daß eine Ablehnung der Volkszählung auf den verschiedensten Motiven beruhen kann. Eine Speicherung in APIS allein aus diesen Gründen halte ich für unverhältnismäßig. Es kommt hinzu, daß die Gerichte die Strafbarkeit einer solchen Verhaltensweise unterschiedlich beurteilt haben und eine höchstrichterliche Entscheidung noch aussteht.

19.3 AIDS-Hinweise im INPOL-System

Im Berichtszeitraum wurde bekannt, daß die Polizeibehörden von Bund und Ländern Ende 1985 übereingekommen sind, zu Zwecken der Eigensicherung der Polizeivollzugsbeamten Hinweise auf eine AIDS-Infektion in den polizeilichen Informationssystemen zu speichern, wenn die betreffende Person aus anderen Gründen dort erfaßt ist. Im Juni 1987 wurde den Datenschutzbeauftragten der im Oktober 1986 beschlossene Wunsch der Innenminister übermittelt, an der Erarbeitung von Kriterien für diese Speicherung mitzuwirken. Die Datenschutzbeauftragten haben daraufhin in zwei Arbeitssitzungen mit Vertretern der Innenminister und -senatoren diese Problematik beraten und am 7. Dezember 1987 bei Gegenstimme des Bayerischen Landesbeauftragten einen Beschluß gefaßt, der als Anlage zu diesem Bericht abgedruckt ist. Ich habe mich zu der Problematik außerdem auf Wunsch der Enquête-Kommission „Gefahren von AIDS und wirksame Wege zu ihrer Eindämmung" des Deutschen Bundestages in deren Sitzung am 14. Juli 1987 sowie im Innenausschuß am 16. September 1987 geäußert. Ferner habe ich mich an Beratungen der interministeriellen Arbeitsgruppe AIDS beteiligt.

Die Speicherung von Hinweisen auf AIDS in INPOL erfolgt überwiegend durch die Polizeibehörden der Länder. Die Beteiligung von Bundesbehörden und deren Verantwortlichkeit darf jedoch deshalb nicht vernachlässigt werden. Zwar hatte das Bundeskriminalamt bis Mitte August „im Bereich seiner originären Strafverfolgungszuständigkeit" keine AIDS-Hinweise in Dateien gespeichert, wie vom Bundesminister des Innern auf die Frage nach einer Speicherung durch das Bundeskriminalamt „im Bereich seiner originären Zuständigkeit" dargelegt wurde (Bundestags-Drucksache 11/729 S. 6 f.). Gleichwohl war das Bundeskriminalamt mit Stand vom 7. September 1987 bei 134 Speicherungen (von insgesamt 255) Besitzer des Datensatzes und damit speichernde Stelle im Sinne des Datenschutzes (am 19. Juli 1987 hatte diese Zahl noch 205 von insgesamt 336 betragen). Seine Zuständigkeit ergibt sich aus § 2 Abs. 1 Nr. 1 BKA-Gesetz.

Teilweise handelt es sich um Fälle, bei denen der AIDS-Hinweis früher von einem Land eingegeben worden war und der Datensatz später nach allgemeinen polizei-internen Absprachen in den Besitz des Bundeskriminalamts übergegangen ist. Durch diese Praxis bestanden im Juli 1987 allein 33 Speicherungen unter der Verantwortung des BKA, ohne daß dieses aus seinen Unterlagen feststellen konnte, welche Polizeidienststelle die Speicherung veranlaßt hatte, wie sich bei einem Arbeitsbesuch beim BKA zeigte. Das BKA hat seinerzeit Maßnahmen ergriffen, um Datenspeicherungen ohne direkten Verweis auf die zugrundeliegenden Unterlagen auszuschlie-

ßen. Dabei ergab sich, daß von den 33 Hinweise nur 16 durch die Landeskriminalämter bestätigt wurden und aktenmäßig belegt werden konnten; die restlichen wurden daraufhin vom BKA gelöscht.

Das Bundeskriminalamt ist an der Speicherung von AIDS-Hinweisen darüber hinaus in der Weise beteiligt, daß es bei Datensätzen, deren Besitzer es ist, auf Wunsch einer Landespolizei den entsprechenden Hinweis eingibt. In diesen Fällen kommt zwar der Anstoß von außen, die Speicherung erfolgt aber in der datenschutzrechtlichen Verantwortung des BKA, da dieses nach den erwähnten Absprachen der Datenbesitzer ist. Eine datenschutzrechtliche Zulässigkeitsprüfung führt das BKA gleichwohl nicht durch.

Der Bundesgrenzschutz hat AIDS-Speicherungen auch im Rahmen seiner Sachaufgaben vorgenommen. Es handelt sich dabei, wie mir der Bundesminister des Innern im Oktober berichtet hat, um insgesamt sechzehn Fälle, von denen fünf zur Grenzfahndung ausgeschrieben und elf weitere im Grenzaktennachweis gespeichert sind. Aus Kapazitätsgründen war es mir bisher nicht möglich, in diesen Einzelfällen die Zulässigkeit der Speicherung zu überprüfen.

Die datenschutzrechtliche Bewertung der AIDS-Speicherungen ist deshalb schwierig, weil einem einmal infizierten Polizeibeamten oder Mithäftling nach heutigen Erkenntnissen medizinisch nicht geholfen werden kann. Es ist deshalb verständlich, wenn jedes Mittel eingesetzt wird, das möglicherweise dazu beiträgt, das Infektionsrisiko zu mindern. Auf der anderen Seite gibt es aber auch kein anderes personenbezogenes Datum, dessen Bekanntwerden den Betroffenen gleich schwer belasten kann. Deshalb ist es aus meiner Sicht wichtig, daß die Frage der Eignung der Speicherung als Mittel zur Eigensicherung der Polizeibeamten im Gesamtzusammenhang mit den anderen von den Polizeiführungen ergriffenen Maßnahmen gesehen wird. Auch sollten die Erfahrungen anderer Länder, zumal solcher mit größerer AIDS-Ausbreitung, ausgewertet werden. Die wichtigsten Argumente, die die Datenschutzbeauftragten veranlaßt haben, Zweifel am Nutzen der AIDS-Speicherung in Polizei-Informationssystemen anzumelden, sind in dem erwähnten Beschluß der Datenschutzkonferenz enthalten.

19.4 Datenabfrage zur Besucherkontrolle

Ein Fachjournalist hat sich verärgert an mich gewandt, weil er an der Pforte des Bundeskriminalamts abgewiesen worden war, als er einen wissenschaftlichen Mitarbeiter des Amtes aufsuchen wollte, der ihm ein Interview zugesagt hatte. Ihm war eröffnet worden, daß „Daten vorhanden" seien, was er sich aber nicht vorstellen konnte.

Meine Überprüfung ergab, daß das Bundeskriminalamt grundsätzlich alle automatisierten Daten abfragt, wenn ein Besucher ihm nicht bekannt ist, und daß es jeden Besucher abweist, über den eine nachteilige polizeiliche Information gefunden wird. Im konkreten Fall hatten Daten eines Landeskriminalamtes, die auf polizeiliche Ermittlungen wegen des Verdachts einer Beleidigung mit politischem Bezug hinwiesen, die Abweisung ausgelöst.

Ich habe das Verfahren beanstandet und vorgeschlagen, künftig von folgenden Grundsätzen auszugehen:

— Die Abfrage von personenbezogenen Daten ist auf die Ermittlung sicherheitsrelevanter Umstände zu beschränken.

— Die Sicherheitsrelevanz der Erkenntnisse muß im Einzelfall und vor dem Hintergrund der sonstigen Sicherheitsmaßnahmen (Besucherbegleitung usw.) bewertet werden.

— Es ist sicherzustellen, daß Dritte, insbesondere der Besuchte, vom Vorhandensein polizeilicher Erkenntnisse nur im unumgänglichen Umfang informiert werden.

Das Bundeskriminalamt hat die Berechtigung meiner Beanstandung zwar nicht anerkannt und geltend gemacht, die Zurückweisung sei in erster Linie deshalb erfolgt, weil der Besucher außerhalb der regulären Dienstzeit gekommen sei. Es hat aber trotzdem zugesagt, das Verfahren der Besucherkontrolle neu zu ordnen.

19.5 Umfang der Auskunft an das Britische Zentralbüro von Interpol

Ein Bürger war anläßlich seiner Einreise nach Großbritannien von der britischen Einwanderungsbehörde zurückgewiesen worden. Als Grund wurden Erkenntnisse deutscher Polizeibehörden angegeben. Er hat sich dann unter Vorlage eines Bescheides der britischen Einwanderungsbehörde an mich gewandt mit der Bitte festzustellen, ob die ihm vorgehaltenen Informationen beim Bundeskriminalamt gespeichert und an die britischen Behörden übermittelt worden sind. Diese Prüfung hat ergeben, daß die dem Petenten vorgehaltenen Angaben eine Teilmenge der Informationen darstellen, die das Bundeskriminalamt an Interpol London im Zusammenhang mit einer dort laufenden Ermittlung wegen Verdachts des Hotel-Einmiet-Betrugs übermittelt hatte. Diese Übermittlung hatte neben Hinweisen auf einschlägige Strafermittlungsvorgänge mehrere Informationen umfaßt (z. B. Selbstmordversuch durch Springen aus einem fahrenden Krankenwagen, Zeiträume und Ort der Verbüßung von Jugendarrest, mehrere Vermißtmeldungen), die in keinem Sachzusammenhang mit dem Anfragegrund standen und deshalb nicht hätten übermittelt werden dürfen. Dies habe ich beanstandet.

Die einschlägige Dienstanweisung, die im Anschluß an die Datenschutzprüfung des Interpol-Auskunftsverkehrs ergänzt worden war (vgl. 5. TB S. 92), sieht vor, daß Erkenntnisse, die offensichtlich nicht im Zusammenhang mit dem Anfragegrund stehen und die das der Anfrage zugrundeliegende Verfahren nicht fördern können, der anfragenden Stelle nicht zu übermitteln sind. Diese Vorschrift wird anscheinend

nicht immer strikt beachtet, wenn der Einfachheit halber der vollständige Inhalt von Fernschreiben der örtlichen Polizeidienststellen weitergeleitet wird. Ich habe deshalb besonders darauf hingewiesen, daß die verfassungsmäßigen Grundsätze für Einschränkungen des Rechts auf informationelle Selbstbestimmung sowie der Verhältnismäßigkeitsgrundsatz eine nähere Bewertung und Filterung der Informationen verlangen.

Bei dem an Interpol London mitgeteilten Selbstmordversuch war der Petent 15 Jahre alt, bei den Vermißtenmeldungen 11 bzw. 14 Jahre. Ich habe deshalb auch auf die Notwendigkeit hingewiesen, die dem Jugendstrafrecht zugrunde liegenden Grundsätze des Jugendschutzes nicht nur bei der Festlegung der Speicherfristen, sondern auch bei der Weitergabe, zumal an ausländische Stellen, zu berücksichtigen und zu prüfen, ob Vorgänge wegen ihres Zusammenhangs mit der Entwicklung des Jugendlichen auszuklammern sind.

Der Bundesminister des Innern hat mir mitgeteilt, daß er meine Auffassung teilt, soweit es um die Vermißtmeldungen geht, und das Bundeskriminalamt entsprechend gebeten hat, im Rahmen des internationalen Nachrichtenaustauschs in Zukunft noch mehr als bisher die Relevanz der übermittelten Erkenntnisse zu prüfen.

Die Mitteilungen über verbüßten Jugendarrest sind dagegen nach Auffassung des Bundesministers des Innern nicht zu beanstanden. Sie seien im Zusammenhang mit der weiteren Mitteilung zu sehen, daß der Petent damals einem Mitgefangenen heißes Wasser ins Gesicht geschüttet habe. Diese Mitteilung hatte ich allerdings auch nicht beanstandet.

Hinsichtlich des mitgeteilten Selbstmordversuchs führt das Bundeskriminalamt jetzt an, es habe sich um einen Fluchtversuch und nicht um einen Selbstmordversuch gehandelt. Für die Annahme eines Selbstmordversuchs habe es keinerlei Anhaltspunkte gegeben. Diese Erklärung ist mir unverständlich, da in der Mitteilung nach London ausdrücklich von einem Selbstmordversuch und nicht von einem Fluchtversuch gesprochen wurde.

Auch meine über den Einzelfall hinausgehenden Überlegungen haben keine positive Resonanz gefunden. Meinem Hinweis auf die Notwendigkeit einer näheren Bewertung und Filterung der Informationen stellt der Bundesminister des Innern die Feststellung entgegen, nach der Dienstvorschrift solle die Nichtübermittlung die Ausnahme darstellen; dieses Verhältnis von Regel und Ausnahme dürfe insbesondere bei der Auslegung in Zweifelsfällen nicht unbeachtet bleiben.

Hinsichtlich der Behandlung Jugendlicher verweist der Bundesminister des Innern auf die Regelung der KpS-Richtlinien, nach denen bei Kindern spätestens nach zwei, bei Jugendlichen spätestens nach fünf Jahren zu prüfen ist, ob eine Aussonderung möglich ist. „Eine darüber hinausgehende Privilegierung" hält er nicht für angemessen.

Ich halte dagegen an meiner Auffassung fest, daß gerade in so empfindlichen Bereichen wie der Datenübermittlung ins Ausland und der Weitergabe von polizeilichen Daten Jugendlicher eine differenziertere Praxis möglich und durch die Verfassungsrechtsprechung auch geboten ist.

19.6 Abgrenzung zwischen Kriminalaktennachweis (KAN) und Vorgangsnachweis Personen (VNP)

Wie bereits mehrfach berichtet (zuletzt 9. TB S. 59) speichert das Bundeskriminalamt Hinweise über Aktenfundstellen, die nicht die Voraussetzungen für eine Einstellung in den Kriminalaktennachweis erfüllen, im Bundeskriminalamt-Aktennachweis (BKA-AN). Die Errichtungsanordnung für den BKA-AN ermöglicht die Erfassung von Hinweisen auf Erkenntnisse aus den kriminalpolizeilichen Meldediensten bis hin zu „sonstigen polizeilich-relevanten Hinweisen". In meiner Stellungnahme vom 11. Oktober 1985 habe ich u. a. eine Konkretisierung dieses Punktes der Errichtungsanordnung gefordert, um sicherzustellen, daß nur tatsächlich relevante Hinweise aufgenommen werden. Eine Antwort des Bundesministers des Innern ist mir bis zum Abschluß dieses Berichts nicht zugegangen.

Nach meiner Aufforderung sollten beim BKA vorhandene Unterlagen, die die eigentliche polizeiliche Aufgabenstellung nicht betreffen, lediglich im Vorgangsnachweis-Personen (VNP) erfaßt werden.

Wie wichtig die Unterscheidung ist, zeigt die Eingabe eines Bürgers, gegen den ein Strafverfahren eingeleitet worden war. Aufgrund eines Vermerks in der Ermittlungsakte vermutete sein Rechtsanwalt eine INPOL-Speicherung. Diese wurde ihm vom BKA auf Anfrage bestätigt. Meine Nachprüfung hat dann ergeben, daß das BKA die vom Rechtsanwalt benannte Polizeidienststelle, die gegen seinen Mandanten ermittelte, um Erkenntnismitteilung ersucht hat – wozu aus meiner Sicht kein Anlaß bestand. Als Antwort erhielt das BKA einen Hinweis auf das neue Strafermittlungsverfahren. Den Hinweis auf diesen Schriftverkehr speicherte das BKA nicht im VNP, sondern im BKA-AN. Damit verwandelte sich die Anfrage des Rechtsanwalts über seinen Mandanten in einen kriminalpolizeilichen Fachvorgang.

Ich halte in solchen Fällen eine Speicherung allenfalls im VNP für zulässig. In dieser Datei können Vorgänge administrativer Art (Vorgänge ohne polizei- oder strafrechtliche Bezüge) erfaßt werden. Im vorliegenden Fall handelt es sich um einen verwaltungsmäßigen Vorgang, der keine polizeifachliche Relevanz besitzt, die eine Speicherung im BKA-AN rechtfertigen würde. Der Bundesminister des Innern hat inzwischen das BKA entsprechend angewiesen.

Den unterschiedlichen Zwecken der vorgenannten Dateien muß auch eine differenzierte Zugriffsberechtigung entsprechen, worauf ich bereits vor Jahren hingewiesen habe (vgl. 4. TB S. 24). So sollte die Zugriffsberechtigung entgegen der bisherigen Praxis innerhalb des BKA auf solche Organisationsein-

heiten beschränkt werden, die administrative Tätigkeit ausüben. Leider ist die von mir vorgeschlagene Änderung der Zugriffsberechtigung bis heute nicht erfolgt.

20 Bundesamt für Verfassungsschutz – Sicherheitsüberprüfungen –

Kurz vor der Fertigstellung dieses Tätigkeitsberichts ist mir die ausführliche Stellungnahme des Bundesministers des Innern zu meinem Prüfbericht vom Januar 1987 über die Kontrolle bei der für Sicherheitsüberprüfungen zuständigen Abteilung V des Bundesamtes für Verfassungsschutz (BfV) zugegangen. Die Auswertung wird noch einige Zeit beanspruchen. Deshalb und wegen der gebotenen Geheimhaltung gehe ich auf Probleme nur in allgemeiner Form ein.

Im Achten Tätigkeitsbericht (S. 49 f.) habe ich über eine Sonderdatei im Rahmen der Sicherheitsüberprüfung beim Bundesamt für Verfassungsschutz berichtet. Sie war Hauptgegenstand meiner datenschutzrechtlichen Kontrolle. In dieser Datei können nach Abschluß einer Sicherheitsüberprüfung deren Ergebnisse in Form von numerisch verschlüsselten Merkmalen gespeichert werden. Unmittelbaren Zugriff auf die Datei hat die Abteilung V des BfV.

Die Kontrolle, die nur unter Schwierigkeiten und mit mehrmaliger Unterbrechung zu Ende geführt werden konnte (vgl. 9. TB S. 55 f.), hat teilweise schwerwiegende datenschutzrechtliche Mängel ergeben, die ich beanstanden mußte. Außerdem habe ich eine Reihe von förmlichen Empfehlungen ausgesprochen.

Meine Beanstandungen beruhen auf grundsätzlichen Rechtsbedenken wie auch auf einer kritischen Bewertung der Handhabung der Sonderdatei. Da bei einer Sicherheitsüberprüfung naturgemäß auch Daten aus dem Kern des Persönlichkeitsbereichs erhoben und bewertet werden müssen, kann eine Speicherung der Ergebnisse in die Nähe eines Persönlichkeitsprofils führen. Hiergegen habe ich unter Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichts, nach der dem Staat der innerste Kern der persönlichen Lebensgestaltung verschlossen bleiben muß, grundsätzlich Bedenken. Ich halte es nur in besonders gelagerten Fallsituationen für zulässig, Daten dieser Art automatisiert zu verarbeiten. Solche Ausnahmegründe habe ich bei der überprüften Datei nicht erkennen können.

Unabhängig davon hat meine Kontrolle ergeben, daß die Datei für die vom Bundesamt angegebenen Zwecke, insbesondere für die Spionageabwehr im Sinne der Aufklärung von Verdachtsfällen, nicht oder nur sehr bedingt geeignet war. Dies hat der Bundesminister des Innern jetzt bestätigt; auch nach seiner Auffassung war eine sinnvolle und aussagekräftige Nutzung der Daten bislang – im Hinblick auf Aufbau der Datei und Datenpflege – kaum möglich. Da nach meiner Auffassung folglich keine überragenden Gründe des Allgemeinwohls für die Erforderlichkeit der Speicherung von Daten dieser Kategorie angeführt werden können, weil die Datei, in der sie verarbeitet werden, nach gegenwärtigem Stand insgesamt für die angegebenen Zwecke praktisch nicht geeignet ist, muß eine Speicherung schon von Verfassungs wegen unterbleiben.

Darüber hinaus habe ich folgende einzelne Mängel beanstandet:

- Belastende Merkmale der hier in Rede stehenden Art wurden auch in Fällen gespeichert, in denen der Sachverhalt dies nicht rechtfertigte oder zweifelhaft geblieben war, ob die Belastungen tatsächlich vorlagen.
- Merkmale wurden gespeichert, obwohl das BfV beim Abschluß der Sicherheitsüberprüfung feststellte, daß ihnen keine Sicherheitsrelevanz zukam.
- Belastende Daten wurden auch zu solchen Personen gespeichert, die nicht in einem sicherheitsempfindlichen Bereich beschäftigt waren oder bei denen das BfV über die Art der Beschäftigung nichts wußte.
- Es wurden zum Teil sehr weit zurückliegende Informationen („Jugendsünden") gespeichert.
- Auch Ehegatten wurden bei bestimmten Überprüfungsarten in die Speicherung einbezogen.
- Informationen wurden oder blieben gespeichert, obwohl sie im Bundeszentralregister längst gelöscht waren.

Mein Prüfbericht enthält noch eine Reihe weiterer Mängelrügen, die im Zusammenhang mit dieser Datei stehen oder sich ganz allgemein auf die Datenverarbeitung bei der Abteilung V des BfV beziehen.

Der Bundesminister des Innern hat die meisten Beanstandungen als berechtigt anerkannt und die Löschung der entsprechenden Datensätze bzw. Einzeldaten veranlaßt. Er hat mich über weitere Einzelweisungen und sonstige Maßnahmen unterrichtet, die im Anschluß an meine Kontrolle eingeleitet worden sind und meinen Bedenken Rechnung tragen sollen. Insbesondere soll in Zukunft durch stete Datenpflege dafür gesorgt werden, daß überholte Daten korrigiert werden. Die gespeicherten Daten sollen in Zukunft auch zeitlich zugeordnet werden, so daß neue und weit zurückliegende Erkenntnisse nicht mehr ununterscheidbar nebeneinander stehen.

Der Katalog der zu speichernden Merkmale soll überprüft und reduziert werden. Welche Informationen in Merkmalsform gespeichert werden, soll präziser bestimmt werden. Zukünftig soll sichergestellt sein, daß nur in der Akte belegte Merkmale gespeichert sind. Der Bundesminister des Innern hat auch die Beseitigung gravierender Mängel in der Datensicherheit zugesagt.

In einem entscheidenden Punkt will der Innenminister allerdings meinen Vorstellungen derzeit noch nicht entsprechen. Statt auf die Speicherung von Daten aus dem Kern des Persönlichkeitsbereichs generell zu verzichten, soll – bei etwa reduziertem Merk-

malskatalog – grundsätzlich an der Speicherung solcher Daten festgehalten werden. Zur Begründung wird nunmehr verstärkt auf Erfordernisse der Spionageabwehr verwiesen und sogar von einer „erweiterten Nutzung" gesprochen. Wegen der besonderen Sensibilität der in der Datei gespeicherten Daten soll aber zunächst ein zweijähriger Probebetrieb durchgeführt werden. Ergänzend hierzu hat mir der Bundesminister des Innern in einem weiteren Schreiben mitgeteilt, daß er im Zusammenhang mit der Umsetzung der neuen Sicherheitsrichtlinien und der Erarbeitung einer „Dienstanweisung für die Durchführung der Sicherheitsüberprüfung" die einzelnen Arbeitsschritte der Sicherheitsüberprüfung beim BfV unter Effektivitäts- wie auch unter datenschutzrechtlichen Aspekten überprüfen werde. Mit der Arbeit werde in Kürze begonnen. Sie soll bis zum 1. Mai 1988 weitgehend abgeschlossen sein. Dabei soll zwischen Sicherheitsinteressen und dem Interesse am Persönlichkeitsschutz abgewogen und geprüft werden, inwieweit die Speicherung von Persönlichkeitsmerkmalen geboten und rechtlich vertretbar ist. Möglicherweise werde es unabhängig vom vorgesehenen Probelauf schon vorzeitig zu einer weiteren Modifizierung der Datei kommen.

Ich werte dies u. a. als Zeichen dafür, daß auch für den vorgesehenen Probelauf vom BMI noch nicht endgültig über die Verwendung von Merkmalen aus der engsten Persönlichkeitssphäre entschieden ist. Aus datenschutzrechtlicher Sicht läßt sich eine Beurteilung der neuen Konzeption nur in Kenntnis der veränderten Verfahrensvorschriften vornehmen.

Problematisch erschiene es mir jedenfalls, wenn die Datei – auch in ihren besonders sensiblen Teilen – so fortgeführt werden sollte, selbst wenn dies auf einer veränderten Grundlage geschähe. Noch in den Jahren 1984 und 1985 war mir zunächst versichert worden, die Speicherung der Merkmale sei aus „statistischen Gründen" bzw. zur Verbesserung der Sicherheitsberatung erforderlich. Die jetzt ins Auge gefaßte Erweiterung auf die Spionageabwehr im Sinne der Aufklärung von Verdachtsfällen wäre für mich auch deshalb überraschend, weil ich im Rahmen meiner Kontrolle festgestellt habe, daß die Datei in ihren besonders sensiblen Teilen dafür bisher nur wenige Male genutzt worden ist.

Die Datenbank ist vom Bundesamt mit erheblichem Aufwand eingerichtet und aufgebaut worden. Deswegen könnte es verständlich erscheinen, wenn nach einer neuen Basis gesucht und dabei an die Spionageabwehr gedacht würde. Jedenfalls aber wäre der mögliche Beitrag der Sonderdatei zur Spionageabwehr abzuwägen gegen die schutzwürdigen Belange der Betroffenen. Es geht dabei um eine Vielzahl Beschäftigter des öffentlichen Dienstes und der Privatwirtschaft. Die Datenspeicherung umfaßt Angaben von teilweise erheblicher Sensibilität. Eine so gravierende Maßnahme ist nur zugunsten überragend wichtiger Gemeinschaftsinteressen zulässig. Ob diese Voraussetzung hier tatsächlich erfüllt ist, erscheint mir – nicht zuletzt auf dem Hintergrund des bisherigen Geschehensablaufs – zweifelhaft.

Ich komme deshalb in bezug auf die von mir besonders kritisierten Teile der Sonderdatei bislang zu der Wertung, daß die Einschränkungen für das informationelle Selbstbestimmungsrecht der Betroffenen zu weitgehend sind, als daß ein bisher jedenfalls fraglicher Sicherheitsgewinn sie rechtfertigen könnte.

21 Bundesnachrichtendienst

Für das abgelaufene Jahr hatte ich geplant, eine 1986 eingeleitete Kontrolle fortzusetzen und mich an der Erarbeitung einer Dienstvorschrift zu beteiligen, durch die der von der Datenverarbeitung betroffene Personenkreis umschrieben und eingegrenzt wird. Beide Vorhaben ließen sich aus Kapazitätsgründen nur ansatzweise verwirklichen.

22 Bundesgrenzschutz

22.1 Kontrolle der Zentralstelle zur Bekämpfung der unerlaubten Einreise von Ausländern bei der Grenzschutzdirektion

Im vergangenen Jahr habe ich die Zentralstelle zur Bekämpfung der unerlaubten Einreise von Ausländern bei der Grenzschutzdirektion (Zentralstelle) in Koblenz kontrolliert. Geprüft wurde die Informationsverarbeitung im polizeilichen Informationssystem INPOL und im Grenzaktennachweis (GAN) (vgl. zum GAN schon 6. TB S. 48 unter Nr. 19; 7. TB S. 71 f. unter Nr. 20.2 und 9. TB S. 63 f. unter Nr. 16.1).

Nach einer Dienstanweisung hat die Zentralstelle alle Erkenntnisse, die für die Bekämpfung der unerlaubten Einreise von Ausländern von Bedeutung sind, zu sammeln, aufzubereiten, zu analysieren und als Grundlage für Gefahrenabwehrmaßnahmen umzusetzen. Darüber hinaus hat sie die von den Grenzdienststellen gemeldeten Erkenntnisse, soweit sie für die Bekämpfung arbeitsrechtlicher Wirtschaftsdelikte (z. B. unerlaubte Arbeitsaufnahme von Ausländern) dienlich sind, zu sammeln, aufzubereiten, auszuwerten und den zuständigen Behörden, Dienststellen und Institutionen zur weiteren Verfolgung mitzuteilen. Diese Aufgaben- und Befugnisbeschreibung wird aus den einschlägigen Regelungen des Bundesgrenzschutzgesetzes abgeleitet, das allerdings keine Vorschriften über die Verarbeitung personenbezogener Informationen enthält. Hierzu gibt es lediglich die Errichtungsanordnung des Bundesministers des Innern, die die Verarbeitung personenbezogener Daten sowohl für die Grenzfahndung als auch für den GAN regelt. Das Fehlen einer den Grundsätzen des Volkszählungsurteils genügenden normenklaren Rechtsgrundlage für die Informationsverarbeitung habe ich bemängelt. Der Bundesminister des Innern hat mir hierzu mitgeteilt, daß die Bundesregierung die zuständigen Gremien veranlaßt habe zu prüfen, ob und inwieweit die für die Erhebung und Verarbeitung personenbezogener Da-

ten im Sicherheitsbereich vorhandenen gesetzlichen Grundlagen präzisiert oder ergänzt werden müssen. Die Bundesregierung sei bestrebt, die Novellierung des Bundesgrenzschutzgesetzes noch in dieser Legislaturperiode durchzuführen. Dies erscheint auch mir geboten.

Im einzelnen erbrachte meine auf verschiedene DV-Auswertungen und Stichproben gestützte datenschutzrechtliche Kontrolle folgende Ergebnisse, zu denen der Bundesminister des Innern im Oktober Stellung genommen hat.

a) Beanstandungen wegen fehlerhafter Datenverarbeitung:

— Speicherung von personenbezogenen Informationen im GAN bei einem Sachverhalt ohne Grenzbezug und damit ohne BGS-Zuständigkeit.

Meine Beanstandung zu einem beispielhaft aufgeführten Einzelfall hat der Bundesminister des Innern anerkannt.

— Ausschreibungen zur Grenzfahndung ohne hinreichende tatsächliche Anhaltspunkte.

Das BGS-Gesetz enthält nur allgemeine Handlungsermächtigungen, aber keine Festlegung, unter welchen materiell-rechtlichen Voraussetzungen Personen im Grenzfahndungsbestand ausgeschrieben werden dürfen. Die Polizeidienstvorschrift 384.2 wird entsprechend angewandt. Danach ist eine Ausschreibung grundsätzlich nur dann zulässig, wenn zumindest tatsächliche Anhaltspunkte dafür vorliegen, daß die Person einer Straftat verdächtig ist, die in den Zuständigkeitsbereich des Bundesgrenzschutzes fällt. Ich stimme mit dem Bundesminister des Innern darin überein, daß Ausschreibungen weiterhin zulässig sind, habe jedoch darauf hingewiesen, daß die Dienstvorschriften nur noch in dem engen Rahmen angewendet werden dürfen, der durch die Rechtsprechung zum Übergangs-Bonus vorgegeben ist.

— Ungleiche Regelfristen für die Ausschreibung zur Grenzfahndung.

Die Frist beträgt sechs Monate für deutsche Staatsangehörige, ein Jahr für Ausländer, ohne daß dies sachlich begründet ist.

— Nichtbeachtung der Kriterien für die Verlängerung von Ausschreibungen zur Grenzfahndung.

Hierzu hat der Bundesminister des Innern meine Anregung aufgenommen, die Gründe einer Verlängerung in der Akte auszuweisen.

— Unzulässige Übermittlungen an Behörden.

Bei der Bearbeitung einer Beschwerde wurden unzulässige Informationen an den Arbeitgeber des Beschwerdeführers (eine Stadtverwaltung) übermittelt.

— Fehlerhafte Auskünfte an Betroffene.

Im gleichen Fall wurde dem Beschwerdeführer, der Auskunft verlangt hatte, nur ein Teil der gespeicherten Daten eröffnet und damit eine falsche Auskunft erteilt.

Beide Beanstandungen hat der Bundesminister des Innern anerkannt.

Ferner habe ich die folgenden Empfehlungen ausgesprochen:

— Asylbewerber, die bei Grenzübertritt zwangsläufig gegen § 47 Ausländergesetz verstoßen, wenn sie keinen Paß bzw. keine Aufenthaltserlaubnis besitzen, sollten nicht gespeichert werden. Die routinemäßige Speicherung in diesen Fällen erscheint mir unangemessen, da das Asylbegehren im Vordergrund steht und auch die Gerichte in aller Regel bei einem solchen Sachverhalt nicht verurteilen. Im übrigen ist mir der Nutzen solcher Speicherungen für das künftige grenzpolizeiliche Handeln nicht ersichtlich.

— Verdächtige Personen sollten im GAN nur für eine kürzere Zeit erfaßt werden, als dies in der Errichtungsanordnung für Beschuldigte vorgesehen ist. Dies wurde zugesagt.

— Bei der Festsetzung der Aussonderungsprüftermine für die im GAN gespeicherten Datensätze halte ich eine flexiblere Handhabung im Sinne kürzerer Fristen für sachgerecht. Auch diese Anregung wurde vom Bundesminister des Innern aufgenommen.

— Wenn die Speicherung auf eine Strafanzeige zurückgeht, sollten die Ergebnisse des Strafverfahrens berücksichtigt werden. Bei Einstellung des Ermittlungsverfahrens bzw. Abschluß des gerichtlichen Verfahrens sind die Aktualität und die Richtigkeit der gespeicherten Daten sowie ihre Speicherungsdauer zu überprüfen. Nach meinen Erkenntnissen geschieht dies tatsächlich aber nur in Ausnahmefällen. Der Bundesminister des Innern verweist darauf, daß die Justizbehörden ihre Verpflichtung zu entsprechenden Mitteilungen weithin nicht erfüllen. Mein Vorschlag, daß die Grenzschutzdirektion in bestimmten Zeitabständen von sich aus bei der Staatsanwaltschaft bzw. den Gerichten nachfragt, wurde insoweit akzeptiert, als künftig nach zwei Jahren die Mitteilung der Justiz angemahnt werden soll.

— Mein Vorschlag, den Datenbestand insoweit auch retrograd zu bereinigen, wurde unter Hinweis auf das Mengenproblem zurückgestellt; die Überprüfung könne nur sukzessive erfolgen. Einen Zeitraum für diese Arbeiten vermochte der Bundesminister des Innern nicht anzugeben. Ich bin der Auffassung, daß dieser Arbeit hohe Priorität eingeräumt werden sollte, da der im GAN gespeicherte Datenbestand insoweit unrichtige Angaben enthält, die von Amts wegen zu löschen oder zu berichtigen sind.

— Aus Anlaß von Beschwerden über Grenzkontrollen sollte eine Speicherung im GAN nicht erfolgen, da hier ein Zugriff sämtlicher Grenzschutzstellen unangemessen erscheint. Die Grenzschutzdirektion wird künftig entsprechend verfahren.

— Eine Ablichtung von Reisedokumenten sollte unterbleiben, wenn die Voraussetzungen für eine erkennungsdienstliche Behandlung nach der Strafprozeßordnung nicht vorliegen. Der Bundesminister des Innern hat die Grenzschutzdirektion entsprechend angewiesen.

— Aus den Dienstvorschriften zum GAN habe ich einige Punkte kritisch angesprochen. Wie bereits früher dargestellt (vgl. 7. TB S. 71, Nr. 20.2.1 erster Anstrich; 8. TB S. 44 f.; 9. TB S. 63, Nr. 16.1, zweiter Anstrich) können im Datenfeld „Sondervermerk" in der Datengruppe „rechtmäßige Personalien" sog. personengebundene Hinweise (PHW) registriert werden, z. B. „Benutzer grüne Grenze" (s. zur Problematik der PHW auch unter 20.4). Die Errichtungsanordnung ist insoweit nicht abschließend, so daß je nach Bedarf und Aktualität neue Hinweise aufgenommen werden können.

  Da der Bundesminister des Innern die Speicherung für erforderlich hält, habe ich gebeten, mir zur näheren Prüfung die bisher verwendeten Begriffe und die Häufigkeit ihrer Vergabe mitzuteilen. Der Bundesminister des Innern sieht jedoch leider „einen zeit- und arbeitsaufwendigen EDV-Ausdruck in keinem Verhältnis zur Notwendigkeit".

Ich habe den Bundesminister des Innern um erneute Prüfung der noch offenen Punkte gebeten und hoffe auf weitere Verbesserungen.

22.2 Bewerbungsverfahren

Wer sich zum Bundesgrenzschutz (oder zum Polizeivollzugsdienst eines Landes) bewirbt, muß damit rechnen, daß bei seiner örtlichen Polizeidienststelle eine umfassende Auskunft zu seiner Person eingeholt wird. Dazu dient ein bundeseinheitlich eingeführtes Formular, das u. a. folgende Fragen enthält:

— Leumund

— Erkenntnisse, soweit sie für die Entscheidung über die Einstellung von Bedeutung sind; insbesondere über Vorleben, Auftreten und Verhalten, Umgang, Familienverhältnisse. Lebt der Bewerber im übrigen in geordneten Verhältnissen?

— Wirtschaftliche Verhältnisse (soweit bekannt).

Ein 17jähriger Bewerber hat sich an mich gewandt, da er vom Bundesgrenzschutz abgewiesen wurde, nachdem durch die polizeiliche Auskunft bekannt geworden war, daß er im Alter von vierzehn Jahren in einem Kaufhaus eine Spielzeugfigur entwendet hatte. Das Gericht hatte das Jugendgerichtsverfahren seinerzeit mit einer mündlichen Verwarnung eingestellt; eine Eintragung im Erziehungsregister erfolgt in solchen Fällen nicht.

Ich habe die Verfahrensweise des Bundesgrenzschutzes generell beanstandet. Zum einen kann es nicht die Aufgabe örtlicher Polizeidienststellen sein, über Bürger ihres Bezirks im Falle einer Bewerbung zum öffentlichen Dienst allgemeine Eignungsurteile abzugeben. Auch wenn man mit dem BGS die Anfrage als Teil der Sicherheitsüberprüfung ansieht, ist eine Auskunft im bisher praktizierten Umfang nicht gerechtfertigt. Zum anderen dürfen Auskünfte nicht in einer Weise eingeholt werden, daß tragende Grundsätze des Jugendstrafrechts umgangen werden. Wenn schon im Erziehungsregister eingetragene Jugendstrafen den Einstellungsbehörden nicht mitgeteilt werden dürfen (vgl. § 31 BZRG) und vom Betroffenen nicht offenbart zu werden brauchen (§ 64 BZRG), so muß dies erst recht für Jugendverfehlungen gelten, bei denen das Gericht eine mündliche Verwarnung für ausreichend gehalten hat.

Der Bundesminister des Innern hat meine Beanstandung anerkannt und dem Petenten eine neue Bewerbung ermöglicht. Maßnahmen zur generellen Korrektur des Verfahrens sowie zur Anpassung an die Sicherheitsüberprüfungsrichtlinien sind eingeleitet. Einzelheiten sind mir noch nicht bekannt.

23. Zollfahndung, Zollkriminalinstitut

Bei der Praxis der zollrechtlichen Überwachung besteht eine äußerst unbefriedigende Situation. Die zollrechtliche Überwachung ist eine Sonderform der polizeilichen Beobachtung, bei der wie folgt verfahren wird:

Das Zollkriminalinstitut schreibt in einem besonderen Bereich der Fahndungsdatei Personen zu dem Zweck aus, sie an der Grenze besonderen zollrechtlichen Maßnahmen (z. B. Anhalten, Durchsuchungen, Überholungen von Beförderungsmitteln und Personen) zu unterziehen, wobei die Tatsache der Ausschreibung den Betroffenen nicht bekannt werden soll. Die Durchsuchung kann auch die körperliche Durchsuchung und zwar mitunter auch von mitreisenden Ehegatten und Kindern umfassen.

Mich erreichen in steigender Zahl Beschwerden von Personen, die an der Grenze aus für sie unerklärlichen Gründen immer wieder intensiv kontrolliert werden.

— So wandte sich eine junge Frau, die im Ausland studierte und bei ihren Heimreisen oft durchsucht wurde, in der zutreffenden Vermutung an mich, daß Daten über sie gespeichert seien. Aus den Unterlagen, die mir für eine Kontrolle des Falles zugänglich waren, ergab sich, daß der Anfangsverdacht auf einen anonymen Hinweis zurückging, wonach sie ständig Rauschgift aus Holland und aus New York hole. Das staatsanwaltschaftliche Ermittlungsverfahren wurde alsbald eingestellt.

— Auf Antrag einer Polizeidienststelle, die einen vertraulichen Hinweis erhalten hatte, der Petent handele vermutlich mit Heroin, wurde diese ohne weitere Prüfung der tatsächlichen Vorausset-

zungen vom Zollkriminalinstitut zur zollrechtlichen Überwachung ausgeschrieben. Aus der mir vorgelegten Ermittlungsakte war keine Grundlage zur Beurteilung der Zuverlässigkeit des Hinweises zu entnehmen. Eine aufgrund der Ausschreibung erfolgte zollrechtliche Durchsuchung hatte auch keinerlei Verdachtsmomente ergeben.

— Ebenfalls auf Antrag einer Polizeidienststelle wurden zwei andere Petenten zur zollrechtlichen Überwachung ausgeschrieben, deren Fahrzeuge auf einem bestimmten Platz in Spanien gesehen worden waren, wo nach Auffassung der spanischen Polizei möglicherweise mit Rauschgift gehandelt und von wo aus Rauschgift in die Bundesrepublik transportiert wird. Die spanische Polizei hatte eine Liste von Kfz-Kennzeichen geliefert; die Halter wurden vom Zollkriminalinstitut ausgeschrieben. Die Unterlagen des Zollkriminalinstituts ergaben aber keinerlei positive Hinweise dafür, daß die Petenten tatsächlich als Rauschgiftschmuggler in Betracht kommen.

Die Probleme gehen zu einem wesentlichen Teil darauf zurück, daß nicht einwandfrei geklärt ist, welche Stelle die datenschutzrechtliche Verantwortung für die Ausschreibung trägt. Da das Zollkriminalinstitut die Ausschreibung in eigener Zuständigkeit vornimmt, bin ich der Auffassung, daß es auch in vollem Umfang dafür verantwortlich ist, daß die Ausschreibung nur erfolgt, wenn sämtliche Voraussetzungen vorliegen. Unstreitig ist, daß eine Speicherung dann und nur dann zulässig ist, wenn die begründete Vermutung besteht, daß die betreffende Person „in nicht unerheblichem Umfang als Schmuggler auftreten" wird (Polizeidienstvorschrift 384.2). Nach meiner Auffassung muß das Zollkriminalinstitut vom Vorliegen dieser Voraussetzung überzeugt sein, wobei es sich allerdings in der Regel darauf verlassen kann, daß ein von einer Polizeibehörde ermittelter und ihr mitgeteilter Sachverhalt auch tatsächlich zutrifft. Die Bewertung jedoch, ob dieser Sachverhalt die Maßnahme der Ausschreibung rechtfertigt, liegt in vollem Umfang beim Zollkriminalinstitut.

Der Bundesminister der Finanzan erkennt eine solche datenschutzrechtliche Verantwortung des Zollfahndungsdienstes nur bedingt an. Wie er mir mitteilte, „beschränkt sich die Prüfung bei Ausschreibungsersuchen von Polizeibehörden schon wegen der beschränkten Nachprüfungsmöglichkeiten der Zollverwaltung nur auf eine Schlüssigkeitsprobe". Das Zollkriminalinstitut prüft demgemäß nur, ob die von einer Polizeidienststelle mitgeteilten Tatsachen nicht in sich widersprüchlich oder sonst offensichtlich fehlerhaft sind. Auch wenn das Zollkriminalinstitut eine rechtliche Bewertung des mitgeteilten Sachverhalts selbst vornimmt – wie der BMF mehrfach betont hat –, wird seine Entscheidung, ob eine Ausschreibung erfolgen soll, praktisch von der jeweiligen Polizeidienststelle vorausbestimmt.

Aufgrund der mir bekannten Einzelfälle muß ich annehmen, daß von dem Instrument der zollrechtlichen Überwachung auch im übrigen großzügig Gebrauch gemacht wird und es infolgedessen zu einer großen Zahl schwerwiegender Eingriffe in das Persönlichkeitsrecht der Betroffenen kommt. Ich habe zwei der vorstehend geschilderten Einzelfälle gegenüber dem Bundesminister der Finanzen beanstandet.

Eine genauere Überprüfung dieser Praxis ist deshalb dringend geboten, zumal die Betroffenen selbst sich wegen der Geheimhaltung der Maßnahme praktisch nicht wehren können. Ich empfinde es deshalb als schwer erträglich, daß der Bundesminister der Finanzen mir jegliche systematische Kontrolle verwehrt. Seine Berufung auf das Steuergeheimnis halte ich für rechtlich unbegründet und der Interessenlage nicht angemessen. Mit der verfassungsrechtlichen Rechtsprechung zum informationellen Selbstbestimmungsrecht ist es nicht vereinbar, die zum Schutz der Inhaber dieses Rechts gebotene unabhängige Datenschutzkontrolle mit dem Argument zu verhindern, dadurch würde das Steuergeheimnis der Betroffenen verletzt.

24. Verteidigung

24.1 Militärischer Abschirmdienst

Die Datenverarbeitung beim Militärischen Abschirmdienst ist derzeit im Umbruch begriffen. Durch die Neukonzeption bestehender Dateien soll in Zukunft eine umfassendere und aussagefähigere Informationsverarbeitung erreicht werden.

Vor einem Jahr hatte ich kritisiert (vgl. 9. TB S. 65), daß der Bundesminister der Verteidigung beabsichtigte, in diesem Zusammenhang die Merkmale aus dem Bereich der innersten Persönlichkeitssphäre, die insbesondere im Rahmen von Sicherheitsüberprüfungen bekannt wurden und als sicherheitserheblich bewertet worden sind, wieder zu speichern, obwohl ich ihre Speicherung im Jahre 1982 beanstandet hatte. Alle Merkmale dieser Art waren aufgrund dieser Beanstandung seinerzeit gelöscht worden.

Der Bundesminister der Verteidigung teilte mir daraufhin mit, über die Wiedereinführung der automatisierten Speicherung der Merkmale aus der Intimsphäre sei noch nicht endgültig entschieden. Die technischen Voraussetzungen für die Zugriffsschutzmaßnahmen seien noch nicht geschaffen; deshalb werde zunächst von der Erfassung der Merkmale abgesehen. Ein vereinbartes Gespräch über die strittigen Punkte fand wegen Terminschwierigkeiten seitens des Ministeriums bislang nicht statt.

24.2 Wehrpflichtige und Soldaten

Im Berichtsjahr haben sich wieder viele Wehrpflichtige und Soldaten an mich gewandt und um Beratung oder Hilfe beim Umgang mit personenbezogenen Daten im Bereich des Bundesministers der Verteidigung gebeten. In einer Vielzahl von Fällen konnte ich in guter Zusammenarbeit mit der für den

Datenschutz bei Bundesminister der Verteidigung zuständigen Stelle die Probleme der Betroffenen bereinigungen und teilweise auch über den Einzelfall hinaus für Verbesserungen sorgen.

Besonders hervorheben möchte ich in diesem Zusammenhang immer wieder auftauchende Fragen, die den Umgang mit Gesundheits-Unterlagen und deren Aufbewahrung betreffen. So bedarf es noch der rechtlichen Klärung, wie Gesundheits-Unterlagen (z. B. Atteste) zu behandeln sind, die der Betroffene selbst, z. B. bei der Musterung, einreicht. Lösungen werden mit dem Bundesminister der Verteidigung noch diskutiert, auch sollten die Betroffenen umfassender aufgeklärt werden. Ebenfalls in diesen Bereich fiel eine Einzeleingabe, in der danach gefragt wurde, ob personenbezogene Daten erhoben werden dürfen, um mit deren Hilfe die Krankheit Alkoholismus zu diagnostizieren, und ob der dafür verwendete Fragebogen Bestandteil der Gesundheits-Unterlagen werden dürfe. Der Fragebogen ist ein bewährtes Hilfsmittel für die Truppenärzte, wenn ein Soldat wegen Verdachts auf Alkoholismus untersucht werden soll. Ich halte die korrekte Verwendung dieses Fragebogens und damit die Erhebung der personenbezogenen Daten für unbedenklich. An dieses Beispiel habe ich aber die grundsätzliche Frage geknüpft, warum Fragebogen oder Tests, die lediglich dem Nachweis einer medizinischen Diagnose dienen, genau so lange aufbewahrt werden müssen, wie alle übrigen Gesundheits-Unterlagen. Diese werden 90 Jahre lang nach dem Geburtsjahr aufbewahrt und danach vernichtet (z. B. Geburtsjahr 1935, Archivierung bis 2025, Vernichtung 2026). Im Interesse des Persönlichkeitsschutzes von Soldaten und Wehrpflichtigen sollte überprüft werden, ob nicht solche Gesundheits-Unterlagen, deren Inhalt von vielen als peinlich empfunden wird, kürzeren Aufbewahrungsfristen unterworfen werden können.

In meinem Neunten Tätigkeitsbericht (S. 67 f.) habe ich über den Umgang mit KDV-Unterlagen berichtet. Zur Aufbewahrung der im Anerkennungsverfahren angefallenen Unterlagen nicht anerkannter Kriegsdienstverweigerer hat der Bundesminister der Verteidigung inzwischen entschieden, daß die gesamten in einem Anerkennungsverfahren angefallenen Unterlagen *abgelehnter* Kriegsdienstverweigerer im verschlossenen Umschlag bis zum Ausscheiden des Antragstellers aus der Wehrüberwachung aufzubewahren sind. Nach § 24 Wehrpflichtgesetz endet die Wehrüberwachung bei Offizieren mit Ablauf des Jahres, in dem sie das 60., bei Unteroffizieren, in dem sie das 45., und bei Mannschaften sowie ungedienten Wehrpflichtigen, in dem sie das 32. Lebensjahr vollenden, im Falle des § 51 des Soldatengesetzes (Wiederverwendung von Berufssoldaten) mit Vollendung des 65. Lebensjahres. Nach dem Ausscheiden aus der Wehrüberwachung sind dann alle Unterlagen mit Ausnahme der letzten bestandskräftigen bzw. rechtskräftigen Entscheidung über den Antrag und der Sitzungsniederschrift zu vernichten. Entscheidung und Niederschrift werden – ebenfalls im verschlossenen Umschlag – bis zum Ende der Wehrpflicht aufbewahrt, also bei Wehrpflichtigen mit Mannschaftsdienstgrad bis zum 45., bei Unteroffizieren und Offizieren bis zum 60. Lebensjahr. Dieses Verfahren kann ich akzeptieren.

Die Aufbewahrungsmodalitäten der Unterlagen *anerkannter* Kriegsdienstverweigerer, die bei den zum Geschäftsbereich des Bundesministers der Verteidigung gehörenden Ausschüssen für Kriegsdienstverweigerung aufzubewahren und nicht an das Bundesamt für den Zivildienst abzugeben sind, müssen noch zwischen dem Bundeswehrverwaltungsamt und dem Bundesamt für den Zivildienst geregelt werden. Zum Zeitpunkt der Erstellung dieses Berichts lag ein Vorschlag für eine solche Regelung noch nicht vor.

Bisher ist der Bundesminister der Verteidigung nicht auf meine Anregungen eingegangen, Sonderregelungen für diejenigen zu schaffen, die ihren Antrag auf Anerkennung zurückziehen oder notwendige Unterlagen (auch nach Mahnung) nicht einreichen und damit bewirken, daß der Antrag abgelehnt wird. Mir kommt es darauf an, daß ein Betroffener nicht deshalb, weil er einmal versucht hat, den Wehrdienst zu verweigern, von bestimmten Aufgaben bei der Bundeswehr ausgeschlossen wird. Ich werde mich weiter bemühen, dies beim Bundesminister der Verteidigung zu erreichen.

25. Wirtschaftsverwaltung

25.1 Bundesamt für Wirtschaft

25.1.1 Organisatorische Mängel

Die Kontrolle des Bundesamtes für Wirtschaft (BAW) war ursprünglich als Querschnittsprüfung aller Fachabteilungen des Bundesamtes angelegt. Es wurde jedoch zu Beginn der Prüfung rasch deutlich, daß die Voraussetzungen für eine ordnungsgemäße Datenschutzkontrolle beim Bundesamt derzeit nicht gegeben waren, weil auch elementare Vorkehrungen zur Sicherstellung des Datenschutzes fehlten. So gab es im Februar 1987 keine vollständige und aktuelle Übersicht gemäß § 15 Satz 2 Nr. 1 BDSG über die beim Bundesamt vorhandenen Dateien und das Amt hatte daher auch keinen Überblick darüber, in welchen Organisationseinheiten des Hauses welche personenbezogenen Daten zu welchen Zwecken und in welcher Art und Weise verarbeitet wurden. Es existierten lediglich einzelne Dateimeldungen verschiedener Referate, die ohne eine erkennbare Systematik abgelegt waren. Dem Bundesamt war es auch unter Zuhilfenahme dieser Aufzeichnungen nicht möglich, die Datenverarbeitung einzelner Organisationseinheiten zu Prüfungszwecken ausreichend zu beschreiben. Allgemeine Anordnungen zum Datenschutz und Bestimmungen zur Meldung neuer oder Abmeldung nicht mehr geführter Dateien bestanden nicht. Nach dem Inkrafttreten des BDSG hat eine Kontrolle der Einhaltung der Meldepflichten nicht stattgefunden.

Das Fehlen der Übersicht, die eine grundlegende Voraussetzung für die Einhaltung der Vorschriften des Datenschutzes darstellt, habe ich gegenüber

dem Bundesminister für Wirtschaft beanstandet, da er insoweit seiner Aufgabe nicht nachgekommen ist, die Ausführung des Bundesdatenschutzgesetzes in seinem Geschäftsbereich sicherzustellen. Das Bundesamt hat inzwischen einen von anderen Aufgaben bis auf weiteres freigestellten Beauftragten für den Datenschutz bestellt und noch weitere Maßnahmen zur Reorganisation des Datenschutzes ergriffen. Mit einer Hausordnung sollen die Bediensteten auf die grundlegenden Regelungen des BDSG einschließlich der Datensicherung sowie auf Aufgaben und Zuständigkeiten des Beauftragten für den Datenschutz und ihre eigenen Pflichten beim Umgang mit personenbezogenen Daten hingewiesen werden. Eine regelmäßige Erinnerung an die Meldepflichten nach dem BDSG soll gewährleisten, daß die inzwischen gefertigte Übersicht über die Datenverarbeitung des Amtes stets ein aktuelles und vollständiges Bild vermittelt.

Ich beabsichtige, die übrigen Abteilungen des Bundesamtes und die Personaldatenverarbeitung im Jahre 1988 zu prüfen.

25.1.2 Förderung der Unternehmensberatung

Das Bundesamt für Wirtschaft ist nach den Richtlinien über die Förderung von Unternehmensberatungen für kleine und mittlere Unternehmen vom 6. Dezember 1984 die Behörde, die diese Subvention zu bewilligen hat. Im Rahmen der Bearbeitung der Förderungsanträge der Unternehmen speichert das Bundesamt auch Angaben über den an dem Subventionsverhältnis rechtlich unbeteiligten Unternehmensberater. Erfaßt werden neben dem Namen und der Anschrift eine Beraternummer und ein Schlüsselzeichen, dem sich entnehmen läßt, ob der Berater wegen in seiner Person liegender Bezuschussungshindernisse „gesperrt" ist, d. h. von ihm durchgeführte Beratungen zukünftig nicht gefördert werden, oder ob er in der Vergangenheit schon einmal gesperrt gewesen war.

Ich halte diese Datenspeicherung für sehr problematisch, weil sie für die Aufgabenwahrnehmung des Bundesamtes nicht erforderlich ist und einer Datenspeicherung auf Vorrat gleichkommt.

Das Förderungsverfahren vollzieht sich in zwei Schritten. Die Richtlinien sehen vor, daß die Förderungsanträge bei sog. Leitstellen – Verbänden des Handels, des Handwerks und der Industrie sowie deren Untergliederungen – eingereicht werden. Aufgabe der Leitstellen ist es, den Antrag und die eingereichten Unterlagen formal und inhaltlich zu prüfen und mit dem Ergebnis dieser Prüfung an das Bundesamt weiterzuleiten. Gegenstand der Prüfung durch die Leitstellen ist dabei auch, ob die Beratung entsprechend den Richtlinien von einem selbständigen Berater durchgeführt wurde, der die für den Beratungsauftrag erforderlichen Fähigkeiten besitzt und über die notwendige Zuverlässigkeit verfügt. Sobald die Leitstelle die Förderungsvoraussetzungen bejaht oder verneint hat und dieses Ergebnis mit oder ohne nochmalige Nachprüfung vom Bundesamt übernommen wird, sobald also eine Entscheidung über das Vorliegen der beraterbezogenen Zuschußvoraussetzungen getroffen ist, fehlt für eine weitere Speicherung der Daten über Berater die Erforderlichkeit. Das Verwaltungsverfahren, zu dessen Durchführung diese Daten gebraucht werden, ist abgeschlossen.

Der Bundesminister für Wirtschaft und das Bundesamt halten gleichwohl bislang an der Speicherung dieser Daten mit dem Argument fest, anders sei nicht zu ermitteln, ob bereits Beratungen eines Beraters gefördert wurden, bei dem die beraterbezogenen Bezuschussungsvoraussetzungen nicht vorlagen. Dieses Argument ist jedoch nur dann verständlich, wenn – anders als es die Richtlinien vorsehen – eine inhaltliche Prüfung der Selbständigkeit, Fachkunde und Zuverlässigkeit des Beraters gar nicht stattfindet, sondern diese Voraussetzungen ungeprüft unterstellt werden. Sollten sich später bei einer Stichprobe oder sonst im Einzelfall Unregelmäßigkeiten herausstellen, können sämtliche geförderten Beratungen des betreffenden Beraters wieder aufgefunden und mit dem Ziel einer eventuellen Rücknahme der Förderungsentscheidung erneut überprüft werden. Dieses Verfahren mag im Hinblick auf den anderenfalls höheren Verwaltungsaufwand sinnvoll sein. Die Vorratsspeicherung der Beraterdaten läßt sich damit jedoch nicht rechtfertigen. Mangels einer gesetzlichen Verarbeitungsgrundlage muß sich das Bundesamt entscheiden, entweder den Berater um seine Einwilligung zur Speicherung seiner personenbezogenen Daten zu bitten oder – ohne eine derartige Speicherung – eine inhaltliche Prüfung der Zuschußvoraussetzungen in jedem Einzelfall durchzuführen. Der Bundesminister für Wirtschaft hat mir hierzu inzwischen mitgeteilt, daß er prüfen werde, ob in künftigen Fällen die Einwilligung der Berater eingeholt werden kann.

Außer der Speicherung der Beraterdaten halte ich es datenschutzrechtlich für bedenklich, daß der antragstellende Unternehmer seinen Förderungsantrag über eine Leitstelle einreichen muß. Er wird damit, ohne daß es von der Sache her erforderlich wäre, gezwungen, einer dritten Stelle Kenntnis von seinem Antrag und, da diesem auch der Beratungsbericht beizufügen ist, Kenntnis auch von Interna seines Betriebes zu gestatten. Da diejenigen, die auf diese Weise Informationen über ihn erhalten können, in aller Regel Berufskollegen oder Konkurrenten sind, ist es nicht auszuschließen, daß mancher deswegen auf die staatliche Förderung einer Unternehmensberatung verzichtet. Aus diesem Grund muß die Möglichkeit geschaffen werden, einen Förderungsantrag auch unmittelbar beim Bundesamt selbst stellen zu können.

25.2 Filmförderungsanstalt

Die Filmförderungsanstalt (FFA), Bundesanstalt des öffentlichen Rechts, darf seit Jahresbeginn zur Finanzierung ihrer vielfältigen Aufgaben im Bereich der wirtschaftlichen Förderung des deutschen Films eine weitere Abgabe erheben. Neben die bereits bestehende Filmabgabe gemäß § 66 Filmförderungsgesetz, zu der jeder Veranstalter einer entgeltlichen Filmvorführung veranlagt wird, ist gemäß § 66 a die-

ses Gesetzes die Filmabgabe der Videowirtschaft getreten. Nach dieser Bestimmung ist grundsätzlich abgabepflichtig, wer „als Gewerbetreibender aus dem Verkauf, aus der Vorführung oder Vermietung von Bildträgern, die mit Filmen mit einer Laufzeit von mehr als 58 Minuten bespielt sind, an Letztverbraucher einen Jahresumsatz von mehr als DM 80.000 erzielt".

Die Erhebung dieser Abgabe erweist sich für die FFA als schwierig, weil das Filmförderungsgesetz keine Bestimmungen darüber enthält, bei welchen Stellen die Anschriften derjenigen ermittelt werden können, die ein entsprechendes Gewerbe angemeldet haben. Das Gesetz sieht weder vor, daß etwa die Gewerbeämter der FFA die entsprechenden Daten übermitteln, noch enthält es eine Verpflichtung der Gewerbetreibenden, abgabepflichtige Umsätze von sich aus an die FFA zu melden. Da es aktuelle und vollständige Verzeichnisse von Videotheken nicht gibt, mußte sich die FFA, um ihre Aufgabe durchführen zu können, ungewöhnlicher Mittel und Möglichkeiten zur Ermittlung der Abgabepflichtigen bedienen. So hat sie zu diesem Zweck sämtliche Branchenverzeichnisse der Bundespost ausgewertet und Adreßbestände eines Direktwerbeunternehmens angekauft.

Außerdem hat die FFA Industrie- und Handelskammern und Gewerbeämter um die Übermittlung der Anschriften von Videothekaren gebeten. Unter den Anschriften, die von diesen Stellen an die FFA übermittelt worden sind, befanden sich auch solche von Gewerbetreibenden, die nach ihrer Geschäftstätigkeit gar nicht abgabepflichtig waren. Sie waren in dem jeweiligen Datenbestand nur deshalb erfaßt und an die FFA übermittelt worden, weil ihr Geschäftstyp eine gewisse Nähe zum Verkauf oder zur Vermietung von Videokassetten hat und abgabepflichtige Vorgänge, wie etwa beim Handel mit Unterhaltungselektronik, vermutet wurden. Die Betroffenen fühlten sich mit Recht durch das anschließende Erhebungsverfahren der FFA, bei dem sie zur Angabe ihres Umsatzes aus der Vermietung und dem Verkauf von Videokassetten aufgefordert wurden, beschwert. Zum Teil haben sie sich an die zuständigen Landesbeauftragten für den Datenschutz und vereinzelt auch an mich gewandt. Bei der Prüfung der Frage, ob die Datenübermittlungen durch Industrie- und Handelskammern sowie Gewerbeämter nach dem jeweiligen Landesrecht zulässig waren, haben die Landesbeauftragten mit unterschiedlicher Akzentuierung, jedoch einheitlicher Tendenz darauf hingewiesen, daß die Generalklauseln des Landesdatenschutzrechts nach den verfassungsrechtlichen Vorgaben keine taugliche Grundlage für derartige Datenübermittlungen seien und es einer bereichsspezifischen Übermittlungsnorm bedürfe.

Ich habe diesen Vorgang zum Anlaß genommen, den Bundesminister für Wirtschaft auf die Notwendigkeit der Schaffung einer Erhebungsgrundlage hinzuweisen. Hier zeigt sich beispielhaft, daß es nicht ausreicht, einer öffentlichen Stelle eine Aufgabe zu übertragen, ohne zu regeln, wo und auf welche Weise sie die personenbezogenen Angaben erheben darf, die sie braucht, um diese Aufgabe durchzuführen. Wenn keine tragfähige Grundlage für die Erhebung der Adreßdaten der Abgabepflichtigen geschaffen wird, ist abzusehen, daß die Erhebung der Filmabgabe der Videowirtschaft undurchführbar werden wird, weil die wirtschaftsverwaltenden Stellen in den Ländern und Gemeinden wegen der fehlenden Rechtsgrundlage keine Daten mehr an die FFA übermitteln werden. Eine Bestimmung über die Erhebung der Adreßdaten der Abgabepflichtigen ist nicht zuletzt auch zur Datenpflege erforderlich. Wenn die FFA ihren Datenbestand nicht laufend aktualisiert, werden die gespeicherten Daten schnell veraltet sein. Eine gleichmäßige und gerechte Erhebung der Abgabe dürfte dann nicht mehr gewährleistet sein; die FFA wird nach kurzer Zeit vor denselben Problemen wie bei der Ersterhebung der Abgabe stehen.

Diese Problematik stellt sich in rechtlicher Hinsicht grundsätzlich auch bei der Erhebung der Filmabgabe nach § 66 FFG Filmförderungsgesetz. Der Bundesminister für Wirtschaft, der zu einer Ergänzung des Gesetzes grundsätzlich bereit ist, sollte deshalb auch hier die Schaffung einer gesetzlichen Erhebungsgrundlage vorsehen.

26. Nicht-öffentlicher Bereich

26.1 Allgemeine Feststellungen

Eine Fortentwicklung des Datenschutzes ist im Bereich der Privatwirtschaft auch vier Jahre nach der Präzisierung der verfassungsrechtlichen Vorgaben durch das Volkszählungsurteil nur ansatzweise zu verzeichnen. Im Vergleich zum Datenschutz im öffentlichen Bereich ist die informationelle Selbstbestimmung der Bürger bei ihrer Teilnahme am Wirtschaftsleben in wichtigen Bereichen weitgehend noch nicht gewährleistet. Während bei öffentlichen Stellen das Bewußtsein dafür zunimmt, daß der Umgang mit personenbezogenen Informationen in der Regel einen Eingriff in das Persönlichkeitsrecht des Betroffenen darstellt und einer Rechtsgrundlage bedarf, wird dieser Aspekt in der Privatwirtschaft häufig vernachlässigt. Zwischen öffentlichem Bereich und Privatwirtschaft besteht ein deutliches Datenschutz-Gefälle. Für die Privatwirtschaft dienen personenbezogene Informationen in erster Linie als Mittel zur Erreichung eines Geschäftszwecks; das Datenschutzbewußtsein ist deshalb oft auf die technischen und organisatorischen Probleme der Datensicherung verengt. Und selbst da, wo die individualrechtliche Dimension der Verarbeitung personenbezogener Daten gesehen wird, fehlt in der Regel die Bereitschaft zur Verwirklichung effektiven Datenschutzes für den Verbraucher. Dem entspricht, daß auch die Anforderungen, die im Bundesdatenschutzgesetz für die Privatwirtschaft an die Verarbeitung personenbezogener Daten – im 3. und 4. Abschnitt des Gesetzes – aufgestellt werden, ungleich weniger differenziert und einschneidend sind als die Regeln für den öffentlichen Bereich.

Wie großzügig mit den schutzwürdigen Belangen Betroffener zuweilen umgegangen wird, zeigt sich

beispielhaft, wenn etwa ein Versandhandelsunternehmen ein bundesweites Verzeichnis in seinem Datenbestand speichert, in dem einzelne Adressen – wenngleich ohne Nennung des Namens – bis hin zu ganzen Straßenzügen mit Bemerkungen wie „asozial" oder „Vorsicht" versehen sind, und alle diejenigen, die unter einer entsprechenden Anschrift bestellen, von der Belieferung ausschließt. Etwas ähnliches wäre heute im öffentlichen Bereich undenkbr.

Besonders deutlich werden die unterschiedlichen Standards dort, wo der einzelne Bürger als Verbraucher oder Kunde Rechtsgeschäfte mit marktmächtigen, wirtschaftlich starken Wirtschaftsunternehmen eingeht, die den Umgang mit den personenbezogenen Angaben des Betroffenen bei der Vertragsdurchführung in ihren Vertragsbedingungen einseitig regeln, ohne daß dem Betroffenen die Möglichkeit bliebe, hierauf Einfluß zu nehmen. Versicherungsunternehmen, Versandhäuser, Wohnungsbaugesellschaften und andere Unternehmen treten dem Bürger dabei ähnlich überlegen gegenüber wie die öffentliche Gewalt. Sie stützen ihren Datenbedarf und ihre Datenverarbeitung dabei in vielen Fällen auf sogenannte Einwilligungen des Betroffenen, etwa zur Datenübermittlung an Dritte. Meist sind diese Klauseln so tief im „Kleingedruckten" versteckt, daß sie vom Betroffenen kaum bemerkt werden. Ist das aber einmal der Fall und ist der Betroffene dann nicht bereit, die erwünschte Erklärung abzugeben, kommt auch der Vertrag insgesamt nicht zustande. In der Praxis ist eine derartige formularmäßige Einwilligung für den Betroffenen mithin kein selbstbestimmter freiwilliger Entschluß, sondern ein faktischer Zwang. Mit einer wirklichen Einwilligung weist sie allenfalls noch formale Gemeinsamkeiten auf. Dieser Umstand führt dazu, daß das Grundrecht auf informationelle Selbstbestimmung, das im Wege der mittelbaren Drittwirkung auch auf die Rechtsbeziehungen zwischen Privaten einwirken soll, in weiten Bereichen des Wirtschaftslebens gerade keinerlei Wirkung entfaltet. Für den Mietbewerber etwa, der zum Abschluß eines Mietvertrages der Vermietungsgesellschaft erheblich weitergehende Einblikke in seine persönliche Sphäre gestatten muß, als sie etwa bei der Volkszählung von ihm verlangt wurden, wird dieses Grundrecht ebenso fragwürdig wie für denjenigen, der beim Abschluß eines privaten Kranken- oder Unfallversicherungsvertrages dem Versicherungsunternehmen gegenüber alle Ärzte, die ihn zukünftig behandeln werden, von ihrer Schweigepflicht entbinden muß.

Als Maßstab dafür, ob in Vertragsverhältnissen, in denen die eine Seite eine einseitige Regelungsmacht im Hinblick auf den Umgang mit den personenbezogenen Angaben des anderen hat, dessen Einwilligungserklärung Grundlage für die Erhebung, Speicherung oder Übermittlung zum Teil intimster personenbezogener Daten sein kann, bietet sich eine Übertragung des verfassungsrechtlichen Grundsatzes der Verhältnismäßigkeit auf das zivile Vertragsrecht an. Für die Beurteilung der Datenverarbeitung im Arbeitsverhältnis wurde dieser Gedanke von der arbeitsgerichtlichen Rechtsprechung bereits aufgegriffen (vgl. Bundesarbeitsgericht, Urteil vom 22. 10. 1986 – 5 AZR 660/85 –). Die Datenverarbeitung, die auf eine so verstandene Einwilligung gestützt werden soll, muß hiernach nach objektiven Kriterien zur Erreichung des von beiden Vertragsparteien angestrebten Vertragszwecks erforderlich, geeignet und angemessen sein. Nur diese objektiven Kriterien und nicht schon bloße wirtschaftliche Überlegungen des vertragsgestaltenden stärkeren Vertragsteils können über deren Zulässigkeit entscheiden. Anderenfalls droht im Privatrecht die Freiheit des wirtschaftlich Schwächeren, selbst über die Preisgabe und Verwendung persönlicher Daten zu entscheiden, auf der Strecke zu bleiben. Der einzelne hätte dann als Stellenbewerber, Mietinteressent, Kredit- oder Versicherungsnehmer keinerlei Schutz gegenüber einem Informationseingriff, den eine öffentliche Stelle nicht einmal auf der Grundlage eines Gesetzes vornehmen dürfte.

Es ist vor allem im Hinblick auf die Datenverarbeitung der genannten Wirtschaftsbereiche vereinzelt die Forderung erhoben worden, die Zulässigkeit der Informationserhebung und -verarbeitung auch insoweit bereichsspezifisch und präzise gesetzlich zu regeln. Diese Forderung ist datenschutzrechtlich konsequent. Ob sie über den Bereich des Arbeitnehmerdatenschutzes hinaus Gehör finden wird, dürfte weitgehend von der Bereitschaft der privaten Wirtschaft abhängen, den Grundsätzen des Datenschutzes vor allem bei der Fassung ihrer allgemeinen Geschäftsbedingungen mehr Beachtung als bisher zu schenken und die informationelle Selbstbestimmung des Verbrauchers in den verfassungsrechtlich vorgegebenen Grenzen zu berücksichtigen.

26.2 Kreditwirtschaft

Über Inhalt und Bedeutung der Neuregelung der sog. SCHUFA-Klausel und des SCHUFA-Verfahrens, die auf der Grundlage des Urteils des Bundesgerichtshofs vom 19. 9. 1985 zwischen den obersten Datenschutzaufsichtsbehörden der Länder und dem Zentralen Kreditausschuß mit meiner Beteiligung erarbeitet worden sind, habe ich in meinem Achten und Neunten Tätigkeitsbericht (8. TB S. 52 f., 9. TB S. 68ff.) ausführlich berichtet. Nachdem das beim Bundeskartellamt wegen des Ausschlusses einer Reihe von früheren SCHUFA-Anschlußpartnern (vornehmlich aus dem Dienstleistungsbereich) anhängige Antidiskriminierungsverfahren eingestellt wurde, ist das Reformpaket im wesentlichen im Frühjahr 1987 in Kraft getreten. Vorläufig letzter noch offener Punkt bei dessen Umsetzung ist die Nutzung des Systems durch Inkasso-Unternehmen. Deren Ausschluß war im Rahmen der Reform ebenfalls vereinbart worden und beschäftigt jetzt in einem weiteren Antidiskriminierungsverfahren wiederum das Bundeskartellamt. Ein eigener SCHUFA-Anschluß von Inkasso-Unternehmen ist datenschutzrechtlich deshalb unzulässig, weil es sich bei diesen Unternehmen nicht um Kreditgeber – auf die sich das System zu beschränken hat – handelt und das Informationssystem von ihnen nicht zur Bonitätsbeurteilung vor Kreditvergabe, sondern ganz

überwiegend zur Aufenthaltsermittlung von Schuldnern genutzt wird.

Ohne die mit der Reform insgesamt erreichten Verbesserungen des Datenschutzes für den betroffenen Kontoinhaber, Kreditnehmer oder Kreditkarteninhaber zu verkennen, darf doch nicht übersehen werden, daß das System noch Schwächen hat. An erster Stelle ist hier immer wieder die Kostenpflicht der Auskunft zu nennen. Ich habe wiederholt darauf hingewiesen, daß die Auskunft über die gespeicherten Informationen und über die anfragenden Stellen eine datenschutzrechtlich gebotene organisatorische Maßnahme beim Betrieb des SCHUFA-Kreditinformationssystems ist. Nur durch die Auskunft an den Betroffenen kann sichergestellt werden, daß die rechtlichen Voraussetzungen, und zwar

— Vollständigkeit, Richtigkeit und Aktualität der gespeicherten Daten,

— Beschränkung der Systemnutzung auf Kreditgeber,

erfüllt werden.

Die Auskunft stellt für den Betroffenen den einzigen Zugang zum System dar. Streng genommen müßte er sogar bei jeder Datenänderung und vor jeder Datenübermittlung unterrichtet werden, da er nur so Berichtigungen oder Sperrungen veranlassen kann, noch bevor für ihn ein Schaden eintritt. Um so wichtiger ist es, die Auskunft ohne Kosten für den Betroffenen zu erteilen. Daß diese Kosten den Systemträger zuzuordnen sind, ergibt sich im übrigen bereits zwingend daraus, daß die Auskunft selbst als datenschutzrechtlich gebotene Maßnahme Zulässigkeitsvoraussetzung des Systems ist. Ich hatte deshalb schon früher (9. TB S. 69) auf die Notwendigkeit hingewiesen, die Kostenfreiheit der SCHUFA-Auskunft bei der Novellierung des BDSG uneingeschränkt zu gewährleisten.

Leider entsprechen die bislang bekannt gewordenen Vorstellungen zur Novellierung des BDSG in diesem Punkt nicht den Erwartungen. Die gegenwärtige Fassung des Entwurfs schreibt zwar vor, daß die Auskunft, die der Betroffene über die zu seiner Person gespeicherten Daten einholt (sog. Eigenauskunft), grundsätzlich unentgeltlich erteilt werden muß; sie nimmt dann aber sogleich die SCHUFA-Eigenauskunft von dieser Regel aus. Für Eigenauskünfte durch Unternehmen, die, wie die SCHUFA, geschäftsmäßig Daten für fremde Zwecke verarbeiten, soll nämlich wie bisher ein Entgelt verlangt werden dürfen, wenn der Betroffene diese Eigenauskunft gegenüber Dritten zu wirtschaftlichen Zwekken nutzen kann.

Diese Möglichkeit der wirtschaftlichen Nutzung ist bei einer SCHUFA-Eigenauskunft umfassend gegeben. Die Eigenauskunft enthält eine Vielzahl von Angaben über die wirtschaftlichen Verhältnisse des Betroffenen. Jeder, dem diese Eigenauskunft vorliegt, kann daraus nicht nur Namen, Geburtsdatum und die aktuelle Anschrift des Betroffenen ersehen, sondern auch dessen Voranschrift, dessen Girokonten und Kreditkarten mit Nummer und Institut sowie alle vom Betroffenen aufgenommenen Konsumentenkredite mit Betrag, Laufzeit, Ratenhöhe und Ratenbeginn. Außerdem enthält die Eigenauskunft Angaben über die in den letzten drei Jahren erledigten Kredite mit Angabe der Art ihrer Erledigung sowie Angaben über die nicht vertragsgemäße Abwicklung von Kontoverbindungen oder Krediten, also Eintragungen über Mahnbescheide, Vollstrekkungsmaßnahmen und offene Forderungen. Damit der Betroffene die rechtmäßige Nutzung des Systems kontrollieren kann, werden seit der Neuordnung des SCHUFA-Verfahrens in der Eigenauskunft zudem auch die Stellen vermerkt, die in den letzten zwölf Monaten vor der Erteilung der Eigenauskunft über den Betroffenen angefragt haben. Die SCHUFA-Eigenauskunft ist damit sogar noch umfangreicher als die sog. Vollauskunft, die den Kreditinstituten vor der Kreditvergabe von der SCHUFA erteilt wird.

Bleibt es bei der im Entwurf vorgesehenen Bestimmung, werden auch zukünftig SCHUFA-Eigenauskünfte nur gegen eine Gebühr von DM 10,00 bis DM 20,00 erteilt werden. Die mit der gesetzlichen Neuregelung angestrebte Erleichterung der Ausübung des Auskunftsrechts wird dann gerade in dem Bereich verfehlt, in dem die Eigenauskunft für den Betroffenen von überragender Bedeutung ist. Ich halte diese Regelung deshalb für unbefriedigend und in verfassungsrechtlicher Hinsicht für fragwürdig. Die vorgesehene Regelung kommt ausschließlich denjenigen Unternehmen zugute, die, weil sie keine Kreditgeber sind, nicht Anschlußpartner der SCHUFA sein dürfen. Diese Unternehmen gehen nämlich in zunehmendem Maße dazu über, den Vertragsabschluß mit den Betroffenen von der Vorlage einer Eigenauskunft abhängig zu machen. Nicht zuletzt hat die SCHUFA selbst diese Unternehmen in ihrem Kündigungsschreiben auf die Möglichkeit hingewiesen, auf diese Weise trotz der Kündigung auch weiterhin den Datenbestand der SCHUFA nutzen zu können. Das Verlangen eines Arbeitgebers oder eines Vermieters nach Vorlage der Eigenauskunft durch den Betroffenen erhielte durch die gesetzliche Erwähnung der Möglichkeit wirtschaftlicher Nutzung einer Eigenauskunft sogar noch den Schein des rechtlich Zulässigen. Dies ist ein solches Verlangen aber gerade nicht. Die datenschutzrechtlich gebotene Beschränkung der Systemnutzung auf solche Stellen, die ein berechtigtes Interesse daran haben, über die Kreditwürdigkeit des Betroffenen unterrichtet zu werden, würde nicht mehr eingehalten. Die Umsetzung des SCHUFA-Urteils des Bundesgerichtshofs durch die Reform von SCHUFA-Klausel und SCHUFA-Verfahren würde in einem ganz wesentlichen Punkt unterlaufen.

Sollte die Entwurfsvorschrift in der vorgesehenen Form Gesetz werden, führte dies zu einem Rückschritt des Datenschutzes in der Privatwirtschaft. Der Betroffene müßte nicht nur wie bisher für seine Eigenauskunft bezahlen, sondern die mißbräuchliche Verwendung dieser Eigenauskunft durch Dritte wäre gesetzlich quasi legitimiert.

Aus diesem Grunde halte ich es für erforderlich, den Anspruch auf kostenfreie Auskunft ohne jede Ein-

schränkung zu gewährleisten. Datenschutzrechtlich wünschenswert wäre es darüber hinaus, wenn die Unternehmen, die geschäftsmäßig Datenverarbeitung für fremde Zwecke betreiben, Eigenauskünfte – auch im eigenen Interesse – in einer Form erteilen, die eine wirtschaftliche Weiterverwendung durch den Betroffenen ausschließen. Denkbar wäre es etwa, die Auskunft zu Merkmalen, die nicht Identifikationsmerkmale sind, auf einem gesonderten Blatt zu erteilen, so daß Dritten die Zuordnung dieser Merkmale zu einer bestimmten Person zumindest zweifelhaft bleibt.

26.3 Versicherungswirtschaft

In meinem Achten und Neunten Tätigkeitsbericht (8. TB S. 53 f., 9. TB S. 70) habe ich über die Gespräche berichtet, die mit meiner Beteiligung zwischen den obersten Aufsichtsbehörden der Länder für den Datenschutz und den Verbänden der Versicherungswirtschaft geführt werden. Es geht dabei um die gebotene Anpassung der von den Versicherungsunternehmen verwendeten Einwilligungsklauseln und des auf ihnen beruhenden Datenaustauschs an die datenschutzrechtlichen Erfordernisse. Diese Gespräche sind im abgelaufenen Jahr fortgesetzt worden, ohne daß es zu einer Einigung in der Sache gekommen ist. Ich halte es, gerade auch im Hinblick auf die vielen Bürgereingaben, die mich zu diesem Problem erreichen, für außerordentlich unbefriedigend, daß hierüber nun schon seit mehr als zwei Jahren ohne ein greifbares Ergebnis verhandelt wird.

Überfällig ist insbesondere die von den Aufsichtsbehörden seit langem geforderte Überarbeitung der Datenverarbeitungsklausel (früher sog. Datenschutzklausel). Die Einwilligung, die dem Versicherungsnehmer mit dieser Klausel abverlangt wird, kann nur dann eine tragfähige Grundlage für die Übermittlung von Daten an zentrale Dateien der Versicherungsverbände etwa im Bereich der Rechtsschutz- oder Lebensversicherung sein, wenn der Betroffene bei Abgabe der Erklärung zur Kenntnis nehmen kann, in welche Datenverarbeitungsvorgänge er einwilligt. Das ist gegenwärtig noch immer nicht der Fall. Die zentrale Registrierung der Kündigung von Rechtsschutzversicherungsverträgen durch die Versicherungsunternehmen oder die zentrale Erfassung der Ablehnung von Lebensversicherungsanträgen oder ihrer Annahme nur unter erschwerten Bedingungen, die durch die Einwilligungserklärung abgedeckt werden sollen, bleibt dem Versicherungsnehmer verborgen.

Auf den dringenden Änderungsbedarf bei der Schweigepflichtentbindungsklausel habe ich ebenfalls bereits früher im einzelnen hingewiesen (8. TB S. 53 f.). Zwar hat die Versicherungswirtschaft inzwischen Entwürfe für Neufassungen der Schweigepflichtentbindungsklauseln vorgelegt. Sie enthalten jedoch keine substantiellen Verbesserungen.

Nach dem Versicherungsvertragsgesetz obliegt es dem Versicherungsnehmer lediglich, dann eine entsprechende Erklärung abzugeben, wenn es zur Feststellung der Leistungspflicht im Einzelfall erforderlich ist, bei Ärzten Informationen über seinen Gesundheitszustand einzuholen. Die vom Bundesaufsichtsamt für das Versicherungswesen genehmigten Versicherungsbedingungen für die Krankenversicherung sehen dies in § 9 auch so vor. Beide Regelungen werden jedoch dadurch vollständig unterlaufen, daß die Versicherungsunternehmen in ihren Antragsformularen – in der sog. Schlußerklärung – gleichsam auf Vorrat eine in ihrer Zukunftswirkung unbegrenzte Schweigepflichtentbindung verlangen. Wie wenig ernst die Rechte des Bürgers von der Versicherungswirtschaft dabei in der Praxis genommen werden, zeigen immer wieder Eingaben, die mich erreichen und die ich an die zuständigen Aufsichtsbehörden weiterleite. So sollte z. B. ein Bürger nach einem Versicherungsverhältnis von zwanzig Jahren Dauer aus Anlaß einer Vertragsänderung zur Abgabe der Schweigepflichtenbindung mit der Drohung genötigt werden, daß anderenfalls sein Krankenversicherungsvertrag „aufgehoben" werde, ein Fall, der besonders deutlich macht, daß die Freiwilligkeit dieser Erklärung nur eine Fiktion ist. Das von mir hierzu um Stellungnahme gebetene Bundesaufsichtsamt für das Versicherungswesen vertritt die Auffassung, es könne den Versicherungsunternehmen die Verwendung dieser Klausel erst auf der Grundlage einer höchstrichterlichen Rechtsprechung untersagen. Das Amt, dessen Aufgabe es ist, den gesamten Geschäftsbetrieb der Versicherungsunternehmen zu überwachen, mutet damit dem einzelnen Versicherungsnehmer zu, zunächst selbst gegen die Klausel zu streiten, die mit Recht von den Datenschutzaufsichtsbehörden der Länder für datenschutzrechtlich unzureichend gehalten wird. Ich habe aus Anlaß dieses in jeder Hinsicht unbefriedigenden Ergebnisses nunmehr auch den Bundesminister der Finanzen als aufsichtsführendes Ressort beteiligt und ihn gebeten, sich zu der Auffassung des Bundesamtes sowie dazu zu äußern, ob er eine Entbindung von der ärztlichen Schweigepflicht für wirksam hält, die unter der Androhung abgegeben wird, anderenfalls den Versicherungsschutz aufzuheben.

Die Gespräche mit der Versicherungswirtschaft sollen im kommenden Jahr fortgesetzt werden. Ich werde mich hieran weiter beteiligen.

27. Datensicherung

Mit dem zunehmenden Einsatz von Anlagen zur automatisierten Datenverarbeitung in fast allen Bereichen der Bundesverwaltung wächst auch der Bedarf an Datensicherheit. Dies gilt sowohl für den Schutz der Daten gegen unbefugte Zugriffe und andere unzulässige Verarbeitungen als auch für die Verfügbarkeit der Daten und die Arbeitsfähigkeit der Systeme beim Auftreten nie ganz ausschließbarer Fehler und sonstiger Störungen.

Weil bei der Umstellung von Arbeitsabläufen auf automatisierte Verfahren die Risiken meist nicht vollständig erkannt werden und die Schwierigkeiten der Umstellung die Beteiligten ohnehin so stark beanspruchen, daß für Gefahrenabwehr und Risikovorsorge kaum Kapazität verfügbar ist, entsteht dabei

oft ein erheblicher Mangel an Sicherheit. Die von mir im Berichtsjahr durchgeführten Kontrollen bestätigen die schon früher gewonnene Erfahrung, daß solche Mängel in unterschiedlicher Ausprägung auch in der Bundesverwaltung verbreitet sind. Dabei beschränken sich diese Mängel keineswegs nur auf die Lösung der von manchem noch immer als eher lästig empfundenen Datenschutzprobleme, sondern sie betreffen auch andere Fragen der Gewährleistung der ordnungsgemäßen Aufgabenerfüllung.

Daß es sich hierbei um eine auch in anderen Ländern sehr ähnliche allgemeine Entwicklung handelt, zeigt z. B. der vom Amerikanischen House of Representatives verabschiedete „Computer Security Act of 1987", in dem für die Amerikanische Bundesverwaltung u. a. Sicherheitsstandards gefordert werden und ein regelmäßiges Training in Sicherheitsfragen für alle Personen, die Computersysteme mit sensitiven Daten betreiben oder nutzen.

Um die Sicherheitsprobleme bei der Datenverarbeitung in der deutschen Bundesverwaltung besser lösen zu können, wurde der interministerielle Ausschuß für die Sicherheit in der Informationstechnik (ISIT) eingerichtet und mit dem Aufbau einer Arbeitseinheit für Fragen der Computersicherheit (COMPUSEC) begonnen. Sie werden ihre Tätigkeit nicht auf diejenigen Bereiche beschränken, in denen Verschlußsachen mit automatisierten Verfahren bearbeitet werden, sondern sehen ihre Aufgabe in der Erhöhung der Sicherheit bei allen Arten des Einsatzes der modernen Informationstechnik.

Nach meinen Erfahrungen aus Kontrollen halte ich diese verstärkten Bemühungen um die Sicherheit der Datenverarbeitung sowohl im Interesse des Datenschutzes als auch unabhängig davon für geboten, und ich sehe diese Aktivitäten der Bundesregierung als eine gute Möglichkeit an, ihrer zentralen Verantwortung für die Lösung dieser Probleme gerecht zu werden.

Mit zentralen Maßnahmen allein kann jedoch die für die einzelnen Verfahren notwendige Sicherheit nicht erreicht werden. Dazu bedarf es vielmehr der Aktivität jeweils derer, die für die Konzeption, Einführung und Durchführung des jeweiligen Verfahrens verantwortlich sind.

Nachfolgend werden Sicherheitsprobleme und Ansätze zu ihrer Lösung beschrieben. Diese Probleme sind nach meinen Erfahrungen und aufgrund von Erkenntnissen aus Kontrollen exemplarisch für die vorstehend erwähnten Mängel. Die Ansätze zu ihrer Lösung müssen – wie übrigens alle Maßnahmen zur Datensicherung – dann auf den konkreten Einzelfall angewandt werden, denn es gibt keine Lösung, die unabhängig von den Gegebenheiten des Einzelfalles als richtig angesehen werden kann.

27.1 Sicherung gegen unbefugten Zugriff

Die heutige Praxis der Datenverarbeitung wird wesentlich durch folgende Entwicklungen bestimmt:

- die Zunahme von real-time-Verarbeitungen, wodurch auch die zentrale Datenverarbeitungsleistung am Arbeitsplatz verfügbar wird,
- die Bereitstellung von Datenbeständen über Online-Anschlüsse, wodurch der Datenbedarf direkt und damit ohne vorhergehende Prüfung der befragten Stelle gedeckt wird,
- und – wenn auch nicht ganz in derselben Weise – die Verbreitung von Arbeitsplatz-Computern,

die Maßnahmen zur Zugriffssicherung an immer mehr Arbeitsplätzen notwendig machen.

Die Sicherung des Zugriffs – und damit auch die Sicherung jeder Eingabe und jeder Programmanwendung – ist aber unter den damit geschaffenen Bedingungen deswegen schwierig, weil außer dem Zugreifenden und der Datenverarbeitungsanlage im Zeitpunkt des Zugriffs niemand mehr beteiligt ist. Bei der Prüfung der Zugriffsberechtigung kann die Datenverarbeitungsanlage nur nach dem im voraus festgelegten Prüfschema (Programm) entscheiden, ob und gegebenenfalls welche Zugriffe dieser Verbindung ermöglicht werden sollen. Dabei kann die Anlage nicht „erkennen", wer in welcher Absicht die Verbindung aufgenommen hat oder nutzt, sondern sie reagiert je nach den bei ihr ankommenden Signalen (elektrischen Impulsen) mit der programmierten Gestattung von Transaktionen oder auf andere, ebenfalls vorher programmierte Weise.

Wem immer es gelingt, die richtigen Impulse an die Datenverarbeitungsanlage (d. h. auch: auf die richtige Leitung) zu schicken, dem werden die vorher zugeordneten Möglichkeiten eingeräumt; er wird wie ein Berechtigter behandelt. Diese Konstellation macht es notwendig, nicht nur sorgfältig vorauszuplanen, sondern auch den Betrieb solcher Systeme daraufhin zu überwachen, ob die notwendige Sicherheit auch tatsächlich erreicht wird. Welche Folgen unzureichende Maßnahmen haben können, wird z. B. durch gelegentliche Erfolge von Hackern demonstriert, zuletzt am großen Einbruch von Hakkern in ein internationales Datenverarbeitungsverbundnetz für Raumforschungsdaten.

Wegen der sehr unterschiedlichen Anwendungsbedingungen gibt es leider kein allgemein gültiges Rezept für die Zugriffssicherung. Es gibt aber eine Reihe von Prinzipien, deren Beachtung zu einer angemessenen Zugriffssicherheit führt.

27.1.1 Überwachung der Anschlüsse

Es gehört zum verantwortungsvollen Betreiben einer Datenverarbeitungsanlage, sich zu vergewissern, über welche Anschlüsse in welcher Weise auf die Anlage zugegriffen werden kann. Dazu muß zunächst geklärt werden, welche Leitungen in eine Anlage hineinführen. Außer den für die planmäßige Benutzung vorgesehenen Leitungen können dies auch solche sein, die nur für Sonderfälle, z. B. für die Wartung, vorgesehen sind. Und Leitungen, auf denen nur „abgehender Verkehr" gewollt ist, können u. U. darüber hinaus auch ungewollten, nämlich den ankommenden Verkehr ermöglichen.

Für jede der Leitungen ist zu prüfen, welche Arten von logischen Verbindungen über sie ermöglicht werden sollen, und wie gesichert wird, daß über diese Vorgaben hinaus keine weiteren Verbindungen aufgebaut werden können.

Die Zuordnung von logischen Verbindungen zu bestimmten Leitungen sollte so präzise wie möglich getroffen werden. Weit besser als die hier oft gewünschte große Flexibilität trägt eine restriktive Tendenz zur Sicherheit bei. So ist es z. B. vielleicht ganz praktisch, wenn alle Funktionen von jedem Terminal und bei Bedarf auch über Wählleitungen angestoßen werden können. Die Erlaubnis, über jede Leitung auch Programme zu erstellen und zu ändern oder auch beliebige Operatoreingriffe durchzuführen, macht ein solches System aber entweder extrem unsicher oder sie muß durch hohen Überwachungsaufwand kompensiert werden. Insbesondere dann, wenn ein System auch über ein öffentliches Netz angewählt werden kann, sollten deshalb sicherheitsrelevante Eingriffe nur über fest definierte Anschlüsse durchführbar sein.

27.1.2 Überwachung der Nutzung

Eine wesentliche Voraussetzung dafür, daß die Nutzung eines Systems überwacht werden kann, ist die Zuordnung jeder Nutzung zu einem bestimmten Benutzer, der für die ihm zugeordneten Nutzungen verantwortlich ist. Dazu muß jeder Nutzer dem System vorher „bekannt" sein, d. h., das System muß vor der ersten Benutzung durch einen Benutzer diesem unter einer bestimmten Identifikation (der sog. USER-ID) verabredete Benutzungsmöglichkeiten (Rechte) einräumen, und der Nutzer muß über Mittel verfügen, mit denen er dem System gegenüber beweisen kann, daß er wirklich dieser zugelassene Benutzer ist (siehe dazu Nr. 27.1.3 Benutzerauthentifikation).

Nur unter sehr günstigen Umständen kann jedoch mit absoluter Sicherheit gewährleistet werden, daß es stets nur dem zugelassenen Benutzer gelingt, dem System „zu beweisen", daß ihm diese Benutzungsrechte zustehen. Insbesondere die bekanntgewordenen Erfolge von Hackern belegen, daß es auch bei vermeintlich sicheren Systemen gelegentlich zu peinlichen Irrtümern kommen kann. Um zumindest die Folgen solcher mißbräuchlichen Nutzungen zu begrenzen und Wiederholungen zu vermeiden, bedarf es zusätzlicher Maßnahmen. Sehr wirksam ist es, dem berechtigten Benutzer immer dann, wenn er sich dem System gegenüber ausgewiesen hat, anzuzeigen, wann das System zuletzt unter seiner Identifikation benutzt wurde. Er selbst kann dann leicht beurteilen, ob die angezeigte Nutzung korrekt war. Ebenfalls der Sicherung dient es, wenn auch angezeigt wird, wieviele erfolglose Versuche in der Zwischenzeit unternommen wurden, das System unter seiner Identifikation zu nutzen. Er kann dann leicht entscheiden, ob er die Fehlversuche für harmlos hält, z. B. weil er sie selbst irrtümlich unternommen hatte, oder ob zu befürchten ist, daß jemand (systematisch) versucht, die ihm vorbehaltenen Möglichkeiten zu erlangen, was stets Gegenmaßnahmen auslösen sollte (s. unten Nr. 27.1.4). Dieses Verfahren trägt jedoch dann kaum zur Sicherheit bei, wenn der zugelassene Benutzer das Verfahren nur unregelmäßig oder in langen Zeitabständen nutzt oder – aus welchen Gründen auch immer – Hinweise auf Gefährdungen ignoriert. Deshalb sollte grundsätzlich eine Beobachtung der Fehlversuche stattfinden, bei der das System nach einer nicht zu großen Anzahl (etwa drei) von Fehlversuchen zum einen die betroffene Identifikation automatisch sperrt oder andere Hindernisse aufbaut und zum anderen das Gesamtsystem daraufhin überprüft wird, ob Fehlversuche, die auf wechselnde Identifikationen bezogen sind, Anlaß zu besonderen Maßnahmen geben. Darüber hinaus empfiehlt es sich, nur solche Benutzer zuzulassen, die das System auch mit einer gewissen Regelmäßigkeit nutzen. Soweit es organisatorisch tragbar ist, sollten Identifikationen, die voraussehbar eine gewisse Zeit lang nicht genutzt werden, z. B. in der arbeitsfreien Zeit des Benutzers, vom System her oder vom Benutzer gesperrt werden.

Wenn es sich nicht vermeiden läßt, daß auch Benutzer zugelassen werden, die das System sehr selten nutzen, z. B. weil Vorsorge für Notfälle getroffen werden muß, oder weil Prestige-Forderungen nicht abgewiesen werden können, dann sollten diese Anschlüsse einer ergänzenden Kontrolle durch den für die Sicherheit des Systems Verantwortlichen unterzogen werden. Damit läßt sich der Mißbrauch voraussichtlich in vielen Fällen verhindern und in weiteren Fällen wenigstens begrenzen.

Mißbrauch wird dagegen geradezu begünstigt, wenn eine Benutzeridentifikation für interaktive Nutzung über ein Jahr lang besteht, ohne daß eine solche Nutzung erfolgt, und zu dieser Identifikation über 100 Fehlversuche möglich sind, was nach einem Pressebericht über den Hackereinbruch in das Nasa-Netz der Fall gewesen sein soll. Es nützt dann auch nichts, wenn die Angaben im Computer geführt, auf dem Bildschirm des „Nutzers" (hier: des Hackers) angezeigt werden, sich sonst aber niemand darum kümmert.

27.1.3 Benutzerauthentifikation

Es ist offensichtlich von erheblicher Bedeutung für die Sicherheit, daß die Benutzer über Mittel verfügen, mit denen nur sie allein dem System beweisen können, daß sie der verabredete, zugelassene Benutzer sind. Verfahren, die dies leisten, werden im allgemeinen als Authentifikationsverfahren bezeichnet.

Die technischen Möglichkeiten erlauben es heute, eine breite Palette von Authentifikationsverfahren zu verwenden. Dazu gehört z. B. die Möglichkeit, durch die Vermessung der Geometrie der Hand festzustellen, ob derjenige, der seine Hand in ein entsprechendes Abtastgerät hineinlegt, auch tatsächlich derjenige ist, dessen Daten bei der Einrichtung dieses Benutzerdatensatzes gespeichert wurden. Andere Verfahren zur Erkennung körpereigener und deshalb nur schwer zu fälschender Merkmale sind die Analyse der Stimme und die Vermessung des Linienbildes der Iris. Verfahren dieser Art haben jedoch bis auf weiteres den Nachteil, recht aufwendig

und damit ziemlich teuer zu sein. Zudem muß durch besondere Vorkehrungen gesichert werden, daß die Daten über die Vermessung nicht unter Umgehung des Meßgerätes auf die Leitung gebracht werden. Für die breite Anwendung sind diese Verfahren deshalb zur Zeit kaum einsetzbar.

Eine einfache und gerade auch für Arbeitsplatzcomputer fast immer erfolgreich einsetzbare Maßnahme ist das Einschließen der Datenträger in den Zeiten, in denen der Zugriffsberechtigte nicht in der Lage ist, die Kontrolle selbst auszuüben. Das Mittel zur Authentifikation ist dann der passende Schlüssel, über den nur der Zugriffsberechtigte verfügen können soll. Bevor auf diese Maßnahme verzichtet wird, sollte bedacht werden, daß eine unzulässige Veränderung der auf den Datenträgern gespeicherten Daten in der Regel keine erkennbaren Spuren – außer der Änderung selbst – hinterläßt. Es ist im nachhinein auch praktisch unmöglich, Feststellungen über die näheren Umstände von unzulässigen Änderungen und über die daran Beteiligten zu treffen. Neben dem Einschließen der Datenträger kommt oft auch ein Abschließen des Geräts oder des Raumes in Frage. Gerade bei der jetzt verstärkt einsetzenden Automatisierung der Büroarbeiten sollten alle Benutzer auf diese Möglichkeiten ausdrücklich hingewiesen werden.

Wenn mehrere Personen ein System nutzen, ist das Zugriffsproblem durch Abschließen nicht zu regeln. Ein wichtiges Authentifikationsmittel, das auch in der Regel mit vertretbarem Aufwand eingesetzt werden kann, ist dann das *persönliche* Paßwort, das vom Betriebssystem der Anlage oder von dem benutzten Anwendungsprogramm darauf geprüft wird, ob es den eingegebenen Benutzernamen (USER-ID) bestätigt.

Weit weniger Sicherheit liefern Gruppenpaßwörter, die für alle Benutzer mit denselben Zugriffsrechten gleich sind, oder Objektpaßwörter, die allen Benutzern bekannt sein müssen, die dieses Objekt – ein Programm oder eine Datei – benutzen sollen. Solche Paßwörter haben die sicherheitsmindernde Eigenschaft, die Verantwortung für einzelne Aktivitäten unsichtbar zu machen, und zugleich die Unsicherheit erzeugende Eigenschaft, – oft aus vernünftigen Gründen – ziemlich vielen Beteiligten bekannt zu werden. Weil sie zudem aus organisatorischen Gründen nur schwer zu ändern sind, überdauern sie häufig auch Personalwechsel und tragen damit zur Sicherheit kaum etwas bei.

Die Verwendung von persönlichen Paßwörtern kann dagegen zusammen mit der Überwachung der Nutzung und weiteren flankierenden Maßnahmen, die ich in meinem Sechsten Tätigkeitsbericht beschrieben habe (s. 6. TB S. 55 f.), für eine breite Palette von Anwendungen ausreichende Sicherheit der Authentifikation bieten. Auch können sie helfen, Mitarbeiter von unberechtigten Vorwürfen mißbräuchlicher Datenverarbeitung zu entlasten.

Als ein neues, in der nächsten Zeit voraussichtlich zu vertretbaren Kosten einsetzbares Authentifikationsmittel können Magnetkarten und Chipkarten als moderne Form der Schlüssel angesehen werden. Diese Mittel erlauben die Ausgabe von persönlichen, nur sehr schwer nachmachbaren „Schlüsseln", bei deren Verwendung zudem noch die Eingabe eines persönlichen Paßwortes verlangt werden kann, das in diesem Zusammenhang auch als persönliche Identifizierungsnummer (PIN) bezeichnet wird. Mit dieser Kombination läßt sich – anders als bei herkömmlichen Schlüsseln – ein Mißbrauch durch Diebstahl oder Finden von Schlüsseln verhindern. Daß aber auch die damit erreichbare Sicherheit begrenzt sein wird, zeigen die – gemessen am Einsatz solcher Systeme – bei Geldausgabeautomaten relativ sehr seltenen, aber eben doch vorkommenden unerlaubten Geldabhebungen. Das verwendete Authentifikationsverfahren allein schafft nämlich noch keine Sicherheit, es kommt vielmehr darauf an, daß die Berechtigten es verantwortungsbewußt und sorgfältig handhaben. Deshalb sind Schulung, Motivation und auch Kontrollen mit dafür maßgebend, wie sicher die Benutzer die Verfahren anwenden, was nach meinen Erfahrungen oft zu wenig beachtet wird.

27.1.4 Sicherheits-Management

Es kann offensichtlich nicht erwartet werden, daß ein System „konstruktionsbedingt sicher" gegen unbefugte Zugriffe ist. Dies gilt schon deswegen, weil die Sicherheit wesentlich vom Verhalten der Beteiligten abhängt. Weil für die Benutzer eines Systems aber die Leistung und damit ihr Nutzen im Vordergrund stehen, sollte das Erzeugen und Erhalten von Sicherheit als besondere Aufgabe erkannt und einer Person (oder einer Gruppe) zur Erfüllung zugewiesen werden.

Zu dieser Aufgabe gehört zunächst eine Prüfung, ob die vorgesehenen Sicherungsmaßnahmen unter den tatsächlichen Einsatzbedingungen ausreichend sind, und bei Bedarf eine Ergänzung der Maßnahmen. Im Rahmen der Sicherheitsverwaltung fallen ferner einige Routinearbeiten an: Es sind Benutzernamen zu vergeben, Nutzungsmöglichkeiten dafür festzulegen, die Authentifikationsmittel zu bestimmen und bei Bedarf zu ändern, und es müssen einige regelmäßige Überwachungsmaßnahmen durchgeführt werden (s. o. Nr. 27.1.2). Ferner sind die Schulung der Benutzer und die wiederkehrende Motivation zu sicherheitsförderndem Verhalten in diesem Zusammenhang unbedingt ernstzunehmende Aufgaben, und erfahrungsgemäß sind auch Kontrollen erforderlich, um die Wirksamkeit von Sicherungsmaßnahmen zu überprüfen und rechtzeitig Schwachstellen und riskante Verfahrensweisen zu erkennen.

Schließlich ist auch die oft vernachlässigte Funktion einer Ansprechstelle für sicherheitsrelevante Hinweise und Fragen auszufüllen. Insbesondere müssen diejenigen Ereignisse geklärt werden, die vermuten lassen, daß unzulässige Aktivitäten durchgeführt wurden. Findet ein Benutzer niemand, dem er z. B. sicherheitsrelevante Beobachtungen zur Weiterverfolgung mitteilen kann, oder wird bei erkannten Sicherheitsverletzungen nicht unverzüglich nach den Ursachen dafür gesucht und Abhilfe geschaffen, so wächst dadurch das Risiko der unbefugten Benutzung unnötig stark an.

27.2 Vorsorge für Katastrophenfälle

In dem Maße, in dem automatisierte Verfahren zur Datenverarbeitung eingesetzt werden, wächst die Abhängigkeit der Aufgabenerfüllung von der Verfügbarkeit der Systeme. Häufig ist bei Störungen das Ausweichen auf andere Verfahren oder auch das Zurückgreifen auf konventionell geführte Unterlagen schon deshalb nicht mehr möglich, weil solche Unterlagen (z. B. im Bundeszentralregister) nicht mehr geführt werden oder in die Arbeitsabläufe – z. B. bei automatisierten Auskunftssystemen – nicht mehr integriert werden können. Selbst in den Organisationen, in denen dies im Prinzip noch denkbar ist, wird es nur für wenige Fälle praktisch durchführbar sein, denn der dafür erhöhte Arbeitsaufwand ist in der Regel nicht zu bewältigen.

Die Behinderungen sind aber nicht auf die Außenleistung beschränkt, auch die Datenerfassung und die Datenbestandspflege können unterbrochen sein, was bei längeren Systemstörungen zu nur sehr schwer aufholbaren Arbeitsrückständen führt. Die für Wirtschaftsunternehmen gelegentlich geäußerte Ansicht, daß ein Betrieb bei einem Totalausfall seiner Datenverarbeitung nach fünf Arbeitstagen konkursreif sei, dürfte auf die Behörden zwar nur sehr eingeschränkt übertragbar sein. Sicher ist jedoch, daß die Aufgabenerfüllung vieler Stellen nachhaltig beeinträchtigt oder weitgehend unmöglich ist, solange ihre Datenverarbeitung nicht verfügbar ist.

Es ist zwar nicht vorrangig eine Aufgabe des Datenschutzes, für die Verfügbarkeit von Datenverarbeitungsleistung zu sorgen. Wenn aber im Katastrophenfall zur Minderung des Schadens Ersatzlösungen gesucht werden müssen, dann kann es dabei leicht zu auch für die Betroffenen folgenschweren Mißachtungen von Datenschutz und Datensicherheit kommen, wenn anders die Verarbeitung nicht wieder in Gang gebracht werden kann. Zumindest insoweit sind deshalb die Notfallvorkehrungen auch unter Datenschutzgesichtspunkten (z. B. Nr. 10 der Anlage zu § 6 BDSG, Organisationskontrolle) von Interesse.

Bei der Notfallvorsorge ist zu berücksichtigen, daß die Leistung eines Datenverarbeitungssystems schon dann nicht mehr oder nur noch sehr eingeschränkt zur Verfügung steht, wenn bestimmte wichtige Teile des Systems ausfallen. Solche Teile sind

- die Stromversorgung,
- die Klimatisierung,
- die Datenspeichereinheiten und die Datenträger,
- die Verarbeitungseinheiten und Programme und
- die Datenübertragungseinrichtungen, zu denen außer den Kabelschächten und Hausverteilern u. U. auch Einrichtungen des öffentlichen Netzes gehören können.

Ebenfalls zahlreich sind auch die Anlässe, aus denen langanhaltende Störungen entstehen können:

- Feuer und Rauchgaseinwirkung
- Überflutung, Wasserrohrbruch, Löschwasser
- Stromausfall
- Überspannung im Netz, Blitzschlag, Kurzschluß
- Softwarefehler (auch als Sabotagefolge)
- Explosion, Gebäudeschäden
- Diebstahl, Beschädigung bei Einbruch
- Maschinenfehler, Verschleiß

Einige der damit verbundenen Risiken lassen sich durch vorbeugende Maßnahmen ausschließen oder ganz wesentlich verringern. Weil dem aber schon aus Kostengründen Grenzen gesetzt sind, bleibt im allgemeinen ein schwer kalkulierbarer Rest an Verletzlichkeit, der in Kauf genommen werden muß. Für diese nicht abwendbaren Risiken ist zu prüfen, ob die danach noch möglichen Systemausfälle einfach hingenommen werden können, oder welche Maßnahmen zu treffen sind, um in vertretbarer Zeit Ersatzlösungen zu realisieren. Wieviel Zeit vergehen darf, bis wenigsten ausgewählte Teile der Datenverarbeitungsleistung (z. B. das Online-Auskunftsverfahren) wieder verfügbar sind, hängt ebenso vom Einzelfall ab, wie die Maßnahmen zur Vorbereitung des Betreibens eines Ersatzsystems (Back-up System). Schon die Analyse zur Feststellung des Ersatzbedarfs für Notfälle wird nach meinen Erfahrungen aber nicht immer durchgeführt.

Als Mindestvoraussetzung für einen Ersatzbetrieb gilt ohne Frage, daß Kopien der Daten und aller benötigten Programme (u. a. die aktuell eingesetzte Version des Betriebssystems, die zur Zeit gültigen Anwendungsprogramme, die Datenübertragungssoftware, eventuell auch Datenbankverwaltungsprogramme, tools und utilities) an einem sicheren Ort ausgelagert sind und auch die zum Betrieb eines Ersatzsystems notwendigen Arbeitsunterlagen verfügbar gehalten werden. Ob darüber hinaus eine gegenseitige Unterstützung mit einem anderen Betreiber eines DV-Systems vereinbart, ein Vertrag mit einem kommerziellen Anbieter von Ausweichrechenzentren geschlossen oder andere Vorsorgemaßnahmen getroffen werden, kann sich immer nur als Kompromiß aus den dafür aufzuwendenden Kosten und dem voraussichtlichen Bedarf im Notfall ergeben. Ist dieser Bedarf so ausgeprägt, daß binnen weniger Tage die Notlösung leistungsfähig sein muß, sind darüber hinaus auch Übungen erforderlich, um die Nutzbarkeit des Konzepts zu prüfen, Planungslücken und -fehler zu erkennen und für den Einzelfall das notwendige Maß an Funktions- und Datensicherheit zu gewährleisten. Es kann nicht übersehen werden, daß dafür unter Umständen auch erhebliche Kosten aufzuwenden sind. Ein Verzicht auf solche Maßnahmen ließe aber möglicherweise nicht verantwortbare Risiken für die Aufgabenerfüllung entstehen.

27.3 Personal-Computer

Auch in der Bundesverwaltung hat der Masseneinsatz von Arbeitsplatzcomputern und Textverarbei-

tungssystemen begonnen. Die technische Basis hierfür ist in der Regel ein Personal-Computer (PC). Der Einsatz der modernen Informationstechnik auch für die Büroarbeit wird gefordert und gefördert, und so gibt es kaum noch einen Geschäftsbereich, in dem diese Geräte nicht eingesetzt werden: für die Personalverwaltung, für die Textverarbeitung, die Disposition von Dienstwagen usw.

Die Dynamik der Zunahme des Einsatzes von Personal-Computern ist sehr stark, und die weitere Entwicklung ist noch nicht abzusehen. Erst jetzt werden nämlich für viele die Vorteile der automatisierten Datenverarbeitung sichtbar und spürbar: Die Bearbeiter werden von Routinearbeiten entlastet, schnell hat der PC eine Grafik mit der neuesten Auslastungsstatistik gedruckt, spielend ist der Dienstplan für die Montagekolonne fertiggestellt und problemlos wird der Urlaubsplan festgelegt, denn alle Kollisionen können mit Hilfe eines guten Auswertungs- und Kontrollprogramms sofort erkannt werden. Das Programm zur Verwaltung der Indizes für die Handakte ist leicht erstellt und künftig zeigt der PC für jedes Stichwort die Fundstelle an.

Doch bei aller Euphorie gibt es inzwischen auch kritische Stimmen: Systementwickler bedauern, daß jetzt, wo man in der sog. Groß-EDV endlich der ingenieurmäßigen Softwareentwicklung nahekommt, der Wildwuchs und die Unkontrollierbarkeit wieder beginnen. Mitarbeiter der Revision fragen, wer denn eigentlich die Kassensicherheit gewährleisten wolle. Organisationsfachleute sehen Probleme hinsichtlich der Ordnungsmäßigkeit der Verwaltung und die für den Haushalt Verantwortlichen bezweifeln die Wirtschaftlichkeit der Entwicklung immer wieder gleichartiger Software.

Auch den Datenschutzbeauftragten bereitet die Ausbreitung der PC schon seit längerem Sorgen (s. 8. TB S. 56ff., 9. TB S. 70ff.). Sie wollen sich keineswegs einer an sich sinnvollen Entwicklung in den Weg stellen, es geht ihnen auch nicht darum, die Probleme der Softwareentwickler oder der für den Haushalt Zuständigen zu lösen, auch wenn ein gemeinsames oder zumindest ein abgestimmtes Vorgehen sehr sinnvoll sein kann. Ihre Aufgabe ist es vielmehr, die Persönlichkeitsrechte zu schützen, die durch den Einsatz von neuen Techniken gefährdet sein können.

Die Gefährdung liegt in der Intransparenz und der Unkontrollierbarkeit, die dadurch entstehen, daß u. U. dieselbe Person den PC beschafft, ihn programmiert, die Daten eingibt und verarbeitet. Solange nicht bekannt ist, wo ein solcher Computer steht, welche Daten dort gespeichert sind und wie diese verarbeitet werden, kann ein Betroffener auch nicht feststellen, ob seine Persönlichkeitsrechte verletzt werden und kein Leiter einer Verwaltung kann wirklich verantworten, was in seinem Zuständigkeitsbereich geschieht. Dieser Mangel an Transparenz steigert sich noch, wenn PC miteinander oder mit Anlagen anderer Art vernetzt werden (vgl. auch 7. TB S. 98ff. und 8. TB S. 56ff.).

Aus Gründen des Datenschutzes, aber auch aus Gründen der Wirtschaftlichkeit und der Verantwortbarkeit ist es daher unumgänglich, dem Wildwuchs vorzubeugen und durch Organisationsmaßnahmen die gebotene Ordnung herzustellen.

27.3.1 Dienstliche Nutzung privater PC

Der Einsatz privater PC für dienstliche Zwecke sollte grundsätzlich untersagt und nur in begründeten Einzelfällen nach sorgfältiger Prüfung zugelassen werden. Vor der Genehmigung der Nutzung eines privaten PC für dienstliche Zwecke müssen die datenschutzrechtliche Zulässigkeit dieser Datenverarbeitung und die Einhaltung der gebotenen Sicherungsmaßnahmen gesichert sein. Dabei kann sich gerade die Erfüllung der auch im allgemeinen dienstlichen Interesse liegenden Sicherungsmaßnahmen, z. B. die Fortsetzbarkeit der Arbeit bei Verhinderung des Mitarbeiters, schnell als unmöglich herausstellen. In jedem Fall müssen die gesetzlichen und damit zugleich auch die aus organisatorischen Gründen zwingend zu stellenden Forderungen nach Transparenz und Ordnungsmäßigkeit der Datenverarbeitung erfüllt werden. Die Beachtung dieser Grundsätze führt nach den bisherigen Erfahrungen dazu, daß die Nutzung eines privaten PC für dienstliche Zwecke nur unter sehr selten gegebenen Umständen vertretbar ist. In diesen Fällen muß dann durch eingehende Belehrung des Benutzers gewährleistet werden, daß zwischen dienstlicher und privater Datenverarbeitung und Datennutzung streng getrennt wird. Dazu gehört selbstverständlich und insbesondere, daß unterschiedliche Datenträger für die dienstliche und die private Nutzung verwendet werden.

Weil die Gründe für diese Zurückhaltung bei der Gestattung der dienstlichen Nutzung privater Computer nicht ohne weiteres allen Mitarbeitern bekannt sind, empfehle ich, entsprechende Regelungen festzulegen und allen Mitarbeitern zur Kenntnis zu geben.

27.3.2 Die Nutzung dienstlicher PC

Zur Kontrolle der dienstlichen PC muß zunächst ermittelt werden, welche Datenverarbeitungsanlagen dieser (und anderer) Art überhaupt vorhanden sind und wo sie stehen. Dabei kommt es darauf an, *alle* Datenverarbeitungssysteme zu erfassen, auch solche, die planmäßig nicht für die Verarbeitung personenbezogener Daten eingesetzt werden (s. 8. TB, S. 57). Dies kann z. B. über einen Gerätenachweis (eine Inventarliste) geschehen, wie er traditionell bei den Material verwaltenden Stellen geführt wird.

In diesem Zusammenhang ist auch zu prüfen, welche Datenträger eingesetzt werden bzw. werden sollen, und wie ihre Verwendung kontrolliert wird. Die Verwendung privateigener Datenträger für dienstliche Zwecke ist wegen des damit verbundenen, unvertretbaren Sicherheitsrisikos zu untersagen.

Als nächster Schritt wäre dann festzustellen, welche personenbezogenen Dateien vorhanden sind bzw. eingerichtet werden sollen und welche Software dafür zur Verfügung steht bzw. entwickelt wird. Es ist

zwar nicht gesetzlich vorgeschrieben, aber aus organisatorischen und wirtschaftlichen Gründen sehr sinnvoll, dabei auch die Verarbeitung nicht personenbezogener Daten einzubeziehen. Auf jeden Fall sind aber diejenigen personenbezogenen Dateien zu berücksichtigen, die auf einer Anlage tatsächlich geführt werden, auch wenn diese Anlage planmäßig nicht für die Verarbeitung personenbezogener Daten bestimmt ist.

Wenn von den Daten, ihrer vorgesehenen und der möglichen Verarbeitung keine Gefährdung für die Rechte der Betroffenen zu erwarten ist, kann die Verarbeitung ohne weiteres auf PC erfolgen. Sind die Daten dagegen von größerer Aussagefähigkeit, so sind je nach Qualität der Daten, dem Verwendungszusammenhang und den daraus resultierenden Gefährdungen zusätzliche Sicherungsmaßnahmen oder auch Beschränkungen geboten.

Es wird häufig eingewandt, in sehr großen Verwaltungen seien die Probleme, die mit dem Einsatz von PC verbunden sind, mit zentralen Melde- und Genehmigungsverfahren nicht zu lösen; die Zahl der Computer und erst recht die der Dateien sei zu hoch. Als Beispiel für eine sachgerechte Lösung dieser Probleme kann das Verfahren zur Verarbeitung von Mitarbeiterdaten gelten, das die Deutsche Bundesbahn mit meiner Beratung entwickelt hat (9. TB S. 27f.) und das von einer Klassifizierung der Daten ausgeht. Die (Mitarbeiter-)Daten bei der Deutschen Bundesbahn werden in zwei Klassen eingeteilt. Die Speicherung der im dienstlichen Umfeld meist ohnehin bekannten Daten:

Name, Vorname
Firma
Dienst- oder Amtsbezeichnung
Anschrift
Rufnummer
Geburtstag

und ihre Verarbeitung zu internen dienstlichen Zwecken kann dezentral (vom jeweiligen Dienststellenleiter) genehmigt werden. Es ist durchaus vorstellbar, daß dieser Katalog bei Bedarf um einige Positionen erweitert werden kann, z. B. um Angaben über die Organisationseinheit und um die Zimmernummer. Über die Speicherung aller weiteren Daten wird zentral entschieden, also bei der Deutschen Bundesbahn durch die Hauptverwaltung.

Im Rahmen der Novellierung des Bundesdatenschutzgesetzes sollte vom Gesetzgeber geklärt werden, ob ein entsprechendes Verfahren nicht auch bezüglich der internen Übersicht nach § 15 BDSG und für die Meldungen zu dem von mir zu führenden Register (§ 19 Abs. 4 BDSG) zugelassen werden sollte. Wenn beim Einsatz von PC in bestimmten Fällen schon über die datenschutzrechtliche Zulässigkeit ebenso wie über die wirtschaftliche Zweckmäßigkeit und die erforderlichen Sicherungsmaßnahmen dezentral entschieden wird, dann sollten detaillierte Übersichten am besten genauso dezentral geführt werden, zusammen mit den aus organisatorischen Gründen dort ohnehin erforderlichen Dokumentationen. Solange dadurch die Transparenz und insbesondere das Auskunftsrecht des Betroffenen gewährleistet bleiben, ist eine solche Lösung durchaus sachgerecht.

Es ist niemand damit gedient, wenn wenig schützenswerte Daten mit demselben Aufwand nachgewiesen werden müssen, der für andere Daten durchaus angebracht ist. Gegenwärtig wäre zum Beispiel eine Adreßdatei, die zum Versand von Drucksachen in einem Textverarbeitungssystem enthalten ist, nicht nur in die Übersicht nach § 15 BDSG aufzunehmen, sie wäre auch nach § 19 Abs. 4 BDSG zum Register beim Bundesbeauftragten für den Datenschutz zu melden und nach § 12 Abs. 1 zu veröffentlichen, was alles zum Datenschutz erfahrungsgemäß nur wenig beiträgt. Für solche Formalpflichten fehlt verständlicherweise oft die Motivation, weshalb sie wohl gelegentlich auch vernachlässigt werden.

Deshalb würde ich es begrüßen, wenn der Gesetzgeber die Formalpflichten in den Fällen einschränken würde, in denen offenbar weniger schützenswerte Daten verarbeitet werden. Die Vorschriften über die Zulässigkeit der Datenverarbeitung sollten aber auch für diese Daten weitergelten und auch die Rechte der Betroffenen sollten nicht geschmälert werden. Für Dateien mit anderen, aussagekräftigen Daten sollten dagegen die Formalpflichten auch dann im vollen Umfang bestehen bleiben, wenn diese Daten auf PC geführt werden; denn es erschiene mir widersinnig, den Datenschutz, der ja besonders den Gefährdungen durch automatisierte Datenverarbeitung begegnen soll, nur deshalb weniger ernst zu nehmen, weil diese Form der Verarbeitung stark zunimmt.

28. Novellierung des Bundesdatenschutzgesetzes

Der Bundesminister des Innern hat mir im November 1987 den Referentenentwurf eines Artikelgesetzes zur Neufassung des Bundesdatenschutzgesetzes und zur Änderung des Verwaltungsverfahrensgesetzes zugeleitet. Ein wesentliches Ziel des Entwurfes ist nach seiner Begründung die Anpassung des Datenschutzrechts an die Grundsätze, die das Bundesverfassungsgericht in seinem Urteil vom 15. Dezember 1983 (Volkszählungsgesetzurteil) zum Recht auf informationelle Selbstbestimmung entwickelt hat. Danach müssen u. a. auch für die Datenverarbeitung in Akten Datenschutzvorschriften geschaffen werden. Die Anpassung soll in der Weise geschehen, daß der Datenschutz, soweit nicht bereichsspezifische Vorschriften eingreifen, für die Datenverarbeitung in bzw. aus Dateien im BDSG und für die Datenverarbeitung in Akten im Bereich der öffentlichen Verwaltung des Bundes im Verwaltungsverfahrensgesetz geregelt werden soll. Diese Rechtsgestaltung ist nicht neu; sie war bereits in den entsprechenden Entwürfen der 10. Legislaturperiode (Drucksachen 10/4737 und 10/5343) vorgesehen.

Neu gegenüber den bisherigen Entwürfen zur Novellierung des BDSG sind dagegen strukturelle Änderungen im Aufbau des Gesetzes, wobei die Zusammenfassung des Dritten und Vierten Abschnitts in

einem einzigen Abschnitt für die Datenverarbeitung im nicht-öffentlichen Bereich besonders augenfällig ist. Da inhaltlich gleichwohl weiterhin zwischen Datenverarbeitung für eigene Zwecke und der für fremde Zwecke unterschieden wird, erscheint es mir fraglich, ob diese strukturelle Änderung wirklich dem besseren Verständnis des Gesetzes dient, zumal damit die gewohnte Paragraphenfolge aufgegeben wird. Indessen ist anzuerkennen, daß durch die Überarbeitung auch der übrigen Abschnitte des Gesetzes, durch eine andere Gliederung und den Verzicht auf manche Querverweisungen die Lesbarkeit des Textes insgesamt gewonnen hat, was angesichts der ohnehin schon schwierigen Materie zu begrüßen ist.

Ich beabsichtige, zu dem Entwurf im einzelnen eine Stellungnahme zu erarbeiten und diese dem Bundesminister des Innern Anfang des Jahres 1988 zuzuleiten. Ohne dieser Stellungnahme vorzugreifen, erscheint es mir angebracht, einen ersten Eindruck, soweit ich ihn mir in der kurzen Zeit bis zum Abschluß dieses Tätigkeitsberichts verschaffen konnte, schon an dieser Stelle wiederzugeben.

Die vorgeschlagene Neufassung des Gesetzes entspricht inhaltlich weitgehend, vielfach sogar wörtlich, dem erwähnten Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes und des Verwaltungsverfahrensgesetzes, der in der 10. Legislaturperiode in den Deutschen Bundestag eingebracht worden ist. Einige mir besonders wichtig erscheinende Aspekte, nämlich Anwendungsbereich, Zweckbestimmung, Transparenz und Kontrolle, habe ich in meinem Neunten Tätigkeitsbericht (S. 75ff.) aufgegriffen und die seinerzeit hierzu vorgesehenen Neuregelungen ausführlich behandelt. Diese überwiegend kritischen Anmerkungen gelten ohne Abstriche nach wie vor. Ich verzichte hier auf eine Wiederholung und verweise ausdrücklich auf meine früheren Ausführungen, mit denen sich weder die Bundesregierung in ihrer Stellungnahme zu meinem Neunten Tätigkeitsbericht noch der Bundesminister des Innern in dem neuen Referentenentwurf auseinandergesetzt haben.

Ich möchte jedoch hier einige weitere mir wichtig erscheinende und in der Neuregelung angelegte Problemkreise zur Erörterung stellen, die nach meiner Auffassung eine Minderung des Datenschutzes und der Kompetenzen des BfD bewirken.

28.1 Einschränkung des Geltungsbereichs

Der Entwurf definiert den Zweck des Gesetzes dahingehend, daß der einzelne davor geschützt werden soll, durch die Verarbeitung seiner personenbezogenen Daten in oder aus Dateien oder ihre „Nutzung unmittelbar aus Dateien" in seinem Persönlichkeitsrecht beeinträchtigt zu werden (§ 1 Abs. 1 E.). Die Vorschrift begrenzt damit zugleich den Anwendungsbereich des Gesetzes. Diese deutliche Einschränkung des durch das BDSG gewährten Datenschutzes auf die Datenverarbeitung in oder aus Dateien habe ich bereits in meinem Neunten Tätigkeitsbericht kritisiert. Sie entspricht weder praktischen Bedürfnissen noch den Interessen der betroffenen Bürger. Sie berücksichtigt auch nicht die neuen Informations- und Kommunikationstechniken, insbesondere nicht die beim Einsatz moderner Bürokommunikationssysteme nicht mehr trennbare Vermengung zwischen automatisierter Datenverarbeitung und Aktenbearbeitung; sie ist insofern nicht mehr zeitgemäß.

Darüber hinaus sehe ich aber auch in der Formulierung „Nutzung (der Daten) unmittelbar aus Dateien" – die so auch für die Kompetenzbeschreibung des BfD verwendet wird (§ 22 E.) – einen nicht hinnehmbaren Rückschritt in der Gewährleistung des Datenschutzes. Wenn in der Begründung des Entwurfs sinngemäß dargelegt wird, daß der Anwendungsbereich des Gesetzes durch die Einbeziehung der Nutzung personenbezogener Daten erweitert wird, so ist dies nur bedingt richtig. Denn die Datennutzung ist bisher schon zumindest Orientierungsmaßstab für die Rechtmäßigkeit der Datenverarbeitung; sie unterliegt insofern auch der datenschutzrechtlichen Überprüfung, als die Zulässigkeit einer Datenverarbeitung sich an der Erforderlichkeit „zur rechtmäßigen Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben" auszurichten hat (§ 9 Abs. 1 BDSG). In diesem Zusammenhang bedeutet Aufgabenerfüllung nichts anderes als Nutzung der Daten, die überprüfbar rechtmäßig sein muß, um den Zulässigkeitsanforderungen zu genügen.

Eine Nutzung der Daten „unmittelbar aus Dateien" dürfte indessen in der Praxis nur selten stattfinden. Sie ist allenfalls dann denkbar, wenn der Bearbeiter die für seine Aufgabenerfüllung notwendigen Daten unmittelbar vom Bildschirm abliest oder einer von ihm selbst geführten Kartei entnimmt. Im Regelfall wird er sich jedoch eines Computerausdrucks, einer Liste oder einer ähnlichen Arbeitsunterlage bedienen, die aus der Datei hergestellt wurde, aber selbst den Dateibegriff nicht erfüllt. Eine Nutzung der in dieser Weise zur Verfügung gestellten Daten würde somit nicht mehr dem BDSG unterliegen. Demgegenüber war es bisher unstreitig, daß personenbezogene Daten auch dann vom BDSG geschützt sind, wenn sie in Akten oder Listen bearbeitet, aus solchen Unterlagen entnommen oder aus dem Gedächtnis heraus verwendet werden, wenn sie nur gleichzeitig bei der verarbeitenden Stelle auch in einer Datei enthalten sind (vgl. u. a. Auernhammer, BDSG, Anm. 8 zu § 1). Ein solcher Schutz wäre künftig nicht mehr gegeben, weil die Daten nicht „unmittelbar aus Dateien" genutzt werden. Das gleiche gilt übrigens für aus Dateien durch Übersendung von Listen oder sonstigen Papierunterlagen übermittelte Daten in bezug auf den Empfänger; er wäre bei der Nutzung solcher Daten nicht mehr an das BDSG gebunden, da auch insoweit keine „Nutzung unmittelbar aus Dateien" vorläge. Die aus der Zweckbindung übermittelter Daten folgende Verwendungsbeschränkung (§ 13 Abs. 3 in Verbindung mit § 12 Abs. 2 und 3 E.) würde also entfallen.

28.2 Defizite bei der Anpassung an die technische Entwicklung

Nach der Begründung des Entwurfs ist der technologische Fortschrift auf dem Gebiet der automatisierten Datenverarbeitung ein weiterer Hauptgrund für die Weiterentwicklung des BDSG. Dem damit erhobenen Anspruch, das informationelle Selbstbestimmungsrecht auch unter den sich ändernden technischen Voraussetzungen zu sichern, wird der Entwurf nicht gerecht.

So fehlt z. B. eine Regelung der für unterschiedliche Zwecke zunehmend eingesetzten Videoüberwachung und zur Speicherung und Verwertung der dabei gewonnenen Aufzeichnungen. Ebenfalls nicht berücksichtigt ist die Entwicklung zu billigen Massenspeichern, die es heute erlaubt, Dokumente wie Briefe, Rechnungen, Fotos, Pläne oder – Blatt für Blatt – umfangreiche Akten als elektronische Faksimiles z. B. auf einer Bildplatte zu speichern. Die Datenorganisation kann dabei so gestaltet werden, daß der enge Dateibegriff des Gesetzes nicht erfüllt ist, das Gesetz auf diese moderne Form der Datenspeicherung also keine Anwendung findet, obwohl die Risiken für den Betroffenen durchaus vergleichbar sind. Wenn aber eine Datei vorliegt, so würde die dann anwendbare neue Löschungsvorschrift dazu führen, daß wegen der besonderen Eigenschaften dieser Techniken die speichernden Stellen von der Pflicht zur Löschung oft befreit wären, weil wegen der Art des Speichermediums damit ein unverhältnismäßig hoher Aufwand verbunden wäre (§ 18 Abs. 3 Nr. 3 E.). Das bedeutet aber eher weniger Datenschutz.

Auch die Entwicklung der Datenübertragung und der Bildung von Datennetzen wird nicht ausreichend berücksichtigt, denn es wird noch nicht einmal verlangt, daß die datenverarbeitenden Stellen eine Übersicht über die interne Vernetzung und über die eingerichteten Datenübertragungsmöglichkeiten von und zu anderen Stellen führen müssen. Stattdessen wird an der unzureichenden Formulierung festgehalten, nach der es genügt, daß – vielleicht erst, wenn es zu spät ist – „überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden können" (Nr. 6 der Anlage zu § 8 Abs. 1 Satz 1 E.). Und die Bestimmung für die Online-Datenübermittlung (§ 9 E.), die ich im Prinzip begrüße, läßt die Datenverwendung beim Empfänger ungeregelt. Durch die technischen Möglichkeiten ist die planmäßige Verarbeitung von Daten aus fremden Beständen fast genauso einfach wie die eigener Daten. Wenn die Technik es aber ermöglicht, Daten im Bedarfsfall zu beschaffen, ohne selbst diese Daten in Dateien zu führen, dann müßte wenigstens die weitere Verwendung der so erhaltenen Daten klar geregelt sein, was nicht vorgesehen ist. Ich räume ein, daß es schwierig sein kann, das Datenschutzrecht der technischen Entwicklung anzupassen. Der Gesetzentwurf läßt aber auch nicht erkennen, ob und welche Bemühungen dazu unternommen worden sind.

28.3 Einschränkung der Kontrollkompetenz

Auf Probleme und Einschränkungen, die sich aus der vorgesehenen Regelung der Kontrollbefugnis des BfD ergeben, habe ich in meinem Neunten Tätigkeitsbericht (S. 78f.) ebenfalls hingewiesen und insbesondere den Wegfall jeglicher Kontrolle bei der Datenerhebung kritisiert sowie die deutlichen Einschränkungen bei der Kontrolle der Einhaltung von Datenschutzvorschriften, die nicht im BDSG, sondern in anderen Gesetzen enthalten sind. Der neue Entwurf engt die Kompetenzen des Bundesbeauftragten noch weiter ein. Denn Empfehlungen zur Verbesserung des Datenschutzes sollen nach § 24 des Entwurfs nur noch gegenüber den obersten Bundesbehörden, dem Vorstand der Bundesbahn und den bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts gegeben werden. Gegenüber den nachgeordneten Behörden, bei denen die personenbezogene Datenverarbeitung einen weitaus größeren Raum einnimmt, sollen sie nur noch im Rahmen von Kontrollen möglich sein (§ 22 Abs. 2 E.), die bekanntlich schon aus Kapazitätsgründen nur in begrenztem Umfang durchgeführt werden können. Diese Neuerung verkennt, welche Bedeutung gerade den fachlichen Beratungen in Fragen des Datenschutzes als vorbeugendes Mittel zukommt. Ich habe Zweifel, ob eine solche Regelung im Interesse der datenverarbeitenden Stellen liegt.

Eine weitere Kompetenzbeschränkung ist in § 22 Abs. 4 des Entwurfs vorgesehen. Während der BfD bisher stets Auskunft zu seinen Fragen und Einsicht in Unterlagen und Akten verlangen konnte, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen, soll dies künftig nur noch im Zusammenhang mit einer Kontrolle möglich sein. Das bedeutet, daß der BfD, wenn er eine Kontrolle nicht oder noch nicht beabsichtigt, keine Fragen nach der Art und Weise der Datenverarbeitung und deren Einzelheiten stellen kann. Dieser Informationsbedarf, der sich erfahrungsgemäß aus dem Dateienregister nicht befriedigen läßt, entsteht aber gerade im Vorfeld einer Kontrolle, wenn es um die Entscheidung geht, ob eine solche notwendig ist oder nicht. Zweifelhaft erscheint mir danach auch, ob eine solche Gesetzesänderung nicht zur Folge hätte, daß bei Anrufung des BfD durch betroffene Bürger (§ 19 E.) die datenverarbeitende Stelle dem BfD Auskünfte und Stellungnahmen verweigern könnte, wenn nicht gleichzeitig eine Datenschutzkontrolle durchgeführt wird. Eine solche Regelung könnte ich nicht akzeptieren; sie widerspricht der Auffassung des Bundesverfassungsgerichts, wonach auch im Interesse eines vorgezogenen Rechtsschutzes durch rechtzeitige Vorkehrungen die Beteiligung der Datenschutzbeauftragten von erheblicher Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung ist.

28.4 Unzureichende Beteiligung am Referentenentwurf

Schließlich sehe ich mich auch veranlaßt, die Art und Weise meiner Beteiligung an der Vorbereitung

des Referentenentwurfs zu kritisieren. Eine Beteiligung im Rahmen der Abstimmung innerhalb des Bundesministeriums des Innern, bei dem der BfD eingerichtet ist (§ 17 Abs. 5 Satz 1 BDSG) hat nicht stattgefunden. Der Entwurf wurde mir erst zur Kenntnis gegeben, als er den Ressorts, den Ländern und den Verbänden zugeleitet wurde. Dieses Verfahren ist jedenfalls insoweit ungewöhnlich, als der Entwurf erhebliche Änderungen meiner Befugnisse vorsieht. Wäre derartiges vergleichsweise bei einer obersten Bundesbehörde beabsichtigt, so wäre diese bereits bei den Vorarbeiten zu den einschlägigen Regelungen zu beteiligen gewesen, also längst bevor ein solcher Entwurf anderen Stellen oder der Öffentlichkeit zugänglich gemacht wird. Darüber hinaus wurde durch die Versendung des Entwurfs (nur an die obersten Bundesbehörden und gesonderte Zuleitung an BfD) auch noch bewirkt, daß mir die obersten Bundesbehörden ihre Stellungnahmen nicht zuleiten und ich mich daher auch dazu nicht äußern kann. Ich habe für dieses von der bisherigen Praxis abweichende Vorgehen kein Verständnis. Selbst ein Versehen dieser Art hätte es nach dem Ergebnis der Koalitionsvereinbarungen vom Frühjahr 1987 nicht geben dürfen. Danach soll für das Procedere bei der Vorbereitung und Einbringung der Entwürfe „ein möglichst transparentes Verfahren gewählt werden. Also: Frühzeitige Beteiligung der von den Regelungen berührten Ressorts und der Länder, des Datenschutzbeauftragten sowie der Verbände und sonstiger Stellen, deren Interessen durch die jeweilige Regelung berührt werden".

29. Ausland und Internationales

29.1 Europarat

Großbritannien hat als sechstes Land die Datenschutzkonvention des Europarats ratifiziert.

Die parlamentarische Versammlung hat eine Resolution über die wechselseitigen Bezüge von Datenschutz und Informationsfreiheit, das Ministerkomitee hat eine Empfehlung an die Mitgliedsstaaten über den Datenschutz bei der Verarbeitung personenbezogener Angaben im Polizeisektor verabschiedet. Vielen Punkten dieser Empfehlungen wird die polizeiliche Datenverarbeitung in der Bundesrepublik bereits gerecht, doch gibt es auch weiterführende Hinweise, die eine genauere Betrachtung durch die datenverarbeitenden Stellen verdienen. Dies gilt etwa für die Vorschäge zur Ausführung von Artikel 5 Buchstabe d der Datenschutzkonvention, wonach personenbezogene Daten genau sein und, soweit notwendig, aktualisiert werden müssen.

29.2 Interpol

Auf der Grundlage einer Vereinbarung mit dem Sitzland Frankreich wurde bei der Interpol-Zentrale eine Datenschutz-Kontrollkommission geschaffen. Der Präsident der luxemburgischen Datenschutzkommission wurde als Vorsitzender dieser Kommission berufen. Er hat der internationalen Datenschutzkonferenz über die Arbeit der Kommission berichtet. Auf der Grundlage des Berichts stimmten die Konferenzteilnehmer darin überein, daß die auftretenden Probleme eine praktische Kooperation der Datenschutzinstanzen erfordern.

29.3 Entwicklung des Datenschutzes im Ausland

Nach langjährigen Bemühungen steht die Datenschutzgesetzgebung in den Niederlanden unmittelbar vor dem Abschluß, nachdem der Gesetzentwurf das Unterhaus bereits passiert hat. Von dem früher vorgesehenen Prinzip einer Registrierung als Zulässigkeitsvoraussetzung hat man, dem internationalen Trend entsprechend, Abstand genommen. Automatische und manuelle Daten behandelt das Gesetz gleich, nur nichstrukturierte manuelle Sammlungen, die nicht leicht auswertbar sind, sind vom Gesetz ausgenommen. Stark betont wird das Prinzip der Selbstregelung: Sowohl die verschiedenen Branchen als auch die einzelnen Gesetzesadressaten sollen sich eigene Regeln geben. Erstmals wird auf dem Gebiet des Datenschutzes auch eine Verbandsklage eingeführt. Für die Bereiche der Polizei, des Strafregisters, der Staatssicherheit und für das Bevölkerungsregister sollen später bereichsspezifische Regeln in Kraft treten. Als gemeinsame Klammer fungiert jedoch das Datenschutzkontrollorgan, die „Registrierungskammer".

In Griechenland wurde ein Gesetzentwurf vorgelegt, der auf einer Abstufung der Daten in drei Empfindlichkeitsklassen beruht, eine Datenschutzkommission mit großen Vollmachten vorsieht und einen Dateienabgleich (file-matching) nur bei Zweckgleichheit erlaubt. In einer gemeinsam mit dem Europarat veranstalteten internationalen Konferenz fand eine grundlegende Diskussion des Entwurfs statt.

In mehreren Ländern dauern Untersuchungen und gesetzgeberische Bemühungen an, die einerseits der technischen Entwicklung Rechnung tragen, andererseits bürokratischen Aufwand reduzieren sollen, damit die vorhandenen Kräfte stärker problemorientiert eingesetzt werden können.

Auch in Irland wurde ein Gesetzentwurf parlamentarisch eingebracht. Er sieht einen mit Exekutivbefugnissen ausgestatteten Datenschutzbeauftragten vor und orientiert sich im übrigen an der Europaratskonvention wie auch am britischen Datenschutzgesetz.

29.4 Zusammenarbeit der Datenschutz-Kontrollinstitutionen

Die Internationale Datenschutzkonferenz fand im September 1987 in Québec City statt und damit erstmals bei einem Einzelstaat eines föderativ organisierten Landes. Unter den kanadischen Provinzen ist Québec beim Datenschutz seit einigen Jahren Vor-

reiter; andere Provinzen schließen sich jetzt an. Die Konferenz befaßte sich mit einem breit gefächerten Themenprogramm, aber auch mit den Möglichkeiten und Grenzen der unabhängigen Datenschutzkontrolle. Der Bundesbeauftragte referierte über die Volkszählung 1987 und über Datenschutzprobleme im Zusammenhang mit AIDS.

30. Bilanz

In meinem Neunten Tätigkeitsbericht habe ich über viele Einzelfragen berichtet, zu denen eine Lösung noch ausstand. Wie die nachfolgende Aufstellung zeigt, ist es in vielen Fällen gelungen, datenschutzrechtlich akzeptable Regelungen zu finden und oft auch schon in der Praxis umzusetzen. Einige Punkte sind nach wie vor offen, zum Teil deswegen, weil die Lösung so schnell nicht zu finden war, erst noch mit anderen Stellen abgestimmt werden muß oder weil ein Gesetzgebungsverfahren einzuleiten war. In einigen Fällen von bedenklichem und durch Rechtsnormen nicht gedecktem Umgang mit personenbezogenen Daten, besonders bei den Sicherheitsbehörden, halten die verantwortlichen Stellen jedoch unverändert an der kritisierten Datenverarbeitung fest.

1. Auf die Notwendigkeit, die Datenverarbeitung des Ausländerzentralregisters gesetzlich zu regeln, habe ich hingewiesen (9. TB S. 15f.). Im Berichtsjahr wurden mit dem Bundesminister des Innern erste Gespräche über ein Ausländerzentralregistergesetz geführt.

2. Für die Benennung von Wahlhelfern durch Behörden habe ich dem Bundesminister des Innern empfohlen, eine geeignete Orientierungshilfe zu geben (9. TB S. 17f.). Er hat diese Anregung aufgegriffen und die in Frage kommenden Stellen darum gebeten, daß auf die Freiwilligkeit bei der Benennung von Wahlhelfern hingewiesen wird.

3. Für die Arbeitsberichte von Zivildienstleistenden, die häufig Angaben aus der Intimsphäre der betreuten Personen enthielten, habe ich Einschränkungen angeregt (9. TB S. 18f.). Nach den jetzt vorliegenden Entwürfen gehe ich davon aus, daß bald eine befriedigende Lösung in die Praxis umgesetzt wird; siehe dazu Nr. 4.6.3 in diesem Bericht.

4. Auf die Notwendigkeit, in der Kontrollmitteilungsverordnung den Sozialdatenschutz ausdrücklich zu berücksichtigen, habe ich hingewiesen (9. TB S. 20f.). Der Bundesminister der Finanzen hat diesen Vorschlag aufgegriffen, siehe dazu Nr. 6.1 in diesem Bericht.

5. Eine konsequente Trennung zwischen den Beihilfestellen und der allgemeinen Personalverwaltung habe ich gefordert (9. TB S. 22f.). Im Berichtsjahr haben weitere Stellen dieser Forderung entsprochen, siehe dazu auch Nr. 7.1.1 in diesem Bericht.

6. Gegen die in den Dienstanschlußvorschriften verlangte Speicherung der Nummer des angerufenen Gesprächspartners habe ich Bedenken geltend gemacht (9. TB S. 28f.). Meine im Berichtsjahr fortgesetzten Bemühungen, diese Zielnummernspeicherung einzuschränken, hatten bisher erst geringen Erfolg, siehe dazu Nr. 7.3 in diesem Bericht.

7. Über datenschutzrechtliche Probleme bei der Kontrolle von Verhalten und Leistung der Mitarbeiter durch Dienststellen der Deutschen Bundespost habe ich berichtet (9. TB S. 29). Nach einer längeren Unterbrechung werden die Gespräche darüber zunächst mit dem Hauptpersonalrat der Deutschen Bundespost wieder aufgenommen, siehe dazu Nr. 7.4.1 in diesem Bericht.

8. Die oft sehr schleppende Behandlung meiner Anfragen durch das Bundesministerium für das Post- und Fernmeldewesen habe ich bedauert (9. TB S. 29f.). Auch im Berichtsjahr ergaben sich in einigen Fällen unverhältnismäßige und störende Verzögerungen, siehe dazu Nr. 8.2.1 in diesem Bericht.

9. Auf Verstöße von Dienststellen der Deutschen Bundespost gegen die Meldepflicht nach § 19 Abs. 4 BDSG habe ich hingewiesen (9. TB S. 30). Nachdem ich auch im Berichtsjahr mehrfach Unterlassungen dieser Art festgestellt habe, mußte ich den zugrundeliegenden Organisationsmangel beanstanden, siehe dazu Nr. 8.2.2 in diesem Bericht.

10. Das Fehlen einer Unterrichtung der Funkfernsprechteilnehmer über die Registrierung der Verbindungsdaten habe ich kritisiert (9. TB S. 31). Die Deutsche Bundespost bereitet jetzt das dazu notwendige Informationsmaterial vor, siehe auch Nr. 8.3.2 in diesem Bericht.

11. Für die baldige Schaffung einer Möglichkeit, aus dem Verkehrszentralregister auch Teilauskünfte zu erteilen, wenn die Auskunft über alle Eintragungen offensichtlich nicht erforderlich ist, habe ich mich eingesetzt (9. TB S. 37). Der Bundesminister für Verkehr hat im Berichtsjahr Überlegungen für eine entsprechende gesetzliche Neuregelung mit mir erörtert, siehe dazu Nr. 9.2.2 in diesem Bericht.

12. Über die nicht erforderliche Erhebung und Speicherung der Heimatanschrift und Paßdaten ausländischer Fahrzeughalter bei der Kfz-Zulassung habe ich berichtet (9. TB S. 37f.). Aufgrund einer erneuten Erörterung des Problems im zuständigen Bund-Länder-Fachausschuß verzichten die Zulassungsstellen aller Bundesländer nunmehr auf die Erhebung und Speicherung dieser Daten.

13. Auf Datenschutzprobleme bei der Durchführung des durch Änderung des Straßenverkehrsgesetzes eingeführten Führerscheins auf Probe habe ich hingewiesen (9. TB S. 39). Die von mir angeregten Auflagen an den Nachschulungs-Kursleiter für die Behandlung der Daten über die Teil-

nehmer der Nachschulungskurse sind inzwischen durch die 6. Verordnung zur Änderung straßenverkehrsrechtlicher Vorschriften (Einfügung des § 12 d StVZO) übernommen worden.

14. Über unzureichende gesetzliche Regelungen für den Umgang des Luftfahrt-Bundesamtes mit personenbezogenen Daten und über die bei einer Wiederholungskontrolle festgestellten technischen und organisatorischen Mängel habe ich berichtet (9. TB S. 39f.). Die technischen und organisatorischen Mängel wurden zum Teil beseitigt; die vom Bundesminister für Verkehr angekündigte Prüfung, ob und wie die Bestimmungen des Luftverkehrsgesetzes und der Luftverkehrszulassungsordnung geändert bzw. ergänzt werden können, hat bisher zu keinen konkreten Lösungsansätzen geführt.

15. Auf die mögliche Beeinträchtigung der Persönlichkeitsrechte durch Videoüberwachungen im Bereich der Deutschen Bundesbahn habe ich hingewiesen (9. TB S. 41f.). Meine Informationsbesuche haben ergeben, daß die Deutsche Bundesbahn diese Mittel behutsam einsetzt, siehe dazu Nr. 9.5.2 in diesem Bericht.

16. Auf die Notwendigkeit, weitere Statistikgesetze den Grundsätzen des Volkszählungsurteils anzupassen, habe ich hingewiesen (9. TB S. 44f.). Inzwischen gibt es für verschiedene Fachstatistiken Bemühungen um entsprechende Änderungen, an denen ich zum Teil beteiligt wurde, siehe auch Nr. 10.2.1 in diesem Bericht; die Novellierung des Bevölkerungsstatistikgesetzes ist vom Bundesminister des Innern in Angriff genommen worden.

17. Auf Probleme bei der Durchführung der Agrarberichterstattung habe ich aufmerksam gemacht (9. TB S. 46). Meine Bemühungen, einige Mängel bei der Durchführung dieser statistischen Erhebung zu vermeiden, hatten keinen Erfolg, siehe dazu Nr. 10.3 in diesem Bericht.

18. Über meine Beteiligung an den Vorbereitungsarbeiten zu einem Gesetz über die Verwendung der Rentenversicherungsnummer habe ich berichtet (9. TB S. 47). Ein entsprechender Gesetzentwurf wurde im Berichtsjahr eingebracht.

19. Für die Arbeitsvermittlung habe ich angeregt, dem Arbeitssuchenden die Entscheidung zu überlassen, ob und an wen das Arbeitsamt seine Bewerbungsunterlagen weitergeben darf (9. TB S. 48). Die Bundesanstalt für Arbeit ist meiner Anregung gefolgt, siehe dazu Nr. 14.1 in diesem Bericht.

20. Von der Fachvermittlung der Arbeitsverwaltung, die für die Vermittlung von Bewerbern an internationale Organisationen zuständig ist, habe ich verlangt, vor der Weitergabe der Bewerbungsunterlagen an das Auswärtige Amt oder ein anderes Ministerium die Einwilligung des Bewerbers einzuholen (9. TB S. 48). Die Bundesanstalt für Arbeit ist dem dadurch nachgekommen, daß jeder Bewerber auf diese Weitergabe hingewiesen wird und er die Gelegenheit zum Widerspruch erhält.

21. Zur Information des Betroffenen über eine im Rahmen der Klageerwiderung mögliche Weitergabe von ärztlichen Gutachten aus der Arbeitsverwaltung an ein Gericht habe ich vorgeschlagen, einen Hinweis in die entsprechende Rechtsmittelbelehrung aufzunehmen (9. TB S. 49f.). Die Bundesanstalt für Arbeit hat diesem Vorschlag dadurch Rechnung getragen, daß sie den Hinweis in ein Merkblatt aufgenommen hat, das jedem Antragsteller ausgehändigt wird.

22. Auf Schwierigkeiten bei der Behandlung psychologischer Beurteilungen bei der Teamberatung von Arbeitssuchenden habe ich hingewiesen (9. TB S. 50). Die Bundesanstalt für Arbeit hat eine befriedigende Lösung dafür gefunden, siehe dazu Nr. 14.3.2 in diesem Bericht.

23. Über die nicht erforderliche Führung von Personalunterlagen bei der Betriebskrankenkasse des Bundesministers für Verkehr habe ich berichtet (9. TB S. 52). Die Unterlagen bei dieser Betriebskrankenkasse wurden inzwischen bereinigt.

24. Auf die Notwendigkeit, für die Datenschutzprobleme bei der Sicherheitsüberprüfung eine verfassungskonforme Lösung zu finden, habe ich hingewiesen (9. TB S. 56f.). Eine befriedigende Lösung wird erst mit entsprechenden Regelungen im Rahmen eines Geheimschutzgesetzes erreicht werden können, das jetzt vorbereitet wird; siehe dazu Nr. 18.4 in diesem Bericht.

25. Über die Beratung neuer Richtlinien für die Sicherheitsüberprüfung des Personals in kerntechnischen Anlagen habe ich berichtet (9. TB S. 57f.). In den jetzt erlassenen Richtlinien konnten weitere Verbesserungen für den Datenschutz der Betroffenen erreicht werden.

26. Auf mehrere datenschutzrechtliche Mängel bei der Führung des Kriminalaktennachweises des Bundeskriminalamtes habe ich hingewiesen (9. TB S. 58f.). Obwohl von dieser Datenspeicherung weit über 2 Millionen Personen betroffen sind, steht eine Antwort des Bundesministers des Innern auf mein Schreiben vom Oktober 1985 noch aus.

27. Die unzureichende Erfüllung der Meldepflicht nach § 19 Abs. 4 BDSG durch das Bundeskriminalamt habe ich beanstandet (9. TB S. 59f.). Auch in diesem Jahr mußten mehrfach Dateimeldungen und Errichtungsanordnungen angemahnt werden.

28. Die Ablehnung meiner Vorschläge, bei der Abteilung Staatsschutz des BKA durch geeignete Maßnahmen sicherzustellen, daß ungeklärte Verdachtsinformationen nicht weiterübermittelt werden, habe ich bedauert (9. TB S. 61). Der Bundesminister des Innern hat auf mein diesbezügliches Schreiben vom November 1985 noch immer nicht geantwortet.

29. Die aufgrund des Ausbaus der Datenverarbeitung des Bundeskriminalamtes für die Aufgaben der Abteilung Staatsschutz nicht mehr erforderliche Einspeicherung von Daten in das Nachrichtendienstliche Informationssystem NADIS habe ich beanstandet (9. TB S. 61f.). Diese Einspeicherungen, die alle so eingegebenen Daten den Geheimdiensten zur Verfügung stellen, werden unverändert fortgesetzt.

30. Eine verständliche Darstellung meiner Arbeit im Bereich des Verfassungsschutzes war mir im Rahmen des veröffentlichten Berichts nicht möglich (9. TB S. 62f.). Gegen den Entwurf der entsprechenden Teile sind diesmal Sicherheitsbedenken nur zurückhaltend geltend gemacht worden, siehe dazu Nr. 20 in diesem Bericht.

31. Auf die Behinderung meiner Kontrolltätigkeit beim Zollkriminalinstitut habe ich hingewiesen (9. TB S. 64). Auch in diesem Berichtsjahr konnte dort keine systematische Kontrolle durchgeführt werden, siehe dazu Nr. 23 in diesem Bericht.

32. Gegen die Absicht des Militärischen Abschirmdienstes, in seiner automatisierten Zentraldatei auch solche Merkmale aus Sicherheitsüberprüfungen zu speichern, die dem innersten Persönlichkeitskern zuzurechnen sind, habe ich Bedenken angemeldet (9. TB S. 65). Der Bundesminister der Verteidigung hat bis zu einer Klärung der noch offenen datenschutzrechtlichen Fragen diese Speicherung zurückgestellt.

33. Über kartellrechtliche Schwierigkeiten beim Ausschluß verschiedener Interessentengruppen von der Nutzung des SCHUFA-Systems habe ich berichtet (9. TB S. 69f.). Die beschriebene Reform des SCHUFA-Verfahrens ist jetzt im wesentlichen abgeschlossen, siehe dazu Nr. 26.2 in diesem Bericht.

Bonn, den 20. Januar 1988

Dr. Baumann

Anlage (zu 19.3)

Speicherung personenbezogener AIDS-Daten in polizeilichen Informationssystemen

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7. Dezember 1987

In zwei gemeinsamen Sitzungen von Arbeitsgruppen der ständigen Konferenz der Innenminister und -senatoren sowie der Datenschutzbeauftragten des Bundes und der Länder wurde das Problem der Speicherung von personenbezogenen AIDS-Hinweisen in polizeilichen Informationssystemen erörtert. Nach eingehender Beratung der Ergebnisse dieser Gespräche faßten die Datenschutzbeauftragten des Bundes und der Länder sowie die Datenschutzkommission des Landes Rheinland-Pfalz bei Gegenstimme des Bayerischen Landesbeauftragten für den Datenschutz folgenden Beschluß:

I.

Die Speicherung von HIV-Hinweisen soll die Eigensicherung von Polizeibeamten und eventuell den Schutz von Personen in Polizeigewahrsam gewährleisten, die mit HIV-Infizierten in Kontakt kommen. Die Datenschutzbeauftragten verkennen nicht, daß Polizeibeamte bei der Berufsausübung spezifischen Gefahren ausgesetzt sind und die notwendigen Maßnahmen ergriffen werden müssen. Insbesondere ein direkter Blutkontakt oder eine Verletzung mit infizierten Injektionskanülen bei Kontakt mit Drogenabhängigen stellen eine solche spezifische Gefährdung dar. Dem Anspruch der Polizeibeamten auf einen weitestgehenden Schutz vor einer Infektion, die zu einer tödlichen Erkrankung führen kann, steht der Anspruch der Betroffenen gegenüber, daß Datenspeicherungen nur dann vorgenommen werden, wenn diese geeignet sind, die Gefährdung wirksam zu verringern, und sie dadurch nicht unverhältnismäßig belastet werden. Hierbei ist auch zu berücksichtigen, daß eine automatisierte Speicherung von medizinischen Daten eine schwerwiegende Beeinträchtigung für die Betroffenen darstellt. Ebenso sind auch die gravierenden sozialen Folgen für diesen Personenkreis zu bedenken, wenn die gespeicherten Daten an Dritte gelangen.

II.

Sowohl medizinische Experten als auch Fachleute aus dem Sicherheitsbereich und dem Gesundheitswesen haben wiederholt Zweifel daran geäußert, daß durch die Speicherung von Informationen über HIV-Infizierte in polizeilichen Informationssystemen die Gefährdung von Polizeibeamten abgewendet werden kann. Hierfür werden folgende Gründe vorgebracht: In vielen Situationen, wie z. B. bei der Hilfeleistung für verletzte Unfallopfer, der Festnahme unbekannter Personen oder auch der plötzlichen Konfrontation mit Straftätern oder Störern, sei eine vorherige Überprüfung vorhandener Dateibestände ohnehin nicht möglich. Hinzu komme, daß der Polizei immer nur ein sehr geringer Teil der Infizierten bekannt sein werde, so daß die Polizei in jedem Fall und auch ohne besondere Hinweise Schutzmaßnahmen treffen müsse.

Angesichts dieser Zweifel, die von den Datenschutzbeauftragten geteilt werden, kann die Speicherung – wenn überhaupt – nur unter sehr eingeschränkten Voraussetzungen hingenommen werden. Möglich erscheint dies allenfalls für Situationen, in denen es mit hoher Wahrscheinlichkeit zu gewaltsamen Auseinandersetzungen mit infizierten Personen kommt; keinesfalls darf eine „AIDS-Datei" entstehen. Im übrigen wäre dabei mindestens folgendes zu beachten:

1. Die Speicherung von HIV-Hinweisen im Datenfeld der „personengebundenen Hinweise" im bundesweiten INPOL-System und in vergleichbaren Landessystemen muß eingestellt werden, da diese Hinweise bei sämtlichen Abfragen erscheinen.

2. HIV-Hinweise dürfen allenfalls in solche Dateien aufgenommen werden, in denen sie als Grundlage für die Eigensicherung bei polizeilichem Einschreiten tatsächlich in Betracht kommen.

3. Die Speicherung von HIV-Hinweisen aufgrund von Verdächtigungen und ungeprüften Informationen verbietet sich in jedem Fall. Kommt die Information vom Betroffenen selbst, muß dieser über die Tatsache und die Bedeutung der Speicherung aufgeklärt werden. Im übrigen kommt nur die Speicherung von ärztlich gesicherten Informationen in Betracht, die die Polizei rechtmäßig erlangt hat.

4. Auf die gespeicherten Daten darf nur ein besonders dazu befugter Benutzerkreis zugreifen, und dies nur zu Zwecken der Eigensicherung. Die Weitergabe an andere Stellen ist nur in besonders festzulegenden Fällen zulässig.

5. Es muß in jedem Fall erkennbar sein, wer wann den HIV-Hinweis in das System eingespeichert hat und hierfür verantwortlich ist, da nur so die Speicherungspraxis überprüft werden kann und notwendige Berichtigungen ermöglicht werden.

Sachregister

Abkürzungsverzeichnis

AO	Abgabenordnung
APIS	Arbeitsdatei PIOS innere Sicherheit
BAFl	Bundesamt für die Anerkennung ausländischer Flüchtlinge
BAG	Bundesarbeitsgericht
BAGE	Bundesarbeitsgerichtsentscheidung
BASt	Bundesanstalt für Straßenwesen
BAW	Bundesamt für Wirtschaft
BAZ	Bundesamt für den Zivildienst
BDSG	Bundesdatenschutzgesetz
BfD	Bundesbeauftragter für den Datenschutz
BfV	Bundesamt für Verfassungsschutz
BG	Berufgenossenschaft
BGB	Bürgerliches Gesetzbuch
BGBl	Bundesgesetzblatt
BGS	Bundesgrenzschutz
BHO	Bundeshaushaltsordnung
BKA	Bundeskriminalamt
BKA-AN	Bundeskriminalamt-Aktennachweis
BKK	Betriebskrankenkasse
BMA	Bundesminister für Arbeit und Sozialordnung
BMBau	Bundesminister für Raumordnung, Bauwesen und Städtebau
BMF	Bundesminister der Finanzen
BMFT	Bundesminister für Forschung und Technologie
BMI	Bundesminister des Innern
BMJ	Bundesminister der Justiz
BMJFFG	Bundesminister für Jugend, Familie, Frauen und Gesundheit
BMP	Bundesminister für das Post- und Fernmeldewesen
BMU	Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit
BMV	Bundesminister für Verkehr
BMVg	Bundesminister der Verteidigung
BMWi	Bundesminister für Wirtschaft
BND	Bundesnachrichtendienst
BPersVG	Bundespersonalvertretungsgesetz
BRH	Bundesrechnungshof
BStatG	Bundesstatistikgesetz
BT-Drs.	Bundestags-Drucksache
Btx	Bildschirmtext
BVerfG	Bundesverfassungsgericht
BVerfGE	Bundesverfassungsgerichtsentscheidung
BVerwGE	Bundesverwaltungsgerichtsentscheidung
BVS	Bundesverband für den Selbstschutz
BZR	Bundeszentralregister
BZRG	Bundeszentralregistergesetz
BZV	Befristeter Zählvergleich
CR	Computer und Recht (Fachzeitschrift)
DB	Deutsche Bundesbahn
DBP	Deutsche Bundespost
DIV	Digitale Vermittlung
DV	Datenverarbeitung
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
EWS	Elektronisches Wählsystem
FFA	Filmförderungsanstalt
FRV	Fahrzeugregisterverordnung
G 10	Gesetz zur Beschränkung der Brief-, Post- und Fernmeldegeheimnisse
GAN	Grenzaktennachweis
GG	Grundgesetz
GMBl	Gemeinsames Ministerialblatt
GOBReg	Geschäftsordnung der Bundesregierung

INPOL	Informationssystem der Polizei
ISDN	Integrated Services Digital Network
JURIS	Juristisches Informationssystem
KAN	Kriminalaktennachweis
KBA	Kraftfahrt-Bundesamt
KDV	Kriegsdienstverweigerer
KpS	Kriminalpolizeiliche personenbezogene Sammlungen
LAG	Landesarbeitsgericht
MAD	Militärischer Abschirmdienst
MiStra	Mitteilungen in Strafsachen
MiZi	Mitteilungen in Zivilsachen
NADIS	Nachrichtendienstliches Informationssystem
NJW	Neue Juristische Wochenzeitschrift
OPD	Oberpostdirektion
PC	Personal-Computer
PersVG	Personalvertretungsgesetz
PIOS	Auskunftssystem über Personen, Institutionen, Objekte und Sachen
PostVwG	Postverwaltungsgesetz
PZD	Personen-Zentral-Datei
RDV	Recht der Datenverarbeitung (Fachzeitschrift)
RVO	Reichsversicherungsordnung
SCHUFA	Schutzgemeinschaft für allgemeine Kreditsicherung GmbH
SGB I	Sozialgesetzbuch Erstes Buch
SGB X	Sozialgesetzbuch Zehntes Buch
SPUDOK	Spurendokumentationssystem
STATIS	Statistisches Informationssystem
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
StVG	Straßenverkehrsgesetz
StVZO	Straßenverkehrs-Zulassungs-Ordnung
TB	Tätigkeitsbericht*)
TEMEX	Telemetry Exchange (Fernwirkdienst der DBP)
TKO	Telekommunikationsordnung
VNP	Vorgangsnachweis Personen
Vwv-Selbstschutz	Allgemeine Verwaltungsvorschrift für Aufbau, Förderung und Leitung des Selbstschutzes
VwVfG	Verwaltungsverfahrensgesetz
VZG	Volkszählungsgesetz 1987
VZR	Verkehrszentralregister
WoBindG	Wohnungsbindungsgesetz
ZDG	Zivildienstgesetz
ZEVIS	Zentrales Verkehrsinformationssystem
ZMK	Zentrale Militärkraftfahrtstelle
ZPO	Zivilprozeßordnung

*) Erster Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 8/2460
Zweiter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 8/3570
Dritter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 9/93
Vierter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 9/1243
Fünfter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 9/2386
Sechster Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 10/877
Siebenter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 10/2777
Achter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 10/4690
Neunter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 10/6816