Deutscher Bundestag
11. Wahlperiode

Drucksache 11/3932

27. 01. 89

Sachgebiet 204

Unterrichtung

durch den Bundesbeauftragten für den Datenschutz

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

Gliederung

Zugeleitet mit Schreiben des Bundesbeauftragten für den Datenschutz vom 27. Januar 1989 — I — 192 111/13 — gemäß § 19 Abs. 2 Satz 2 des Bundesdatenschutzgesetzes.

1. Überblick über das Berichtsjahr

1.1 Einleitung

Am 9. Juni 1988 hat sich mein Amtsvorgänger Dr. Reinhold Baumann im Rahmen einer Feierstunde, bei der auch der Bundesminister des Innern und Vertreter der Medien zugegen waren, aus seinem Amt verabschiedet. Zur gleichen Zeit habe ich das Amt des Bundesbeauftragten für den Datenschutz übernommen. Bei dieser Gelegenheit habe ich Herrn Dr. Baumann sowie allen Mitarbeiterinnen und Mitarbeitern meiner Dienststelle dafür gedankt, daß sie während der vergangenen Jahre Schneisen in eine vom Datenschutz zunächst weitgehend unberührte Landschaft geschlagen haben, die — was an mir liegt — nicht mehr verwildern sollen. Entsprechend dieser Ankündigung nehme ich meine Aufgabe in Kontinuität mit der erfolgreichen Arbeit meiner Amtsvorgänger wahr. Ich habe mir das Ziel gesetzt, den Datenschutz maßgebend an den praktischen Belangen der Bürgerinnen und Bürger auszurichten und dies auch erkennbar zu machen.

Nach jetzt etwa sieben Monaten meiner Amtszeit ziehe ich folgende erste Zwischenbilanz über den Stand des Datenschutzes und die Arbeit des Bundesbeauftragten:

1. *Die Bürgerinnen und Bürger vertrauen dem Datenschutz*

   Das Vertrauen der Bürger, denen die Arbeit des Datenschutzbeauftragten gilt, zeigt sich in der unverändert beachtlichen Zahl der Eingaben, die die verschiedensten Bereiche meiner Zuständigkeit betreffen. Da beklagen sich

   - ein Arbeitssuchender über seiner Auffassung nach inhaltlich unzutreffende Unterlagen in seiner Vermittlungsakte beim Arbeitsamt,
   - ein Kraftfahrer, der infolge einer unrichtigen Eintragung im Zentralen Fahrzeugregister und einer auf dieser Basis erteilten falschen Auskunft zu Unrecht einen Bußgeldbescheid erhalten hatte,
   - Adoptiveltern über die Datenerhebung eines Rentenversicherungsträgers, durch die das Adoptionsgeheimnis verletzt wird,
   - ein ausländischer Mitbürger über ständige intensive Zollkontrollen an der Grenze, die er auf eine unrichtige Datenspeicherung zurückführt,
   - eine Bewerberin um eine Anstellung bei einer Bundesbehörde über ihrer Meinung nach unzulässige Fragen auf einem Bewerbervordruck,
   - Postkunden über den gegen ihren Willen erfolgten Eintrag ihrer Anschrift in das amtliche Telefonbuch,
   - ein Bürger über vermutete Speicherungen in Dateien des Bundeskriminalamtes, des Bundesamtes für Verfassungsschutz und des Militärischen Abschirmdienstes,
   - eine bei einer Krankenkasse Versicherte über eine nach ihrer Ansicht unzulässige Weitergabe von Gesundheitsdaten,
   - eine Personalvertretung über die Verarbeitung von Personaldaten mittels besonderer technischer Arbeitsmittel, die zur Verhaltens- und Leistungskontrolle geeignet sind,
   - ein Mitarbeiter einer Bundesbehörde über die Installation einer Videoüberwachungsanlage in einem Arbeitsraum seiner Dienststelle,
   - eine von ihrem Ehemann getrennt lebende Ehefrau darüber, daß sie ihre Arztrechnungen, aus denen sich ihre jeweiligen Erkrankungen ergeben, nur über ihren Ehemann bei der Krankenversicherung und der für die Festsetzung der beamtenrechtlichen Beihilfe zuständigen Stelle einreichen kann.

   Die Aufzählung ließe sich noch fortsetzen und einige Fälle stehen für viele ähnliche. Wichtig für mich ist daran, daß die Bürger sich — ganz im Sinne der Rechtsprechung des Bundesverfassungsgerichts — in allen Fragen, in denen sie ihr Recht auf informationelle Selbstbestimmung beeinträchtigt sehen, ganz selbstverständlich an den Datenschutzbeauftragten wenden, weil sie von ihm — und oft nur von ihm — Hilfe erwarten. Sie fragen nicht danach, ob ihr Problem Daten betrifft, die in Dateien gespeichert oder in Akten festgehalten sind. Sie halten es für gänzlich unerheblich, ob die Frage, die sie bedrückt, ein Problem der Datenverarbeitung im Sinne des Bundesdatenschutzgesetzes, der Datennutzung oder der Datenerhebung ist.

   Ich bemühe mich, in allen Fällen ohne Rücksicht darauf, ob ein Dateibezug besteht oder ob es sich um ein Problem der Datenerhebung, der Datenverarbeitung oder der Datennutzung handelt, dem Bürger zu helfen, obwohl infolge zu enger Auslegung des § 19 BDSG meine Kompetenz dafür gelegentlich angezweifelt wird. Es freut mich, daß die ganz überwiegende Zahl der Bundesbehörden mich auch in solchen Fällen bei meinen Bemühungen nach besten Kräften unterstützt. Sie sind offenbar mit mir der Auffassung, daß es auch im Interesse der Verwaltung ist, wenn einem Bürger geholfen wird, und sei es auch „nur" dadurch, daß staatliches Handeln verständlich gemacht wird. Fälle, in denen unter Hinweis auf meine fehlende Kompetenz Auskünfte verweigert wurden, sind äußerst selten und konnten meistens durch Gespräche bereinigt werden.

   Nicht selten nimmt eine Behörde meine Intervention oder das Anliegen des Bürgers zum Anlaß, ihre Verwaltungspraxis generell zu ändern. Eingaben von Bürgerinnen und Bürgern haben daher oft auch über den Einzelfall hinaus Bedeutung.

   Eine Gesamtwertung der Eingaben zeigt, wie hoch das Recht auf informationelle Selbstbestimmung geschätzt wird und welche Bedeutung die Bürger dem Amt des Datenschutzbeauftragten als Garanten dieses Rechts beimessen.

Dieses aus den Eingaben der Bürger gewonnene Bild wird bestärkt durch eine vom Institut für praxisorientierte Sozialforschung — IPOS — erstellte Studie „Einstellungen zu aktuellen Fragen der Innenpolitik 1988", die der Bundesminister des Innern in Auftrag gegeben hatte. Aufgrund einer Repräsentativbefragung nennt die Studie unter den zehn von der Bevölkerung als sehr wichtig eingestuften politischen Aufgaben und Zielen auch die Verbesserung des Datenschutzes. Dies werte ich als eine sehr bedeutsame Aussage, wenn man bedenkt, daß in dieser Kategorie sich auch so wesentliche Politikbereiche wie Bekämpfung der Arbeitslosigkeit, Umweltschutz, Sicherung der Renten oder die Ausländerpolitik befinden. Der hohe Anspruch an den Datenschutz ergibt sich auch aus der Feststellung, daß etwa zwei Drittel der Bevölkerung — mit steigender Tendenz — der Ansicht sind, der Staat habe zu viel Einblick in die ganz privaten Dinge des Bürgers.

Die Schlußfolgerung, die ich aus diesen Feststellungen ziehe, kann nur sein, nicht darin nachzulassen, den Datenschutz wirksam durchzusetzen und weiter auszubauen, aber auch — soweit ich das aus eigenen Erkenntnissen verantworten kann — unbegründete Besorgnisse der Bürger zu zerstreuen.

2. *Der Datenschutz bei den Behörden*

Der Bundeskanzler hat für die Bundesregierung anläßlich des 40. Jahrestages der Verabschiedung der Allgemeinen Erklärung der Menschenrechte durch die Generalversammlung der Vereinten Nationen am 9. Dezember 1988 vor dem Deutschen Bundestag eine Erklärung abgegeben. Er hat darin u. a. ausgeführt:

„Wir erkennen in der Erklärung der Vereinten Nationen die geistigen Wurzeln unserer eigenen Wertvorstellungen wieder:

- insbesondere die Überzeugung von der Einzigartigkeit jedes einzelnen Menschen,
- eine Überzeugung, die neben vielem anderen Christen und Juden verbindet,
- sowie die Idee einer jedem Menschen eigenen Individualsphäre, die der Staat zu respektieren hat."

Das Bekenntnis der Bundesregierung zur Idee einer jedem Menschen eigenen Individualsphäre, die der Staat zu respektieren hat, ist für den Datenschutz von grundsätzlicher Bedeutung und eine Bestätigung von hohem Wert.

Mein Amtsvorgänger hat in seinem letzten Tätigkeitsbericht festgestellt, das Datenschutzbewußtsein habe bei den öffentlichen Stellen zugenommen. Dem kann auch ich zustimmen. Gleichwohl muß gesagt werden, daß in der praktischen Handhabung des Datenschutzes bei den Behörden noch manches verbessert werden kann und muß.

Der Deutsche Bundestag hat bereits im Zusammenhang mit der Beratung des Zweiten und Dritten Tätigkeitsberichts des Bundesbeauftragten für den Datenschutz im Jahr 1982 seine Auffassung bekundet, es sei zweckmäßig, „daß die Bundesregierung möglichst frühzeitig von der Möglichkeit des § 19 Abs. 2 Satz 1 des Bundesdatenschutzgesetzes Gebrauch macht, soweit sie beabsichtigt, Gesetzentwürfe einzubringen, in denen bereichsspezifische datenschutzrechtliche Fragen berührt werden". Tatsächlich ist meine Beteiligung an der Vorbereitung von Gesetzen aber noch recht unterschiedlich. Fällen mit vorbildlicher rechtzeitiger Einschaltung des Datenschutzbeauftragten, in denen auch versucht wird, auf die Belange des Datenschutzes einzugehen, stehen solche gegenüber, in denen erkennbar ist, daß die Beteiligung eher als Erfüllung einer ungeliebten Pflicht angesehen wird. Zuweilen sieht man zunächst völlig davon ab, den Rat des Bundesbeauftragten für den Datenschutz einzuholen. In diesen Fällen versuche ich, meine Auffassung noch den zuständigen Ausschüssen des Parlaments mitzuteilen, bei denen ich in aller Regel auf großes Verständnis stoße. Besser wäre es freilich, eine generelle Beteiligung des Bundesbeauftragten für den Datenschutz bei der Vorbereitung aller datenschutzrechtlich bedeutsamen Regierungsentwürfe vorzusehen. Dies könnte am besten durch eine entsprechende Regelung im neuen Bundesdatenschutzgesetz erreicht werden. Erfahrungsgemäß führt eine solche Beteiligung zur Verbesserung der Entwürfe sowohl im Interesse der betroffenen Bürger als auch zum Nutzen der vollziehenden Behörden.

Auch die organisatorischen und technischen Maßnahmen zur Sicherung des Datenschutzes lassen noch zu wünschen übrig. Wenn in einer Bundesbehörde auch 1988 wichtige Aufgaben des Datenschutzes und der Datensicherheit überhaupt noch keinem Bediensteten organisatorisch zugewiesen waren, wenn Behörden einräumen müssen, daß für die Aufgaben des Datenschutzes keine ausreichende Personalkapazität zur Verfügung gestellt war, wenn datenschutzrechtlich gebotene Erlasse „wegen anderer dringender dienstlicher Tätigkeit" zunächst zurückgestellt werden oder wenn technische Maßnahmen, die zum kleinen ABC der Datensicherheit gehören, fehlen, so entstehen Zweifel, ob der Datenschutz überall den Stellenwert besitzt, der ihm aufgrund unseres Verfassungsverständnisses zukommen muß.

3. *Rechtliche Grundlagen*

Das Bundesverfassungsgericht hat entgegen manchen Erwartungen von seinen Aussagen in der Entscheidung zum Volkszählungsgesetz nichts zurückgenommen. Es hat vielmehr — in Kenntnis der teilweise kritischen Reaktionen auf das Volkszählungsurteil — seine Rechtsprechung zum Recht auf informationelle Selbstbestimmung konsequent fortentwickelt. Dies ist im Zusammenhang mit der Volkszählung in mehreren Beschlüssen über die Nicht-Annahme von Verfassungsbeschwerden geschehen, aber auch in weiteren Entscheidungen, die mit dem damaligen Streitgegenstand nichts zu tun haben. Stets wird das verfassungsrechtlich geschützte Recht auf informationelle Selbstbestimmung bestätigt, keiner der dazu im Volkszählungs-

urteil entwickelten Grundsätze wird aufgegeben oder auch nur relativiert. Von besonderem Interesse sind dabei die Entscheidungen, in denen klargestellt wird, daß das Recht auf informationelle Selbstbestimmung sich keineswegs nur auf die Verarbeitung personenbezogener Daten in automatisierten Verfahren beschränkt. Im sog. Entmündigungsbeschluß des Bundesverfassungsgerichts vom 9. März 1988 — 1 BvL 49/86 — (NJW 88 S. 2031) heißt es zum Recht auf informationelle Selbstbestimmung: „In dieses Recht wird nicht nur dann eingegriffen, wenn der Staat vom einzelnen die Bekanntgabe persönlicher Daten verlangt oder diese der automatisierten Datenverarbeitung zuführt. Die Möglichkeiten und Gefahren der automatischen Datenverarbeitung haben zwar die Notwendigkeit eines Schutzes persönlicher Daten deutlicher hervortreten lassen, sind aber nicht Grund und Ursache ihrer Schutzbedürftigkeit. Das Recht auf informationelle Selbstbestimmung schützt vielmehr wegen seiner persönlichkeitsrechtlichen Grundlage generell vor staatlicher Erhebung und Verarbeitung personenbezogener Daten und ist nicht auf den jeweiligen Anwendungsbereich der Datenschutzgesetze des Bundes und der Länder oder datenschutzrelevanter gesetzlicher Sonderregelungen beschränkt."

Wesentlich für die Fortentwicklung des Datenschutzes erscheint mir auch eine andere Entscheidung des Bundesverfassungsgerichts vom 25. Juli 1988 — 1 BvR 109/85 — (NJW 88 S. 3009), in der ausgeführt wird: „Es (Anm.: das Recht auf informationelle Selbstbestimmung) beinhaltet die Befugnis des einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Diese Verfügungsbefugnis erfaßt auch solche personenbezogenen Informationen, die zum Bereich des wirtschaftlichen Handelns gehören." Diese Klarstellung einer umstrittenen Frage kann nicht außer Acht gelassen werden, wenn es darum geht, angemessene Datenschutzregelungen auch für den nicht-öffentlichen Bereich zu schaffen.

4. *Anpassung unseres Rechts*

Der Auftrag des Bundesverfassungsgerichts im Volkszählungsurteil vom 15. Dezember 1983, die zum Recht auf informationelle Selbstbestimmung entwickelten Grundsätze in der Gesetzgebung umzusetzen, ist in wichtigen Bereichen noch nicht erfüllt. Ich verkenne nicht, daß auf einzelnen Gebieten bereits große Anstrengungen mit befriedigenden Ergebnissen unternommen worden sind; frühere Tätigkeitsberichte des Bundesbeauftragten für den Datenschutz geben darüber Aufschluß.

Die Anpassung unserer Rechtsordnung an die vom Bundesverfassungsgericht zum Recht auf informationelle Selbstbestimmung formulierten Maximen muß jedoch mit Nachdruck fortgesetzt werden. Sie ist in vielen Bereichen dringlich geworden.

Von ganz besonderer Bedeutung für die Zukunft des Datenschutzes ist der am 20. Dezember 1988 vom Bundeskabinett beschlossene Entwurf eines Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes. Ich begrüße diese Vorlage, auch wenn sie in wichtigen Punkten meinen Vorstellungen nicht entspricht (vgl. hierzu unten 25.1), weil es jetzt möglich erscheint, bei zügiger Beratung die darin enthaltenen Einzelgesetze noch in dieser Legislaturperiode zu verabschieden. Insbesondere die vorgesehenen Neuregelungen für die Informationsverarbeitung der Nachrichtendienste sind äußerst dringlich geworden, nachdem einige Gerichte die Übergangszeit, während der ein eigentlich verfassungswidriger Rechtszustand noch hingenommen werden kann, als bereits abgelaufen bezeichnet haben. Es kommt hinzu, daß das Bundesverfassungsgericht in einer Entscheidung vom 14. Juli 1988 — 1 BvR 537/81 — seine frühere Rechtsprechung zum sog. Übergangsbonus mit der Feststellung fortgesetzt hat, daß innerhalb der Übergangsfrist die bisherige Rechtspraxis nicht ohne weiteres so fortbestehen dürfte, als sei sie unbedenklich. Vielmehr „reduzieren sich die Befugnisse . . . zu Eingriffen in verfassungsrechtlich geschützte Positionen auf das, was für die geordnete Weiterführung eines funktionsfähigen Betriebs unverzichtbar ist". Ich würde meiner Aufgabe nicht gerecht werden, wenn ich bei meinen Kontrollen nicht auf diese verfassungsrechtlich gebotenen Beschränkungen des Verwaltungsvollzugs achtete, auch wenn den betroffenen Behörden daraus Schwierigkeiten erwachsen.

Ich appelliere an alle Verantwortlichen, den in einigen Bereichen, die den Bürger in besonderem Maße berühren, fragwürdigen Rechtszustand möglichst rasch zu beseitigen.

In diesem Zusammenhang verweise ich darauf, daß der am 20. Dezember 1988 beschlossene Gesetzentwurf nur einen Teil der erforderlichen Rechtsanpassung betrifft. Weitere wichtige Bereiche, wie die Strafprozeßordnung, das Gesetz über das Bundeskriminalamt, das Gesetz über den Bundesgrenzschutz, das Strafvollzugsgesetz, das Jugendgerichtsgesetz, die Regelungen über das Schuldnerverzeichnis und andere Vorschriften der Zivilprozeßordnung, das Personenstandsgesetz müssen geändert, ein Gesetz über den Arbeitnehmerdatenschutz, über Mitteilungen in Justizangelegenheiten und über das Ausländerzentralregister geschaffen werden, um nur einige besonders wichtige Vorhaben zu nennen.

5. *Wichtige Gesetze im Berichtszeitraum*

Ein politisch besonders bedeutsames Gesetzgebungswerk, an dem ich mitgewirkt habe, ist das Gesetz zur Strukturreform im Gesundheitswesen. Ich stelle mit Befriedigung fest, daß es in gemeinsamer Arbeit mit dem Bundesminister für Arbeit und Sozialordnung und den zuständigen Ausschüssen des Bundestages gelungen ist, ein datenschutzgerechtes Gesetz zu erarbeiten. Ich sehe einen besonderen Erfolg darin, daß der nicht selten behauptete angeblich unvermeidbare Gegensatz zwischen den fachlichen Erfordernissen und den Geboten des Datenschutzes auf einem besonders schwierigen Gebiet überwunden werden konnte (vgl. hierzu unten 12.1).

Ein weiteres wesentliches Vorhaben, zu dem ich Stellung genommen habe, ist das Poststrukturgesetz (vgl. hierzu unten 6.1).

6. *Bedeutung von technischer Entwicklung und Organisation für den Datenschutz*

Bei datenschutzrechtlichen Kontrollen und Beratungen treten organisatorische und technische Fragen immer mehr in den Vordergrund. Die Entwicklung der Datenverarbeitung von dem Modell des Zentralen Großrechners hin zu Arbeitsplatzcomputern, den Neuen Medien und den durch das Stichwort ISDN gekennzeichneten Angeboten der Kommunikationstechnik mit vielfältigen und ganz anderen Problemlagen, als sie in den Beratungen des Bundesdatenschutzgesetzes vor über 12 Jahren absehbar waren, hat ihr Spiegelbild auch in der Arbeit und im Vorgehen der Datenschutzkontrolle. Dieser Wandel durchzieht schon die Tätigkeitsberichte des Bundesbeauftragten für den Datenschutz in den vergangenen Jahren; vor allem in den letzten Berichten nimmt die Behandlung von Datensicherungsproblemen und von organisatorischen Fragen mit Bezug zum Datenschutz breiteren Raum ein. Die aufgezeigte Entwicklung wird sich fortsetzen. Ebenso wie sich in den Verwaltungen immer mehr Personal an die neuen Arbeitsmittel gewöhnen und den Umgang mit ihnen erlernen muß, ist auch die Datenschutzkontrollinstanz gezwungen, sich darauf einzustellen, und zwar nicht nur bei der Qualifizierung der Mitarbeiter für die neuen Techniken, sondern auch bei der Kontrolle ihrer Anwendung und der Beratung der Behörden. Während früher das Rechenzentrum die Datenverarbeitung zentral erledigte und die Ergebnisse zur konventionellen Weiterverarbeitung zur Verfügung stellte, finden große Teile der Datenverarbeitung jetzt mit Hilfe von Personalcomputern statt, die am gleichen Arbeitsplatz sowohl die Daten verfügbar halten als auch die Bearbeitungsgänge automatisiert unterstützen. Die Datenschutzkontrolle ist dadurch und auch angesichts der Vernetzung der Geräte erheblich schwieriger und aufwendiger geworden; die Datensicherung gewinnt ungleich höhere Bedeutung. Ich sehe in diesen technikbedingten Veränderungen neue Herausforderungen an den Datenschutz, denen ich mich zu stellen habe. Als ersten Schritt dazu habe ich ein eigenes Referat Informationstechnik in meiner Dienststelle eingerichtet.

7. *Gentechnologie*

Mit welch neuen Fragen, die dem Datenschutz auf den ersten Blick fernzuliegen scheinen, ich mich befassen muß, zeigt das Beispiel der Gentechnologie. Hier gilt es dafür zu sorgen, daß bei den hohen Erwartungen, die von den verschiedensten Seiten an die Nutzung dieser Technologie gestellt werden, die Persönlichkeitsrechte der Betroffenen und namentlich auch der Datenschutz in diesem sehr sensiblen Bereich von vornherein berücksichtigt werden. Es handelt sich dabei um außerordentlich komplexe Fragen, die im Grunde nur interdisziplinär bearbeitet werden können. Der Rechtsausschuß des Bundestages hat eine öffentliche Anhörung zur Frage der Genomanalyse im Strafverfahren durchgeführt, bei der ich als Sachverständiger gehört wurde. Weitere Fragen wie „Genomanalyse im Arbeitsverhältnis" oder „Genomanalyse und pränatale Diagnostik" werden in einem Arbeitskreis der Datenschutzbeauftragten von Bund und Ländern erörtert. Der zuständige Ausschuß des Deutschen Bundestages erwartet hierzu entsprechend den Empfehlungen der Enquete-Kommission „Chancen und Risiken der Gentechnologie" eine Stellungnahme der Datenschutzbeauftragten (vgl. auch unten 9.3).

8. *Internationale Entwicklung*

Datenverarbeitung findet zunehmend im internationalen Rahmen statt. Im Zusammenhang mit dem Ausbau der Europäischen Gemeinschaft, aber auch im übrigen internationalen Bereich gewinnen deshalb auch Fragen des Datenschutzes an Bedeutung. Die Entwicklung auf diesem Gebiet verläuft bisher recht unkoordiniert. Die datenschutzrechtlichen Standards sind ungleich und die Regelungsansätze entsprechend den vielfältigen nationalen Rechtssystemen und Rechtstraditionen durchaus unterschiedlich. Bisher ist noch kein Konzept in Sicht, mit dem in überschaubarer Zeit eine Vereinheitlichung auf breiter Front und hohem Niveau erreicht werden könnte. Die Internationale Konferenz der Datenschutzbeauftragten wird sich im August 1989 in Berlin mit diesem Fragenkreis beschäftigen.

9. *Gesamtbewertung*

Nach den Eindrücken und Erfahrungen des ersten Halbjahres meiner Amtszeit, die in den nachfolgenden Abschnitten dieses Berichts noch im einzelnen wiedergegeben sind, zeigt sich ein komplexes Bild:

Der Datenschutz hat bei den Bürgern und in der öffentlichen Meinung einen hohen Stellenwert. Bei den Behörden bestehen trotz eines im ganzen gesehen erfreulichen Maßes an Datenschutzbewußtsein bei der praktischen Durchführung des Datenschutzes noch Defizite. Ich hoffe, daß es gelingt, Rechtsgrundlagen für die Datenverarbeitung und den Datenschutz zu schaffen, die den Geboten der Verfassung entsprechen und die Interessen der Bürger und der Verwaltung angemessen berücksichtigen. Andererseits habe ich die Sorge, daß die allenthalben zu beobachtende Entwicklung der Informationstechnik und deren Anwendung in der Praxis — wie auch auf anderen Gebieten des technischen Fortschritts — weitergehen werden, ohne daß die zum Schutz der Betroffenen notwendigen Regulative damit Schritt halten. Zunehmende Risiken für den Datenschutz erwachsen auch aus der internationalen Entwicklung. In dieser Situation bedarf es der Phantasie und der Kraft aller Verantwortlichen, das Recht des Bürgers auf informationelle Selbstbestimmung zu wahren. Dem Bundesbeauftragten für den Datenschutz fällt dabei die Rolle eines Anwalts des Bürgerrechts auf informationelle Selbstbestimmung, notwendigerweise aber auch die eines Mahners und Ratgebers zu. Ich

habe diese Aufgabe gern übernommen, weil ich zuversichtlich bin, daß ich bei den gesetzgebenden Körperschaften, der Bundesregierung und der Verwaltung die für den Erfolg meiner Arbeit maßgebliche Resonanz finde.

1.2 Kontrollen und Beratungen

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

Bundesminister des Innern

Bundesminister der Justiz

Bundeszentralregister

Bundesdruckerei

Bundesgesundheitsamt

Statistisches Bundesamt

Bundesamt für Zivilschutz (Technisches Hilfswerk)

Deutsche Bundesbahn

Bundesnachrichtendienst

Militärischer Abschirmdienst

Bundeskriminalamt

Deutsches Patentamt

Kraftfahrt-Bundesamt

Bundesamt für Finanzen (Informationszentrale für steuerliche Auslandsbeziehungen)

Bundesamt für Wirtschaft

Bundesaufsichtsamt für das Versicherungswesen

Bundesanstalt für Straßenwesen

Deutsche Bundespost u. a. mit folgenden Dienststellen

- Fernmeldetechnisches Zentralamt
- zwei Fernmeldeämter
- ein Postamt

Sozialwissenschaftliches Institut der Bundeswehr

Oberprüfungsamt für die höheren technischen Verwaltungsbeamten

Bahnpolizei

Landwirtschaftliche Alterskasse Hessen-Nassau

eine Bank unter Aufsicht des Bundes

vier Dienststellen des Bundesministers der Verteidigung in den USA

zwei Arbeitsämter

zwei Kreiswehrersatzämter

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

Thema	Art der Erledigung
Novellierung der Rechtsgrundlagen für Einzelstatistiken, u. a. zum Entwurf eines Agrarstatistikgesetzes, zur Änderung des Straßenverkehrsunfallstatistikgesetzes und des Lohnstatistikgesetzes	Beratung und schriftliche Stellungnahmen gegenüber Ausschüssen des Deutschen Bundestages und den zuständigen Bundesministerien
Achter und Neunter Tätigkeitsbericht	Teilnahme an neun Sitzungen der Berichterstattergruppe „Tätigkeitsberichte des Bundesbeauftragten für den Datenschutz" des Innenausschusses des Deutschen Bundestages
Speicherung von Ein- und Ausreisedaten von Bürgern arabischer Staaten	Beratung und schriftliche Stellungnahme gegenüber dem Innenausschuß des Deutschen Bundestages und dem BMI
Entwurf eines Dritten Gesetzes zur Änderung des Waffengesetzes	Schriftliche Stellungnahme gegenüber dem Innenausschuß des Deutschen Bundestages und Anhörung durch den Ausschuß
Genomanalyse im Strafverfahren	Schriftliche Stellungnahme gegenüber dem Rechtsausschuß des Deutschen Bundestages und Anhörung durch den Ausschuß
Entwurf eines Artikelgesetzes zur Neufassung des Bundesdatenschutzgesetzes und des Verwaltungsverfahrensgesetzes	Schriftliche Stellungnahme gegenüber dem BMI
Entwurf eines Gesetzes zur Strukturreform im Gesundheitswesen (Gesundheits-Reformgesetz — GRG)	— Beratung und schriftliche Stellungnahme gegenüber dem BMA — Schriftliche und mündliche Stellungnahmen gegenüber dem Ausschuß für Arbeit und Sozialordnung des Deutschen Bundestages und Anhörung durch den Ausschuß
Erstes Gesetzes zur Änderung des Sozialgesetzbuches (1. SGBÄndG)	— Beratung und schriftliche Stellungnahme gegenüber dem BMA — Schriftliche und mündliche Stellungnahmen gegenüber dem Ausschuß für Arbeit und Sozialordnung des Deutschen Bundestages und Anhörung durch den Ausschuß
Neustrukturierung der Deutschen Bundespost	— Schriftliche Stellungnahme gegenüber dem BMP und anschließende Erörterung von Einzelfragen mit BMP — Schriftliche und mündliche Stellungnahmen gegenüber dem Ausschuß für das Post- und Fernmeldewesen des Deutschen Bundestages und Anhörung durch den Ausschuß
Entwurf eines Gesetzes über den Bundesnachrichtendienst	Schriftliche Stellungnahme gegenüber dem Staatssekretär beim Bundeskanzler
Weisung über Einrichtung von Dateien beim Bundesnachrichtendienst	Beratung des Staatssekretärs beim Bundeskanzler
Schaffung von Diskretionszonen bei konsularischen Stellen	Schriftliche Stellungnahme gegenüber dem AA

Thema	Art der Erledigung
Auswertung der Protokolle des Zentralen Verkehrsinformationssystems (ZEVIS) beim Kraftfahrt-Bundesamt	Beratung und schriftliche Stellungnahme gegenüber BMI, BMF und KBA
Entwurf eines Bundesverfassungsschutzgesetzes	Schriftliche Stellungnahme gegenüber dem BMI und Besprechung
Entwurf eines Bundesverfassungsschutzmitteilungsgesetzes	Schriftliche Stellungnahme gegenüber dem BMI und Besprechung
Entwurf eines Bundeskriminalamtsgesetzes	Schriftliche Stellungnahme gegenüber dem BMI
Entwurf eines Gesetzes über das Ausländerzentralregister	Schriftliche Stellungnahme gegenüber dem BMI
Sicherheitsrichtlinien	Beratung und schriftliche Stellungnahme gegenüber dem BMI
Neufassung des Verkartungsplans der Abteilung VI des BfV	Beratung und schriftliche Stellungnahme gegenüber dem BMI
Neukonzeption der Merkmalspeicherung im Rahmen des Verfahrens Sicherheitsüberprüfung beim BfV	Schriftliche Stellungnahme gegenüber dem BMI
Verschiedene neue Dateien beim BfV	Schriftliche Stellungnahmen gegenüber dem BMI
Datenverarbeitung der Zentralstelle zur Bekämpfung der unerlaubten Einreise von Ausländern bei der Grenzschutzdirektion	Schriftliche Stellungnahme gegenüber dem BMI
Bewerbungsverfahren beim BGS	Beratung und schriftliche Stellungnahme gegenüber dem BMI
Speicherung von AIDS-Daten in INPOL	Schriftliche Stellungnahme gegenüber dem BMI
Entwurf einer Neufassung des Gesetzes zum Schutz Deutschen Kulturgutes gegen Abwanderung	Schriftliche Stellungnahme gegenüber dem BMI
Entwurf eines Gesetzes zur Ergänzung des Katastrophenschutzgesetzes und anderer Vorschriften hierzu	Schriftliche Stellungnahme gegenüber dem BMI
Überarbeiteter Vorentwurf eines Fünften Gesetzes zur Änderung und Ergänzung des Personenstandsgesetzes	Schriftliche Stellungnahme gegenüber dem BMI
Informationstechnisches System zur Unterstützung bei Kostenrechnungen im Dienstrechtsbereich (ISKB)	Beratung und schriftliche Stellungnahme gegenüber dem BMI
Durchführung des Gesetzes über Personalausweise und des Paßgesetzes	Schriftliche Stellungnahme gegenüber dem BMI
Fehlleitungsgefahr bei Telex und Teletex	Schriftliche Empfehlung an den BMI
Strafprozeßordnung; Vorschläge für allgemeine Bestimmungen über die Speicherung, Verwendung und Übermittlung personenbezogener Daten durch die Strafverfolgungsbehörden	Schriftliche Stellungnahme gegenüber dem BMJ
Zivilprozeßordnung	Schriftliche Stellungnahme gegenüber dem BMJ
Referentenentwurf eines Ersten Gesetzes zur Änderung des Jugendgerichtsgesetzes	Schriftliche Stellungnahme gegenüber dem BMJ

Thema	Art der Erledigung
Arbeitspapier zur Novellierung des Bundeszentralregistergesetzes	Schriftliche Stellungnahme gegenüber dem BMJ
Entwurf eines Betreuungsgesetzes	Schriftliche Stellungnahme gegenüber dem BMJ
Justizstatistikinformationssystem (JUSTIS)	Beratung und schriftliche Stellungnahme gegenüber dem BMJ
Entwurf eines Gesetzes zur Änderung von Vorschriften über das Schuldnerverzeichnis und Entwurf einer Verordnung über die Erteilung von Abdrucken und Listen aus dem Schuldnerverzeichnis	Beratung und schriftliche Stellungnahme gegenüber dem BMJ
Entwurf eines Steuerreformgesetzes 1990	Schriftliche Stellungnahme gegenüber dem BMF
Entwurf einer Kontrollmitteilungsverordnung	Schriftliche Stellungnahme gegenüber dem BMF
Entwurf einer Steuerdaten-Abruf-Verordnung	Schriftliche Stellungnahme gegenüber dem BMF
Neufassung der Dienstanschlußvorschriften — DAV —	Schriftliche Stellungnahme und Beratung gegenüber dem BMF
Förderung der Unternehmensberatung	Beratung und schriftliche Stellungnahme gegenüber dem BMWi und dem Bundesamt für Wirtschaft
Datenübermittlung an Verwertungsgesellschaften nach § 20a Urheberrechtswahrnehmungsgesetz	Beratung und schriftliche Stellungnahme gegenüber dem BMWi, dem Bundesamt für Wirtschaft und dem Deutschen Patentamt
Entwurf eines Gesetzes zur Einführung eines Sozialversicherungsausweises und zur Änderung anderer Sozialgesetze	Beratung und schriftliche Stellungnahme gegenüber dem BMA
Entwurf eines Gesetzes über die Beratung von Schwangeren (Schwangerenberatungsgesetz)	Beratung und schriftliche Stellungnahme gegenüber dem BMA
Entwurf eines Gesetzes zur Änderung des Künstlersozialversicherungsgesetzes	Schriftliche Stellungnahme gegenüber dem BMA sowie Beratung des BMA und der zuständigen Ausschüsse des Bundestages
Einrichtung eines Organisationsdienstes für nachgehende Untersuchungen (ODIN) durch die Unfallversicherungsträger	Beratung und schriftliche Stellungnahme gegenüber dem BMA
Durchführung eines Forschungsvorhabens über die Lage Arbeitsloser	Beratung des BMA
Entwurf eines Gesetzes über den Militärischen Abschirmdienst (MADG)	Schriftliche Stellungnahme gegenüber dem BMVg
Novellierung des Wehrpflichtgesetzes	Beratung des BMVg
Gesetzliche Regelung für eine Veröffentlichung der beim Luftfahrt-Bundesamt gespeicherten Daten der Eigentümer von Luftfahrzeugen	Beratung und schriftliche Stellungnahme gegenüber dem BMV
Änderung der Telekommunikationsordnung	Beratungen und schriftliche Stellungsnahmen gegenüber dem BMP
Änderung der Postordnung	Beratungen und schriftliche Stellungnahmen gegenüber dem BMP

Thema	Art der Erledigung
Einsatz von Buchungs- und Berechtigungskarten im Telefondienst	Beratung des BMP und des Fernmeldetechnischen Zentralamtes
Erlaß über Bahnhofsverbotskarteien	Beratung des Vorstandes der Deutschen Bundesbahn
Automatisierte Fahrkartenausgabe	Beratung und schriftliche Stellungnahme gegenüber der Deutschen Bundesbahn
Automatisierte Personaldatenverarbeitung einschließlich PC-Einsatz, Telefondatenverarbeitung, Textverarbeitung und entsprechende Dienstvereinbarungen	Beratungen und schriftliche Stellungnahmen gegenüber mehreren Behörden und Personalvertretungen
SCHUFA-Kreditinformationssystem	Zusammenarbeit mit den Aufsichtsbehörden der Länder
Datenschutz in der Versicherungswirtschaft	Zusammenarbeit mit den Aufsichtsbehörden der Länder
Datenschutz bei Handels- und Wirtschaftsauskunfteien	Zusammenarbeit mit den Aufsichtsbehörden der Länder

1.3 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; 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 BDSG und gegen untergesetzliche Normen beim Bundeskriminalamt und Bundesamt für Verfassungsschutz (s. 15.2 und 16.3)
Bundesminister der Justiz	Verstoß gegen das Personalaktengeheimnis und § 19 Abs. 4 BDSG beim Deutschen Patentamt (s. 5.1)
Bundesminister der Verteidigung	— Verstöße gegen das BDSG und gegen untergesetzliche Normen beim MAD (s. 21.1.2) — Verstoß gegen § 20a Wehrpflichtgesetz (Eignungs- und Verwendungsprüfung) (s. 21.2.1)
Bundesminister für Jugend, Familie, Frauen und Gesundheit	Verstoß gegen § 19 Abs. 3 BDSG (unzureichende Unterstützung meiner Mitarbeiter bei einer Kontrolle beim Bundesgesundheitsamt) (s. 14.1)
Bundesminister für das Post- und Fernmeldewesen	— Nicht ordnungsgemäßer PC-Einsatz in einem Fernmeldeamt (s. 6.6) — Unzulässige Speicherung der Verbindungsdaten im Funktelefondienst (Verstoß u. a. gegen § 9 BDSG) (s. 6.2) — Verstoß gegen Datenschutzbestimmungen und gegen postinterne Vorschriften in einem Einzelfall

Bundesanstalt für Arbeit	Verstoß gegen das Sozialgeheimnis durch ein Arbeitsamt in einem Einzelfall
Bundesversicherungsanstalt für Angestellte	Verstoß gegen das Sozialgeheimnis (s. 13.1)
Vorstand der Deutschen Bundesbahn	Verstoß gegen das BDSG bei der Übermittlung von Daten der Bahnhofsverbotskartei an die Kriminalpolizei Köln (s. 18.)
eine Ersatzkasse	Verstoß gegen das Sozialgeheimnis (s. 12.2)
Landwirtschaftliche Alterskasse Hessen-Nassau	Verstöße gegen § 6 (Datensicherung), § 15 (nicht ordnungsgemäße Führung der Übersicht) und § 19 Abs. 4 BDSG (Dateimeldungen zu meinem Register) (s. 13.2)

1.4 Kooperation

Durch die Novellierung einiger Landesdatenschutzgesetze ist in den letzten Jahren die bis dahin weitgehend bestehende Rechtseinheit im Datenschutz teilweise verloren gegangen. Dies ist im Grundsatz zu bedauern. Erfreulich ist allerdings, daß es sich bei den Neuregelungen um bürgerfreundlichere, den Forderungen des Volkszählungsurteils des Bundesverfassungsgerichts besser entsprechende Gesetze handelt. Deshalb ist zu wünschen, daß die anzustrebende Rechtseinheit möglichst bald auf der Grundlage der neueren Ländergesetze wieder hergestellt wird. Die gute Zusammenarbeit mit den Landesbeauftragten für den Datenschutz und der Datenschutzkommission Rheinland-Pfalz konnte unbeeinflußt von dieser hoffentlich nur vorübergehenden Auseinanderentwicklung des Datenschutzrechts im wesentlichen erfolgreich fortgesetzt werden. Obwohl die gegenseitige Abstimmung bei Stellungnahmen zu allgemein interessierenden Gesetzentwürfen gelegentlich wegen unterschiedlicher Auffassungen mühsam und zeitraubend ist, so halte ich es doch für sachdienlich, gemeinsame Antworten des Datenschutzes auf die datenschutzrechtlich bedeutsamen Rechtssetzungsvorhaben und auf den verstärkten Einsatz von Datenverarbeitungstechniken in fast allen Lebensbereichen zu suchen.

Die wichtigsten Themen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der ihr zuarbeitenden Arbeitskreise waren im Berichtsjahr

- die polizeiliche Datenverarbeitung bis zum Erlaß bereichsspezifischer gesetzlicher Regelungen (dazu Konferenzbeschluß vom 14. 3. 1988, Anlage 1)
- der Gesetzentwurf zur Neufassung des Bundesdatenschutzgesetzes (dazu Konferenzbeschluß vom 6. 6. 1988, Anlage 2)
- der Gesetzentwurf zur Strukturreform im Gesundheitswesen (dazu Konferenzbeschluß vom 6. 6. 1988, Anlage 3)
- die Datensicherheit beim Einsatz kleinerer Datenverarbeitungsanlagen (dazu Konferenzbeschluß vom 10. 10. 1988, Anlage 4)
- der Gesetzentwurf zur Poststrukturreform (dazu Konferenzbeschluß vom 10. 10. 1988)
- der Entwurf einer Steuerdatenabrufverordnung (dazu Konferenzbeschluß vom 10. 10. 1988, Anlage 5)
- aktuelle Probleme des Datenschutzes bei der Telekommunikation (dazu Konferenzbeschluß vom 10. 10. 1988)
- die Neukonzeption des Ausländerzentralregisters
- die Novellierung der Strafprozeßordnung
- Datenschutzprobleme bei der Gentechnologie.

Auch im Berichtsjahr habe ich die Gelegenheit wahrgenommen, durch Teilnahme an den Sitzungen und durch die Mitarbeit in besonderen Arbeitsgremien des Düsseldorfer Kreises, in dem die Aufsichtsbehörden der Länder (§§ 30, 40 BDSG) gemeinsame Probleme beraten, mich über den Datenschutz im nicht-öffentlichen Bereich zu informieren und an der Lösung der dort auftretenden Probleme mitzuwirken. Das wichtigste Ergebnis war die seit langem diskutierte Neufassung der Schweigepflichtentbindungsklauseln der Versicherungswirtschaft, für die ein akzeptabler Kompromiß gefunden werden konnte. Einzelheiten dazu und zu anderen Themen aus dem nicht-öffentlichen Bereich sind unter Nr. 23. dargestellt.

Neben der Zusammenarbeit mit Datenschutzkontrollinstanzen ist für mich auch die Diskussion mit Institutionen innerhalb und außerhalb der öffentlichen Verwaltung wichtig, die sich mit Fragen der Datensicherung beschäftigen. Besonders erwähnen möchte ich hier den interministeriellen Ausschuß für die Sicherheit in der Informationstechnik (ISIT), die Arbeitsgemeinschaft für wirtschaftliche Verwaltung (AWV) und meine Mitarbeit in Gremien des Deutschen Instituts für Normung e.V. (DIN).

1.5 Öffentlichkeitsarbeit

Das Interesse der Öffentlichkeit an meiner Arbeit ist groß und nimmt noch immer zu. So stieg z. B. die Zahl der Besuchergruppen, die sich in meiner Dienststelle über meine Arbeit informierten und über den Datenschutz diskutierten, im Berichtsjahr auf über fünfzig an. Diese direkten Gespräche, bei denen zwar nicht

ein bestimmter Beschwerdefall im Mittelpunkt steht, aber doch immer eigene Erfahrungen der beteiligten Bürger mit öffentlicher oder nicht-öffentlicher Verwaltung die Themen bestimmen, geben mir oft auch Hinweise für meine Arbeit. Sie zeigen auch, daß einzelne Erfahrungen mit zu weitgehender, unnötiger oder auch nur undurchsichtiger Verarbeitung personenbezogener Daten leicht verallgemeinert werden und zur Besorgnis Anlaß geben, die technische Entwicklung führe „zwangsläufig" zu mehr Überwachung.

Nach wie vor groß ist auch das Interesse an den von mir herausgegebenen Broschüren

- Bürgerfibel Datenschutz,
- Der Bürger und seine Daten und
- Der Bürger und seine Daten im Netz der sozialen Sicherung.

Häufig auf Einzelanforderungen, aber auch zu Unterrichts- und Schulungszwecken an Bildungseinrichtungen, Behörden und Firmen habe ich von diesen Broschüren im Berichtsjahr insgesamt etwa 112 000 Exemplare versandt.

Überwiegend aus jeweils aktuellem Anlaß haben meine Mitarbeiter und ich wieder zahlreiche Presse- und Rundfunkinterviews gegeben und Journalisten über die Hintergründe von Datenschutzfragen und die damit zusammenhängenden Datenverarbeitungen informiert; in einigen Fällen habe ich auch durch besondere Erklärungen die Medien auf wichtige Fragen aufmerksam gemacht. Die faire und überwiegend positive Darstellung meiner Arbeit ist oft nicht nur für meine Bemühungen hilfreich, sondern sie zeigt auch den Bürgern, daß wirksamer Datenschutz Gefährdungen der Bürgerrechte — auch durch neue Datenverarbeitungstechniken — erfolgreich abwenden kann.

In vielen Vorträgen und Seminarveranstaltungen haben meine Mitarbeiter und ich für den Datenschutz geworben sowie über meine Arbeit und die Anforderungen berichtet, die richtig verstandener Datenschutz an die Datenverarbeitung und die Datenverarbeiter stellt. Ich begrüße das große Interesse an diesem Thema, das sich sowohl bei speziell fachlich als auch bei allgemein politisch orientierten Veranstaltern zeigt. Veranstaltungen dieser Art bieten immer wieder Gelegenheit, außerhalb der Kontrolltätigkeit und ohne den Druck einer aktuellen Kontroverse um Verständnis für den Datenschutz zu werben. Die intensive Mitwirkung meiner Mitarbeiter an den Seminaren der Bundesakademie für öffentliche Verwaltung, aber auch in anderen Fortbildungseinrichtungen trägt sicher dazu bei, daß Datenschutzverstöße von vornherein vermieden werden und meine Dienststelle noch mehr als eine Einrichtung bekannt wird, deren Beratung gesucht werden sollte.

1.6 Die Dienststelle

Für die 32 Angehörigen der Dienststelle und den Dienstbetrieb war das wichtigste Ereignis im Berichtsjahr der Wechsel im Amt des Bundesbeauftragten für den Datenschutz. Nach Ablauf der fünfjährigen Amtszeit meines Vorgängers händigte mir der Bundesminister des Innern am 30. Mai 1988 meine Ernennungsurkunde aus. Ich habe die äußere Organisation der Dienststelle im Interesse einer kontinuierlichen Fortsetzung der Arbeit im wesentlichen beibehalten und auch die bewährten Arbeitsabläufe nicht verändert.

Eine organisatorische Neuerung erschien mir allerdings geboten, nämlich die Einrichtung eines selbständigen Referats „Informationstechnik". Nachdem sich einerseits die Beratung zu bereichsspezifischen Gesetzgebungsvorhaben von datenschutzrechtlichem Belang und andererseits die Behandlung von praktischen Problemen der Datensicherung im Zusammenhang mit neuen Informations- und Kommunikationstechniken (s. auch oben 1.1) als die beiden neuen Arbeitsschwerpunkte der Dienststelle herausgebildet haben, lag es nahe, die auf dem einen Gebiet tätigen Mitarbeiter mit vorwiegend juristischer Vorbildung von den technisch-organisatorischen Fragen zu entlasten und das auf jenem anderen Gebiet vorhandene technisch-organisatorische Spezialwissen in einer besonderen Arbeitseinheit zusammenzufassen. Nur so konnte die erforderliche Arbeitskapazität im technisch-organisatorischen Bereich geschaffen werden, um dem insoweit bestehenden Kontroll- und Beratungsbedarf verantwortlich Rechnung zu tragen. Die Maßnahme hat sich schon nach kurzer Zeit bewährt.

Das Personal für das neue Referat „Informationstechnik" ließ sich nur durch Umsetzung entsprechend qualifizierter Mitarbeiter aus anderen Referaten gewinnen, wodurch dort zum Teil empfindliche Lücken entstanden sind. Auch das neue Referat ist noch unzureichend besetzt. Ich muß deshalb dringend darum bitten, meiner Dienststelle die für ein Mindestmaß an kompetenter Kontrolle und Beratung erforderlichen Stellen zu bewilligen. Dabei verkenne ich weder die Notwendigkeiten einer sparsamen Personalwirtschaft noch die in den letzten Jahren vereinzelt bewilligten Verbesserungen des Stellenplans meiner Dienststelle, für die ich dankbar bin. Sie entsprechen jedoch noch nicht dem schon vor Jahren im einzelnen dargelegten Bedarf und berücksichtigen auch nicht die neuen Anforderungen, die auch vom Innenausschuß des Deutschen Bundestages gesehen werden, ohne daß daraus allerdings die erforderlichen Konsequenzen gezogen wurden. Dies schließe ich daraus, daß dort im Rahmen der Beratungen zum Bundeshaushalt 1989 Anträge der Fraktion der SPD und der Fraktion DIE GRÜNEN auf Verbesserung der Personalausstattung des BfD abgelehnt wurden, obwohl auch die Koalitionsfraktionen eine Personalverstärkung für wünschenswert hielten (vgl. Bericht des Haushaltsausschusses zum Entwurf des Haushaltsgesetzes 1989, Drucksache 11/3230, S. 2).

Das schon von meinen Amtsvorgängern mit dem Bundesministerium des Innern abgesprochene Verfahren über die personelle Besetzung der Dienststelle hat sich auch im Berichtsjahr bewährt. Es gewährleistet, daß in meiner Dienststelle Mitarbeiter nur mit meiner Zustimmung verwendet werden. Die Einbindung in den Personalkörper eines großen Geschäftsbereichs erleichtert einerseits die Gewinnung qualifizierter Mitarbeiter und gibt andererseits diesen die Möglich-

keit, sich nach einer gewissen Zeit der Tätigkeit im Datenschutz für eine andere Aufgabe im Geschäftsbereich des BMI zu bewerben. Dabei können Mitarbeiter nicht selten besser gefördert werden als dies in einer kleinen Dienststelle, wie sie der Bundesbeauftragte für den Datenschutz darstellt, möglich wäre.

Seit Anfang des Berichtsjahres wird in der Dienststelle zeitgemäße Informationstechnik zur Bewältigung der Service-Funktionen eingesetzt. Es besteht die Absicht, damit mittelfristig auch das hier geführte Dateienregister automatisiert zu verwalten, dessen Umfang zunimmt und nach dem Entwurf zur Novellierung des Bundesdatenschutzgesetzes auch die konventionell geführten Dateien der Behörden und sonstigen öffentlichen Stellen des Bundes umfassen soll. Daneben dienen die beschafften Geräte der praxisnahen Selbstschulung meiner Mitarbeiter, was ich angesichts der zunehmenden Technikorientierung der Kontrollaufgaben als hoch einzuschätzenden Vorteil betrachte.

Die meiner Dienststelle für Sachausgaben zur Verfügung stehenden Haushaltsmittel sind knapp, aber ausreichend bemessen. Wenn die Gesamtausgaben des Kapitels 06 07 im Haushaltsplan 1989 niedriger veranschlagt sind als im Berichtsjahr 1988, so beruht dies ausschließlich darauf, daß im Jahr 1988 einmalige Ausgaben für Ausstattungsgegenstände und für die Renovierung des Dienstgebäudes zu leisten waren. Daraus gelegentlich abgeleitete Vermutungen, daß mir die nach § 17 Abs. 5 BDSG zustehende notwendige Sachausstattung vorenthalten werde, sind unbegründet.

2. Innere Verwaltung

2.1 Asylverfahren

2.1.1 Durchführung des Schengener Übereinkommens

Die Regierungen der Staaten der Benelux-Wirtschaftsunion, der Bundesrepublik Deutschland und der Französischen Republik haben sich in dem Übereinkommen von Schengen betreffend den schrittweisen Abbau der Kontrollen an den gemeinsamen Grenzen (GMBl 1986, S. 79ff.) u. a. verpflichtet, soweit erforderlich ihre Regelungen in bestimmten Teilbereichen des Ausländerrechts gegenüber Angehörigen von Staaten, die nicht Mitglieder der Europäischen Gemeinschaften sind, zu harmonisieren. Nach Mitteilung des Bundesministers des Innern wird in diesem Rahmen angestrebt,

- jedem Asylbewerber das Recht auf Prüfung seines Asylantrags in einem Vertragsstaat zu gewährleisten,
- jedoch die Einreichung paralleler oder sukzessiver Asylanträge durch denselben Ausländer in verschiedenen Vertragsstaaten zu vermeiden.

Dies soll dadurch erreicht werden, daß vertraglich festgelegt wird, welcher Vertragsstaat bei Vorliegen bestimmter Kriterien jeweils für die Durchführung des Asylverfahrens zuständig ist. Der im Einzelfall zuständige Staat soll zugleich verpflichtet werden, einen Asylbewerber gegebenenfalls von einem anderen Vertragsstaat auf dessen Ersuchen zu übernehmen oder zurückzunehmen.

Um die Zuständigkeit festzustellen, ist vorgesehen, daß zwischen genau bezeichneten Behörden der Vertragsstaaten auf Ersuchen eines Vertragsstaates auch Informationen zur Identität, zu Ausweispapieren, Aufenthalten, Reisewegen und zum Stand eines etwaigen Asylverfahrens ausgetauscht werden. Die entsprechenden Regelungen, an denen derzeit gearbeitet wird, sollen in einen ratifizierungsbedürftigen Vertrag aufgenommen werden.

Ich habe hierzu deutlich gemacht, daß die Übermittlung personenbezogener Daten von Asylbewerbern an einen anderen Vertragsstaat wegen des damit verbundenen Eingriffs in das Recht auf informationelle Selbstbestimmung einer gesetzlichen Grundlage bedarf. In dieser sind die Interessen der Vertragsstaaten an geordneter Durchführung von Asylverfahren und die Belange der betroffenen Asylbewerber sorgfältig abzuwägen. Ich habe den Bundesminister des Innern um Unterrichtung über den Entwurf der entsprechenden Vertragsbestimmungen gebeten und meine Beratung angeboten. Eine Antwort steht noch aus.

2.1.2 Gesundheitsdaten von Asylbewerbern

In meinem Zehnten Tätigkeitsbericht (S. 15) habe ich mich mit der Frage auseinandergesetzt, ob eine ausreichende Rechtsgrundlage für die routinemäßige ärztliche Untersuchung der Asylbewerber besteht. Der Bundesminister für Jugend, Familie, Frauen und Gesundheit hat mir auf Anfrage mitgeteilt, die Arbeitsgemeinschaft der Leitenden Medizinalbeamten der Länder habe diese Frage eingehend beraten. Im Hinblick auf unterschiedliche Ansichten sei aber zunächst der Ausschuß für Seuchen- und Umwelthygiene der Konferenz der für das Gesundheitswesen zuständigen Minister und Senatoren der Länder eingeschaltet worden. Ich hoffe, daß die Diskussion möglichst bald zu einer den Belangen des Datenschutzes entsprechenden Lösung führt.

2.2 Ausländerzentralregister

Der Bundesminister des Innern hat mir im August 1988 den Referentenentwurf eines Gesetzes über das Ausländerzentralregister (AZR-Gesetz, Stand: 12. Juli 1988) zugeleitet. Ich habe hierzu in Abstimmung mit Landesbeauftragten für den Datenschutz schriftlich Stellung genommen. Eine den Anforderungen des Volkszählungsurteils des Bundesverfassungsgerichts entsprechende gesetzliche Regelung für das Ausländerzentralregister habe ich bereits seit Jahren gefordert (vgl. frühere Tätigkeitsberichte, zuletzt 9. TB S. 15f.).

Mit einer gesetzlichen Regelung nach dem Muster des Regierungsentwurfs werden allerdings die datenschutzrechtlichen Defizite im Bereich des Ausländerrechts nicht vollständig beseitigt. Es bedarf weiterer Gesetzesvorschriften, um Eingriffe in das informationelle Selbstbestimmungsrecht von Ausländern auf

eine klare rechtliche Grundlage zu stellen, z. B. darüber

- welche tatsächlichen Ereignisse Einreisebedenken begründen und in welcher Weise AZR-Auskünfte, in denen Einreisebedenken vermerkt sind, verwertet werden dürfen,
- welcher Zweckbindung Informationen aus dem AZR bei dem Empfänger von AZR-Auskünften unterliegen.

Als noch nicht abgeschlossen betrachte ich auch die zwischen mir und dem Bundesminister des Innern bereits 1986 eingeleitete Erörterung der Frage, ob nicht für bestimmte Ausländergruppen (EG-Angehörige, Staatenlose) auf eine zentrale Speicherung personenbezogener Daten teilweise verzichtet werden kann und muß (vgl. 9. TB a. a. O.).

Einer Ergänzung bedarf der vorliegende Gesetzentwurf im übrigen besonders bezüglich der Dauer der Aufbewahrung und des Zeitpunkts der Löschung personenbezogener Daten im Register sowie zur Sicherstellung der Protokollierung von Datenübermittlungen für Zwecke der datenschutzrechtlichen Kontrolle, aber auch zur Berichtigung falscher Auskünfte nach Änderung eines im AZR gespeicherten Datums durch die mitteilende Behörde. Letzteres gilt insbesondere — aber nicht nur — für Abrufe im automatisierten Verfahren. Eine Protokollierung sollte Aufzeichnungen über die im Auskunftsersuchen verwendeten Daten, die übermittelten Daten (wegen des unterschiedlichen Umfangs der Auskunft bei Ersuchen zu verschiedenen Zwecken derselben Auskunftsberechtigten), den Zeitpunkt der Übermittlung und den Empfänger der Daten enthalten. Die für das Verkehrszentralregister und das Zentrale Verkehrsinformationssystem (ZEVIS) geschaffenen Gesetzesbestimmungen, namentlich die §§ 30 a Abs. 3 und 4 sowie 36 Abs. 6 und 7 des Straßenverkehrsgesetzes, könnten hier als Vorbild dienen. Auch sollte — so habe ich empfohlen — im Gesetz selbst festgelegt werden, welche Behörden welche Auskünfte im automatisierten Verfahren abrufen dürfen.

Daten über Deutsche — auch wenn sie zugleich eine ausländische Staatsangehörigkeit besitzen (Doppelstaater) — dürfen nicht im Ausländerzentralregister gespeichert werden. Dieses von mir von Anfang an befürwortete Prinzip soll in dem vorliegenden Entwurf insofern eingeschränkt werden, als die Speicherung von Daten von Personen vorgesehen ist, „deren Antrag auf Feststellung der Eigenschaft als Deutscher oder auf Übernahme oder Anerkennung als Vertriebener abgelehnt oder wegen erheblicher Zweifel am Bestehen der erforderlichen Voraussetzungen voraussichtlich abgelehnt werden wird oder dem innerhalb von sechs Monaten nach der Einreise nicht stattgegeben worden ist". Dies bedeutet, daß ein Aussiedler, solange sein Status noch nicht festgestellt ist, bei Anwendung des AZR-Gesetzes für eine Übergangszeit von sechs Monaten grundsätzlich einem Deutschen, danach aber einem Ausländer gleichgestellt wird. Eine solche Regelung erscheint mir im Grundsatz vertretbar. Ich habe aber empfohlen zu prüfen, ob angesichts der gegenwärtigen Aussiedler-Zahlen eine Frist von sechs Monaten nach Einreise nicht zu kurz ist, um dem Betroffenen Gelegenheit zu geben, Zweifel an seiner Eigenschaft als Deutscher auszuräumen, und über den Antrag zu entscheiden.

2.3. Neue Personalausweise und Pässe

Im Jahre 1988 habe ich bei der Bundesdruckerei erstmals eine datenschutzrechtliche Kontrolle des Verfahrens zur Herstellung der neuen Personalausweise und Pässe durchgeführt. Dem sind vor Aufnahme der Produktion dieser Dokumente im Rahmen der Erprobung mehrere Beratungsbesuche vorausgegangen, bei denen ich zahlreiche datenschutzrechtliche Verbesserungen empfohlen habe (vgl. 9. TB S. 14 f., 10. TB S. 16). Meine Mitarbeiter haben sich jetzt davon überzeugen können, daß die Verfahrensabläufe in der Praxis den datenschutzrechtlichen Anforderungen und meinen hierzu gegebenen Empfehlungen sehr weitgehend entsprechen.

Ein besonders wichtiger Punkt meiner Kontrolle war ein inzwischen verbessertes Verfahren zur Erkennung von mehrfach vergebenen Seriennummern. Auf diese Problematik bin ich bereits in meinem Zehnten Tätigkeitsbericht (S. 16 ff.) eingegangen. Ich habe seinerzeit empfohlen, durch geeignete Verfahren die Herstellung eines Ausweisdokuments mit bereits anderweitig vergebener Seriennummer durch die Bundesdruckerei von vornherein auszuschliessen. Dieser Empfehlung ist der Bundesminister des Innern nur insoweit gefolgt, als bei der Bundesdruckerei inzwischen zwar ein Verfahren eingesetzt wird, das eine mehrfach vergebene Seriennummer zu erkennen vermag, aber nicht verhindern kann, daß zunächst ein solches Dokument hergestellt wird. Es ist jedoch sichergestellt, daß ein solcher Personalausweis oder Paß die Bundesdruckerei nicht mehr — wie früher — verläßt und ordnungsgemäß vernichtet wird. Die bestellende Behörde erhält einen Hinweis auf die Mehrfachvergabe.

Ein weiteres datenschutzrechtliches Problem sehe ich bei der Herstellung der neuen Pässe darin, daß der Bundesdruckerei vollständig ausgefüllte Antragsvordrucke der Paßbehörden zugehen, die neben Wohnort, Größe, Augenfarbe und Ordens- bzw. Künstlernamen auch Daten von Kindern enthalten, obwohl die Eintragung dieser letztgenannten Daten in die Pässe vorerst nicht durch die Bundesdruckerei, sondern durch die Paßbehörden selbst erfolgt. Diese Angaben werden somit für die Herstellung der Pässe von der Bundesdruckerei zur Zeit nicht benötigt.

Ähnlich verhält es sich mit personenbezogenen Daten, die die Ausweisbehörden aus verwaltungsinternen Gründen auf den Rückseiten von Anträgen auf Ausstellung von Personalausweisen oder Pässen anbringen. Auch diese Daten sind für die Herstellung der Ausweisdokumente nicht erforderlich.

Der Bundesminister des Innern hat meiner Kritik mit dem Argument widersprochen, es handele sich nicht um Datenübermittlungen von Ausweisbehörden an die Bundesdruckerei. Vielmehr betreibe die Bundesdruckerei insoweit Datenverarbeitung im Auftrag.

Demgegenüber bin ich der Ansicht, daß § 3 Abs. 3 Satz 2 Personalausweisgesetz und § 16 Abs. 3 Satz 2 Paßgesetz als bereichsspezifische Vorschriften für den Datenschutz erkennbar darauf gerichtet sind, der Bundesdruckerei nur die zur Herstellung dieser Dokumente jeweils erforderlichen Daten zugehen zu lassen. Im übrigen kann auch nicht von einer Datenverarbeitung im Auftrag durch die Bundesdruckerei ausgegangen werden. Auftragsdatenverarbeitung liegt nur vor, wenn der Auftrag sich ausschließlich auf die Verarbeitung personenbezogener Daten bezieht und nicht noch andere Tätigkeiten zum Gegenstand hat. Ziel der Weitergabe personenbezogener Daten in Form der als Datei anzusehenden Antragsformulare ist hier primär nicht eine Datenverarbeitung durch die Bundesdruckerei für die Ausweisbehörden, sondern vielmehr die Herstellung der Personalausweise und Pässe in eigener (durch den Bundesgesetzgeber geregelter) Verantwortung. Der Bundesdruckerei personenbezogene Daten zur Verfügung zu stellen, die sie zur Herstellung der Ausweisdokumente nicht benötigt, widerspricht somit auch dem im allgemeinen Datenschutzrecht, namentlich in § 10 BDSG, enthaltenen Grundsatz der Erforderlichkeit.

An der Erörterung dieser Probleme sind auch die Landesbeauftragten für den Datenschutz und die Datenschutzkommission Rheinland-Pfalz beteiligt. Sie teilen meine Auffassung und haben sich mit Empfehlungen gleichen Inhalts an die Innenressorts der Länder gewandt. Ich habe dem Bundesminister des Innern empfohlen, diese Bemühungen zu unterstützen und die Bundesdruckerei anzuweisen, bei der Gestaltung und der Herstellung von Antragsformularen den Beschränkungen, die die Gesetze vorsehen, Rechnung zu tragen.

In einer Reihe von Eingaben haben sich Bürger über die Schreibweise von Umlauten und Datumsangaben in der Lesezone der maschinenlesbaren Personalausweise und Pässe beschwert. Ihre Namen würden im allgemeinen Teil des Personalausweises oder Passes richtig — also mit Umlauten und „ß" —, in der Lesezone aber verändert wiedergegeben. Hier werde z. B. ein „ü" als „ue", ein „ß" als „ss" wiedergegeben.

Personalausweisgesetz und Paßgesetz sehen jeweils die Angabe des Familiennamens im allgemeinen Teil und in der Lesezone vor. Dies bedeutet nach meinem Verständnis, daß in beiden Fällen eine authentische und gleiche Wiedergabe des Familiennamens verlangt wird.

Der Bundesminister des Innern ist demgegenüber der Auffassung, für die Lesezone sei § 1 Abs. 3 Personalausweisgesetz bzw. § 4 Abs. 2 Paßgesetz maßgebend, wonach die Ausweisdokumente „eine Zone für das automatische Lesen" enthalten. Entsprechend dieser Zweckbestimmung sei die Lesezone „nach internationalen Standards so gestaltet, daß die in ihr enthaltenen Angaben auch in anderen Staaten automatisch gelesen werden könnnen". Die Lesezone entspreche der Empfehlung der Internationalen Zivil-Luftfahrt-Organisation (ICAO), einer Sonderorganisation der Vereinten Nationen.

Auf meine Empfehlung, die Verordnungen zur Bestimmung der Muster der Personalausweise und der Pässe diesen Anforderungen anzupassen, ist der Bundesminister des Innern bislang nicht eingegangen.

Ein ähnliches Problem stellt sich auch bei der Wiedergabe von Datumsangaben in der Lesezone. So sehen die genannten Verordnungen für die Wiedergabe des Geburtsdatums des Ausweisinhabers und der Gültigkeitsdauer des Ausweises in der Lesezone die Reihenfolge Tag, Monat, Jahr vor. Tatsächlich werden diese Daten in der Lesezone des Personalausweises und der Pässe in umgekehrter Reihenfolge — nämlich Jahr, Monat, Tag — wiedergegeben. Ich vermag nicht auszuschließen, daß dies im Einzelfall zu einer Fehlinterpretation der in der Lesezone enthaltenen Daten Anlaß geben kann. Da die Muster der Dokumente als Teil der Rechtsverordnung der tatsächlichen Gestaltung der Ausweise leichter angepaßt werden können als umgekehrt, habe ich dem Bundesminister des Innern empfohlen, entsprechende Änderungen der Rechtsverordnungen vorzusehen.

2.4 Bundesanstalt Technisches Hilfswerk

Bei der Bundesanstalt Technisches Hilfswerk (THW) habe ich im zurückliegenden Jahr eine datenschutzrechtliche Kontrolle durchgeführt. Dabei wurde die Verarbeitung der personenbezogenen Daten der THW-Helfer auf den verschiedenen Ebenen der Bundesanstalt vom Ortsverband bis hin zur Leitung des THW verfolgt.

Gegenüber dem Bundesminister des Innern habe ich angeregt, künftig ein Einsichtsrecht des Helfers in die Helferakte ausdrücklich vorzusehen. Auch sollte der Umfang der Datenübermittlungen zu den Landesverbänden und der Leitung des THW auf die Erforderlichkeit hin überprüft werden. So übermitteln z. B. Ortsverbände über den jeweils zuständigen Geschäftsführer eine Vielzahl von Daten der Helfer an den Landesverband zum Zweck der Lehrgangsbeschickung, obwohl die Daten dort für diese Aufgabe nur teilweise benötigt werden.

Mängel zeigten sich auch bei der Führung der nach § 15 BDSG geforderten Übersicht und der vorgeschriebenen Meldungen von Dateien zu dem bei mir geführten Register sowie bei der Veröffentlichung von Dateien im Bundesanzeiger.

Einen weiteren Schwerpunkt der Kontrolle stellte der Einsatz der automatisierten Datenverarbeitung, namentlich von Personalcomputern, bei der Verarbeitung von Helferdaten dar. Die automatisierte Datenverarbeitung ist im Bereich des THW unkontrolliert und im wesentlichen ungeregelt gewachsen. Maßnahmen, diesen Bereich übersichtlich, funktionssicher und datenschutzgerecht zu gestalten, wurden praktisch ausschließlich in lokaler Eigeninitiative getroffen. Sie sind weitgehend unzureichend. Ein besonderes Problem stellt hierbei der Einsatz privater oder nicht THW-eigener Personalcomputer dar, die z. B. im Bereich der Datensicherung eine Reihe von Schwachstellen erkennen ließen.

Insgesamt hat mir die Kontrolle der Bundesanstalt Technisches Hilfswerk gezeigt, daß dem Datenschutz in diesem Bereich noch nicht ausreichend Beachtung

geschenkt worden ist. Als ein geeignetes Mittel zur Abhilfe sehe ich zunächst eine Bestandsaufnahme der bisherigen im Bereich des THW verfügbaren personenbezogenen Daten an. In einem weiteren Schritt müßte, orientiert an dem Kriterium der Erforderlichkeit zur Aufgabenerfüllung, geprüft und entschieden werden, ob und in welchem Umfang an welcher Stelle eine automatisierte Datenverarbeitung zugelassen werden sollte. Diese Maßnahmen halte ich nicht nur aus Gründen des Datenschutzes für erforderlich; sie gewährleisten auch, daß im Bedarfsfalle und ggf. auch unabhängig vom planmäßigen Bediener die automatisierte Datenverarbeitung auch wirklich zur Steuerung und Unterstützung des Einsatzes der Helfer zur Verfügung steht.

In einer ersten Reaktion hat mich der Bundesminister des Innern wissen lassen, daß 1989 eine Untersuchung beim THW über Einsatzpotentiale der Informationstechnik durchgeführt werden soll. In diesem Zusammenhang sei auch beabsichtigt, den für jede Speicherung erforderlichen Datenumfang zu ermitteln und festzulegen.

Ich werde die Entwicklung weiter verfolgen.

2.5 Zivildienst

2.5.1 Aufbewahrung von Anerkennungsunterlagen

Mit dem Bundesminister für Jugend, Familie, Frauen und Gesundheit erörtere ich schon seit längerer Zeit Fragen der Dauer der Aufbewahrung von Anerkennungsunterlagen der anerkannten Kriegsdienstverweigerer beim Bundesamt für den Zivildienst (s. 9. TB S. 18, 10. TB S. 19).

Aufgrund meines Drängens hat der Bundesminister inzwischen angeordnet, daß die Anerkennungsunterlagen beim Bundesamt für den Zivildienst nicht erst nach Vollendung des 60. Lebensjahres der Betroffenen, sondern bereits „frühestens sechs Monate" nach Dienstende des Kriegsdienstverweigerers vernichtet werden. Ich betrachte dies zwar als einen beachtlichen Schritt in die richtige Richtung, habe dem Bundesminister aber wiederholt dargelegt, daß die notwendige Vernichtung der Vorgänge des Anerkennungsverfahrens — einschließlich der darin enthaltenen, besonders schutzwürdigen Daten über die Gewissensentscheidung des Betroffenen — unmittelbar nach bestandskräftiger Anerkennung erfolgen sollte. Die Vernichtung sollte durch die für das Anerkennungsverfahren zuständige Abteilung des Bundesamtes für den Zivildienst erfolgen, nachdem der Anerkennungsbescheid sowie etwa schon während des Anerkennungsverfahrens ausdrücklich vorgetragene Einsatzwünsche des Betroffenen der für den Einsatz zuständigen Abteilung dieses Amtes zugeleitet worden sind. Noch ist offen, ob der Bundesminister für Jugend, Familie, Frauen und Gesundheit meinen Vorstellungen folgen wird. Zugleich wiederhole ich die schon in meinen früheren Berichten gegebene Empfehlung, gesetzliche Festlegungen darüber zu treffen, für welchen Zeitraum Anerkennungsunterlagen des Kriegsdienstverweigerers aufbewahrt werden dürfen und welche Daten aus diesen Unterlagen für welche Zwecke genutzt werden dürfen.

2.5.2 Arbeitsberichte von Zivildienstleistenden

Der Bundesminister für Jugend, Familie, Frauen und Gesundheit hat mir mitgeteilt, daß die Dienstanweisung für Zivildienstleistende, die in der Individuellen Schwerstbehindertenbetreuung eingesetzt sind, inzwischen in Kraft getreten ist (vgl. 10. TB S. 19 f.). Zum Schutze der Privatsphäre dieses Personenkreises ist damit erreicht worden, daß Zivildienstleistende keine Angaben über die Art der einzelnen Betreuungsleistungen, sondern nur über den benötigten Zeitaufwand zu machen haben. Ich habe empfohlen, die für den genannten Betreuungsbereich entwickelten Prinzipien auch für den Einsatz von Kriegsdienstverweigerern bei den Mobilen Sozialen Hilfsdiensten zu übernehmen.

3. Rechtswesen

3.1 Bundeszentralregister

Beim Bundeszentralregister (BZR) als einem der umfangreichsten Datenverarbeitungssysteme des Bundes habe ich auch im Jahre 1988 einen Kontroll- und Beratungsbesuch durchgeführt. Sowohl aus diesem Anlaß wie auch aufgrund laufender Kontakte zu dieser Dienststelle des Generalbundesanwalts kann ich wiederum feststellen, daß man dort ständig bemüht ist, bei einem überaus hohen Arbeitsvolumen ein Höchstmaß an Präzision und Zuverlässigkeit der Datenverarbeitung zu gewährleisten.

Dazu dient auch ein von mir empfohlenes und in gemeinsamen Besprechungen mit dem Bundeszentralregister entwickeltes Prüfprogramm, dessen Konzeption ich schon in meinem Zehnten Tätigkeitsbericht (S. 20 f.) skizziert habe: Die an Regierungspräsidenten und Kommunalbehörden erteilten unbeschränkten Auskünfte, die nicht den in § 41 Abs. 1 Nrn. 6, 7 und 9 Bundeszentralregistergesetz (BZRG) enumerativ genannten Zwecken dienen, sollen damit stichprobenweise festgestellt werden können. In einem ersten Lauf wurde das Programm für zwei Wochen im Dezember 1987 unter Federführung der hausinternen Revisionsgruppe des BZR zur Anwendung gebracht. Ein zweiter Lauf im April 1988 diente zugleich als Instrument meiner datenschutzrechtlichen Kontrolle beim Bundeszentralregister. Dabei wurden im Rahmen einer stichprobenmäßigen Durchsicht in mehreren hundert Auskunftfällen Zweckangabe und Empfänger miteinander verglichen. Im ersten wie im zweiten Lauf wurde jeweils ein Fall festgestellt, in dem eine unbeschränkte Auskunft für einen nach § 41 Abs. 1 BZRG nicht zugelassenen Verwendungszweck durch eine Kommunalbehörde beantragt und durch das BZR erteilt worden war. Die Auskunftsersuchen mit den Zweckangaben „Eintragung in das Vereinsregister" und „Reisegewerbekarte" hätten gemäß § 41 Abs. 1 BZRG zurückgewiesen werden müssen; unbeschränkte Auskünfte hätten in diesen Fällen nicht erteilt werden dürfen.

Wenn man davon ausgeht, daß bei der Masse der zu erteilenden unbeschränkten Auskünfte Fehler auch künftig nicht völlig ausgeschlossen werden können, so lassen es diese ersten mit dem Prüfprogramm gewonnenen Erfahrungen trotz der Seltenheit von Fehlentscheidungen doch geboten erscheinen, die Fehlerrate weiter zu beobachten. Die erkannten Fehler sollten zur Unterrichtung aller Bearbeiter Anlaß geben. In den festgestellten Fällen habe ich ferner die zuständigen Landesbeauftragten für den Datenschutz auf die mangelnde Auskunftsberechtigung der jeweils beantragenden Behörde hingewiesen und anheim gegeben, verstärkt darauf hinzuwirken, daß die Regelung des § 41 Abs. 1 BZRG schon bei der Antragstellung beachtet wird.

Das genannte Prüfprogramm betrachte ich nach diesen ersten Erfahrungen als ein hilfreiches Kontrollmittel, das ich auch bei meinen künftigen Prüfungen im BZR einsetzen werde.Es ergänzt außerdem den verfügbaren Bestand an unterschiedlichen Prüfverfahren der *hausinternen Revisionsgruppe*. Anknüpfend an frühere Bemerkungen (vgl. 8. TB S. 11, 10. TB S. 20) betone ich erneut, daß meine Kontrolltätigkeit und die Arbeit der Revisionsgruppe einander nicht ersetzen, sondern sich in sinnvoller Weise ergänzen können und müssen.

Seit Jahren habe ich die Notwendigkeit datenschutzrechtlicher Verbesserungen des Bundeszentralregistergesetzes betont und hierzu dem Bundesminister der Justiz eine Vielzahl von Vorschlägen gemacht (10. TB S. 20ff., 8. TB S. 12f., 7. TB S. 13, 6. TB S. 12, 5. TB S. 18). Desgleichen hat der Deutsche Bundestag in seinem Beschluß vom 10. Dezember 1986 (zu meinem Sechsten und Siebenten Tätigkeitsbericht) die Bundesregierung aufgefordert, im Rahmen einer weiteren Novellierung des Bundeszentralregistergesetzes meine Empfehlungen soweit wie möglich zu berücksichtigen oder, soweit sie nicht aufgegriffen werden, darauf in der Begründung zum Gesetzentwurf einzugehen (BT-Drucksache 10/6583; Niederschrift der 255. Sitzung des Deutschen Bundestages in der 10. Wahlperiode, S. 19897). Als ein erstes Echo auf die genannten Initiativen ist mir im April 1988 ein Arbeitspapier des Bundesministers der Justiz zugegangen. Um die schutzwürdigen Belange der Betroffenen mit überwiegenden Allgemeininteressen in Einklang zu bringen, beabsichtigt der BMJ, in einer Reihe von Fragen den unabweisbaren Auskunftsbedarf noch eingehender zu ermitteln. Dies entspricht meinem Anliegen. In meiner dem Bundesminister der Justiz zugeleiteten Stellungnahme zu dem Arbeitspapier habe ich deutlich gemacht, daß ich weitere Erörterungen für notwendig halte, in die auch — da Bedarfsträger in der Mehrzahl der Fälle Behörden und öffentliche Stellen der Länder sind — die Landesbeauftragten für den Datenschutz einzubeziehen sind.

3.2 Strafprozeßordnung

Auch im Berichtsjahr hat der Bundesminister der Justiz sich weiter um die Schaffung von den Anforderungen der Rechtsprechung des Bundesverfassungsgerichts genügenden Vorschriften für den Umgang mit personenbezogenen Daten im Strafverfahren bemüht (vgl. 9. TB S. 19f., 10. TB S. 22). Ein Arbeitspapier des BMJ, das einen früheren Entwurf betreffend Fahndungsmaßnahmen, Fahndungshilfsmittel und die Akteneinsicht ergänzte, enthielt Vorschläge für „Allgemeine Bestimmungen über die Speicherung, Verwendung und Übermittlung personenbezogener Daten durch die Strafverfolgungsbehörden". Ich habe dem Bundesminister der Justiz auch hierzu in Abstimmung mit den Landesbeauftragten für den Datenschutz eine Stellungnahme zugehen lassen und datenschutzrechtliche Empfehlungen gegeben.

Nach einer im April 1988 durchgeführten Erörterung mit Vertretern von Justiz- und Innenressorts der Länder, an der auch ich beteiligt war, hat der Bundesminister der Justiz mir nunmehr als zusammenfassende Überarbeitung seiner bisherigen Konzepte den Referentenentwurf eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts — Strafverfahrensänderungsgesetz 1988 — zugesandt. Der Entwurf verfolgt im wesentlichen das Ziel, für die Ermittlungstätigkeit der Strafverfolgungsbehörden mit Hilfe bestimmter hergebrachter und neuartiger Ermittlungsmethoden, für die Verarbeitung personenbezogener Daten in Dateien und ihre Nutzung für Zwecke der Strafverfolgung sowie für die Verwendung personenbezogener Daten für verfahrensfremde Zwecke die im Interesse der Rechtssicherheit und Normenklarheit gebotenen präzisen Rechtsgrundlagen zu schaffen. Er geht auf wichtige, wenn auch nicht auf alle von den Datenschutzbeauftragten des Bundes und der Länder empfohlenen Datenschutzregelungen im Strafverfahren ein. Eine Stellungnahme bereite ich derzeit vor.

Eine unter datenschutzrechtlichen Gesichtspunkten zentrale Frage ist, inwieweit von der Polizei erhobene Daten nach dem Zweck der Erhebung — Prävention oder Strafverfolgung — differenziert werden können und müssen und wo die Trennlinie zwischen Präventiv- und Repressivdaten zu ziehen ist. Datenschutzrechtliche Konsequenzen dürften sich auch daraus ergeben, daß der Entwurf die „Vorsorge für künftige Strafverfolgung", d. h. die Sammlung personenbezogener Daten für die künftige Aufklärung von Straftaten, der Strafverfolgung und nicht der Gefahrenabwehr zurechnet. Besondere Aufmerksamkeit verdient die Regelung über die Speicherung personenbezogener Daten in zentralen Dateien. Hier geht es um die Schaffung zeitgemäßer Befugnisse zur Nutzung moderner Datenverarbeitungstechniken durch die Strafverfolgungsbehörden unter Berücksichtigung der Anforderungen, die das Bundesverfassungsgericht für Eingriffe in das informationelle Selbstbestimmungsrecht aufgestellt hat. Es bedarf eingehender Prüfung, unter welchen Voraussetzungen überregionale Datensammlungen angelegt werden dürfen, um zu einem ausgewogenen Verhältnis zwischen effizienter Strafverfolgung und Datenschutz zu gelangen.

3.3 Jugendgerichtsgesetz

Zu den gesetzlichen Regelungen, die auf ihre Vereinbarkeit mit dem Recht auf informationelle Selbstbestimmung geprüft werden müssen, zählen auch die Vorschriften des Jugendgerichtsgesetzes (JGG). Hier-

über besteht Einvernehmen mit dem Bundesminister der Justiz und den Justizverwaltungen der Länder.

Notwendig erscheint mir, insbesondere für Datenerhebungen, Datenspeicherungen und Datenübermittlungen — namentlich zwischen Gerichten, Behörden, Lehrern, Arbeitgebern, Kirchen, Deutschem Roten Kreuz usw. — im Zusammenhang mit ambulanten Maßnahmen zur sozialen Betreuung jugendlicher Straftäter präzise bereichsspezifische gesetzliche Regelungen zu schaffen. Die geltenden Vorschriften des Jugendgerichtsgesetzes (insbesondere § 38 Abs. 2 und § 24 Abs. 2 JGG) reichen nicht aus; sie sollten bei der anstehenden Novellierung ergänzt werden.

Unter datenschutzrechtlichen Gesichtspunkten verdienen auch Vorschriften besondere Aufmerksamkeit, in denen es um die Anhörung oder um die Unterrichtung der Schule eines Jugendlichen geht. Kriterium einer Novellierung dieser Regelungen in § 43 Abs. 1 Satz 3 und § 70 Satz 1 JGG muß sein, ob dieses Vorgehen dem Betroffenen mehr nützt, als es ihn gegebenenfalls beeinträchtigt. Darüber hinaus sollte geprüft werden, wie durch eine geeignete Gesetzesformulierung gewährleistet werden kann, daß im Falle der Anhörung der Schule der unterrichtende Lehrer zu Wort kommt.

Der Bundesminister der Justiz hat mir mitgeteilt, daß die unter Gesichtspunkten des Datenschutzes angestrebte Überprüfung der geltenden Vorschriften des Jugendgerichtsgesetzes nicht mehr im Rahmen des gegenwärtig vorliegenden Entwurfs eines Ersten Gesetzes zur Änderung des Jugendgerichtsgesetzes erfolgen könne, weil sonst die dringend wünschenswerte Verabschiedung noch in dieser Legislaturperiode nicht mehr gewährleistet sei. Ein weiteres Änderungsgesetz zum Jugendgerichtsgesetz sei ohnehin geplant; die von mir aufgeworfenen Fragen sollten den weiteren Reformarbeiten vorbehalten werden. Ich bedauere diese Verschiebung.

3.4 Zivilprozeßordnung

Zu der Frage der Vereinbarkeit von Vorschriften der Zivilprozeßordnung mit dem Recht auf informationelle Selbstbestimmung habe ich mich bereits in meinem Zehnten Tätigkeitsbericht (S. 23 f.) geäußert. Zu der dort beschriebenen Problematik der Pfändungs- und Überweisungsbeschlüsse mit einer Mehrzahl von Drittschuldnern, die als Folge des derzeit praktizierten Verfahrens jeweils voneinander Kenntnis erhalten, ist die Erörterung mit dem Bundesminister der Justiz noch nicht abgeschlossen.

Inzwischen haben sich weitere Kritikpunkte ergeben. Der erste betrifft sog. Ehescheidungsverbundurteile. Das sind Scheidungsurteile, in denen auch über sog. Folgesachen entschieden worden ist (§§ 623 Abs. 1, 621 Abs. 1 ZPO). Dies bedeutet, daß in demselben Urteil neben dem Ausspruch der Scheidung z. B. — als Folgesachen — über den Umgang eines Elternteils mit dem ehelichen Kind, über die Übertragung von Rentenanwartschaften oder auch über die Zahlung eines Zugewinnausgleichs entschieden ist. Die vollstreckbare Ausfertigung eines solchen Urteils für eine Zwangsvollstreckung — z. B. wegen des Zugewinnausgleichs — enthält damit im Tenor und ebenso im Tatbestand und in den Entscheidungsgründen eine Reihe von Daten der Parteien, deren es für die Durchführung der Zwangsvollstreckung nicht bedarf. Sobald die vollstreckbare Ausfertigung eines solchen Urteils dem Gerichtsvollzieher übergeben wird, gelangen solche Daten (z. B. über den Umgang eines Elternteils mit dem ehelichen Kind oder über die Übertragung von Rentenanwartschaften) zu dessen Kenntnis, ohne daß hierfür eine sachliche Notwendigkeit besteht. Dieses Problem dürfte sich auch ergeben, wenn Scheidungsurteile Behörden vorgelegt werden, die nur am Scheidungsausspruch interessiert sind, aber zwangsläufig auf diese Weise etwa auch Daten über die Abwicklung des Zugewinnausgleichs der Betroffenen erhalten.

Ich habe den Bundesminister der Justiz um Stellungnahme gebeten und als möglichen Lösungsansatz vorgeschlagen, in Tenor, Tatbestand und Entscheidungsgründen — wie dies zumindest teilweise bereits geschieht — sorgfältig zwischen den einzelnen Entscheidungen (z. B. Scheidung/Rentenanwartschaft/Zugewinn/Kosten), zu trennen. Zugleich müßte sichergestellt werden, daß die Geschäftsstellen der Gerichte entsprechend dem jeweiligen Verwendungszweck auszugsweise Ausfertigungen der Einzelentscheidungen herstellen.

In seiner Antwort hat der BMJ auf § 624 Abs. 4 ZPO hingewiesen. Hiernach werden am Verfahren beteiligten *Dritten* (z. B. Versorgungsträger, Jugendamt) Ausfertigungen, Abschriften etc. nur insoweit mitgeteilt oder zugestellt, als das mitzuteilende oder zuzustellende Schriftstück sie betrifft. Dasselbe gilt für die Zustellung von Entscheidungen an Dritte, die zur Einlegung von Rechtsmitteln berechtigt sind. Darüber hinaus bedarf es aber noch der näheren Erörterung mit dem BMJ, welche Informationen *dem Gerichtsvollzieher* für die Zwangsvollstreckung *einzelner* Ansprüche aus dem Ehescheidungsverbundurteil gegenüber dem Prozeßgegner gegeben werden dürfen.

Einen weiteren Problembereich, in dem es einer dringenden Überarbeitung und Ergänzung zivilprozessualer Vorschriften bedarf, bilden die Befugnisse von Sachverständigen zur Feststellung der Identität zu untersuchender Personen. Richtlinien des Bundesgesundheitsamtes für die Erstattung von Blutgruppengutachten sehen die Aufnahme eines Finger- oder Fußabdruckes des Betroffenen in die vom Gutachter zu fertigende Niederschrift vor. Damit werde — so heißt es in den Richtlinien — dem Auftraggeber die Prüfung ermöglicht, ob tatsächlich die zu untersuchende Person untersucht wurde.

Auf die Problematik dieser Maßnahme habe ich unter Gesichtspunkten der Erforderlichkeit wie auch der Rechtmäßigkeit schon Anfang 1983 in meinem Fünften Tätigkeitsbericht hingewiesen (S. 22 f.) — allerdings ohne eine Reaktion der zuständigen Ressorts. Nunmehr hat eine beabsichtigte Neufassung der genannten Richtlinie Anlaß für eine erneute Erörterung zwischen dem Bundesminister der Justiz, dem Bundesminister für Jugend, Familie, Frauen und Gesundheit, dem Bundesgesundheitsamt und mir gegeben.

Ein Teil der Literatur stützt die Rechtmäßigkeit der Abnahme von Finger- oder Fußabdrucken auf § 372 a

ZPO. Übereinstimmend haben BMJ, BMJFFG und BGA die Notwendigkeit dieser Maßnahmen zur Identitätssicherung betont.

Deshalb habe ich empfohlen, für die Aufnahme von Finger- oder Fußabdrucken als Identitätsnachweis bei Blutgruppengutachten bereichsspezifische gesetzliche Vorschriften zu schaffen, die normenklar die Verpflichtung der Betroffenen festlegen, solche Maßnahmen zu dulden, und ferner bestimmen, wie diese Abdrucke verwandt werden dürfen.

Außerdem habe ich darauf hingewiesen, daß nur auf der Basis des Übergangsbonus für eine beschränkte Zeit Betroffene weiterhin in Fällen einer durch Beweisbeschluß angeordneten Blutgruppenuntersuchung im gerichtlichen Verfahren zur Duldung von Finger- oder Fußabdrucken verpflichtet werden können. Soweit eine gerichtliche Anordnung nicht zugrunde liegt, können diese Maßnahmen nur mit Einwilligung des Betroffenen durchgeführt werden.

Ich habe deutlich gemacht, daß sich die angesprochene Problematik nicht nur bei Blutgruppengutachten, sondern auch bei anderen Sachverständigengutachten stellt, die sich auf natürliche Personen beziehen. Ich habe dem Bundesminister der Justiz empfohlen, den behandelten Fragen nicht nur in bezug auf die Zivilprozeßordnung, sondern auch in bezug auf andere Verfahrensordnungen nachzugehen.

Ein weiteres datenschutzrechtliches Problem — wiederum nicht nur im Zivilprozeß — ergibt sich aus dem Fortbestand personenbezogener Daten (Protokollbücher mit Befunden, Durchschriften der Gutachten und der Niederschriften) bei einem Gutachter nach Erstattung des Gutachtens. BMJFFG, BMJ und BGA begründen die Notwendigkeit einer Aufbewahrung von Unterlagen über Blutgruppengutachten mit der Verpflichtung des Sachverständigen, ein schriftlich vorgelegtes Gutachten im laufenden Verfahren gegebenenfalls auch mündlich vortragen und begründen zu müssen, mit der ärztlichen Standespflicht sowie mit möglichen Restitutionsklagen, bei denen es um die einwandfreie Durchführung der Untersuchung und Erstellung des Gutachtens gehe. Zwischen den beteiligten Behörden und mir zeichnet sich eine Übereinstimmung ab, daß für die Dauer der Aufbewahrung personenbezogener Daten beim Sachverständigen durch Rechtsnormen zeitliche Grenzen gesetzt werden müssen.

3.5 Zentrales Handelsregister

Ein privater Wirtschaftsinformationsdienst ist an Amtsgerichte und Landesjustizverwaltungen mit dem Anliegen herangetreten, ihm zu gestatten, das Handelsregister vollständig auf Mikrofilm abzulichten, um so ein zentrales Handelsregister für das Bundesgebiet zu schaffen. Das Register soll durch Aufnahme der Eintragungsveröffentlichungen im Bundesanzeiger auf aktuellem Stand gehalten und unter Einsatz moderner Techniken durch die Erteilung von Auskünften und Informationen kommerziell verwertet werden. Der Wirtschaftsinformationsdienst beruft sich für sein Vorhaben auf das unbeschränkte Einsichtsrecht in das Handelsregister nach § 9 Abs. 1 des Handelsgesetzbuches (HGB).

Ich habe dem Bundesminister der Justiz in Abstimmung mit den Landesbeauftragten für den Datenschutz meine Bedenken gegen die Zulässigkeit eines solchen privaten zentralen Handelsregisters mitgeteilt: Das Handelsregister enthält personenbezogene Daten (vgl. § 29 HGB, § 39 GmbHG). Die Übermittlung personenbezogener Daten berührt das informationelle Selbstbestimmungsrecht der Betroffenen und bedarf nach dem Volkszählungsurteil (BVerfGE 65, 1) einer Rechtsgrundlage.

Für die Übermittlung von Daten aus dem Handelsregister enthält § 9 HGB eine bereichsspezifische Regelung. Hiernach ist jedermann ohne Nachweis eines berechtigten Interesses die „Einsicht" in das Handelsregister gestattet. Die Übernahme des gesamten Registerinhalts zur Gewinnung eines vermarktbaren Produkts kann jedoch begrifflich nicht mehr als „Einsicht" im Sinne von § 9 Abs. 1 HGB angesehen werden. Für die Übermittlung des gesamten Datenbestandes des Handelsregisters kann § 9 HGB daher nicht als Rechtsgrundlage herangezogen werden.

Der Bundesminister der Justiz hat mir mitgeteilt, daß diese Auslegung des § 9 HGB seiner Auffassung entspricht und sich auch die Landesjustizverwaltungen übereinstimmend gegen die Zulässigkeit der Verfilmung des gesamten Handelsregisters ausgesprochen haben. Der BMJ hat allerdings gleichzeitig darauf verwiesen, daß die Kommission der Europäischen Gemeinschaften die Auffassung vertrete, es widerspräche dem Sinn der Ersten gesellschaftsrechtlichen Richtlinie vom 9. März 1968 (68/151/EWG ABl. Nr. L 65/8), einem Dritten die zentrale Erfassung des Handelsregisters unmöglich zu machen. Die Argumentation der Kommission der Europäischen Gemeinschaften wird im einzelnen zu prüfen sein. Dabei ist allerdings die Rechtsprechung des Bundesverfassungsgerichts zu berücksichtigen, das in einem Beschluß vom 25. Juli 1988 — 1 BvR 109/85 — (NJW S. 3009) ausdrücklich festgestellt hat, daß das Recht auf informationelle Selbstbestimmung auch solche personenbezogenen Informationen umfaßt, die zum Bereich des wirtschaftlichen Handelns gehören.

4. Finanzwesen

Im Berichtsjahr habe ich eine datenschutzrechtliche Kontrolle bei der Informationszentrale für Auslandsbeziehungen (IZA), einer Organisationseinheit des Bundesamtes für Finanzen, durchgeführt. Dabei habe ich zur Durchführung von Anforderungen, die das Bundesdatenschutzgesetz in Verfahrensfragen stellt, eine Reihe von Verbesserungen empfohlen, Verstöße gegen materielles Datenschutzrecht aber nicht festgestellt.

4.1 Kontrollmitteilungen

Der Entwurf für das inzwischen verkündete Steuerreformgesetz 1990 sah ursprünglich einen neuen § 93 b der Abgabenordnung (AO) vor, wonach die

Träger von Sozialleistungen zur Sicherung der Besteuerung abweichend von § 35 Abs. 2 SGB I i. V. m. §§ 67 und 71 SGB X den Finanzbehörden unter bestimmten Voraussetzungen zum Schluß eines Kalenderjahres den Empfänger, den Rechtsgrund und die Höhe der in diesem Kalenderjahr geleisteten Zahlungen im Sinne des § 32 b des Einkommensteuergesetzes (EStG) schriftlich mitteilen sollten. Das hätte bedeutet, daß z. B. auch die Zahlung von Arbeitslosengeld oder Arbeitslosenhilfe zu offenbaren gewesen wäre. Gegen diese Kontrollmitteilungen habe ich gegenüber dem Bundesminister der Finanzen Bedenken erhoben. Ein überwiegendes Allgemeininteresse, das eine derartige Einschränkung des Rechts auf informationelle Selbstbestimmung der Empfänger von Lohnersatzleistungen im Sinne des § 32b EStG rechtfertigen könnte, ist für mich nicht erkennbar. Die Verpflichtung aller Steuerpflichtigen, den Finanzbehörden die für die Besteuerung erheblichen Umstände vollständig und wahrheitsgemäß anzugeben, gilt auch für diese Steuerpflichtigen. Eine Unterrichtung der Betroffenen über ihre Erklärungspflicht gegenüber den Finanzbehörden erscheint daher ausreichend.

Aufgrund meiner Bemühungen hat der Bundesminister der Finanzen von der vorgesehenen Regelung Abstand genommen und statt dessen im Steuerreformgesetz 1990 mit einem neuen § 32b Abs. 3 EStG die Träger der Sozialleistungen verpflichtet, dem Empfänger eine Bescheinigung über die gewährten Leistungen auszustellen und ihn auf deren steuerliche Behandlung sowie auf seine Steuererklärungspflicht hinzuweisen. Dies entspricht dem in § 93 Abs. 1 Satz 3 AO enthaltenen — den Belangen des Datenschutzes entsprechenden — Grundsatz, daß andere Personen oder Stellen als die Beteiligten erst dann zur Auskunft angehalten werden sollen, wenn die Sachverhaltsaufklärung durch die Beteiligten selbst nicht zum Ziele führt oder keinen Erfolg verspricht.

Eine andere Problematik im Rahmen des vorliegenden Themas betraf Kontrollmitteilungen, die Empfänger von Zuwendungen aus dem Bundeshaushalt allein aufgrund von Verwaltungsvorschriften zur Bundeshaushaltsordnung gegenüber ihrem Finanzamt abzugeben hatten, wenn sie aufgrund von Verträgen z. B. an Gutachter, Übersetzer, Unterrichtende, Vortragende oder Sitzungsteilnehmer Zahlungen leisteten. Zweifel an der Zulässigkeit dieser Kontrollmitteilungen habe ich schon in meinem Zehnten Tätigkeitsbericht (S. 25) geltend gemacht. Ich begrüße es, daß der Bundesminister der Finanzen wegen des Fehlens einer gesetzlichen Grundlage an diesen Kontrollmitteilungen nicht mehr festhält und — im Vorgriff auf eine vorgesehene Änderung der Verwaltungsvorschriften zur Bundeshaushaltsordnung — auf meinen Vorschlag hin in einem Rundschreiben an die obersten Bundesbehörden gebeten hat, die Verpflichtung der Zuwendungsempfänger zu Mitteilungen an Finanzämter „als aufgehoben zu betrachten".

Nachdem durch das Steuerbereinigungsgesetz 1986 in § 93 a AO ein Rahmen zulässiger Kontrollmitteilungen abgesteckt worden ist, habe ich schon in meinem Zehnten Tätigkeitsbericht (S. 25) auch auf das datenschutzrechtliche Interesse am Erlaß einer entsprechenden Rechtsverordnung hingewiesen. Damit würde eine noch immer ungeregelte und unklare Praxis bereinigt werden. Der Bundesminister der Finanzen hat mich an den noch andauernden Vorarbeiten zu dieser Rechtsverordnung beteiligt. Ich bedauere, daß deren Erlaß noch immer aussteht.

4.2. Steuerdaten-Abruf-Verordnung

In meinem Zehnten Tätigkeitsbericht (S. 25f.) habe ich berichtet, daß ich die im Entwurf des Bundesministers der Finanzen für eine „Verordnung über den automatisierten Abruf von Steuerdaten des Bundesamts für Finanzen, der Finanzämter und Gemeinden (Steuerdaten-Abruf-Verordnung — StDAV)" vorgesehene Kontrolle der Datenabrufe nicht für ausreichend halte und für einen Teil der Zugriffsberechtigten eine Protokollierung *aller* Datenabrufe — also nicht nur von Stichproben — empfohlen habe. Dabei habe ich eine Protokollierung der Abrufe durch den nach der Geschäftsverteilung zuständigen Sachbearbeiter nicht gefordert. Aus heutiger Sicht halte ich auch die Aufzeichnung der Datenabrufe durch seinen zuständigen Vertreter für verzichtbar, weil beide auf „eigene", d. h. bei der Bearbeitung des Falles erhobene Daten zugreifen. Deshalb befürworte ich grundsätzlich die vom Bundesminister der Finanzen nunmehr gewählte Abgrenzung, die eine Aufzeichnung von Datenabrufen durch Abrufberechtigte der speichernden Behörde nur vorsieht, wenn es sich um Abrufberechtigte *anderer als der für die Sachbearbeitung zuständigen Organisationseinheiten* handelt. Während der Bundesminister der Finanzen allerdings für die Aufzeichnung solcher Datenabrufe ein zufallsbedingtes Stichprobenverfahren für ausreichend hält, bin ich der Auffassung, daß alle derartigen Datenabrufe ebenso wie die Datenabrufe der Abrufberechtigten aus anderen Behörden programmgesteuert aufgezeichnet werden sollten. Ich begrüße es, daß der Bundesminister der Finanzen für letztere inzwischen bereits teilweise die programmgesteuerte Aufzeichnung sämtlicher Datenabrufe für Kontrollzwecke vorgesehen hat. Die Diskussion zu diesem Fragenkreis dauert noch an.

Weiterhin hat der Bundesminister der Finanzen in den Entwurf der Steuerdaten-Abruf-Verordnung eine Regelung aufgenommen, wonach für besonders ermächtigte Amtsträger der obersten Finanzbehörden und der Oberfinanzdirektionen automatisierte Datenabrufverfahren eingerichtet werden sollen, mit denen diese in steuerlichen Einzelfällen oder zur Wahrung von Aufsichts- und Kontrollbefugnissen unmittelbar auf Daten der Finanzämter zugreifen können. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz hat in ihrem Beschluß vom 10. Oktober 1988 hiergegen Bedenken erhoben (s. Anlage 5). Nach ihrer Ansicht sind solche zentralen Datenabrufmöglichkeiten für die Erfüllung der Aufgaben der Aufsichtsbehörden nicht erforderlich. Bei etwaigen Verfahren im Rahmen der Aufsicht sind ohnehin die Akten heranzuziehen. Die Bearbeitung von steuerlichen Einzelfällen erfordert von den Aufsichtsbehörden in aller Regel auch keine Entscheidungen unter

Zeitdruck. Von der Einrichtung solcher Datenabrufverfahren ist auch sonst kein ins Gewicht fallender Rationalisierungseffekt zu erwarten. Solche Verfahren können aber dazu führen, daß dem Steuergeheimnis unterliegende Daten auf sehr einfache Weise Personen bekannt werden, die sie für die Erfüllung ihrer Aufgabe nicht benötigen. Dem gilt es vorzubeugen. Die Datenschutzbeauftragten haben daher in ihrem Beschluß vorgeschlagen, in dem Entwurf für eine Steuerdaten-Abruf-Verordnung keine automatisierten Datenabrufverfahren für oberste Finanzbehörden und für Oberfinanzdirektionen vorzusehen.

Nach Informationen aus dem Bundesministerium der Finanzen haben die Finanzminister und -senatoren der Länder in einer gemeinsamen Beschlußfassung den Bundesminister der Finanzen gebeten, in der Steuerdaten-Abruf-Verordnung auf eine Datenabrufberechtigung der obersten Finanzbehörden zu verzichten. Es ist zu erwarten, daß der Bundesminister der Finanzen diesem Votum folgen wird. Hinsichtlich der Datenabrufberechtigung der Oberfinanzdirektionen ist dagegen noch nicht zu erkennen, ob sich die Empfehlungen der Datenschutzbeauftragten durchsetzen werden.

5. Personalwesen

5.1 Deutsches Patentamt

Eine erneute Datenschutzkontrolle der bereits im Jahre 1986 von mir überprüften Personaldatenverarbeitung des Deutschen Patentamtes (DPA), bei der auch seinerzeit nicht berücksichtigte Teilbereiche miterfaßt werden konnten, führte im wesentlichen zu folgenden Feststellungen:

— Am Personalinformationssystem des DPA sind aufgrund meiner Verbesserungsvorschläge umfangreiche Veränderungen vorgenommen worden. Dies gilt insbesondere für die technisch-organisatorischen Maßnahmen, die inzwischen als zufriedenstellend bezeichnet werden können.

  Auf anderen Gebieten war dagegen noch eine Reihe von Mängeln festzustellen; auf die meisten hatte übrigens der interne Datenschutzbeauftragte des DPA schon Anfang Februar 1988 hingewiesen. Hervorzuheben ist insbesondere, daß dem internen Datenschutzbeauftragten keine Übersicht über die konventionellen Dateien zur Verfügung stand; sie konnte auch während des Kontrollbesuchs nicht zusammengestellt werden. Eine Dokumentation der Programme und Listenausdrucke war während der Kontrolle ebensowenig verfügbar wie das Benutzerhandbuch; diese Unterlagen wurden allerdings inzwischen nachgereicht.

  Entgegen meiner Empfehlung im Kontrollbericht von 1986 sind die Beurteilungsnoten aller Beschäftigten beim DPA im Personalinformationssystem gespeichert. Die automatisierte Verarbeitung beschränkt sich auch nicht auf die von mir noch akzeptierte bloße Einzelanzeige am Bildschirm; die Noten werden vielmehr bei zahlreichen Programmen ausgedruckt.

  Die Anzahl der Listenausdrucke aus dem Personalinformationssystem mit zahlreichen teils sensiblen Daten ist zwar inzwischen von rund 450 auf 87 reduziert worden. Jedoch ist auch diese Zahl noch immer zu hoch, und die Streuung der Listen zu groß. Ihre Kenntnis ist für die Aufgabenerfüllung vieler Empfänger entweder überhaupt nicht oder nur zu bestimmten Anlässen erforderlich; die Verwendung der Ausdrucke entspricht auch nicht dem Grundsatz der Zweckbindung. Es war auch nicht sichergestellt, daß nach Herstellung neuer Listenausdrucke der notwendige Austausch der Listen alt gegen neu in allen Fällen erfolgte.

  Die mit diesen Mängeln verbundenen Verstöße gegen datenschutzrechtliche Vorschriften über die Behandlung von Personaldaten habe ich erneut gemäß § 20 Abs. 1 BDSG beanstandet.

— Ich mußte weiter feststellen, daß auch meine weitere Empfehlung im Kontrollbericht von 1986, nämlich die Beschreibung der Auswertungen, deren Verteiler und das gesamte Verfahren unter Beteiligung des internen Datenschutzbeauftragten und des Personalrats entsprechend den Vorgaben des Bundespersonalvertretungsgesetzes gemeinsam zu erarbeiten, nicht umgesetzt worden war.

— Schließlich gab auch die Kontrolle des Posteingangsverfahrens Anlaß für Verbesserungsempfehlungen. So habe ich angeregt, erkennbar sensible Postsendungen, wie ärztliche Gutachten und Personalvorgänge, den zuständigen Stellen des DPA ungeöffnet direkt zuzuleiten und nicht wie bisher über das Hauptbüro.

  Ich habe darüber hinaus empfohlen, bei der Einschaltung von Amtsärzten in Personalverwaltungsangelegenheiten nicht ausführliche ärztliche Gutachten, sondern lediglich ärztliche Zeugnisse nach der Praxis des Ärztlichen Dienstes der obersten Bundesbehörden in Auftrag zu geben. Diese sollten sodann in den Personalakten in verschlossenen Umschlägen abgelegt werden, die mit dem Aufdruck „Arztsache" zu versehen und nur im Bedarfsfall zu öffnen sind. Tag und Anlaß der Öffnung sollten auf dem Umschlag mit Namenszeichen des Bearbeiters vermerkt werden.

— Bei der Nachkontrolle ergab sich, daß in einer Hauptabteilung eine sog. „Aktengeburtstagsliste" dv-gestützt geführt wird. Die eingehenden Vorgänge werden mit Bearbeitungsfristen in das System eingegeben. Aus dem Aktenzeichen sind die zuständige Organisationseinheit und mit dieser der jeweilige Mitarbeiter erkennbar. Es handelt sich damit um eine Datei, die zur Verhaltens- und Leistungskontrolle genutzt werden kann, weil Überschreitungen festgesetzter Bearbeitungstermine vom Vorgesetzten dem jeweiligen Bearbeiter zugeordnet werden können.

  Diese Datei ist bisher weder in die Dateiübersicht aufgenommen noch ist sie gemäß § 19 Abs. 4 BDSG zum Register gemeldet. Ein Mitbestimmungsverfahren nach § 75 Abs. 3 Nr. 17 BPersVG wurde nicht durchgeführt.

- Der für Beurteilungen im DPA vorgesehene Vordruck enthält einige datenschutzrechtlich problematische Felder wie „äußere Erscheinung", „Gesundheit", „Charakter und persönliche Eigenschaften". Ich habe angeregt, den Vordruck anhand des unter datenschutzrechtlichen Gesichtspunkten bedenkenfreien Beurteilungsbogens des BMI zu überprüfen.

- Obwohl bereits im Kontrollbericht 1986 besonders kritisch angesprochen, stellte sich bei der Nachkontrolle heraus, daß dem inzwischen eingesetzten neuen internen Datenschutzbeauftragten für eine auch nur annähernd effiziente Wahrnehmung seiner Aufgaben erforderliche personelle und zeitliche Ressourcen in noch höherem Maße fehlen als seinem Vorgänger. Ich habe daher dringend empfohlen, ihn von sonstigen Dienstpflichten möglichst zu entbinden und ihm einen dv-erfahrenen Mitarbeiter zur Seite zu stellen.

5.2 Neuordnung des Personalaktenwesens

Die interministerielle Arbeitsgruppe, über deren vorläufige Arbeitsergebnisse ich in meinem Zehnten Tätigkeitsbericht (S. 26 ff.) berichtet habe, hat ihre Arbeiten im Juli 1988 abgeschlossen und ihren Schlußbericht dem Bundesminister des Innern zugeleitet. Der Schlußbericht entspricht inhaltlich mit nur wenigen Abweichungen der Darstellung in meinem Zehnten Tätigkeitsbericht. Der Bundesminister des Innern beabsichtigt, auf der Grundlage des Schlußberichts Entwürfe für entsprechende Regelungen zu erarbeiten; ein Zeitpunkt für die Ressortabstimmung über die vorgeschlagenen Maßnahmen ist allerdings noch nicht abzusehen.

Bei der wesentlichen Frage, ob die vorgeschlagenen Regelungen alle in einem Gesetz oder, wie vielfach angeregt worden war, in einer Rechtsverordnung zusammengefaßt werden sollten, verständigte sich die Arbeitsgruppe darauf, Regelungen mit Grundsatzcharakter und hohem materiellen Stellenwert in ein Gesetz aufzunehmen, und diejenigen Regelungen, die mehr verfahrensmäßigen Charakter haben, einer Rechtsverordnung vorzubehalten.

Insbesondere in folgenden wesentlichen Punkten ist die interministerielle Arbeitsgruppe meinen Vorschlägen *nicht* gefolgt:

- Ich hatte vorgeschlagen, den wesentlichen Inhalt — keinesfalls alle Einzelheiten — von Bewerberfragebögen und darüber hinaus einen Negativkatalog von Fragen festzulegen, die nicht gestellt werden dürfen. Die in die vorgesehene Rechtsverordnung aufzunehmende Regelung sollte zwischen Bewerbungsunterlagen und Einstellungsunterlagen differenzieren (vgl. bereits 3. TB S. 26). Inhalt der Bewerbungsunterlagen sollten nur die für die Entscheidung über die Eignung des Bewerbers für die in Betracht kommende Tätigkeit erforderlichen Informationen sein. Darüber hinaus habe ich eine Präzisierung des Inhalts von Personalbögen auf dem Erlaßweg für einzelne Verwaltungsbereiche empfohlen.

  Die interministerielle Arbeitsgruppe beschloß mehrheitlich, dieses Problem nicht zu behandeln, da eine gesetzliche Regelung aufgrund der umfassenden Rechtsprechung nicht geboten sei. Diese Auffassung teile ich schon wegen der durchaus unterschiedlichen Rechtsprechung nicht.

- Die interministerielle Arbeitsgruppe ist zwar meiner Forderung nach getrennter Führung und Aufbewahrung der Beihilfevorgänge in Teilakten und einem Verbot der Heranziehung von Beihilfedaten bei Personalentscheidungen gefolgt. Sie war jedoch nicht bereit, auch eine strikte Abschottung der Beihilfestelle von der übrigen Personalverwaltung für die gesetzliche Regelung vorzuschlagen. Ähnliches gilt für meine entsprechenden Vorschläge hinsichtlich der Besoldungs-, Kostenerstattungs- und Disziplinarvorgänge, deren Sensibilität ebenfalls grundsätzlich ein funktional begründetes und entsprechend begrenztes Zugangsrecht innerhalb der Personalverwaltung erfordert. Die Auffassung der interministeriellen Arbeitsgruppe, solche Organisationsentscheidungen jeweils in das Ermessen der betreffenden Dienststelle zu stellen, läßt sich m. E. kaum mit der jüngsten höchstrichterlichen Rechtsprechung des Bundesverwaltungs- und des Bundesarbeitsgerichts vereinbaren. Danach hat der Dienstherr den Kreis der mit Personalakten befaßten Beschäftigten möglichst eng begrenzt zu halten und darf auch Teilakten, Auszüge oder einzelne Angaben nicht ohne dienstlichen Grund anderen Beschäftigten zur Kenntnis geben (BVerwG in NJW 1987, S. 1214 ff.). Dabei sind sensible Daten, zu denen insbesondere solche über den Gesundheitszustand gehören, als besonders schutzbedürftig mit besonderer Vertraulichkeit zu behandeln und nur dem insoweit zuständigen Personenkreis zugänglich zu machen (BAG in RDV 1988, S. 27).

- Fachvorgesetzten sollte nach meiner Auffassung der Zugang zu Personalakten ausdrücklich versagt sein, es sei denn, sie gehören in einem institutionalisierten Verfahren zur Personalauswahl und -förderung einem Entscheidungsgremium an. Personalwirtschaft wird zentral von den Personalreferaten betrieben. Sie können sich von den Fachabteilungen die notwendigen Informationen beschaffen, um die fachliche Qualifikation und Eignung eines Bediensteten zu beurteilen. Andererseits können die Fachvorgesetzten vom Personalreferat Auskunft über alle Daten erhalten, die für ihr Einverständnis mit einer Personalentscheidung bzw. zu ihrer Information über einen neuen Mitarbeiter wichtig sind. Für alle Entscheidungen im Rahmen der Fürsorgepflicht sowie für die zur Personalführung erforderlichen Kenntnisse können die Informationen aus dem Kontakt mit den Bediensteten, der Beobachtung ihrer Befähigung und ihrer Leistung gewonnen werden. Außerdem bleibt es einem Vorgesetzten unbenommen, seinen Mitarbeiter zu befragen. Dieser muß selbst bestimmen können, ob er z. B. private Gründe für einen Leistungsabfall preisgibt. Jedenfalls ist es erstrebenswert, daß sich der Fachvorgesetzte aus eigener Wahrnehmung ein Urteil bildet, da Mitarbeiter mit für sie ungünstigen Personalakteninhalten aus der

Vergangenheit (z. B. Beurteilungen) nur so die Chance haben, unvoreingenommen eingeschätzt zu werden. Aus diesen Gründen hat ein Informationsinteresse des Fachabteilungsleiters hinter dem Grundsatz des besonderen Vertrauensschutzes des Bediensteten zurückzutreten.

— Im Unterschied zu vorausgegangenen Überlegungen sieht der Schlußbericht den grundsätzlichen Ausschluß der automatisierten Speicherung und Verarbeitung dienstlicher Beurteilungsnoten nicht mehr vor. Hiervon abgesehen entsprechen die für die automatisierte Personaldatenverarbeitung vorgeschlagenen Regelungen weitgehend meinen Vorstellungen.

Mit den dargestellten Einschränkungen kann das Arbeitsergebnis der interministeriellen Arbeitsgruppe aus meiner Sicht positiv bewertet werden.

Diese positive Gesamtbewertung versteht sich nicht zuletzt vor dem Hintergrund, daß es nach der Koalitionsvereinbarung der die Bundesregierung tragenden Parteien noch in dieser Legislaturperiode zu einer Verbesserung der Mitbestimmung bei der Einführung neuer Techniken kommen soll. Die in Hessen, Nordrhein-Westfalen, Rheinland-Pfalz und Niedersachsen verabschiedeten Neuregelungen liegen bereits auf dieser Linie.

In diesem Zusammenhang ist zu bemängeln, daß der Referentenentwurf für eine bereichsspezifische Regelung des Arbeitnehmerdatenschutzes immer noch nicht vorliegt, obwohl der Deutsche Bundestag und die Bundesregierung selbst schon 1985 dieses Gesetzgebungsvorhaben für vordringlich erklärt haben.

Im Hinblick auf den Abstimmungsbedarf bei der Neuregelung des Personalaktenrechts und bei der vorgesehenen Regelung des Arbeitnehmerdatenschutzes hat die Konferenz der Datenschutzbeauftragten von Bund und Länder beschlossen, einen Arbeitskreis Personalwesen einzurichten. Er wird seine Arbeit im Jahre 1989 aufnehmen.

5.3 Telefondatenverarbeitung/ Dienstanschlußvorschriften

Bereits im Siebenten Tätigkeitsbericht (Seite 19f.) habe ich dargelegt, wie bei einer automatisierten Verarbeitung der Telefondaten den Anforderungen des Datenschutzes entsprochen werden kann. Meine Empfehlungen sind nunmehr vom Bundesminister der Finanzen in dem Entwurf der Neufassung der Allgemeinen Verwaltungsvorschriften über die Einrichtung und Benutzung dienstlicher Fernmeldeanlagen für die Bundesverwaltung mit Ausnahme der Deutschen Bundespost (Dienstanschlußvorschriften — DAV —) im wesentlichen berücksichtigt worden.

1. Positiv bewerte ich die Regelung, daß bei privaten Gesprächen u. a. nur noch die Vorwahl und/oder die *um die letzten beiden Ziffern verkürzte Rufnummer* des Wählanschlusses des Angerufenen (sog. „Zielnummer") nachzuweisen ist. Darüber hinaus sind durch schriftliche Aufzeichnungen oder durch Speicherung mittels Fernmeldedatenerfassungsanlage das Datum, die Nebenstellennummer und — sofern nicht anders festgehalten — der Name des Anmelders, die Gebühreneinheiten bzw. der Gebührenbetrag und eine besondere Kennzeichnung als Privatgespräch festzuhalten. Für die Speicherung des Namens des Anmelders sehe ich nur dann einen Grund, wenn sich mehrere Berechtigte einen Telefonanschluß teilen und eine konkrete Zuordnung des geführten Gesprächs zu dem Anmelder anderweitig nicht vorgenommen werden kann oder wenn der Name für die Zustellung der Gebührenabrechnung unter den gegebenen Umständen benötigt wird.

   Beim Einsatz von Fernmeldedatenerfassungsanlagen unterbleibt ein Ausdruck der verkürzten Zielnummer, es sei denn, daß auf Verlangen des Bediensteten ein Auszug der Nachweisung einschließlich der verkürzten Zielnummer zu erstellen ist.

   Die gespeicherten Daten sind nach Abrechnung der Nachweisung unverzüglich zu löschen; handschriftlich aufgezeichnete Daten sind nach Zahlung der Gebühren zu vernichten oder, soweit möglich, dem Bediensteten auszuhändigen. In diesem Zusammenhang vermisse ich allerdings eine klare Regelung, wer die Telefondaten zwecks Abrechnung der privat geführten Gespräche erhalten darf, für deren Löschung verantwortlich ist und wie bei etwaigen Streitigkeiten im Zusammenhang mit der Gebührenabrechnung verfahren werden soll. Der BMF vertritt hierzu die Auffassung, daß eine detaillierte Regelung der Frage, welchen Stellen die Abrechnung der Privatgespräche und das Löschen der Daten obliegt, wegen der unterschiedlichen Gegebenheiten bei den einzelnen Dienststellen nicht möglich ist und der Entscheidung des jeweiligen Dienststellenleiters vorbehalten bleiben muß.

2. Der Entwurf sieht vor, daß bei dienstlichen Gesprächen die Vorwahl und/oder Rufnummer des Wählanschlusses des Angerufenen in vollem Umfang nachzuweisen ist. Der BMF hält die vollständige Speicherung für erforderlich, damit die wirtschaftliche und sparsame Verwendung von Haushaltsmitteln kontrolliert werden kann. Nur in Kenntnis der vollständigen Zielnummer könnten die Notwendigkeit und der dienstliche Bezug der geführten Gespräche im einzelnen nachgeprüft sowie die dienstlichen von den privaten Gesprächen unterschieden werden.

   Die Nachweisungen dienstlicher Gespräche sollen stichprobenweise durch den Dienstvorgesetzten oder den von ihm Beauftragten überprüft werden. Ich vertrete nach wie vor die Ansicht, daß Ausdrucke nur fallweise für Stichprobenzwecke gefertigt und grundsätzlich nur dem jeweiligen (Fach-) Vorgesetzten zugehen dürfen, da allein dieser in der Lage ist, die fachliche Notwendigkeit eines dienstlichen Telefongesprächs zu beurteilen (vgl. 7. TB S. 20). Aus diesem Grunde erachte ich auch einen bisher zuweilen praktizierten Umlauf von Nachweisungen über Ferngespräche verschiedener Verantwortungsbereiche auf demselben Ausdruck bei dem jeweils betroffenen Fachvorgesetzten wegen fehlender Erforderlichkeit für unzu-

lässig. Gleiches gilt, wenn jeweils ein solcher „Gesamt"-Listenausdruck jedem einzelnen Fachvorgesetzten gesondert für evtl. Prüf- und Kontrollzwecke zur Verfügung gestellt wird. Auch eine lückenlose Kontrolle der Kommunikationsgewohnheiten der Beschäftigten mit Hilfe entsprechender Auswertungen halte ich nicht für zulässig.

Die schriftlichen oder automatisiert gespeicherten Nachweisungen sind nach Abschluß der Prüfung, spätestens nach drei Monaten, zu vernichten oder zu löschen. Eine Verknüpfung mit anderen Dateien ist in dem Entwurf zwar nicht vorgesehen, jedoch sollte eine entsprechende Verwendungsbeschränkung noch deutlicher herausgestellt werden, z. B. durch eine Regelung, daß die Daten *ausschließlich* für die Abrechnung und ggf. für die im Rahmen der Aufsicht stattfindende Kontrolle verwendet und nur dem hierfür verantwortlichen Personenkreis zugänglich gemacht werden dürfen.

Ich betrachte die getroffenen Regelungen unter datenschutzrechtlichen Gesichtspunkten als noch zu vertretende Lösung, sofern meine zusätzlichen Anregungen bei der Neufassung der DAV berücksichtigt werden.

3. Ich begrüße es ferner, daß nach dem Entwurf bei dienstlichen Gesprächen der Personalvertretung und anderer Stellen, deren Telefonverkehr nicht der Aufsicht unterliegt, auf meine Anregung hin *nur die Gesprächsgebühren* festzuhalten sind, sofern nicht die genannten Stellen eine Aufzeichnung/Speicherung auch der übrigen Gesprächsdaten verlangen. Diese Regelung verhindert eine unzulässige Kontrolle dieser Stellen bei der Erfüllung ihrer originären gesetzlichen Aufgaben oder ihrer besonderen Vertrauensbeziehungen.

4. Die Schlußbestimmungen des Entwurfs sehen u. a. vor, daß Gebühren für private Gespräche im Telefondienst, private Telex-, Teletex-, Telefax- und Bildschirmtextschreiben sowie Telegramme nicht im Gehaltsabzugsverfahren einbehalten werden dürfen. Eine Verarbeitung der Telefondaten im Rahmen der Berechnung und Zahlbarmachung der Bezüge und Vergütungen findet somit nicht statt.

5.4 Automatisierte Fahrkartenausgabe

Bereits im Jahre 1987 war mir bekannt geworden, daß das bisherige Fahrkartenausgabesystem „MOFA" der Deutschen Bundesbahn (DB) durch die Mitbenutzung des Systems „START" (Studiengesellschaft zur Automatisierung von Reise und Touristik) ersetzt wurde. Hierbei handelt es sich um ein Reisebuchungssystem, das bereits von einer Reihe von Reisebüroketten wie auch von der DB genutzt wird. Die Verkaufsstellen der DB speichern die anfallenden Daten im Zentralrechner der START-GmbH in Frankfurt, wo auch die weitere Verarbeitung vorgenommen wird. Die Verkaufsstellen korrespondieren über Personalcomputer mit dem Zentralrechner.

Die Eingabe eines Bürgers und die nachfolgende Prüfung der „Vorläufigen Anweisung für Erstellung, Verkauf und Abrechnung von Fahrausweisen und sonstigen Belegen bei Fahrkartenausgaben mit SIEMENS PCD 2 (START-System)" veranlaßten mich zu einem Informationsbesuch in einem Hauptbahnhof der DB. Dabei ergaben sich folgende Feststellungen:

Bei Erstellung, Verkauf und Abrechnung von Fahrausweisen sowie sonstiger Belege werden personenbezogene Daten erfaßt und verarbeitet. Der Personenbezug ist durch eine Expedientennummer, die für jeden Verkäufer (Expedient), eingerichtet wird, gegeben. Die zusätzliche Speicherung der Expedientennummer im Zentralrechner neben dem kassenmäßigen Tagesabschluß ist erforderlich, damit bestimmte Auswertungen (kassentechnische Maßnahmen zum Zwecke der Prüfung und Abrechnung) auch zu einem späteren Zeitpunkt möglich sind.

Darüber hinaus wird ein (systeminternes) Log-Band im START-Rechner zum Wiederanlauf nach Systemzusammenbrüchen geführt. Zum Datenbestand des Log-Bandes gehört ebenfalls die Expedientennummer. Es handelt sich also um eine personenbezogene Datei. Eine Auswertung des Log-Bandes ermöglicht einen detaillierten Überblick über wesentliche Teile des Arbeitsablaufs eines Expedienten pro Schicht. Auswertungen des Log-Bandes werden sowohl von der DB als auch von der START-GmbH zur Aufklärung systembedingter Mängel vorgenommen. Darüber hinaus dient der Log-Band-Ausdruck zur Kontrolle der Kosten, die von der START-GmbH der DB für die Nutzung des Systems in Rechnung gestellt werden, und für die Aufklärung von Kassenunstimmigkeiten, wenn vermutet wird, daß die Ursachen im System liegen.

Ich halte derartige Auswertungen des Log-Bandes zur Erfüllung der genannten Aufgaben datenschutzrechtlich für vertretbar, wenn die gebotenen Verwertungsbeschränkungen festgelegt und die zu ihrer Einhaltung erforderlichen technischen und organisatorischen Maßnahmen getroffen sind.

Ein Genehmigungsverfahren für die Verarbeitung der Mitarbeiterdaten war zunächst entgegen der internen Dienstvorschrift (DS 114/2 Teil I) und der Vereinbarung mit der Personalvertretung über Einführung und Betrieb computergestützter Personaldatenverarbeitung nicht durchgeführt worden. Inzwischen hat der Datenausschuß (s. unten 5.6) die Dateien in den START-Logbändern unter bestimmten Auflagen genehmigt und erklärt, daß auf diese Dateien die internen Datenschutzrichtlinien (DS 114/2) anzuwenden sind. Ich begrüße diesen Hinweis. Die DB teilt jedoch nicht die Auffassung des Datenausschusses. Ich werde die Angelegenheit daher mit der Bundesbahn weiter erörtern. Eine Meldung der Datei zum Register nach § 19 Abs. 4 BDSG ist ebenfalls unterblieben. Auch dies ist nachzuholen.

Das System erlaubt bei Rücknahme von Fahrausweisen die Speicherung der Kundennummern, Reisetage, Namen und Anschriften von Kunden und der Werte der zurückgenommenen Fahrausweise, ebenso deren Ausdruck. Die DB hat versichert, daß sie eine derartige Speicherung weder angeordnet noch als zulässig bezeichnet hat, weil die Verarbeitung dieser Daten für die Aufgabenerfüllung nicht erforderlich ist. Es hätte jedoch ein entsprechendes Verbot in die hierfür von

der DB erlassene „Vorläufige Anweisung" aufgenommen werden müssen.

Das START-Verfahren wird voraussichtlich Ende 1989 von einer Eigenentwicklung der DB (Verfahren „KURS '90") abgelöst. Bereits während der Entwicklungsphase wurde mir Gelegenheit gegeben, mich aus datenschutzrechtlicher Sicht dazu zu äußern.

Dabei habe ich u. a. auf folgende Punkte hingewiesen:

- Die Möglichkeit, unbegrenzt Paßworte „auszuprobieren" muß beseitigt werden.
- Eine enge Zweckbindung der Daten, die dem Kassenverwalter bei der möglichen Aufklärung von Kassenunstimmigkeiten mit dem Ausdruck der Verkaufsdatensätze über die Zentralstelle Absatz der DB zugänglich werden, muß gewährleistet sein.
- Bei einer Speicherung von Kundendaten müssen die Betroffenen von der Speicherung ihrer personenbezogenen Daten Kenntnis erhalten.

Die datenschutzrechtlichen Erörterungen zum Verfahren „KURS '90" dauern noch an.

5.5 Bundesbaudirektion

Im Berichtszeitraum hat die Bundesbaudirektion die anläßlich meiner Kontrolle ihres Personalwesens im Jahre 1987 gegebenen Empfehlungen (vgl. 9. TB S. 22) überwiegend verwirklicht oder mir eine Umsetzung in absehbarer Zeit zugesagt. Dies gilt insbesondere für

- die Trennung der Funktion des internen Datenschutzbeauftragten von dem für Rechts-, Personal- und Haushaltsangelegenheiten zuständigen Zentralbüro,
- die Gewährleistung einer umfassenden Unterrichtung des Personalrats über die Planung von Maßnahmen der Personaldatenverarbeitung und seiner Beteiligung an solchen Maßnahmen,
- die Telefondatenverarbeitung und das Zugangskontrollsystem im Dienstgebäude Berlin.

Noch nicht abgeschlossen sind die Gespräche über datenschutzgerechte Lösungen der Beihilfebearbeitung im Sinne einer vollständigen personellen Trennung von der Personalsachbearbeitung sowie über den Schutz von Mitarbeiterdaten vor unzulässiger Verarbeitung auf Personalcomputern, die u. a. den Baustellenleitern für andere Zwecke zur Verfügung stehen.

5.6 Personalinformationssysteme bei der Deutschen Bundesbahn

Bereits in meinem Neunten Tätigkeitsbericht (S. 27) hatte ich darauf hingewiesen, daß die Entwicklung der automatisierten Personaldatenverarbeitung bei der Deutschen Bundesbahn (DB) insgesamt positiv zu bewerten ist. Dieser schon bei Einführung der Personalinformationssysteme ÖPDV und PSV (s. u.) entstandene Eindruck hat sich insbesondere durch den Inhalt der zwischen dem Vorstand und dem Hauptpersonalrat der DB abgeschlossen „Vereinbarung über Einführung und Betrieb computergestützter Personaldatenverarbeitung bei der Deutschen Bundesbahn" vom 2. 2. 1988 bestätigt. Aus datenschutzrechtlicher Sicht sind folgende Regelungen von Bedeutung:

Ein Datenausschuß, bestehend aus Vertretern der Zentrale der DB und des Hauptpersonalrates der DB, soll bei Entwicklung neuer sowie bei Änderung und Erweiterung bestehender Datenverarbeitungsverfahren die Interessen der Unternehmensleitung und der Mitarbeiter in Einklang bringen und eine Abstimmung der für die Personaldatenverarbeitung vorgesehenen Verfahren herbeiführen. Dabei wird u. a. über Art und Umfang der Zugriffsberechtigungen entschieden. Der Datenausschuß kann sich durch externe Sachverständige beraten lassen.

Die Vereinbarung regelt auch, daß für die Personaldatenverarbeitung bereits eingesetzte Datenverarbeitungsverfahren baldmöglichst dem Datenausschuß zur Genehmigung vorzulegen sind. Dies konnte noch nicht in allen Fällen geschehen, weil der Datenausschuß erst seit September 1988 besteht.

Anzuerkennen ist, daß „freie Abfragesprachen" in den Personaldatenverarbeitungssystemen der DB nicht verwendet werden: die Personaldatenverarbeitung erfolgt nur mit kompilierten, freigegebenen und dokumentierten Programmen. Darüber hinaus muß die Dokumentation Art, Umfang und Inhalt sowie den Verwendungszweck der zu speichernden Daten erkennen lassen. Die Programmdokumentation wird beim zuständigen Fachdienst aufbewahrt. Die Mitglieder des Datenausschusses dürfen jederzeit die Programmdokumentation einsehen. Die Programme dürfen nur für den genehmigten Verwendungszweck verwendet werden. Die Programmdurchführung ist entsprechend zu dokumentieren (Log-Datei).

In meinem Achten Tätigkeitsbericht (S. 16) hatte ich die Systematik der Personalinformationssysteme bei der Deutschen Bundesbahn aufgezeigt. Die örtliche Personaldatenverarbeitung (ÖPDV) wird nach erfolgreicher Erprobung nunmehr Zug um Zug bei den einzelnen Dienststellen eingeführt. Die örtliche Mitarbeiterdatei im Verfahren ÖPDV ersetzt nach ihrer jeweiligen Einführung örtliche Dateien mit ähnlichen Daten, soweit die Hauptverwaltung der Deutschen Bundebahn nicht in Einzelfällen Ausnahmen zuläßt. Bestehende Dateien mit personenbezogenen Daten, für deren Einrichtung keine Genehmigung vorliegt, sind grundsätzlich zu löschen, ihre Verwendung ist ausdrücklich verboten.

Daneben führte die DB zwischenzeitlich die Personalstammdatenverwaltung (PSV) ein. Seit Juli 1988 werden im Verfahren PSV die Stammdaten von insgesamt rund 16 000 Beamten aller Laufbahngruppen aus den vorhandenen manuellen Dateien und Personalakten erfaßt. PSV dient im wesentlichen der Personaldisposition und Personalverwaltung. Dieses System, das

bei den Bundesbahndirektionen und den zentralen Stellen der Deutschen Bundesbahn eingerichtet wird, ist ein modernes, außergewöhnlich klar strukturiertes Personalinformationssystem.

Auch dieses System kommt ohne eine freie Abfragesprache aus. Es werden nurin eine strikte Menüführung eingebundene Programme angewendet. Der Zugang zu den Daten und Programmen ist durch programmbezogene, gestaffelte Zugriffsberechtigungen bis auf die Datenfeldebene beschränkt und kontrollierbar. Neben einer vom Sicherheitsbeauftragten vergebenen Benutzeridentifikation legitimiert sich der Anwender durch ein — allerdings nur — vierstelliges Paßwort, das verdeckt einzugeben ist. Es ist zweimal wiederholbar, danach erfolgt ein Abbruch der Verbindung, der nur vom Systemverwalter behoben werden kann. Darüber hinaus wird der Wechsel des Paßwortes nach einer bestimmten Zeit vom System zwingend vorgeschrieben.

Insgesamt sind sowohl die strikte Zweckbindung als auch die Transparenz der Verwendung der Daten gegenüber den Betroffenen, der Personalvertretung und den Kontrollorganen (interner Datenschutzbeauftragter, BfD) gewährleistet.

Das Verfahren sieht u. a. Freitextfelder vor. Ich habe vorgeschlagen, diese durch Schlüsselverzeichnisse zu ersetzen oder den Umfang der definierten (also erlaubten) Eintragungen bindend vorzugeben und die Einhaltung dieser Regelung zu kontrollieren.

Darüber hinaus ist vorgesehen, sog. „sonstige personenbezogene Besonderheiten" zu speichern und zu verarbeiten. Es handelt sich dabei um Daten, die darüber Aufschluß geben, ob und inwieweit der betroffene Mitarbeiter im Rahmen der Personalplanung disponibel ist. Ich habe darauf hingewiesen, daß im Hinblick auf die höhere Sensibilität dieser Daten deren strikte Zweckbindung gewährleistet sein muß. Außerdem habe ich empfohlen, die insoweit in Betracht kommenden Datenarten in einem möglichst abschließenden Katalog zusammenzufassen und durch Stichproben sicherzustellen, daß die Eintragungen in diesem Feld dem entsprechen. Diese Daten müssen unverzüglich gelöscht werden, wenn sie für die Personaldatenverarbeitung nicht mehr relevant sind.

Eine Log-Datei bietet dem sog. „Hauptsicherheitsbeauftragten" der DB in den jeweiligen Stellen, für die PSV eingerichtet ist, die Möglichkeit, jede einzelne An- und Abmeldung eines Benutzers zu jedem einzelnen Menü mit genauem Zeitpunkt festzustellen. Auch in diesem Zusammenhang habe ich eine strikte Zweckbindung der jeweiligen Auswertungen, die nur zu Datenschutz- und Datensicherungszwecken verwendet werden dürfen, gefordert. Eine Verwendung für Zwecke der Verhaltens- und Leistungskontrolle ist durch entsprechende Maßnahmen zu verhindern. Dazu gehört u. a., daß der Sicherheitsbeauftragte keine Vorgesetztenfunktion haben und nicht in den Verantwortungsbereich für Personalführung und Personalplanung eingebunden sein darf. Auch auf die Mitbestimmungsrechte nach § 75 Abs. 3 Ziffer 17 Bundespersonalvertretungsgsetz habe ich vorsorglich hingewiesen.

6. Post- und Fernmeldewesen

Die Deutsche Bundespost bildet mit ihren rund 500 000 Beschäftigten den größten Behördenbereich in der Bundesrepublik Deutschland, zu dem fast jeder Bürger täglich Kontakt hat. Zugleich zeigt sich hier deutlicher als in allen anderen Bereichen, wie stark die modernen Techniken für die Informationsübermittlung hergebrachte Strukturen verändern und wie gering die tatsächlichen Möglichkeiten des einzelnen sind, die Auswirkungen des technischen Wandels selbst mitzugestalten, und zwar selbst für seine eigenen Kommunikationsbeziehungen.

Daraus ergibt sich zwangsläufig, daß Vorhaben wie die Digitalisierung des gesamten Fernmeldewesens und die damit einhergehende Zusammenfassung aller Fernmeldedienste in *einem* Netz (Integrated Services Digital Network = ISDN) breit und kontrovers diskutiert werden, wobei teilweise das Fernmeldegeheimnis oder sogar der Datenschutz allgemein bei der Telekommunikation als gefährdet bezeichnet werden. Umso wichtiger ist es, daß die für diese Entwicklungen verantwortlichen Stellen, besonders der Bundesminister für das Post- und Fernmeldewesen, alles tun, um nicht nur den Datenschutz in diesem wichtigen Bereich tatsächlich zu gewährleisten, sondern auch in jeder Phase der Entwicklung und für jedermann deutlich zu machen, daß dies auch ihr Ziel ist.

Aus diesem Grund war es bedauerlich, daß gerade die Zusammenarbeit des Bundesbeauftragten für den Datenschutz mit dem BMP in den letzten Jahren sehr schwierig war (s. 8. TB, S. 19; 9. TB, S. 29f.; 10. TB S. 35). Im Laufe des Berichtsjahres konnten in einer Reihe von grundsätzlichen Besprechungen die Voraussetzungen für eine sinnvolle Zusammenarbeit verbessert werden, wozu auch die Empfehlungen des Bundestagsausschusses für das Post- und Fernmeldewesen beigetragen haben.

Dabei wurden auch schon einige inhaltliche Punkte behandelt, bei denen zum Teil Annäherungen der Standpunkte erzielt werden konnten. Wichtig war für mich insbesondere die erkennbare Absicht des Bundespostministers, durch aktuelle und zusätzlich eingeleitete Maßnahmen die Qualität der Zusammenarbeit zu verbessern und die Dauer der Bearbeitungsvorgänge, vor allem, wenn sie Bürgereingaben betreffen, zu verkürzen. Auch sollen die Bemühungen verstärkt werden, im nachgeordneten Bereich — Oberpostdirektionen und Ämter — Datenschutz als wichtige Aufgabe der Verwaltung zu verdeutlichen.

Ich würde es begrüßen, wenn die ersten bereits erkennbaren Verbesserungen der Beginn einer Entwicklung in Richtung auf eine konstruktive und dem Bürger dienende Zusammenarbeit zwischen Datenschutz und Bundespostministerium wären. Eine solche könnte auch als Modell für die Kooperation mit den infolge der Umstrukturierung der Deutschen Bundespost entstehenden Unternehmen Deutsche Bundespost POSTDIENST, Deutsche Bundespost POSTBANKDIENST und Deutsche Bundespost TELEKOM dienen (siehe unten 6.1).

6.1 Neustrukturierung des Post- und Fernmeldewesens und der Deutschen Bundespost

Am 11. Mai 1988 beschloß das Bundeskabinett den Entwurf eines Gesetzes zur Neustrukturierung des Post- und Fernmeldewesens und der Deutschen Bundespost (Poststrukturgesetz). Abgesehen davon, daß jede umfassende rechtliche Neuordnung im Postbereich auch die Verarbeitung personenbezogener Daten der Postkunden berührt, ist dieser Entwurf datenschutzrechtlich deshalb von besonderer Bedeutung, weil in bestimmten Bereichen des Fernmeldewesens die Monopolstellung der Post durch die Konkurrenz zwischen der Post und privaten Anbietern von Kommunikationsdiensten ersetzt werden soll. Damit entsteht das Risiko, daß zunächst im privaten Bereich wegen der dort geltenden weniger strengen Vorschriften ein geringeres Maß an Datenschutz realisiert und danach mit den Argumenten einer bestehenden Wettbewerbssituation und der „Gleichbehandlung" der Datenschutz auch bei der Post abgebaut wird.

Weil ich — anders als bei Vorhaben anderer Ressorts üblich — bei der Vorbereitung des Entwurfs vom Bundesminister für das Post- und Fernmeldewesen nicht beteiligt wurde, konnte ich auf diese und weitere datenschutzrechtliche Probleme erst nachträglich hinweisen. Ich habe dies zunächst in einer Stellungnahme an den Bundespostminister getan.

Im Rahmen der parlamentarischen Behandlung des Gesetzentwurfes führte der Ausschuß für das Post- und Fernmeldewesen des Deutschen Bundestages im November eine Anhörung durch, zu der er auch mich als Sachverständigen eingeladen hat. Ich hatte dort Gelegenheit, meine datenschutzrechtlichen Überlegungen vorzutragen. Meine schriftliche Stellungnahme an den Ausschuß ist als Anlage 6 zu diesem Bericht abgedruckt.

Als Ergebnis der Anhörung erteilte mir der Ausschuß den Auftrag, meine Vorstellungen zur Änderung und Ergänzung der im Entwurf enthaltenen Datenschutzvorschriften für seine weiteren Beratungen zu formulieren. Es geht mir dabei vor allem darum, einen gleichwertigen und jedenfalls nicht hinter der gegenwärtigen Rechtslage zurückbleibenden Datenschutz bei allen künftigen Anbietern postalischer Dienstleistungen zu gewährleisten. Im Rahmen der inzwischen deutlich verbesserten Zusammenarbeit mit dem Bundespostministerium ist vereinbart worden, die zu behandelnden Sachfragen miteinander zu diskutieren. Auch wenn sich derzeit noch nicht absehen läßt, ob die aus den verschiedenen Positionen erwachsenden Differenzen vollständig ausgeräumt werden können, gehe ich doch davon aus, daß als Ergebnis eine gegenüber dem Regierungsentwurf datenschutzrechtlich erheblich verbesserte Lösung erreicht werden kann.

6.2 Funktelefondienst

Das grundgesetzlich geschützte Brief-, Post- und Fernmeldegeheimnis sichert dem Bürger ein Recht auf vom Staat unbeobachtete Kommunikation. Auch die näheren Umstände — insbesondere die Verbindungsdaten wie z. B. Zeitpunkt und angewählte Telefonnummer eines Telefonates — unterliegen diesem Schutz. Seit Einführung der digitalen Fernsprechvermittlungstechnik und — noch mehr — seit Aufnahme der ISDN-Betriebsversuche (vgl. 10. TB, S. 39 f.) gehen die Besorgnisse vieler Bürger dahin, daß Verbindungsdaten nicht nur für die Dauer eines Gespräches gespeichert, sondern darüber hinaus längere Zeit aufbewahrt werden. Bezüglich des drahtgebundenen Telefonnetzes sind solche Besorgnisse schon deswegen weitgehend unzutreffend, weil erst ein sehr geringer Teil in dieser modernen Technik ausgebaut ist. Demgegenüber werden im Funktelefondienst grundsätzlich die Verbindungsdaten *aller* Telefongespräche gespeichert. Davon sind bislang bereits fast 130 000 Teilnehmer betroffen (vgl. 10. TB, S. 36 f.). Besonderes Augenmerk ist in diesem Zusammenhang auf die Registrierung der Verbindungsdaten im C-Netz des Funktelefondienstes — seiner modernsten Ausbaustufe — zu richten. Die Erkenntnisse einer im Berichtsjahr vorgenommenen Datenschutzkontrolle lassen sich wie folgt zusammenfassen:

Das Funktelefonnetz erkennt und unterscheidet die Teilnehmer nicht anhand des Funktelefongerätes oder des Fahrzeuges, in dem es installiert ist, sondern durch Daten aus der sogenannten Berechtigungskarte, die zentral für die Bundesrepublik Deutschland erstellt und den Teilnehmern zugeschickt wird. Diese Berechtigungskarte enthält in der zur Zeit ausgegebenen Form als Speicherelemente neben einem Magnetstreifen einen Speicherchip gleichen Dateninhalts und kann außer im Funktelefondienst ab 1989 auch für öffentliche (Draht-) Kartentelefone verwendet werden. Kennzeichnendes Merkmal für einen Teilnehmer am Funktelefondienst ist die Funktelefonnummer, die auf die Berechtigungskarte aufgedruckt ist und nach Maßgabe der Telekommunikationsordnung (TKO) in das amtliche Telefonbuch eingetragen wird. Auf der Karte gespeichert ist außerdem eine (optisch nicht lesbare) Sicherungsnummer, die Manipulationen und Mißbrauch verhindern soll.

Ein Teilnehmer wird über die Berechtigungskarte vom System erkannt, wenn die Karte in den Kartenleser des Funktelefongerätes eingeführt wird, was den Vorgang des „Einbuchens" einleitet. Dabei wird zunächst überprüft, ob für die Funktelefonnummer ein Anschluß besteht und ob die im System gespeicherte Sicherungsnummer mit der auf der Karte übereinstimmt. Nach erfolgreichem Einbuchen wird in der jeweils zuständigen Funkvermittlungseinrichtung (FuVE) der DBP ein Datensatz angelegt, aus dem sich ergibt, daß dieser Teilnehmer „auf Empfang" ist, somit angerufen werden und auch selbst telefonieren kann. Dabei wird u. a. auch die Nummer der sog. Funkzelle gespeichert, in der sich das Fahrzeug gerade aufhält. Als Funkzelle wird dabei ein regionaler Bereich bezeichnet, der zumal in Ballungsräumen (als sog. Kleinzelle) sehr klein sein kann — z. B. nur einen Stadtteil umfaßt — und damit den Standort des Fahrzeuges verhältnismäßig genau erkennen läßt. Meldet sich der Teilnehmer — durch Entnahme der Berechtigungskarte — beim System wieder ab, wird dieser Datensatz gelöscht, wechselt er in eine andere Funkzelle, so wird der Datensatz entsprechend geändert.

Führt ein Teilnehmer nach erfolgreichem Einbuchen ein „gehendes" Gespräch, entsteht ein Verbindungsdatensatz in der FuVe, in dem nach Beendigung des Gespräches u. a. die folgenden Daten gespeichert bleiben:

- Funktelefonnummer,
- Rufnummer des angerufenen Teilnehmers,
- Angaben über Zeitpunkt, Dauer und Gebühreneinheiten des Gespräches,
- Angaben der Funkzellen, in denen die Verbindung aufgebaut und beendet wurde,
- Anzahl der Funkkanalwechsel sowie
- Gesprächskennzeichen (GKZ).

Diese Registrierungen erfolgen — mit entsprechenden Einzelangaben, wie „Gesprächsdauer: 0 Sek." — auch für Verbindungen, die z. B. wegen Nichtmelden des Angerufenen nicht zustande kamen.

Für *ankommende* Gespräche — die für den Angerufenen gebührenfrei sind — wird ein ähnlicher Datensatz angelegt; lediglich die Telefonnummer des Anrufers fehlt.

Durch Angabe sowohl der Beginn- als auch der Endfunkzelle der Verbindung sowie der Anzahl der Funkkanalwechsel — in etwa Anzahl der durchfahrenen Funkzellen — ist der ungefähre Verlauf der Fahrstrecke aus den gespeicherten Daten erkennbar. Das Gesprächskennzeichen enthält Aussagen über den äußeren Ablauf der Benutzung des Funktelefons; „24" bedeutet z. B., daß der angerufene Teilnehmer sich auch nach längerer Rufzeit nicht gemeldet hat.

Die Speicherung der Verbindungsdaten, die dem grundrechtlichen Schutz des Fernmeldegeheimnisses unterliegen, wirft erhebliche Probleme auf. Wegen ihres Eingriffscharakters kommt es in besonderem Maße darauf an, daß Speicherungen und Verarbeitungen nur dann und nur soweit erfolgen, wie es für die Aufgabenerfüllung erforderlich und aufgrund der geltenden Rechtsvorschriften zulässig ist.

Die Speicherung und Verarbeitung reiner *Verbindungsdaten,* d. h. der Daten, die für die Bereitstellung der Verbindung erforderlich sind, ist in § 450 TKO geregelt. Solche Daten sind nach Beendigung der Verbindung zu *löschen,* es sei denn, sie würden zur Gebührenrechnung (§ 451) oder aus sonstigen betrieblichen Gründen (§ 452) weiterhin benötigt. Diejenigen Daten, „die zur ordnungsgemäßen Ermittlung und Abrechnung der Fernmeldegebühren notwendig sind", gelten gemäß § 451 Abs. 1 als *Gebührendaten* und werden gemäß Absatz 3 dieser Vorschrift erst 80 Tage nach Absendung der Fernmelderechnung gelöscht.

Gemäß § 452 TKO können, soweit erforderlich, weitere personenbezogene Daten *aus betrieblichen Gründen,* insbesondere zur Störungseingrenzung und -beseitigung, Verhinderung mißbräuchlicher Verwendung von Telekommunikationseinrichtungen sowie zur Optimierung des öffentlichen Telekommunikationsnetzes erhoben, gespeichert und verarbeitet werden.

Die Speicherungen im Funktelefondienst tragen dieser rechtlichen Differenzierung zwischen Verbindungsdaten und Gebührendaten nicht Rechnung, vielmehr werden alle Verbindungsdaten wie Gebührendaten behandelt und entsprechend über die Beendigung der Verbindung hinaus gespeichert. Bedenklich ist dies insbesondere hinsichtlich der Rufnummer des angerufenen Teilnehmers, der Funkzellen, des Zeitpunktes und der Dauer sowie des Gesprächskennzeichens. Zumindest bezüglich solcher Verbindungen, für die keine tatsächlichen Anhaltspunkte etwa für eine mißbräuchliche Benutzung des Funktelefonanschlusses bestehen und auch kein Antrag des Anschlußinhabers nach § 84 Abs. 1 Nrn. 5 und 6 TKO gestellt ist, sind diese Daten gemäß § 450 Abs. 2 TKO zu löschen, da sie zu Gebührenabrechnungen nicht länger benötigt werden.

Die Fortdauer der Speicherung der Daten *aller* Verbindungen — über die Beendigung der Verbindung hinaus — kann auch nicht mit dem betrieblichen Erfordernis der Erkennung und Aufklärung von Mißbräuchen i. S. des § 452 TKO begründet werden, denn dies würde voraussetzen, daß ein durch Sicherheitsmängel bedingtes hohes Mißbrauchsvolumen besteht oder — bei selteneren Mißbräuchen — besonders schwerwiegende Folgen eintreten. Dies ist jedoch nicht der Fall: Infolge des sehr hohen und gegenüber dem älteren, aber noch weiter benutzten B-Netz erheblich gesteigerten Sicherheitsniveaus ist das Mißbrauchsvolumen gering; dies belegt auch die gegenüber dem B-Netz viel geringere Einwendungsrate der Kunden.

Auch die möglichen, durch die Sicherungsmaßnahmen aber praktisch ausgeschlossenen Folgen — überhöhte Fernmelderechnungen einzelner weniger Betroffener — können es nicht rechtfertigen, daß ein Grundrecht aller Teilnehmer auf die dargestellte Weise eingeschränkt wird.

Überdies ist derzeit noch ungeklärt, ob und in welchem Umfange Speicherung und Auswertung aller Verbindungsdaten für die Erkennung und Aufklärung von Mißbrauchsfällen überhaupt erforderlich sind; denn das System, das die — bislang überwiegend ungenutzten, „auf Vorrat" gespeicherten — Daten künftig für solche Zwecke auswerten soll, ist noch nicht einsatzbereit. Die Speicherung der genannten Daten über die Beendigung der Verbindung hinaus ist somit durch die einschlägigen bereichsspezifischen Vorschriften nicht gerechtfertigt.

Die Datensätze der *ankommenden* Gespräche beschreiben das Kommunikationsverhalten der Angerufenen, ohne daß dies erkennbar erforderlich wäre: sie sind überflüssig für die Berechnung der Gebühren und leisten auch keinen Beitrag zu einer Mißbrauchserkennung, da der Angerufene sich dem Anruf nicht entziehen und auch keinen Mißbrauch verursachen kann.

Entsprechendes gilt für die Datensätze der nicht zustande gekommenen Gespräche.

Sowohl die Speicherung dieser Daten als auch ihre Übermittlung an das Fernmeldeamt Mannheim (s. u.) sind demnach unzulässig. Ich habe die genannten Speicherungen gemäß § 20 Abs. 1 BDSG beanstandet;

die Stellungnahme des Bundespostministers liegt mir noch nicht vor, weil die dort zur Zeit stattfindende kritische Prüfung der einzelnen Datenspeicherungen auf Erforderlichkeit noch nicht abgeschlossen ist.

Die im Zusammenhang mit einer Funktelefonverbindung anfallenden Verbindungsdaten werden im Rechner der jeweils regional zuständigen FuVE auf Platten gespeichert. Nach Bedarf — in der FuVE Frankfurt etwa zweimal wöchentlich — werden aus diesen Datenbeständen die Magnetbänder erzeugt, die jeweils etwa 300 000 Verbindungsdatensätze — auch der ankommenden und nichtzustandegekommenen Gespräche — enthalten. Diese Bänder werden per Postversand dem bundesweit zuständigen Rechenzentrum Fernmeldewesen beim Fernmeldeamt Mannheim zur weiteren Verarbeitung zugeleitet. Ein Doppel des Bandes wird in der FuVE für Sicherungszwecke zurückbehalten.

Die Rechner der derzeit acht FuVEn sind durch ein bundesweites Datennetz miteinander verbunden, wodurch der Zugriff auf einen Teil der dort gespeicherten Daten — über die betreibenden Stellen mit derzeit 16 Druckterminals hinaus — einer Vielzahl weiterer Stellen eröffnet wird. Besondere Risiken ergeben sich dadurch, daß 18 dieser Anschlüsse als leistungsfähige Mehrplatz-Kleinrechner ausgeführt sind. Die Verarbeitung personenbezogener Daten mit Hilfe von Kleinrechnern wie PC u. ä. birgt gegenüber der Groß-EDV besondere und zusätzliche Risiken, auf die ich wiederholt hingewiesen habe (s. unten Nr. 24.2).

Im Rahmen der Kontrolle konnte nicht abschließend geklärt werden, auf welche Daten die etwa 45 Datenterminals sowohl bei den Fernmeldeämtern im ganzen Bundesgebiet als auch beim Fernmeldetechnischen Zentralamt (FTZ) im einzelnen zugreifen können und mit welcher Aufgabenstellung die Erforderlichkeit des Zugriffs begründet wird. Insbesondere wurde nicht klar, durch welche Aufgabenzuweisungen an die entsprechenden Referate des FTZ die Erforderlichkeit des Zugriffs auf teilnehmerbezogene Daten begründet wird und auf welche Daten im einzelnen diese Zugriffsmöglichkeit sich erstreckt.

Angesichts der — insbesondere durch den PC-Einsatz — erhöhten Risiken für den Datenschutz habe ich dem Bundesminister für das Post- und Fernmeldewesen empfohlen, bezüglich *aller* Stellen, die auf diese Daten über das Netz zugreifen können, Art und Umfang der möglichen Zugriffe unter Erforderlichkeitsgesichtspunkten zu überprüfen und — wie oben dargelegt — entsprechende Maßnahmen zu veranlassen. Über das Ergebnis dieser Überprüfung werde ich mich informieren.

Wie bereits oben erwähnt, werden die Magnetbänder, die die Daten aller über die jeweilige FuVE geführten Gespräche enthalten, dem Rechenzentrum Mannheim zur weiteren Verarbeitung zugeleitet. Dort werden mit Hilfe geeigneter Programme aus den Verbindungsdaten die entsprechenden Gebührendaten errechnet und dem Fernmelderechnungsdienst übergeben.

Das Rechenzentrum nimmt jedoch auch Auswertungen in Form von Listen vor, die z. T. auch Verbindungsdaten enthalten und an andere Stellen der DBP weitergeleitet werden. Bei einigen dieser listenmäßigen Auswertungen erscheint mir die Erforderlichkeit und somit die Zulässigkeit fraglich. Insbesondere gilt dies für eine Liste der abgewiesenen Einbuchungsversuche. Hierbei werden nicht nur mißbräuchliche Einbuchungsversuche erfaßt, sondern auch jene, die wegen technischer Probleme, z. B. schlechter Funkversorgung abgewiesen wurden. Ich halte es für geboten, hier — sofern möglich — stärker nach den Ursachen der Abweisung zu differenzieren und nur solche Datensätze ausdrucken zu lassen, die konkrete Anhaltspunkte für mißbräuchliches Handeln bieten. Ich habe auch hierzu um Stellungnahme gebeten.

Bei der FuVe Frankfurt habe ich festgestellt, daß seit etwa Mitte Juli dieses Jahres Kopien der Magnetbänder auch an das FTZ geschickt wurden.

Eine Erforderlichkeit für diese Übermittlung ist nicht erkennbar geworden. Bevor ich endgültig über eine Beanstandung entscheide, habe ich um Mitteilung gebeten, durch welche Aufgabenstellung des FTZ die Erforderlichkeit begründet ist.

6.3 Speicherung von Telefon-Verbindungsdaten

In der Bundesrepublik Deutschland gibt es etwa 27 Millionen Telefonhauptanschlüsse, über die nahezu 30 Milliarden Gespräche jährlich geführt werden. Dies belegt die Bedeutung des Telefons nicht nur für den Bereich der Wirtschaft, sondern auch für die persönliche Lebensführung der Menschen. In meinen vielen Bürgerkontakten — insbesondere auch in den Diskussionen mit den Besuchergruppen der Bundestagsabgeordneten — wird deutlich, wie wichtig in diesem Zusammenhang das grundgesetzlich geschützte Fernmeldegeheimnis gesehen wird. Dabei gehen die Bürger im allgemeinen davon aus, daß der Staat *Gesprächsinhalte* nur im Rahmen der engen gesetzlichen Vorschriften (vgl. unten Nr. 6.5) zur Kenntnis nimmt. Fast genauso wichtig ist den Bürgern aber auch der Schutz ihrer Telefon-*Verbindungsdaten*, d. h. der Angaben über Zeitpunkt, Gesprächspartner und Dauer der Gespräche, den viele als weniger gut gewährleistet ansehen.

Die bisher in den Vermittlungsstellen der Deutschen Bundespost eingesetzte Technik gestattete in der Regel keine Speicherung der Verbindungsdaten: Sobald das Telefongespräch beendet war, blieben keinerlei „Spuren" zurück, lediglich der Gebührenzähler wurde um die entsprechende Anzahl der Einheiten weitergeschaltet. Nachträglich konnte die Bundespost deshalb nur in Ausnahmefällen Aussagen über Zeitpunkt und angerufene Telefonnummern eines Teilnehmers machen, z. B. wenn auf Antrag des Teilnehmers durch eine besondere Zusatzeinrichtung ein Einzelgesprächsnachweis geführt wurde oder bei der Benutzung eines Funktelefons. Die Vorschrift des § 12 des Fernmeldeanlagengesetzes, nach der unter bestimmten Voraussetzungen in strafgerichtlichen Untersuchungen der Richter und bei Gefahr im Verzuge auch die Staatsanwaltschaft Auskunft über den Fernmeldeverkehr verlangen kann, wirkte in bezug auf den Telefonverkehr deshalb auch nur in solchen Ausnahmefällen.

Bereits vor einigen Jahren hat die Deutsche Bundespost begonnen, die alte Technik gegen neue, digitalisierte Techniken auszutauschen (vgl. 10 TB S. 39). Vorerst letzter technischer Stand ist die sogenannte ISDN-Technik (Integrated Services Digital Network). Künftig werden alle Teilnehmervermittlungsstellen der Deutschen Bundespost mit dieser Technik ausgerüstet. Ein wichtiger Unterschied zur alten Technik ist, daß bei der neuen Art der Verbindungsvermittlung die Verbindungsdaten zur Herstellung und Aufrechterhaltung der Verbindung im Computer gespeichert sein müssen und daß aus diesen Daten nach dem Ende der Verbindung die Gebühren durch ein Programm errechnet werden. Welche anderen Verarbeitungen mit den Verbindungsdaten durchgeführt werden können, hängt — weil sie jetzt verfügbar sind — nur noch von der Programmierung der Anlagen ab. Seit Ende 1986 führt die Deutsche Bundespost mit zwei ISDN-Ortsvermittlungsstellen und nahezu ausschließlich kommerziellen Teilnehmern einen Pilotversuch durch, und seit Ende des Berichtsjahres können auch private Teilnehmer ISDN-Anschlüsse erhalten. Dadurch gewinnt der Datenschutzaspekt der Speicherung von Verbindungsdaten in diesen Vermittlungsstellen auch erhebliche praktische Bedeutung.

Die Post unterscheidet bei der Speicherung von Verbindungsdaten in den ISDN-Vermittlungsstellen zur Zeit zwei Arten von Teilnehmern, nämlich solche mit analogen und solche mit digitalen Anschlüssen. Bei analogen Anschlüssen, d. h. bei „normalen" Telefonen, die an eine ISDN-Vermittlungsstelle angeschlossen sind, werden alle Verbindungsdaten nach Beendigung der Verbindung automatisch gelöscht; gespeichert bleibt lediglich die Anzahl der durch die Verbindung verursachten Gebühreneinheiten.

Bei digitalen Anschlüssen, den sogenannten „Universalanschlüssen", bleibt nach Beendigung der Verbindung in der örtlichen Vermittlungsstelle zunächst ein vollständiger Verbindungsdatensatz — mit Zeitpunkt, Dauer und Zielnummer — gespeichert. Alle Verbindungsdatensätze werden in der zeitlichen Reihenfolge, in der sie erzeugt wurden, auf ein Magnetband geschrieben und einer zentralen Dienststelle „Kommunikationsdatenverarbeitung" (KDV) übergeben. In der örtlichen Vermittlungsstelle werden die Verbindungsdaten gelöscht.

Erst in der KDV werden die Datensätze nach Teilnehmern geordnet und die Gesamtsumme der pro Teilnehmer verursachten Gebühreneinheiten errechnet. Die hierbei erzeugten Magnetbänder — die keine Verbindungsdaten mehr enthalten — werden dann dem Fernmelderechnungsdienst zugeleitet. Diese sowie die Verbindungsdaten in der KDV werden gemäß § 451 Abs. 3 TKO 80 Tage nach Absendung der Fernmelderechnung gelöscht, d. h. sie bleiben in der Praxis bis zu 100 Tagen gespeichert.

Wie oben unter Nr. 6.2 dargelegt, werden derzeit bereits im Funktelefondienst alle Verbindungsdaten gespeichert. Auch für die Buchungskarte des öffentlichen Kartentelefons, für die ganz erhebliche Zuwachszahlen erwartet werden (vgl. 10. TB S. 37 f.), soll die Verbindungsdatenspeicherung „wählbares Leistungsmerkmal" werden. Ich habe daher Verständnis für die Besorgnisse mancher Bürger, die Verbindungsdatenspeicherung in den ISDN-Vermittlungsstellen könne ein weiterer und nunmehr entscheidender Schritt hin zur Vollerfassung aller Telefongespräche werden. Ich beabsichtige, mich nicht nur über die Praxis, sondern auch über die Vorhaben der Post zur zukünftigen Verarbeitung von Verbindungsdaten zu informieren, und werde dafür sorgen, daß das Fernmeldegeheimnis und der Datenschutz der Betroffenen gewahrt bleiben.

6.4 Bildschirmtext

Im Berichtszeitraum wurde die Telekommunikationsordnung (TKO) durch die Zweite und Dritte Änderungsverordnung geändert, wovon auch die Regelungen über Bildschirmtext betroffen waren.

Besonders wichtig ist aus der Sicht des Datenschutzes die Änderung des § 423 Abs. 2 in Verbindung mit § 456 Abs. 2 TKO. Die Vorschrift räumt jetzt dem Anbieter das Recht ein, sich von der Bundespost über den vom Teilnehmer nicht bezahlten Vergütungsbetrag eine präzisere Aufstellung der Vergütungsdaten erstellen zu lassen. Diese Aufstellung läßt nun erkennen, ob der Teilnehmer selbst oder welcher seiner Mitbenutzer (z. B. Familienmitglieder) die betreffenden Seiten abgerufen hat, an welchem Tag und zu welcher Zeit dies geschah.

Der Bundespostminister begründet die Aufgabe der bisherigen, datenschutzfreundlicheren Regelung mit dem nachdrücklichen Verlangen der Bildschirmtextanbieter, gegenüber den Nichtzahlern ihre Forderungen vor Gericht durchsetzen zu können. Einige Gerichte hatten nämlich den Anspruch der Kläger als nicht hinreichend substantiiert bezeichnet, weil — nach altem Recht — nicht einmal der Zeitpunkt des betreffenden Seitenabrufes nachgewiesen worden sei. Ich habe mich davon überzeugen lassen, daß die Einführung einer Aufschlüsselung der Vergütungsdaten bei nicht bezahlten Vergütungen erforderlich und somit auch zulässig ist. Zusätzliche, von der Bundespost eingeführte organisatorische Maßnahmen — wie z. B. eine zweite Mahnung in Fällen nicht bezahlter Vergütungen — sollen helfen, unnötige Datenübermittlungen, etwa in Fällen einer vom Teilnehmer nicht zu vertretenden Zahlungsverzögerung, zu vermeiden.

Einen Schutz soll ferner die neu geschaffene Möglichkeit bieten, notorische Nichtzahler vom weiteren Abruf vergütungspflichtiger Seiten durch Einrichtung einer Zugriffssperre auszuschließen (§ 423 Abs. 2a TKO). Gegen eine solche Vorschrift bestehen aus meiner Sicht keine Bedenken, zumal gemäß Abs. 2b der Vorschrift die Zugriffssperre wieder aufgehoben wird, wenn „der Teilnehmer glaubhaft gemacht hat, daß er seine Pflicht zur Zahlung der rückständigen Anbietervergütung gegenüber dem betroffenen Anbieter bestritten hat."

Die Notwendigkeit, jetzt mit den Mitteln zusätzlicher personenbezogener Datenverarbeitung Fehlentwicklungen beim Btx-Vergütungssystem aufzufangen, ist die Folge einer vor Jahren getroffenen Entscheidung zugunsten einer detaillierten, beinahe perfektionisti-

schen Erfassung und Abrechnung von Vergütungen für einzelne Nutzungen von Btx, die zu einem erheblichen Teil aus Pfennigbeträgen bestehen. Daß Vergütungen für private Anbieter auch erheblich einfacher abgerechnet werden können, zeigt das wirtschaftlich durchaus erfolgreiche französische System. Dort rechnet die Post vergleichbare Leistungen nach nur drei verschiedenen Zeittakten sowohl mit den Teilnehmern als auch den Anbietern ab, ohne daß dafür Daten über individuelle Einzelaktionen benötigt werden.

6.5 Mitwirkung der Deutschen Bundespost bei der Telefonüberwachung

Die Deutsche Bundespost ist zur Mitwirkung bei der Überwachung des Fernmeldeverkehrs verpflichtet, soweit gesetzliche Vorschriften das Fernmeldegeheimnis beschränken. So hat z. B. in den Fällen, in denen die Strafprozeßordnung eine Überwachung des Fernmeldeverkehrs auf Grund richterlicher Anordnung vorsieht, „die Deutsche Bundespost dem Richter, der Staatsanwaltschaft und ihren im Polizeidienst tätigen Hilfsbeamten das Abhören des Fernsprechverkehrs . . . zu ermöglichen" (§ 100b Abs. 3 StPO). In der richterlichen Anordnung ist stets nicht nur der Betroffene mit Namen und Anschrift genau anzugeben, sondern u. a. auch, welcher Anschluß zu überwachen ist, wann die Überwachung beginnt und wann sie endet.

Häufig wenden sich Bürger an mich mit der Besorgnis, ihr Telefonanschluß sei Gegenstand von Überwachungsmaßnahmen (gewesen), ohne daß die gesetzlichen Voraussetzungen hierfür erfüllt seien. Zur Begründung ihrer Annahme bringen sie vor, ihr Telefon läute oft, ohne daß sich ein Anrufer meldet, bei Gesprächsverbindungen sei die Verständigung auffällig unterschiedlich, gelegentlich seien im Hintergrund eines Gesprächs fremde Stimmen vernehmbar oder häufiges „Knacken in der Leitung" und „Schaltgeräusche" während ihrer Telefongespräche seien anders nicht erklärbar. Dies alles sind bei objektiver Betrachtung keine Anzeichen für Abhörmaßnahmen nach der Strafprozeßordnung oder dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G 10); subjektiv können zufällige Häufungen solcher kleinen Störungen den Betroffenen aber durchaus beunruhigen. Deshalb bedauere ich, daß ich außer allgemeinen Erläuterungen und einer Darstellung der Rechtslage nichts aus konkreter eigener Kontrolltätigkeit zum Abbau solcher Besorgnisse beitragen kann. Dabei ließe sich durchaus die Auffassung vertreten, daß es in meiner Kompetenz liegt, das Handeln der Behörden und sonstigen öffentlichen Stellen meines Zuständigkeitsbereiches — insbesondere der Bundespost — im Zusammenhang mit der *Durchführung* der Telefonüberwachung zu kontrollieren: § 19 Abs. 1 BDSG verpflichtet mich nicht nur, die Einhaltung der Vorschriften dieses Gesetzes zu kontrollieren, sondern ebenso die „anderer Vorschriften über den Datenschutz". Die Vorschriften über das Fernmeldegeheimnis und die bei seiner Beschränkung vorgeschriebenen Regelungen sind nach meiner Überzeugung solche „anderen Vorschriften über den Datenschutz".

Wirkt die Deutsche Bundespost bei einer Maßnahme der Telefonüberwachung mit, kommt es zur Wahrung der schutzwürdigen Belange der Betroffenen auch darauf an, daß die von der Deutschen Bundespost getroffenen technisch-organisatorischen Maßnahmen der richterlichen oder staatsanwaltschaftlichen Anordnung entsprechen. Dabei ist es zum einen wichtig, daß die festgelegten Zeitpunkte von Beginn und Ende der Maßnahme entsprechend der Anordnung eingehalten werden und daß der richtige Anschluß überwacht wird. Zum anderen muß auch durch geeignete technische und organisatorische Vorkehrungen Vorsorge getroffen werden, daß Informationen über Telefonüberwachungsmaßnahmen innerhalb der Deutschen Bundespost auf einen möglichst kleinen Personenkreis beschränkt werden und eine Kenntnisnahme durch unbefugte Dritte verhindert wird. Eine Kontrolle dieser Sachverhalte ist nicht nur als Kontrolle der Einhaltung anderer Vorschriften über den Datenschutz zulässig, sondern zur Gewährleistung der Rechte des Bürgers — insbesondere, wenn er sich unter Inanspruchnahme seines Rechtes auf Anrufung aus § 21 BDSG an mich wendet — sogar geboten.

Trotzdem hat mir die Deutsche Bundespost wiederholt meine Kontrollkompetenz in dieser Angelegenheit bestritten. Im Rahmen einer Datenschutzkontrolle im Jahre 1984 wurde mir sogar die Einsichtnahme in die einschlägigen Dienstanweisungen verweigert und stattdessen lediglich eine „abstrakte Darstellung" der betreffenden Maßnahmen gegeben. Auch zu konkreten Einzelfällen wurden mir Auskünfte verweigert, so daß ich Bürgern, die sich in der Zwischenzeit an mich wandten, stets nur — in für sie und für mich unbefriedigender Weise — die Rechtslage sowie die Weigerung der Deutschen Bundespost mitteilen konnte.

Im Februar dieses Jahres wandten sich in Zusammenhang mit den Vorgängen in der Hamburger Hafenstraße über 40 Bürger an den Hamburgischen Datenschutzbeauftragten mit der Bitte, u. a. auch die datenschutzrechtlichen Aspekte der von der Staatsanwaltschaft angeordneten Telefonüberwachung zu überprüfen. Der Hamburgische Datenschutzbeauftragte, dem die Kontrolle der Maßnahmen bei den Hamburgischen Behörden schließlich gestattet worden war, wandte sich im Wege der Amtshilfe an mich, um Sachverhalte bei der Deutschen Bundespost festzustellen, die auch für seine Beurteilung des Verhaltens Hamburgischer Behörden von Bedeutung waren. Ich ersuchte deshalb die Oberpostdirektion Hamburg unter genauer Bezeichnung des Vorganges um Auskunft zu zwei konkreten Fragen, die lediglich den Zeitpunkt bestimmter Vorgänge betrafen.

Sowohl die Oberpostdirektion als auch das daraufhin von mir anschriebene Bundesministerium für das Post- und Fernmeldewesen lehnten eine Auskunftserteilung „mangels Zuständigkeit" ab. Der Bundespostminister teilte mir mit: „Im G 10-Bereich werden keine Dateien im Sinne des BDSG geführt. Die Kontrollbefugnis des BfD entfällt schon deshalb, weil er lediglich die Einhaltung der Vorschriften des BDSG sowie anderer Vorschriften über den Datenschutz zu kontrollieren hat und ihm Auskunft zu Fragen nur zu gewähren ist, soweit sie in Zusammenhang mit der Verarbei-

tung personenbezogener Daten in Dateien stehen. Rechtssystematisch bin ich darüber hinaus der Auffassung, daß das G 10 als lex specialis das staatliche Kontrollverfahren abschließend regelt. Es findet eine Kontrolle sui generis statt."

Mein Auskunftsersuchen bezog sich allerdings gar nicht auf Maßnahmen nach dem G 10, sondern auf eine Überwachung nach der Strafprozeßordnung. Der Hinweis des BMP auf das nicht einschlägige Gesetz erklärt sich aber wohl daraus, daß die DBP für die Durchführung von Telefonüberwachungsmaßnahmen Dienstanweisungen erlassen hat, die unabhängig von der Rechtsgrundlage der ergangenen Anweisung sind. Gleichwohl muß festgestellt werden, daß das Argument, das G 10 gehe als spezielle Kontrollregelung den Vorschriften des Datenschutzgesetzes vor, gegenüber Maßnahmen, die auf die Strafprozeßordnung gestützt werden, noch nicht einmal formal vorgebracht werden kann. Es ist in der Sache aber auch für Maßnahmen nach dem G 10 unzutreffend, denn die von den Gremien nach dem G 10 durchzuführende Nachprüfung tritt nach dem klaren Wortlaut und Sinn des Art. 10 Abs. 2 GG an die Stelle des Rechtsweges; sie ersetzt nicht die Kontrolle durch unabhängige Datenschutzbeauftragte, der das Bundesverfassungsgericht neben dem Rechtsweg besondere Bedeutung beimißt. Gerade weil die Fernsprechteilnehmer — seien sie nun betroffen oder, was regelmäßig der Fall ist, nicht betroffen — keine Möglichkeit zur eigenen Nachprüfung haben, ist die Beteiligung der unabhängigen Datenschutzbeauftragten von erheblicher Bedeutung für den effektiven Schutz der Rechte der Bürger. Zugleich könnte damit unbegründeten Befürchtungen besser als bisher entgegengetreten werden.

6.6 Kontrolle eines Fernmeldeamtes

In meinem Zehnten Tätigkeitsbericht (S. 37 f.) habe ich Probleme beim Einsatz von Personalcomputern (PC) in einem Fernmeldeamt geschildert und darauf hingewiesen, daß Datenschutz und Datensicherheit nicht gewährleistet waren. Der Bundesminister für das Post- und Fernmeldewesen hat mir daraufhin u. a. erwidert, der Einsatz von PC sei geregelt, die Ausführung des BDSG sei sichergestellt (s. 10. TB, S. 37 f.)

Diese Beurteilung kann ich nach einer erneuten Kontrolle des PC-Einsatzes bei einem anderen Fernmeldeamt jedoch nicht teilen, denn dort waren folgende Mängel festzustellen:

- Die mit den PC verarbeiteten personenbezogenen Daten waren überwiegend nicht in der Übersicht nach § 15 Satz 2 Nr. 1 BDSG nachgewiesen,
- die mit PC automatisch betriebenen Dateien waren überwiegend nicht zum Register gemäß § 19 Abs. 4 BDSG gemeldet,
- es bestanden keine ausreichenden, schriftlichen Dienstanweisungen, die — unter Berücksichtigung der besonderen Risiken — Umfang und Bedingungen des Einsatzes regeln (vgl. Anlage zu § 6 BDSG, Nr. 10),
- es war nicht sichergestellt, daß nur Befugte personenbezogene Daten zur Kenntnis nehmen und ändern können (vgl. Anlage zu § 6 BDSG, Nrn. 6 und 7),
- es war nicht sichergestellt, daß Datenträger nicht unbefugt entfernt werden können (vgl. Anlage zu § 6 BDSG, Nr. 2), und
- die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme wurde bei den PC nicht überwacht (vgl. § 15 Satz 2 Nr. 2 BDSG).

Gerade in technisch orientierten Bereichen wie den Fernmeldeämtern ist die Bereitschaft der Mitarbeiter sehr groß, zur Bewältigung ihrer Aufgaben auch Personalcomputer zu nutzen und diese Unterstützung durch Einfallsreichtum und Geschick besonders wirksam zu gestalten. Dabei müssen jedoch Datenschutz und Datensicherung gewährleistet sein; dazu sind auch in solchen Bereichen die Vorschriften des BDSG einzuhalten.

Ich habe die Verstöße gegen das BDSG beanstandet und zur Verbesserung des Datenschutzes folgende Maßnahmen empfohlen:

- das Aufnehmen des Ist-Zustandes (PC, Datenträger, Dateien, Verwendung, zugehörige Arbeitsabläufe),
- die Analyse der Aufgaben der PC-Benutzer,
- das Prüfen der Erforderlichkeit der (vorhandenen und künftigen) Dateien und Verfahren für die Aufgabenerfüllung,
- die Entwicklung eines Melde- und Freigabeverfahrens unter Einbeziehung des Personalrates, soweit Personalcomputer auch der Personaldatenverarbeitung dienen sollen, und
- die Schulung der Mitarbeiter in Fragen des Datenschutzes und der Datensicherung.

Dazu habe ich meine Beratung angeboten.

Die Stellungnahme des Bundesministers für das Post- und Fernmeldewesen konnte aus Zeitgründen bis zur Fertigstellung dieses Berichts noch nicht vorliegen; nach einer Vorabinformationen gehe ich aber davon aus, daß die zur Gewährleistung des Datenschutzes und der Sicherung einer ordnungsgemäßen Datenverarbeitung gebotenen Maßnahmen inzwischen getroffen sind oder noch getroffen werden.

6.7 Kontrolle des Schalterterminal-Systems EPOS

Die Deutsche Bundespost plant, in den nächsten Jahren ihre etwa 20 000 Postschalter bundesweit mit dem Datenverarbeitungssystem EPOS (Einsatz der Datenverarbeitung am Postschalter) auszustatten. Dieses System soll die unterschiedlichen Schaltervorgänge, beispielsweise Briefmarkenverkauf, Scheckauszahlung, Rückzahlung im Postsparkassendienst sowie kassenmäßige Abwicklung durch den Schalterbediensteten, wirtschaftlicher und schneller gestalten.

Im Rahmen einer datenschutzrechtlichen Kontrolle habe ich beim Postamt Hannover 1 das EPOS-Schal-

tersystem in der Pilotanwendung geprüft. Ich habe dabei festgestellt, daß EPOS nur in geringem Umfang personenbezogene Daten verarbeitet. So werden Kundendaten, die bei einer Ausweisvorlage vom Postbediensteten erfaßt werden, nicht gespeichert, sondern — wie auch im konventionellen Schalterverfahren — als Beleg separat ausgedruckt und archiviert. Daten des Schalterbediensteten werden sowohl im System als auch auf einem ausgedruckten Papierjournal festgehalten, welches sämtliche Geschäftsvorfälle und die Summe der vom Bediensteten vorgenommenen Stornierungen notiert. Während zum Zweck der Benutzeridentifizierung Name und Personalnummer notwendigerweise vorübergehend gespeichert werden müssen, vermag ich die Erforderlichkeit der personenbezogenen Notierung der Summen der Geschäftsvorfälle und der Stornierungen nicht zu erkennen. Diese Summennotierungen könnten auch als Mittel zur Verhaltens- und Leistungskontrolle eingesetzt werden, die aber nach einem Einigungsstellenbeschluß von 1986 während der Pilotanwendung des Systems EPOS nicht stattfinden darf. Zu dieser Problematik sowie zu der Frage, ob eine Leistungs- und Verhaltenskontrolle auch bei der bundesweiten Einführung von EPOS unterbleiben soll, habe ich den Bundesminister für das Post- und Fernmeldewesen um Stellungnahme gebeten.

6.8 Anschriftenprüfung

In meinem Fünften Tätigkeitsbericht (S. 34) habe ich über die datenschutzrechtliche Problematik bei der Anschriftenprüfung nach einem Wohnungswechsel des Postkunden berichtet. Dabei habe ich bemängelt, daß die Deutsche Bundespost den Kunden, der einen Nachsendeantrag stellt, nicht über die ihm eingeräumte Möglichkeit aufklärt, der Mitteilung seiner neuen Anschrift an Dritte zu widersprechen. Nach der bisherigen Praxis der Post wird nicht nur für die Dauer eines halben Jahres auf Antrag unentgeltlich Post an die neue Anschrift nachgesandt, sondern darüber hinaus auch jedem, der dies möchte, die geänderte Postanschrift mitgeteilt. Daneben gibt es einen weiteren, mit einer eigens geschaffenen Anschriftenberichtigungskarte zu beantragenden Service der Bundespost, wonach überprüft wird, ob die bisherige Anschrift noch zutreffend ist. In beiden Fällen erfährt der Postempfänger nichts davon, daß seine — möglicherweise geänderte — Postanschrift einem Dritten mitgeteilt wird. Insbesondere weiß er nicht, daß er aufgrund interner Vorschriften der Bundespost ein schriftlich geltend zu machendes Widerspruchsrecht gegen die Anschriftenmitteilung besitzt. In aller Regel besteht für ihn auch keinerlei Anlaß, sich nach einem solchen Recht zu erkundigen. Die geschilderte Praxis der Bundespost bei der Anschriftenprüfung widerspricht dem Grundsatz, daß der Postkunde selbst entscheiden können muß, wem er seine Anschrift überläßt.

Der Bundesminister für das Post- und Fernmeldewesen ist aufgrund meiner Bedenken gegen das bisherige Verfahren nunmehr bereit, datenschutzrechtlich notwendige Änderungen des einschlägigen § 38 Postordnung vorzunehmen, die voraussichtlich im Herbst 1989 in Kraft treten werden. So wird künftig in Absatz 1 der Vorschrift erstmalig normenklar ausgesprochen, daß die Post bei ihrer Anschriftenüberprüfung einem Anfragenden die zutreffende Anschrift mitteilen werde. In einem neu einzufügenden Absatz 7 wird das Recht des Postkunden normiert, dieser Anschriftenmitteilung schriftlich zu widersprechen. Gleichzeitig wird bestimmt, daß die Post verpflichtet ist, den Kunden über dieses Recht in geeigneter Weise zu informieren. Zur Umsetzung dieser Hinweispflicht hat der Bundesminister für das Post- und Fernmeldewesen zugesagt, auf der Nachsendeantragskarte einen deutlich lesbaren Hinweis auf das Widerspruchsrecht anzubringen. Auf diese Weise ist gewährleistet, daß der Postkunde Kenntnis von seinem Verfügungsrecht über seine Anschrift erhält. Mit dieser Verbesserung wird einem wichtigen Anliegen Rechnung getragen.

6.9 Wartezonen vor Postschaltern

Zahlreiche Postkunden sehen ihre schutzwürdigen Belange dadurch beeinträchtigt, daß bei der Abwicklung von Bankgeschäften vor Postschaltern ihre personenbezogenen Daten anderen wartenden Kunden zur Kenntnis gelangen können. Insbesondere bei regem Schalterbetrieb ist es leicht möglich, daß unbeteiligte Dritte — auch unbeabsichtigt — Einblick in sensible Bankgeschäfte erhalten, etwa Auszahlungsvorgänge oder die Rückgabe von Schecks nach erfolgter Deckungsanfrage. Im Ausland sind Wartezonen oder Wartelinien in angemessenem Abstand vor Post-, Bank- oder Bahnhofsschaltern häufiger anzutreffen, so daß der Kunde dort seine Angelegenheiten ungestört erledigen kann. Im Bereich der Bundesbehörden werden entsprechende Modelle zwar hin und wieder diskutiert, sind bisher aber hier nur selten realisiert worden. Um so mehr ist die Absicht des Bundesministers für das Post- und Fernmeldewesen zu begrüßen, im Laufe des Jahres 1989 gekennzeichnete Wartezonen vor Schaltern mit Bankgeschäften bundesweit einzurichten.

7. Verkehrswesen

Schwerpunkte meiner Tätigkeit auf dem Gebiet des Verkehrswesens im Berichtsjahr waren:

- Klärung von Fragen im Zusammenhang mit dem Betrieb des Zentralen Verkehrsinformationssystems (ZEVIS), insbesondere zum Umfang und zur Auswertbarkeit von ZEVIS-Protokollierungen (s. 7.2), sowie Beratung des Kraftfahrt-Bundesamtes (KBA) in diesen Fragen,
- Erarbeitung eines Konzeptes, das eine aus datenschutzrechtlicher Sicht unbedenkliche Übermittlung von Kfz.-Zulassungsdaten durch das KBA an die Automobilindustrie ermöglicht (s. 7.3.3),
- Kontrolle und Beratung der Bundesanstalt für Straßenwesen (s. 7.4).

Für den Berichtszeitraum vorgesehene Kontrollen bei der Bundesanstalt für Flugsicherung und beim Deut-

schen Hydrographischen Institut konnten wegen begrenzter Personalkapazitäten nicht durchgeführt werden.

7.1 Straßenverkehrsgesetz

Es zeichnet sich ab, daß im Rahmen des dem Deutschen Bundestag zu erstattenden Berichts über die in den ersten 4 Jahren mit dem Informationssystem ZEVIS gemachten Erfahrungen (10. TB S. 45f.) Vorschläge zur Änderung des Straßenverkehrsgesetzes unterbreitet werden, die sich beim Vollzug des Gesetzes als erforderlich erwiesen haben. Erste Überlegungen hierzu sind in einer Arbeitsgruppe der Datenschutzbeauftragten des Bundes und der Länder erörtert worden.

Um weitere Erkenntnisse zu den einzelnen Themen des ZEVIS-Berichts zu gewinnen, werde ich im kommenden Jahr ein Informations- und Prüfkonzept erarbeiten und hierauf gestützt vermehrt ZEVIS-Kontrollen vornehmen. Dabei arbeite ich mit den Landesbeauftragten für den Datenschutz zusammen.

7.2 Zentrales Verkehrsinformationssystem (ZEVIS)

Mit dem Kraftfahrt-Bundesamt (KBA) habe ich die Auswertung der zur Kontrolle automatischer Abrufe gefertigten Aufzeichnungen (ZEVIS-Protokolle) erörtert. Dabei haben sich folgende Probleme ergeben:

Das KBA ist derzeit noch nicht in der Lage, die Informationen aus den ZEVIS-Protokollen programmgesteuert je nach Anforderung auszuwerten. Ich habe daher empfohlen, ein Auswertungsprogramm für Minimalauswertungen zu erstellen. Da dieses Programm auch als Muster für die Auswertung von Aufzeichnungen bei den örtlichen Fahrzeugregistern dienen soll, war eine Abstimmung über das Auswertungsverfahren mit den Landesbeauftragten für den Datenschutz und der Datenschutzkommission Rheinland-Pfalz erforderlich. Insoweit ist inzwischen eine Einigung erfolgt. Die abschließende Abstimmung des Programms mit dem für Kfz-Zulassungsfragen zuständigen Bund/Länder-Fachausschuß steht indessen noch aus.

ZEVIS-Protokolle sind für Kontrollzwecke nur verwertbar, wenn die darin enthaltenen Informationen vollständig, übersichtlich und möglichst unverschlüsselt zur Verfügung stehen. Die mir vom KBA übersandten Ausdrucke erfüllen diese Anforderungen noch nicht. Vor allem erhalte ich getrennte Ausdrucke der nach § 36 Abs. 6 StVG zu fertigenden Aufzeichnungen über die Anfrage- und Auskunftssätze (Grundprotokolle) und der nach § 36 Abs. 7 StVG aufzuzeichnenden Zusatzangaben über den Anlaß der Abrufe und die hierfür verantwortlichen Personen (Auswahlprotokolle). Eine Zuordnung der Auswahlprotokollierung zum Grundprotokoll ist nur mit erheblichem Aufwand möglich. Ich werde dem KBA daher ein Muster über die Art der aus meiner Sicht notwendigen Aufbereitung der Protokolldaten übermitteln, die Grund- und Auswahlprotokollierungen inhaltlich zusammenfaßt.

Die Auswertung der mir vom KBA übersandten Auswahlprotokollierungen über ZEVIS-Anfragen von Bundesdienststellen hat ergeben, daß dann, wenn die abrufende Stelle den Anlaß eines Abrufs angeben muß (vgl. § 14 der Fahrzeugregisterverordnung — FRV —), die Verwendung von Schlüsselzahlen für diese zusätzliche Angabe Probleme bereitet. Insbesondere sind bei der — verhältnismäßig häufigen — Verwendung der Schlüsselzahl 6 (sonstige Anlässe) oftmals entweder keine oder unvollständige Zusatzangaben gemacht worden oder solche, die den tatsächlichen Grund des Abrufes auch nicht annähernd richtig wiedergeben. Auffällig war, daß bei insgesamt 37 Dienststellen der größte Teil der Abrufe mit mangelhaften Angaben von Dienststellen des BGS (rd. 62 %) und des Zolls (rd. 32 %) stammte. Ich habe daher den Bundesministerien des Innern und der Finanzen die betroffenen Dienststellen benannt und gebeten, diese gezielt auf die Pflicht zur korrekten Anwendung des § 14 Abs. 2 und 3 FRV hinzuweisen. Das Bundesministerium des Innern hat mir inzwischen mitgeteilt, daß die betreffenden Dienststellen des BGS und des Zolls durch die für die Fachaufsicht zuständige Grenzschutzdirektion erneut auf die Einhaltung der Bestimmungen hingewiesen worden sind.

7.3 Zulassung von Kraftfahrzeugen

7.3.1 Erhebung und Speicherung von Beruf und Gewerbe

Über meine Bedenken gegen die Erhebung und Speicherung von Angaben über Beruf und Gewerbe des Halters bei der Kraftfahrzeug-Zulassung für Aufgaben nach dem Bundesleistungsgesetz und dem Verkehrssicherstellungsgesetz habe ich berichtet (8. TB S. 24 und S. 62, 9. TB S. 81 Nr. 12). Die Problematik hat sich mit der Änderung des Straßenverkehrsgesetzes (StVG) Anfang 1987 entschärft: Berufsdaten werden seither nur noch von beruflich Selbständigen erhoben (vgl. §§ 33 Abs. 2, 34 Abs. 2 StVG). Meine zunächst noch bestehenden Zweifel, ob diese Erhebung unter dem Gesichtspunkt der Verhältnismäßigkeit aufrechterhalten bleiben oder bei der nächsten Änderung des StVG weiter beschränkt werden solle, habe ich eingehend mit den Bundesministerien für Verkehr, der Verteidigung und des Innern erörtert. Mir wurde dabei versichert, daß die Angaben zu Beruf und Gewerbe nicht nur zur Deckung des zivilen und militärischen Transportbedarfs im Spannungsfall — bei gleichmäßiger Belastung einer Gewerbegruppe — benötigt würden, sondern auch für die Festlegung des Personenkreises, der im Spannungsfall von einem Fahrverbot auszunehmen und im Rahmen der Mineralölbewirtschaftung zu bevorzugen sei.

Diese Argumente haben mich davon überzeugt, daß die Erhebung der Berufsdaten im Rahmen der Zulassung aller Kraftfahrzeuge von Selbständigen für Maßnahmen nach dem Bundesleistungsgesetz und dem Verkehrssicherstellungsgesetz erforderlich ist. Meine früheren Bedenken sind damit ausgeräumt.

7.3.2 Halterauskünfte des Kraftfahrt-Bundesamtes

Landkreise und kreisfreie Städte wenden sich bei Verkehrsordnungswidrigkeiten (vor allem falsches Parken) vor Einleitung eines Verfahrens fast ausschließlich an das KBA, um den Fahrzeughalter festzustellen. Inzwischen werden täglich ca. 68 000 Kennzeichen-Anfragen gestellt, die nur noch mit Hilfe technischer Mittel (Datenfernübertragung, Magnetband-Austausch, Erfassung über Belegleser und dv-technische Bearbeitung während der Nachtstunden) bewältigt werden können.

Da die aufgrund dieser Anfragen erteilten Auskünfte des KBA Folgen für die Betroffenen haben, ist die Aktualität des Zentralen Fahrzeugregisters beim KBA von überragender Bedeutung. Immer wieder erreichen mich jedoch Eingaben von Bürgern, die zu Unrecht einer Verkehrsordnungswidrigkeit beschuldigt worden sind. Menschliche Unzulänglichkeiten (unrichtiges Ablesen des Kfz-Kennzeichens) und technische Fehler (unrichtiges Erkennen eines Buchstabens oder einer Ziffer durch einen Belegleser) lassen sich als Ursachen nicht völlig ausschließen. Soweit die Registerauskünfte jedoch wegen organisatorischer und technischer Unzulänglichkeiten beim KBA unrichtig sind, darf dies nicht hingenommen werden; die Aktualität des Registers wird auch durch das StVG gefordert.

In diesem Zusammenhang bin ich darauf aufmerksam geworden, daß fehlerhafte Mitteilungen von Kfz-Zulassungsstellen über Besitzumschreibungen, Stillegungen und andere fahrzeugbezogene Änderungen vom KBA bei dessen Plausibilitätsprüfung abgewiesen werden, wenn eine Übereinstimmung des neuen Datensatzes mit einem bereits vorhandenen Satz bei den wichtigsten Identifizierungsdaten nicht erzielt wird. Sofern der vom System erzeugten Fehlermeldung nicht unverzüglich nachgegangen wird und eine entsprechende Berichtigung des Zentralen Fahrzeugregisters deshalb unterbleibt, ist nicht auszuschließen, daß das KBA Falschauskünfte über Halter und Fahrzeuge erteilt.

Ich habe daher gegenüber dem KBA gefordert, durch geeignete organisatorische und technische Vorkehrungen sicherzustellen, daß das Register auf Grund von Änderungsmitteilungen unverzüglich korrigiert und so eine unrichtige Auskunft vermieden wird. Das KBA hat hierzu mitgeteilt, zunächst sei mit einer eingehenden Analyse der als nicht verarbeitbar abgewiesenen Fahrzeugmeldungen der Zulassungsstellen begonnen worden. Außerdem werde noch geprüft, durch welche Maßnahmen eine zügigere Bearbeitung fehlerhafter Mitteilungen der Zulassungsstellen erreicht werden könne. Ich werde die Angelegenheit weiter verfolgen.

7.3.3 Datenübermittlung an die Automobilindustrie

Über das Problem, ob und unter welchen Voraussetzungen eine Übermittlung vom Kfz-Zulassungsdaten durch das KBA an die Automobilindustrie nach dem Straßenverkehrsgesetz (StVG) zulässig ist, habe ich berichtet (10. TB S. 46f.). Aufgrund meiner Anfang 1988 gegenüber dem Bundesminister für Verkehr ausgesprochenen Beanstandung und meiner Bitte um eine entsprechende Weisung gegenüber dem KBA wurde die Datenübermittlung an die Automobilindustrie ausgesetzt. Mit einer Wiederaufnahme der Datenübermittlung habe ich mich bisher noch nicht einverstanden erklären können.

Durch die mir inzwischen zugegangenen Informationen bin ich in meiner Auffassung bestärkt worden, daß bei dem früheren Verfahren die Automobilhersteller und -importeure in der überwiegenden Zahl der Fälle aus den übermittelten Datensätzen mit Hilfe der eigenen Verkaufsinformationen Rückschlüsse auf ein einzelnes Fahrzeug (Unikat) und dessen Halter ziehen konnten.

Ich habe in zahlreichen Gesprächen mit dem Bundesminister für Verkehr, dem KBA und Vertretern der Automobilhersteller versucht, einen datenschutzrechtlich gangbaren Weg zu finden, der eine Wiederaufnahme der Datenlieferung ermöglicht. Dabei hat sich zunächst erwiesen, daß alle Versuche einer Reduzierung des Datensatzes zu keiner nennenswerten Minderung der Unikatanteile führen; andererseits hält die Automobilindustrie an der Übermittlung des Datensatzes im bisherigen Umfang fest.

Eine weitere datenschutzrechtlich akzeptable Lösung wäre die Einholung einer Einwilligung der Käufer in die Übermittlung der Zulassungsdaten durch das KBA an die Industrie. Dieser Weg wird von den Herstellern abgelehnt, weil erfahrungsgemäß eine Vielzahl von Personen ihre Einwilligung verweigern und unvollständige Informationen ohne Wert seien. Die Automobilimporteure prüfen z.Z. noch, ob für sie die Einwilligungslösung gangbar ist.

Denkbar wäre schließlich auch, daß die Automobilhersteller in Zukunft auf die Übermittlung der Kundendaten durch die Kfz.-Händler verzichten, so daß eine Verknüpfung der KBA-Zulassungsdaten mit den Kundendaten unmöglich wäre. Die Verhandlungen über diese Variante sowie über eine den Datenschutzanforderungen genügende Einwilligungserklärung der Kfz.-Händler zur Übermittlung ihrer personenbezogenen Daten an das KBA und von dort an die Hersteller (vgl. 10. TB S. 47) konnten noch nicht abgeschlossen werden.

7.4 Bundesanstalt für Straßenwesen

7.4.1 Technische und organisatorische Maßnahmen des Datenschutzes

Die Kontrolle der Bundesanstalt für Straßenwesen (BASt) hat ergeben, daß dort dem Datenschutz bisher nicht die gesetzlich gebotene Beachtung eingeräumt wurde. So ist dem internen Datenschutzbeauftragten lediglich die Führung der Übersicht über die in der BASt geführten Dateien nach § 15 BDSG und die Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme übertragen worden. Mit der Überwachung der Durchführung von Datensicherungsmaßnahmen und der materiellen datenschutzrechtlichen Bestimmungen wurde „wegen Personalmangels" niemand beauftragt. Infolgedessen

konnte sich der Datenschutzbeauftragte mit Fragen des Datenschutzes kaum befassen. In der Bundesanstalt fehlen Regelungen über die datenschutzrechtlich erforderlichen Vorkehrungen bei der Verarbeitung personenbezogener Daten (s. hierzu 7.4.2), über datenschutzrechtliche Verantwortlichkeiten innerhalb der BASt sowie über die organisatorische Einbindung des Datenschutzbeauftragten in Entscheidungsprozesse des Amtes mit datenschutzrechtlichen Bezügen. Ich habe die BASt um Prüfung gebeten, ob eine Stärkung der Stellung des internen Datenschutzbeauftragten durch Aufgabenverlagerungen herbeigeführt werden kann. Ferner habe ich vorgeschlagen, die datenschutzrechtlichen Anordnungen der BASt auf ihre Aktualität zu überprüfen, die Einzelregelungen übersichtlich zusammenzufassen und die von mir aufgedeckten Regelungsdefizite zu beheben.

Die BASt hat inzwischen meiner Bewertung grundsätzlich zugestimmt und eingeräumt, daß Ursache für die festgestellten Mängel eine „unzureichende personelle Kapazität" sei. Die festgestellten datenschutzrechtlichen Defizite müssen unverzüglich beseitigt werden. Der Bundesminister für Verkehr ist aufgerufen, die BASt dabei zu unterstützen.

7.4.2 Organisation der automatisierten Datenverarbeitung

Bei der Kontrolle der BASt hat sich ferner ergeben, daß ein wirksamer Paßwort-Schutz gegen unbefugten Zugriff, unzulässige Veränderung und gegen aufgabenfremde Verarbeitung der Dateien nicht bestand: Es lag im Ermessen jedes Mitarbeiters, ob und wie er eine von ihm eingerichtete Datei überhaupt durch ein Paßwort schützen wollte. Ich habe zumindest für die dem BDSG unterliegenden Dateien verlangt, daß ein Paßwort bestimmte Minimalanforderungen hinsichtlich des Aufbaus und der Länge erfüllen muß und dafür entsprechende Software-Vorkehrungen zu treffen sind.

Zur Sicherstellung wichtiger Forderungen der Anlage zu § 6 Abs. 1 Satz 1 BDSG ist es erforderlich, daß insbesondere im Bereich der automatisierten Datenverarbeitung eine Aufgabentrennung gewährleistet ist. Dies bedeutet, daß dem jeweiligen Bediensteten Zugang zu Räumen und Zugriff zu technischen Einrichtungen nur in dem Umfang möglich ist, der seiner geschäftsplanmäßigen Aufgabenzuweisung entspricht. Eine solche Trennung besteht im EDV-Bereich der BASt nicht; jeder dort Tätige kann alle Räume betreten und hat — mit Ausnahme der Personaldatei — Zugang bzw. Zugriff zu allen Datenträgern. Ich habe gegenüber der BASt gefordert, daß zumindest für Dateien mit größerer Sensibilität umgehend erhöhte Sicherheitsvorkehrungen getroffen werden. Diese Forderung hat die BASt anerkannt; sie wird ihr durch entsprechende Regelungen in einer umfassenden Verfügung zum Datenschutz Rechnung tragen.

Meine Prüfung hat schließlich auch im Zentralbereich des Amtes Regelungsdefizite und datenschutzrechtliche Mängel bei der Führung und Auswertung der Personaldatei (PERSDAT) sowie der Telefondatenerfassung ergeben. Die Prüfung der Personaldatenverarbeitung bei der BASt dauert indessen noch an.

Über die Kontrolle des Forschungsbereichs in der BASt berichte ich gesondert (s. 9.1).

7.5 Luftfahrt-Bundesamt (LBA)

Über unzureichende gesetzliche Regelungen für den Umgang des Luftfahrt-Bundesamtes mit personenbezogenen Daten habe ich berichtet (9. TB S. 39f.). Inzwischen hat der Bundesminister für Verkehr (BMV) anerkannt, daß die regelmäßige Veröffentlichung personenbezogener Daten der Eigentümer von Luftfahrzeugen, die im Rahmen der Verkehrszulassung erhoben und in der Luftfahrzeugrolle eingetragen sind, auf eine gesetzliche Grundlage gestellt werden muß. Meine Überlegungen zu entsprechenden Änderungen des Gesetzes über das Luftfahrt-Bundesamt und der Luftverkehrszulassungsordnung habe ich zu Beginn des Berichtsjahres mit dem BMV erörtert. Dabei wurde Einvernehmen erzielt, daß lediglich die Veröffentlichung im amtlichen Verkündungsorgan der Bundesanstalt für Flugsicherung „Nachrichten für Luftfahrer" Regelungsgegenstand sein könne. Das von einem privaten Verlag herausgegebene internationale Luftfahrzeugregister „Régistre Aéronautique International" kann die von ihm benötigten Daten entweder den „Nachrichten für Luftfahrer" oder sonstigen öffentlich zugänglichen Quellen entnehmen; einer Veröffentlichung so gewonnener Daten kann aus datenschutzrechtlicher Sicht nicht widersprochen werden.

Der BMV hat mir inzwischen mitgeteilt, die Entwurfsarbeiten gestalteten sich unerwartet schwierig und er könne nicht absehen, wann der erste besprechungsreife Entwurf vorliege. Welche Gründe einer baldigen Umsetzung der von mir vorgeschlagenen Gesetzesänderungen entgegenstehen, vermag ich nicht zu erkennen, zumal ich dem BMV bereits schriftliche Formulierungsvorschläge zugeleitet habe.

Die vom Luftfahrt-Bundesamt geführte Datensammlung über Luftfahrer enthält für jeden Luftfahrer die Daten seiner Flugerlaubnisse und -berechtigungen (Positiv-Datei) sowie Daten über rechtskräftige Entscheidungen in Straf-, Bußgeld- und Verwaltungsverfahren (Negativ-Datei). Der BMV hatte die Notwendigkeit der von mir bereits im Jahre 1984 geforderten gesetzlichen Regelung für die Führung der Datensammlung für Luftfahrer grundsätzlich akzeptiert (7. TB S. 36, 9. TB S. 39). Leider sind mir noch keine Ergebnisse der im Jahre 1986 angekündigten Untersuchung über die Möglichkeiten einer Verbesserung der Rechtsgrundlagen bekannt geworden.

Der BMV hat inzwischen auch meine Forderung grundsätzlich anerkannt, den Umgang mit personenbezogenen Informationen bei der Wahrnehmung der Aufgaben der Flugunfalluntersuchungsstelle (FUS) beim Luftfahrt-Bundesamt auf eine gesetzliche Grundlage zu stellen (vgl. 9. TB S. 40). Das Ministerium hat als erste Maßnahme eine Dienstanweisung über die Aktenführung im Bereich der FUS erlassen, die auch die Einsicht Dritter in die Flugunfallunter-

suchungsakten regelt. Ich verkenne nicht, daß diese Regelung einen Fortschritt gegenüber der bisherigen Praxis darstellt. Sie kann jedoch nur als Zwischenlösung bis zu einer gesetzlichen Regelung akzeptiert werden. Insofern hat mir der BMV mitgeteilt, mit der Erarbeitung einer Verordnung über die Untersuchung von Flugunfällen und Flugbetriebsstörungen könne nicht vor Ablauf von weiteren zwei Jahren gerechnet werden. Der Grund hierfür sei eine Organisationsprüfung der FUS, die sich auch auf deren Aufgaben erstrecke und deshalb Auswirkung auf die beabsichtigte gesetzliche Regelung haben werde. Ich bedauere die Verzögerung auch auf diesem Sektor und hoffe, daß der BMV die auch von ihm für notwendig gehaltenen gesetzlichen Regelungen so rasch wie möglich in Angriff nimmt.

7.6 Deutsche Bundesbahn — Schwarzfahrerdatei —

Über die Speicherung personenbezogener Daten strafunmündiger Kinder bei Schwarzfahrten im Verbundverkehr, an dem die Deutsche Bundesbahn beteiligt ist, habe ich berichtet (10. TB S. 49f.). Die Deutsche Bundesbahn hält weiterhin daran fest, daß diese Speicherung zur Feststellung von Mehrfachtätern sowie zur Verfolgung von Schadensersatzansprüchen wegen Verletzung der Aufsichtspflicht nach § 832 BGB erforderlich sei.

Nach meiner Auffassung liegt in solchen Fällen ein berechtigtes Interesse der Deutschen Bundesbahn an einer solchen Speicherung nach Zahlung des erhöhten Beförderungsentgelts für die bis dahin festgestellten Schwarzfahrten nicht mehr vor, da weder ein zivilrechtlicher Anspruch besteht, noch ein Strafantrag nach § 265 a StGB gestellt werden kann. Ich habe die Deutsche Bundesbahn daher erneut gebeten, die persönlichen Daten strafunmündiger Kinder im Verbundverkehr nur noch bis zur Zahlung des erhöhten Beförderungsentgelts zu speichern. Die Stellungnahme der Deutschen Bundesbahn hat mich erst nach Redaktionsschluß dieses Berichts erreicht, so daß ich darauf nicht mehr näher eingehen konnte.

8. Statistik

8.1 Volkszählung 1987

Gegen Ende der Berichtszeit wurden die ersten Ergebnisse der Volkszählung 1987 veröffentlicht. Die Erhebungsvordrucke sind gemäß den Regelungen des Volkszählungsgesetzes 1987 nunmehr zügig zu vernichten. Der Zeitpunkt der Vernichtung der Erhebungsbogen darf nach übereinstimmender Auffassung der Datenschutzbeauftragten von Bund und Ländern auch nicht durch etwaige verwaltungsgerichtliche Verfahren hinausgezögert werden, die einzelne Gemeinden anstrengen könnten, weil sie mit der festgestellten Einwohnerzahl nicht einverstanden sind. Da die verwaltungsgerichtliche Kontrolle sich auf die ordnungsgemäße Durchführung der Volkszählung beschränkt, der Inhalt des einzelnen Erhebungsbogens somit nicht Gegenstand des Prozesses ist, besteht keine Notwendigkeit, die Bogen bis zum Abschluß solcher Verfahren aufzubewahren. Das Volkszählungsgesetz 1987 sieht vor, daß nunmehr die auf den Erhebungsvordrucken ausgedruckten laufenden Nummern und die im Erhebungsverfahren verwendeten Ordnungsnummern, die vorübergehend mit den für die Auswertung bestimmten Merkmalen auf die für die maschinelle Weiterverarbeitung bestimmten Datenträger übernommen werden durften, zu verfremden sind. Dadurch soll der Bezug der Volkszählungsdaten zu kleineren Einheiten als der Blockseite, z. B. einem einzelnen Haus oder einer Wohnung, beseitigt werden. Die verfremdeten Nummern sollen nur noch Auskunft geben über die Zugehörigkeit von Personen zu Haushalten, von Haushalten zu Wohnungen und von Wohnungen zu Gebäuden. Wenn durch diese Verfremdungsmaßnahmen der Personenbezug der Volkszählungsdaten auch nicht endgültig aufgehoben werden kann, so wird damit doch ein für eine Reidentifizierung wesentliches Verbindungsglied beseitigt.

Das von den Statistischen Ämtern des Bundes und der Länder vorgesehene Verfremdungsprogramm wurde in einer Arbeitsgruppe von Mitarbeitern zweier Landesdatenschutzbeauftragter und meiner Dienststelle geprüft. Die Arbeitsgruppe hat Vorschläge für die konkrete Anwendung des Programms erarbeitet, die die vom Gesetzgeber beabsichtigte Schutzwirkung für die Betroffenen sicherstellen. Es ist zu erwarten, daß die Statistischen Ämter diese Vorschläge aufgreifen werden.

Eine weitere Aufgabe für die Datenschutzbeauftragten im Zusammenhang mit der Volkszählung wird die Prüfung der Tabellenerstellungsprogramme sein. Hierbei gilt es zu verhindern, daß durch die Art der Gliederung von Tabellen auf einen einzelnen Auskunftsgebenden beziehbare Angaben offenbart werden. Da das Volkszählungsgesetz 1987 die Übermittlung von nicht vollständig anonymisierten Einzelangaben an solche Stellen der Gemeinden zuläßt, die von anderen kommunalen Verwaltungsstellen getrennt sind, werden sich die Datenschutzbeauftragten ferner mit den Statistischen Ämtern über die erforderlichen Organisations- und Verfahrensstandards zu verständigen haben, die die Sicherung des Statistikgeheimnisses auch innerhalb der Gemeinden gewährleisten.

8.2 Novellierung der Rechtsgrundlagen einzelner Statistiken

Nachdem in den vergangenen Jahren das Volkszählungs-, das Mikrozensus- und das Bundesstatistikgesetz verabschiedet worden waren, hatte sich meine Dienststelle im Berichtszeitraum geradezu mit einer Welle von Novellierungsentwürfen statistischer Rechtsgrundlagen zu befassen. Rund 20 Entwürfe insbesondere aus dem Bereich der Wirtschaftsstatistiken waren datenschutzrechtlich zu prüfen, wobei die Rechtssetzungsvorhaben der EG noch nicht eingerechnet sind.

Die Kernfrage bei der Beurteilung dieser Entwürfe war, inwieweit die Ausführungen im Volkszählungs-

urteil auch für Wirtschaftsstatistiken gelten. Ich habe dabei die Auffassung vertreten, daß das Recht auf informationelle Selbstbestimmung auch dann wirksam ist, wenn der Bürger sich am Wirtschaftsleben beteiligt. In dieser Weise hat sich auch das Bundesverfassungsgericht in jüngster Vergangenheit geäußert und insbesondere ausgeführt, daß „kein Grund dafür ersichtlich" ist, „die den Gewerbetreibenden im Wirtschaftsleben betreffenden personenbezogenen Daten einem prinzipiell abgeschwächten grundrechtlichen Schutz zu unterstellen" (so Beschluß vom 25. 7. 1988 — 1 BvR 109/85). Das Bundesverfassungsgericht hat ergänzend ausgeführt, der regelmäßig gesteigerte Sozialbezug solcher Daten müsse bei der Prüfung der Einschränkbarkeit des Rechts auf informationelle Selbstbestimmung im Einzelfall berücksichtigt werden.

Die Frage, welche Grundsätze bei der Verarbeitung von Wirtschaftsstatistikdaten zu beachten sind, stellt sich in zugespitzter Form bei der Nutzung solcher Daten in Verbindung mit den in § 13 Bundesstatistikgesetz vorgesehenen „Adreßdateien". Bei diesen Dateien handelt es sich um auf Dauer angelegte Register mit den Namen, Anschriften und einigen typisierenden Merkmalen aller Unternehmen, Betriebe und Arbeitsstätten, die zu bundesstatistischen Erhebungen herangezogen werden. Mit Hilfe dieser Register können die Statistischen Ämter des Bundes und der Länder alle wirtschaftsstatistischen Daten betriebsbezogen miteinander verknüpfen. Adreßdateien nach der genannten Vorschrift dürfen angelegt werden, soweit dies für bundesstatische Zwecke „erforderlich" ist. Für diesen Fall ist vorgesehen, alle Angaben, die über die betroffenen Wirtschaftseinheiten für Zwecke einer Wirtschaftsstatistik erteilt werden, mit einer Kennummer zu versehen, die über die Adreßdatei die Feststellung ihres Namens erlaubt. Auf diese Weise wird es u. a. möglich, die betreffenden statistischen Angaben auf ihre Plausibilität zu kontrollieren, sie im Wege einer Längsschnittanalyse über einen längeren Zeitraum mit den Angaben der Folgejahre zu vergleichen oder sie mit den Angaben über dieselbe Arbeitsstätte aus den anderen Statistiken zu verknüpfen.

Es ist unverkennbar, daß die beschriebenen Verknüpfungsmöglichkeiten der amtlichen Statistik beachtliche Möglichkeiten für statistische Analysen an die Hand geben. Ebenso offensichtlich sind allerdings auch die damit verbundenen Risiken für die Betroffenen. Wie ich bereits in meinem 9. TB (S. 44) ausgeführt habe, sehe ich darin die Gefahr des Entstehens von Abbildern der betroffenen Wirtschaftseinheiten, zu denen überwiegend natürliche Personen, wie z. B. Einzelkaufleute, gehören. Außerdem wird der Grundsatz der frühestmöglichen Anonymisierung statistischer Angaben, den das Bundesverfassungsgericht als „konstitutiv" für die Statistik bezeichnet hat, für einen weiten Bereich der Statistik verlassen.Nach mehreren Besprechungen, die ich mit betroffenen Ressortvertretern und dem Statistischen Bundesamt über denkbare Lösungen dieses Problems geführt habe, beginnen sich Kompromisse abzuzeichnen. Dazu hat auch beigetragen, daß der Bundesminister des Innern seine grundsätzliche Bereitschaft erklärt hat, daran mitzuwirken, § 13 Bundesstatistikgesetz um Regelungen zu ergänzen, die u. a. die Persönlichkeitsrechte der von der Registervorschrift Betroffenen möglichst weitgehend berücksichtigen.

Zu einigen datenschutzrechtlich problematischen Gesetzentwürfen nehme ich nachfolgend im einzelnen Stellung.

8.2.1 Agrarstatistikgesetz

Mit dem Entwurf eines Gesetzes über Agrarstatistiken (Agrarstatistikgesetz) hat es die Bundesregierung zum ersten Mal unternommen, ein Gesetz für statistische Erhebungen im Bereich der Wirtschaft an die Anforderungen des Volkszählungsurteils und des Bundesstatistikgesetzes 1987 anzupassen. Der Entwurf war Gegenstand mehrerer Ressortbesprechungen, an denen ich beteiligt worden bin. Die endgültige Entwurfsfassung, die noch nicht allen datenschutzrechtlichen Anforderungen genügte, wurde mir allerdings so spät zugestellt, daß meine schriftliche Stellungnahme nicht mehr vor der Verabschiedung des Entwurfs im Bundeskabinett berücksichtigt werden konnte. Ich hatte aber Gelegenheit, den Innenausschuß des Deutschen Bundestages auf meine datenschutzrechtlichen Bedenken hinzuweisen.

Der Entwurf des Agrarstatistikgesetzes faßt Regelungen über Landwirtschaftsstatistiken in einem Gesetz zusammen, die bisher in verschiedenen Rechtsgrundlagen enthalten waren. Gleichzeitig erlaubt der Entwurf, die für die verschiedenen Statistiken erhobenen Angaben mit Hilfe eines Betriebsregisters betriebsbezogen zu verknüpfen. Auf diese Weise kann ein zentrales, maschinell betriebenes Informationssystem entstehen, das Abbilder aller Landwirtschaftsbetriebe enthält. Dabei können nicht nur reine Produktionsdaten gespeichert, sondern auch personenbezogene Informationen über soziale Verhältnisse des Betriebsinhabers, seines Ehegatten und der auf dem Betrieb lebenden Verwandten und Verschwägerten einbezogen werden.

Mein Haupteinwand richtet sich auch gegen diese Vorschrift. Das Bundesverfassungsgericht hat die möglichst frühzeitige Anonymisierung von Einzelangaben, die für statistische Zwecke erhoben worden sind, verbunden mit Vorkehrungen gegen eine Deanonymisierung zum Schutz des Rechts auf informationelle Selbstbestimmung der Betroffenen für „unverzichtbar" erklärt. Ein Betriebsregister in der vorgesehenen Form läßt dagegen eine dauernde personenbezogene Speicherung der erhobenen Daten zu. Daher müssen nach meiner Überzeugung besondere Vorkehrungen innerhalb der statistischen Ämter über Aufbewahrung und Verwendung des Betriebsregisters und einschränkende Regelungen für die Verknüpfung von Erhebungen mit Hilfe des Registers vorgesehen werden. Über die bereits bisher zugelassenen Zusammenführungen von Daten für die sog. Agrarberichterstattung hinaus sollten Verknüpfungen nur dann stattfinden, wenn deren Erforderlichkeit feststeht. Keinesfalls sollten aber Verknüpfungen von Daten über andere Personen als den Betriebsinhaber erfolgen. Auf die in dem Entwurf vorgesehene Möglichkeit, aufgrund einer Verordnung des Bundesministers für Ernährung, Landwirtschaft und Forsten

Agrarstatistiken auch mit anderen Wirtschaftsstatistiken zu verknüpfen, will die Bundesregierung aufgrund der von mir erhobenen Einwände nunmehr verzichten.

Bedenken habe ich ferner gegen einzelne Erhebungsmerkmale, z. B. die außerbetrieblichen Erwerbs- und Unterhaltsquellen des Ehegatten des Betriebsinhabers und der auf dem Betrieb lebenden und im Betrieb mithelfenden Verwandten und Verschwägerten. Weiterhin habe ich gefordert, noch bessere organisatorische und verfahrensmäßige Vorkehrungen zu treffen. So sollte gewährleistet werden, daß

- den einzelnen betreffende Angaben bei diesem selbst und ohne Einsichtsmöglichkeit durch Dritte erhoben,
- die von den Ländern mit der Durchführung von Landwirtschaftsstatistiken betrauten Erhebungsstellen von anderen Verwaltungsbereichen abgeschottet und
- bei der Weinbauerhebung die Gefahr einer Vermischung von Aufgaben der Statistik mit denen des Verwaltungsvollzugs beseitigt werden.

Die Bundesregierung hat während der Beratungen im Innenausschuß des Deutschen Bundestages meinen Empfehlungen in weitem Umfang zugestimmt. Der Ausschuß hat sich den übereinstimmenden Voten der Bundesregierung und des Bundesbeauftragten für den Datenschutz angeschlossen und darüber hinaus dafür ausgesprochen, die Notwendigkeit der Datenerhebung sowie die Möglichkeiten einer besseren Anonymisierung zu prüfen. Die Punkte, in denen noch keine Einigkeit erzielt werden konnte, sollen bei den Beratungen des federführenden Ausschusses für Ernährung, Landwirtschaft und Forsten geklärt werden.

8.2.2 Handwerkstatistikgesetz

An dem Novellierungsentwurf des Gesetzes über die Statistik im Handwerk (Handwerkstatistikgesetz) habe ich im Hinblick auf die vom Bundesverfassungsgericht geforderte möglichst frühzeitige (faktische) Anonymisierung kritisiert, daß das Merkmal „Gesamtumsatz" zusammen mit den Namen und Anschriften der Handwerker gespeichert und laufend aktualisiert werden soll. Darüber hinaus ist für mich nicht ohne weiteres verständlich, warum zur Erzielung repräsentativer Ergebnisse der Statistik heute 40 000 der — laut Begründung — 491 000 Unternehmen befragt werden müssen, während beim Erlaß des früheren Gesetzes noch 35 000 der damals rund 750 000 Betriebe ausreichten. Die Weiterentwicklung der statistischen Methodik sollte eigentlich — wie auch vom Bundesverfassungsgericht gefordert — zu einer Reduzierung der Zahl der einzubeziehenden Erhebungseinheiten genutzt werden können.

Der mir nunmehr vorgelegte überarbeitete Entwurf des Handwerkstatistikgesetzes sieht nicht mehr ausdrücklich vor, den Umsatz zusammen mit den Namen der Handwerksbetriebe zu speichern. Statt dessen soll der Bundesminister für Wirtschaft ermächtigt werden, mit Zustimmung des Bundesrates festzulegen, mit welchen Merkmalen aus anderen Wirtschaftsstatistiken die Angaben aus der Handwerkstatistik über die Adreßdatei des § 13 Bundesstatistikgesetz (siehe oben 8.2) verknüpft werden dürfen. Um eine solche Verknüpfung zu ermöglichen, soll jeder Handwerksbetrieb eine Kennummer erhalten. Nunmehr sollen 37 000 selbständige Handwerker in die Statistik einbezogen werden; diese Zahl darf aber um 3 000 überschritten werden.

8.2.3 Rohstoff- und Produktionswirtschaftsstatistikgesetz

Der Bundesminister für Wirtschaft hat mir den Novellierungsentwurf des Gesetzes über Statistiken der Rohstoff- und Produktionswirtschaft einzelner Wirtschaftszweige (Rohstoffstatistikgesetz) zugeleitet. Der Entwurf entsprach im wesentlichen den Anforderungen des Datenschutzes. Die in dem Entwurf vorgesehene Zuständigkeit des Bundesamtes für Wirtschaft für die Durchführung der Statistik der Nichteisen- und Edelmetallwirtschaft setzt nach der Rechtsprechung des Bundesverfassungsgerichts voraus, daß die Abschottung des Statistikbereichs im Bundesamt gesetzlich vorgeschrieben wird (vgl. dazu auch 8.3). Aufgrund meiner Stellungnahme hat der Bundesminister für Wirtschaft die betreffende Regelung des Entwurfs entsprechend meinen Vorstellungen überarbeitet. Unterschiedliche Auffassungen bestehen noch über die Zusammenführung der aufgrund dieses Gesetzes zu erhebenden Daten mit anderen Dateien unter Inanspruchnahme der sogenannten Adreßdateien der statistischen Ämter nach § 13 des Bundesstatistikgesetzes. Insoweit hoffe ich auf eine Klärung im weiteren Gesetzgebungsverfahren.

8.2.4 Lohnstatistikgesetz

Der Referentenentwurf des Bundesministers für Arbeit und Sozialordnung für ein Drittes Gesetz zur Änderung des Gesetzes über die Lohnstatistik, mit dem das Gesetz über die Lohnstatistik an die Anforderungen des Volkszählungsurteils und des Bundesstatistikgesetzes angepaßt werden soll, erfüllt im wesentlichen die datenschutzrechtlichen Anforderungen.

Zu bedauern ist jedoch, daß eine datenschutzrechtliche Schutzvorschrift, die nach dem Volkszählungsurteil erlassen worden war, wieder aufgehoben werden soll. Mit dem Zweiten Gesetz zur Änderung des Gesetzes über die Lohnstatistik war eine erfreulich präzise Regelung geschaffen worden, wonach Namen und Anschriften von auskunftspflichtigen Arbeitgebern und Namen und Kennziffern der betroffenen Arbeiter nach Abschluß der Prüfung der Angaben auf Vollständigkeit und Plausibilität von den Erhebungsbogen zu trennen und nach dem Vergleich mit den Angaben der folgenden Erhebung zu vernichten sind. Darüber hinaus hatte es diese Regelung für zulässig erklärt, die Namen und Anschriften der Auskunftspflichtigen als Adreßmaterial für eine nachfolgende Erhebung zu nutzen.

Mit der vorgesehenen Aufhebung dieser Vorschrift soll zugelassen werden, daß Namen und Anschriften

der Auskunftspflichtigen — über die bisherigen Verwendungsmöglichkeiten hinaus — jederzeit den von einem bestimmten Arbeitgeber erteilten Angaben zugeordnet und diese mit den Angaben zu allen nachfolgenden Erhebungen nach dem Lohnstatistikgesetz sowie mit allen sonstigen Wirtschaftsstatistiken verknüpft werden. Die Vernichtung der Namen und Anschriften der betroffenen Arbeiter soll nun nicht mehr — wie bisher — nach einem präzise bezeichneten Arbeitsgang, sondern aufgrund der Regelung des Bundesstatistikgesetzes nur noch „zum frühestmöglichen Zeitpunkt" erfolgen.

Die vorgesehenen neuen Verwendungsmöglichkeiten bedeuten einen wesentlich stärkeren Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen, da die Angaben zur Lohnstatistik, z. B. die nach Verdienstbestandteilen gegliederten Bruttoverdienste eines Arbeitnehmers und die Arbeitsstunden einschließlich der Mehrarbeitsstunden, nun nicht mehr anonym gespeichert werden sollen. Der Bezug der Angaben zu einem bestimmten Arbeitgeber soll jederzeit herstellbar sein mit der Folge, daß sich hierdurch auch die Reidentifizierungsmöglichkeit der betroffenen Arbeitnehmer wesentlich erhöht.

Die ins Auge gefaßte Nutzungserweiterung wurde bisher lediglich mit einer angeblich gebotenen Anpassung an die durch das Volkszählungsurteil veranlaßte Neufassung des Bundesstatistikgesetzes begründet. Das Bundesstatistikgesetz sieht aber nur vor, daß für derartige Verwendungszwecke Register u. a. mit Namen und Anschriften von Auskunftspflichtigen geführt werden dürfen, „soweit sie ... erforderlich sind". Diese Voraussetzung ist bisher nicht nachgewiesen. Zu kritisieren ist ferner, daß die in der Begründung zum Entwurf enthaltene Auffassung, das Dritte Änderungsgesetz berühre „weder den bisherigen Inhalt noch den bisherigen Umfang der amtlichen Lohnstatistik", nicht zutrifft.

In meiner Stellungnahme habe ich weiterhin erneut bemängelt, daß der Entwurf es den Arbeitgebern freistellt, ob sie die erforderliche Individualisierung der geforderten Angaben über ihre Arbeitnehmer durch Beifügung des Namen oder einer Nummer erreichen wollen. Ich bin ganz entschieden der Auffassung, daß eine namentliche Übermittlung der Daten ausgeschlossen werden sollte, weil sie dazu führen würde, daß über die betroffenen Arbeitnehmer ohne deren Kenntnis personenbezogen so sensible Merkmale wie Bruttoverdienst und Qualifikation gespeichert werden. Der Zweck dieser Regelung, nämlich im Falle erforderlicher Rückfragen beim Arbeitgeber wegen Unvollständigkeit oder Inplausibilität von Angaben einzelne Arbeitnehmer eindeutig zu identifizieren, kann auch mit einer laufenden Nummer erreicht werden. Ich fühle mich in meiner Auffassung auch dadurch bestätigt, daß in der Vergangenheit einzelne Statistische Landesämter bei der Lohnstrukturerhebung die Erfassung des Namens der Arbeitnehmer für verzichtbar erklärt haben und ein solcher Verzicht bei der Sozialhilfestatistik, bei der sich das Problem der Rückfragen in gleicher Weise stellt, schon seit Jahren allgemein praktiziert wird (vgl. dazu bereits meinen 3. TB S. 24).

8.2.5 Umweltstatistikgesetz

Der Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit hat einen ersten Entwurf zur Novellierung des Gesetzes über Umweltstatistiken vorgelegt.

Der Novellierungsentwurf zeichnet sich gegenüber dem bisher geltenden Gesetz durch eine präzisere Beschreibung der für die Statistik zu erhebenden Merkmale und des Kreises der zu Befragenden aus. Auch im übrigen trägt er den Belangen des Datenschutzes im wesentlichen Rechnung. Einigen der von mir vorgeschlagenen kleineren Korrekturen des Entwurfs hat der Bundesminister zugestimmt. Datenschutzrechtlich problematisch sind nur noch die Bestimmungen des Entwurfs über die Übermittlung und Veröffentlichung von Umweltstatistikdaten. Dabei handelt es sich zum einen um die Ermächtigung zur Weitergabe von Einzelangaben in Tabellen für Planungszwecke durch die Statistischen Ämter des Bundes und der Länder an die für Umweltfragen zuständigen oberen Bundes- und Landesbehörden. Im Hinblick auf die Ausführungen im Volkszählungsurteil muß sichergestellt sein, daß den begünstigten Behörden keine auf einzelne Auskunftspflichtige beziehbare statistische Daten offenbart werden. Bedenken bestehen auch gegen die vorgesehene Veröffentlichung von bestimmten Einzelangaben, die sich auf einzelne Auskunftspflichtige beziehen.

In der weiteren Vorbereitung des Entwurfs werde ich mich bemühen, auch in diesen Fragen noch zu vertretbaren Lösungen beizutragen.

8.2.6 Straßenverkehrsunfallstatistikgesetz

Zu der Novellierung des Gesetzes über die Statistik der Straßenverkehrsunfälle (Straßenverkehrsunfallstatistikgesetz) habe ich bereits in meinem 10. Tätigkeitsbericht Stellung genommen (vgl. S. 55 f.). Bisher ungelöst war die Frage, wie es der Bundesanstalt für Straßenwesen (BASt) ermöglicht werden könnte, mit Hilfe der Statistikdaten Unfallforschung zu betreiben, ohne das Statistikgeheimnis zu gefährden. Da die BASt ihre Forschungsziele nicht mit anonymen Datensätzen erreichen kann und die Schaffung einer eigenen Rechtsgrundlage für Unfallforschung als Lösungsmöglichkeit nicht weiterverfolgt wurde, habe ich vorgeschlagen, bei der BASt eine räumlich, organisatorisch und personell abgeschottete Statistikstelle einzurichten. Nach dem Volkszählungsurteil ist nämlich die Übermittlung personenbezogener Statistikdaten durch die Statistischen Ämter an andere Behörden nur dann zulässig, wenn sie zum Zweck statistischer Aufbereitungen erfolgt und die empfangende Stelle von den übrigen Verwaltungseinheiten wirksam abgeschottet ist.

Die Bundesregierung hat diesen Vorschlag aufgegriffen und in den Gesetzesentwurf eine Regelung aufgenommen, wonach bei der BASt eine Organisationseinheit eingerichtet wird, die den Vorgaben für eine wirksame Abschottung entspricht. Ferner ist ausdrücklich sichergestellt, daß die Straßenverkehrsunfallstatistikdaten nicht mit anderen Daten der BASt

zusammengeführt werden dürfen. Nach meiner Auffassung ist damit eine verfassungsrechtlich unbedenkliche Lösung gefunden worden. Auch bei anderen problematischen Regelungen des Entwurfs konnten zufriedenstellende Ergebnisse erzielt werden, so daß meine Bedenken gegen den Gesetzentwurf der Bundesregierung nunmehr ausgeräumt sind.

Der Bundesrat hat allerdings in seiner Stellungnahme zum Gesetzentwurf die Aufnahme von Regelungen gefordert, die nur schwer mit den für die Statistik geltenden Geheimhaltungsgrundsätzen in Einklang zu bringen sind. Es handelt sich dabei insbesondere um eine Vorschrift, wonach unter anderem den mit der Wahrnehmung von Aufgaben der Verkehrssicherungspflicht und der Unfallverhütung betrauten Landesbehörden Einzelangaben über Verkehrsunfälle übermittelt werden sollen. Aufgrund der eingehenden Diskussion des Gesetzentwurfs und des dadurch geschärften Problembewußtseins bin ich aber zuversichtlich, daß die Bundesregierung in ihrer Gegenäußerung zur Stellungnahme des Bundesrates keinem Änderungswunsch zustimmen wird, der datenschutzrechtlich bedenklich und auch mit einem verfassungsrechtlichen Risiko behaftet ist.

8.2.7 Ausbildungsförderungsstatistik

Im Zehnten Tätigkeitsbericht (S. 62f.) hatte ich die Datenerhebung durch die Ämter für Ausbildungsförderung nach § 55 Abs. 3 des Bundesausbildungsförderungsgesetzes (BAföG) kritisiert. Nach meinen Feststellungen umfaßten die Erhebungen nicht nur Auskünfte, die für deren Verwaltungstätigkeit erforderlich sind, sondern — unzulässigerweise — auch Daten, die allein für Zwecke der Bundesstatistik benötigt werden (z. B. Berufstätigkeit oder Art der Ausbildung des Ehegatten, Familienstand und Berufstätigkeit der Eltern).

Im Entwurf des Elften Gesetzes zur Änderung des BAföG hat der Bundesminister für Bildung und Wissenschaft den Versuch unternommen, meinen Bedenken durch eine Ergänzung des § 55 Abs. 3 Rechnung zu tragen. Der den gesetzgebenden Körperschaften zugeleitete Entwurf, an dessen Ausarbeitung ich nicht beteiligt worden war, konnte jedoch weder unter datenschutzrechtlichen noch unter statistisch-fachlichen Gesichtspunkten befriedigen. Auf meine Intervention hat der Bundestagsausschuß für Bildung und Wissenschaft zwar davon abgesehen, die von der Bundesregierung vorgeschlagene Vorschrift zu verabschieden; eine befriedigende Lösung für mein Hauptanliegen wurde damit jedoch nicht mehr erreicht. Die Schaffung einer datenschutzrechtlich unbedenklichen Erhebungsgrundlage für die Ausbildungsförderungsstatistik muß daher leider der in Kürze anstehenden Zwölften Änderung des BAföG vorbehalten bleiben. Hierbei muß § 55 BAföG auch an die Anforderungen des Bundesstatistikgesetzes angepaßt werden, und zwar sind insbesondere die erforderlichen Hilfs- und Erhebungsmerkmale zu bestimmen. In entsprechender Weise ist auch der von den Ämtern für Ausbildungsförderung genutzte Fragebogen abzuändern.

8.2.8 Krankenhausstatistik

Nach dem im Rahmen des Gesundheits-Reformgesetzes vorgelegten Entwurf einer Neufassung des § 28 Abs. 2 des Krankenhausfinanzierungsgesetzes war vorgesehen, daß die Statistischen Landesämter den zuständigen Landesbehörden für Zwecke der Krankenhausplanung und Krankenhausfinanzierung die Erhebungsbögen der zur Krankenhausstatistik herangezogenen Krankenhäuser zur Verfügung stellen. Aus diesen Bögen ergibt sich eine Reihe von Daten vor allem über Personal und Patienten in den Krankenanstalten, die — vor allem in kleineren Krankenhäusern — unschwer den Betroffenen zugeordnet werden können; darüber hinaus sind bei privat geführten Krankenhäusern auch die personenbezogenen Daten der Leiter dieser Einrichtungen berührt.

Eine derartige Weitergabe der Erhebungsbögen an die zuständigen Landesbehörden hätte die Übermittlung nicht anonymisierter, zu statistischen Zwecken erhobener Daten an Verwaltungsbehörden zu nichtstatistischen Zwecken bedeutet. Dies hätte gegen den im Volkszählungsurteil besonders herausgestellten Grundsatz der Trennung von Statistik und Verwaltungsvollzug verstoßen. Eine gesetzliche Regelung, die Erhebung und Verwertung personenbezogener Daten zu statistischen Zwecken und zugleich zu Zwecken des Verwaltungsvollzuges erreichen will, ist hiernach jedenfalls dann verfassungswidrig, wenn sie tendenziell Unvereinbares miteinander verbindet. Eine zuverlässige Statistik ist nur dann zu erwarten, wenn die Auskunftgebenden darauf vertrauen können, daß ihre Angaben ausschließlich für statistische Zwecke verwendet werden. Bei der vorgesehenen Regelung wäre dies aber deshalb nicht gewährleistet gewesen, weil die erhobenen Angaben auch zu nachteiligen Maßnahmen gegen die betroffenen Krankenhäuser — etwa Kürzung oder Streichung von Mitteln — hätten genutzt werden können. Die beiden vorgesehenen Erhebungszwecke waren deshalb miteinander unvereinbar.

Weil diese Vorschrift des Entwurfs der Bundesregierung nicht mit mir abgestimmt war, konnte ich diese datenschutzrechtlichen Bedenken dem Bundesminister für Arbeit und Sozialordnung erst nach der Einbringung des Entwurfs im Bundestag mitteilen. Während der Beratung im Deutschen Bundestag ist es gelungen, die Vorschrift entscheidend zu verbessern.

Nach der erreichten Neufassung des § 28 gibt es eine klare Trennung zwischen der Auskunftspflicht der Krankenhaus- und Sozialleistungsträger zum Zwecke der Verwaltung und Planung (Abs. 1) und der statistischen Auskunftspflicht der Krankenhausträger gegenüber den Statistischen Ämtern der Länder (Abs. 2). Daß ein Teil der Krankenhausträger gleichzeitig die von der Statistik umfaßten Sachverhalte auch den zuständigen Landesbehörden mitzuteilen hat, weicht den Grundsatz der Trennung zwischen Statistik und Vollzug nicht auf, weil die Befragten die Angaben jeweils getrennt machen dürfen. Ich habe mich deshalb mit der Regelung einverstanden erklären können.

In der Neufassung sind auch die Sachverhalte, zu denen Erhebungen — nach näherer Maßgabe einer

Rechtsverordnung — durchgeführt werden können, durch eine abschließende Aufzählung im Gesetz verbindlich festgelegt. Damit konnte im Vergleich zum Regierungsentwurf die Normenklarheit der Regelung wesentlich erhöht werden.

Mit dem Inkrafttreten des Gesundheits-Reformgesetzes ist die Krankenhausstatistik auf eine verfassungs- und datenschutzrechtlich befriedigende Grundlage gestellt.

8.2.9 Schwangerschaftsabbruchstatistik

Der Bundesminister für Jugend, Familie, Frauen und Gesundheit beabsichtigt, die Schwangerschaftsabbruchstatistik neu zu regeln. Um das bisherige Statistikverfahren zu verbessern, ist vorgesehen, kassenärztliche Leistungen für Schwangerschaftsabbrüche nur dann zu gewähren, wenn der Arzt zuvor den Nachweis erbracht hat, daß der Schwangerschaftsabbruch dem Statistischen Bundesamt gemeldet worden ist. Offen ist dabei noch, wie der Nachweis der Statistikmeldung zu führen ist; in Betracht kommen die Übersendung einer Durchschrift der Meldung an das Statistische Bundesamt oder die Mitteilung der Nummer des Bogens, auf dem die Meldung erfolgt ist. Unklar ist ferner, ob zu diesem Zweck auch personenbezogene Daten zwischen dem Statistischen Bundesamt und den Krankenkassen übermittelt werden sollen. Sollte das letztere der Fall sein, müßte dies unter Beachtung des Abschottungsgebots der amtlichen Statistik gesetzlich geregelt werden.

Ich habe gegenüber dem Bundesministerium angeregt zu prüfen, ob das angestrebte Ziel einer Verbesserung der Schwangerschaftsabbruchstatistik nicht einfacher durch eine sekundärstatistische Erhebung bei den Kassenärztlichen Vereinigungen erreicht werden könnte. Hierbei müßte in den Erhebungsbögen angegeben werden, ob ärztliche Leistungen über einen Schwangerschaftsabbruch abgerechnet worden sind oder nicht. Diese Lösung würde den Austausch personenbezogener Daten zwischen dem Statistischen Bundesamt und den Kassen entbehrlich machen.

In dem endgültigen Entwurf müßte auch entschieden werden, ob das angestrebte Ziel — wie im Vorentwurf — im Rahmen der Änderung der Reichsversicherungsordnung oder aus Gründen der Rechtsklarheit nicht besser dort geregelt werden sollte, wo sich die Rechtsgrundlage dieser Bundesstatistik befindet, nämlich im Strafrechtsreformgesetz von 1974.

8.2.10 Ausländerstatistik

Zu dem Entwurf eines Gesetzes über das Ausländerzentralregister habe ich mich bereits an anderer Stelle geäußert (vgl. 2.2). In meiner Stellungnahme gegenüber dem Bundesminister des Innern habe ich auch auf meine Bedenken gegen die in diesem Entwurf enthaltene Rechtsgrundlage für die Ausländerstatistik hingewiesen.

Diese bestehen zum einen darin, daß sich entgegen der Überschrift der betreffenden Vorschrift das Zugangsrecht des Statistischen Bundesamts zu Informationen aus dem Ausländerzentralregister keinesfalls auf anonyme Daten beschränkt. Zum anderen halte ich die gewählte Konstruktion der Rechtsgrundlage für die Durchführung der Statistik nicht für tragfähig. Der Gesetzentwurf legt nur fest, zu welchen Daten das Statistische Bundesamt Zugang hat. Laut Begründung soll sich aus dieser Regelung in Verbindung mit § 5 Abs. 5 Satz 2 Bundesstatistikgesetz zugleich die Ermächtigung für das Statistische Bundesamt ergeben, die Ausländerstatistik durchzuführen. Nach dieser Vorschrift ist nämlich ausnahmsweise eine ausdrückliche Anordnung durch Gesetz oder Rechtsverordnung für solche Bundesstatistiken entbehrlich, bei denen Angaben ausschließlich aus öffentlichen Registern verwendet werden, zu denen dem Statistischen Bundesamt oder den Statistischen Landesämtern in einer Rechtsvorschrift ein Zugangsrecht gewährt wird. Das Ausländerzentralregister ist aber keineswegs ein „öffentliches Register" im Sinne dieser Vorschrift. So hat auch die Bundesregierung bei den Beratungen des Entwurfs des Bundesstatistikgesetzes im Innenausschuß des Deutschen Bundestags vorgetragen, daß sich die Regelung des § 5 Abs. 5 Satz 2 auf „offenkundige Daten" beziehe.

Darüber hinaus habe ich kritisiert, daß — entgegen dem Grundsatz der Trennung von Statistik und Verwaltungsvollzug — auch solche Daten in das Ausländerzentralregister aufgenommen werden sollen, die allein für statistische und planerische Zwecke benötigt werden. Dafür bedürfte es einer eigenen statistischen Vorschrift, die eine derartige Aufgabe mit allen Gewährleistungen der amtlichen Statistik (insbesondere Einhaltung des Statistikgeheimnisses, Einrichtung eines abgeschotteten statistischen Bereiches) im einzelnen regelt. Zweckmäßigerweise sollte eine solche Aufgabe aber einem Statistischen Amt und nicht einer hierzu nicht eingerichteten Verwaltungsbehörde zugewiesen werden.

Schließlich habe ich angeregt, die laut Begründung zum Entwurf beabsichtigten Übermittlungen von Daten aus dem Ausländerzentralregister durch das Statistische Bundesamt an die Statistischen Ämter der Länder für regionale Sonderaufbereitungen aus Gründen der Normenklarheit im Gesetz zu regeln.

8.3 Bundesstatistik beim Bundesamt für Wirtschaft

Wie an anderer Stelle des Berichts ausführlich dargelegt (vgl. unten 22.1.1), habe ich eine Kontrolle und Beratung des Bundesamtes für Wirtschaft (BAW) durchgeführt. Die Prüfung in der mit statistischen Aufgaben befaßten Organisationseinheit des BAW hat mich veranlaßt, die alsbaldige Vorlage eines Konzepts zur Trennung des Statistikbereichs des Amtes von den übrigen Organisationseinheiten und die Neugestaltung von Erhebungsunterlagen zu fordern.

Der Statistikbereich des BAW, der im wesentlichen die Nichteisen- und Edelmetallstatistik nach dem Gesetz über Statistiken der Rohstoff- und Produktionswirtschaft einzelner Wirtschaftszweige durchführt,

muß nach dem Bundesstatistikgesetz zum 1. Januar 1989 von den übrigen Organisationseinheiten des Amtes abgeschottet sein. Zum Zeitpunkt des Kontrollbesuchs lag ein Konzept dafür noch nicht einmal in den Grundzügen vor. Inzwischen hat mir das Bundesamt den Entwurf einer Anordnung vorgelegt, der eine geeignete Grundlage für die Sicherstellung der organisatorischen, räumlichen und personellen Trennung seines Statistikbereichs von dem übrigen Amtsbereich darstellt.

Die von mir im BAW vorgefundenen Erhebungsbogen der Nichteisen- und Edelmetallstatistik entsprachen noch nicht den Anforderungen des Bundesstatistikgesetzes von 1987. Insbesondere fehlte es an der für die Befragten wichtigen Unterrichtung über die Rechtsgrundlage der Erhebung, die verwendeten Hilfsmerkmale und weitere Sachverhalte, über die zwingend aufzuklären ist. Die technische Gestaltung des Erhebungsbogens erlaubte es nicht, die Hilfsmerkmale zum frühestmöglichen Zeitpunkt von den übrigen Angaben abzutrennen. Das BAW hat mir inzwischen Entwürfe neu gestalteter Erhebungsbogen und der zur Unterrichtung der Befragten vorgesehenen Beiblätter zugeleitet, die bis zur völligen Neugestaltung der Erhebungsbogen nach Inkrafttreten des neuen Rohstoffstatistikgesetzes (vgl. 8.2.3) verwendet werden sollen.

1.4 JUSTIS

Aufgrund der Eingabe eines Richters habe ich das Justizstatistikinformationssystem des Bundesministers der Justiz (JUSTIS) kontrolliert. In der Eingabe war die Befürchtung geäußert worden, mit Hilfe von JUSTIS sei die Erstellung von Entscheidungs- und Arbeitsprofilen einzelner Richter möglich. Diese Befürchtung wurde durch meine Feststellungen nicht bestätigt.

Das Informationssystem JUSTIS enthält Angaben über Gerichtsverfahren, die von den Landesjustizverwaltungen im Rahmen einer Zählkartenerhebung in Zivilsachen (einschließlich Familiensachen) laufend erfaßt werden. Im wesentlichen handelt es sich dabei um Angaben über den Gegenstand des Verfahrens, die Art der Erledigung, den Inhalt der Entscheidung (einschließlich der Entscheidung über die Gerichtskosten), allgemeine Daten über die Parteien und die Bezeichnung des entscheidenden Gerichts. Einige Angaben der Zählkartenerhebung, z. B. die Geschäftsnummer und die Kennzahl der Richtergeschäftsaufgabe, werden in JUSTIS nicht gespeichert. Zweck von JUSTIS ist es, auf der Grundlage von Einzeldatensätzen statistische Auswertungen über die betroffenen Gerichtsverfahren vornehmen zu können. Außer dem Bundesminister der Justiz hat derzeit nur der Justizminister Nordrhein-Westfalen unmittelbaren Zugang zu dem System.

Obwohl weder der Name eines Richters noch die Kennzahl der Richtergeschäftsaufgabe erfaßt werden, ist es insbesondere bei kleinen Gerichten mit Hilfe von Zusatzinformationen über die Geschäftsverteilung möglich, einzelne Entscheidungen einem bestimmten Richter zuzuordnen. JUSTIS ermöglicht jedoch nicht eine totale Kontrolle richterlichen Handelns. Dafür ist zunächst von Bedeutung, daß JUSTIS derzeit mit der Beschränkung auf Zivilsachen (einschließlich der Familiensachen) nur einen Ausschnitt richterlicher Entscheidungen erfaßt. Die überwiegende Zahl der Richter wird während ihrer beruflichen Karriere auch in anderen Gerichtszweigen eingesetzt oder in Spruchkörpern tätig, in denen ihre Identififizierung nicht möglich ist, weil eine Entscheidung nicht dem einzelnen Richter, der sie abgesetzt hat, sondern nur seiner Kammer oder seinem Senat zugeordnet werden kann. Bereits dadurch dürfte in aller Regel gewährleistet sein, daß die Erstellung eines „Totalabbildes" der Tätigkeit eines einzelnen Richters ausgeschlossen ist. Die gespeicherten Daten sind auch nicht unmittelbar auf einen bestimmten Richter bezogen; eine Deanonymisierung könnte nur mit Hilfe von Zusatzwissen erfolgen. Eine weitere Schwierigkeit der Zuordnung zu einem bestimmten Richter besteht darin, daß die Möglichkeit einer Dezernatsvertretung durch einen anderen Richter einkalkuliert werden muß. Dadurch kann selbst mit Hilfe von Zusatzwissen zumindest nicht in allen Fällen eine korrekte Zuordnung der Verfahrensdaten erreicht werden.

Die somit nur in Einzelfällen mögliche Zuordnung von Entscheidungen beeinträchtigt nach meiner Auffassung das Recht auf informationelle Selbstbestimmung der entscheidenden Richter nicht unzumutbar. Dabei gehe ich davon aus, daß das Recht auf informationelle Selbstbestimmung in bezug auf die amtliche Tätigkeit eines Richters ohnehin bereits durch den Grundsatz der Öffentlichkeit von Gerichtsverhandlungen, Publizitätsgebote sowie nicht zuletzt durch das allgemeine Interesse an einer möglichst verläßlichen Abschätzung von Prozeßrisiken in zulässiger Weise eingeschränkt wird. Diese Einschränkungen kommen auch in der Übermittlungs- und Veröffentlichungspraxis von Gerichtsentscheidungen zum Ausdruck, bei der die Schwärzung des Namens des entscheidenen Richters als hinreichende Maßnahme zu dessen Persönlichkeitsschutz angesehen wird.

Hinzu kommt, daß die nach einer Deanonymisierung aus JUSTIS zu erhaltenden Informationen im Hinblick auf die Besonderheiten jedes Einzelfalles nur schwerlich geeignet sind, sichere Rückschlüsse auf ein bestimmtes Entscheidungsverhalten eines Richters zu ziehen. Am ehesten ist hierfür noch die Kostenentscheidung geeignet; doch kann auch sie allein kaum ein zutreffendes Bild über den Ausgang eines Verfahrens vermitteln, zumal teilweise Klagerücknahmen hierin nicht zum Ausdruck kommen.

Unter Abwägung aller Gesichtspunkte habe ich bisher keine Veranlassung gesehen, die derzeitige Datenverarbeitung von JUSTIS zu beanstanden. In weiteren Gesprächen mit dem Bundesminister der Justiz werde ich allerdings noch den Fragen nachgehen, ob für JUSTIS eine eigenständige Rechtsgrundlage erforderlich ist und ob die Anonymität der von den Gerichtsverfahren Betroffenen hinreichend gesichert ist.

8.5 Nutzung von Angaben zur Todesursachenstatistik für staatsanwaltschaftliche Ermittlungen

Ein Statistisches Landesamt hat auf Anweisung seiner vorgesetzten Behörde den vertraulichen Teil von drei Leichenschauscheinen, die es zur Durchführung der Todesursachenstatistik erhalten hatte, für strafrechtliche Ermittlungen an eine Staatsanwaltschaft weitergegeben, obwohl es selbst gegen diese Durchbrechung des Statistikgeheimnisses rechtliche Bedenken geltend gemacht hatte. Die Staatsanwaltschaft hatte demgegenüber angeführt, daß die Leichenschauscheine, die von Ärzten auszustellen, vom Gesundheitsamt auf die Vollständigkeit der medizinischen Daten zu überprüfen und dem Statistischen Landesamt zu übermitteln sind, beim Gesundheitsamt ohne weiteres hätten beschlagnahmt werden dürfen; daher könne nichts anderes gelten, wenn sich die Scheine bereits beim Statistischen Landesamt befänden.

Auch nach meiner Auffassung ist eine möglichst umfassende Geheimhaltung der in den Statistischen Ämtern des Bundes und der Länder aufbewahrten Daten zwingend notwendig. Wie im Volkszählungsurteil ausgeführt wird, ist die ausschließliche statistische Nutzung der Daten in den Statistischen Ämtern nicht nur zum Schutz der Betroffenen im Einzelfall erforderlich, sondern auch die Basis für eine verläßliche Statistik, da sie das Vertrauen in den Schutz der Daten schafft, ohne das die Erteilung wahrheitsgemäßer Angaben nicht zu erwarten ist. Diese Auffassung habe ich auch gegenüber dem Statistischen Bundesamt und der Presse, die mich zu dem geschilderten Sachverhalt befragt hat, zum Ausdruck gebracht.

Als Konsequenz daraus ist meines Erachtens bereits bei der Organisation statistischer Erhebungen stärker darauf zu achten, daß für die Gewinnung statistischer Informationen Erhebungsverfahren gewählt werden, die möglichst wenige Berührungspunkte mit der Aufgabenerfüllung der Vollzugsverwaltung haben. So ist zu fordern, daß Daten grundsätzlich auf getrennten Erhebungswegen beschafft werden. Wenn also — wie im vorliegenden Fall — die Auskunftspflicht des Arztes normiert ist, so sollte er seine Meldung unmittelbar dem Statistischen Landesamt erteilen. Falls auch das Gesundheitsamt die Daten aus dem Leichenschauschein benötigen sollte, müßten ihm diese Informationen auf gesondertem Erhebungsweg mitgeteilt werden. Sollten hingegen Daten, die bereits bei Verwaltungsbehörden vorliegen, für eine Bundesstatistik genutzt werden, so sollten diese bei den betreffenden Behörden auf statistischen Meldeformularen erhoben und bereits so aufbereitet werden, daß sie einen möglichst geringen Bezug zu den betroffenen Personen aufweisen.

Die Novellierung des Bevölkerungsstatistikgesetzes, das die Grundlage für die Todesursachenstatistik darstellt, steht unmittelbar bevor. Ich werde mich bei dessen Beratung darum bemühen, daß diesen Gesichtspunkten Rechnung getragen wird.

8.6 Informationstechnisches System zur Unterstützung bei Kostenrechnungen im Dienstrechtsbereich (ISKD)

Der Bundesminister des Innern plant die Einführung eines Informationssystems beim Statistischen Bundesamt, für das Bund und Länder Personaldaten ihrer Beschäftigten zur Verfügung stellen sollen. Aufgabe dieses „Informationstechnischen Systems zur Unterstützung bei Kostenrechnungen im Dienstrechtsbereich (ISKD)" soll es sein, rasche und zuverlässige Kostenberechnungen im Besoldungs-, Tarif- und Versorgungsbereich zu ermöglichen. Da die geplante Datenverarbeitung auch personenbezogene Besoldungsdaten umfaßt, ergibt sich eine Reihe von datenschutzrechtlichen Problemen. Ich habe daher in einer Stellungnahme gegenüber dem Bundesminister des Innern ausgeführt, welche datenschutzrechtlichen Voraussetzungen erfüllt sein müssen, damit ISKD eingerichtet werden kann.

Da der vom Bundesminister des Innern angeführte Artikel 74 a Grundgesetz nicht als ausreichende Ermächtigungsgrundlage für die Übermittlung der Beschäftigtendaten angesehen werden kann, ist es notwendig, entweder bereits bei den Ausgangsbehörden eine Anonymisierung der Datenbestände vorzunehmen oder das Statistische Bundesamt im Wege der Datenverarbeitung im Auftrag unmittelbar für diese Stellen tätig werden zu lassen. Ferner muß sich die Zugriffbefugnis der beteiligten Stellen auf diejenigen Datenbestände im Statistischen Bundesamt beschränken, die keine personenbeziehbaren Einzelangaben mehr enthalten. Darüber hinaus habe ich die Prüfung angeregt, ob die von den Ausgangsbehörden gelieferten Individualdatensätze im Statistischen Bundesamt auch dann noch aufbewahrt werden müssen, wenn sie — wie vorgesehen — zu Ergebnissen für vier große Gruppen, z. B. Bereich „Länder", aggregiert worden sind. Jedenfalls erscheint mir die Notwendigkeit ihrer Aufbewahrung für den Zeitraum von fünf Jahren nicht zwingend.

Eine Antwort des BMI auf meine Stellungnahme steht noch aus.

9. Wissenschaft und Forschung

9.1 Forschung in der Bundesanstalt für Straßenwesen

Wie bereits an anderer Stelle des Berichts ausgeführt (vgl. 7.4), habe ich die Einhaltung datenschutzrechtlicher Vorschriften bei der Bundesanstalt für Straßenwesen (BASt) kontrolliert. Die stichprobenweise Kontrolle im Bereich Unfallforschung hat weder hinsichtlich der Eigenforschung der BASt noch im Hinblick auf die Forschung Dritter im Auftrag der BASt (Fremdforschung) zur Feststellung datenschutzrechtlicher Verstöße geführt. Gleichwohl habe ich einige Verbesserungen vorgeschlagen.

So habe ich angeregt, eine Hausverfügung zu erlassen, die alle datenschutzrechtlich relevanten Aspekte eines Forschungsvorhabens zusammenfaßt. Die bisherigen Bestimmungen zum Schutz personenbezoge-

ner Daten bei der Durchführung von Forschungsvorhaben waren auf verschiedene Verfügungen verteilt und zudem ergänzungsbedürftig. Insbesondere erscheint es mir erforderlich, in der Verfügung den Unterschied zwischen personenbezogenen und anonymen Einzelangaben herauszustellen. In der Frage des Personenbezugs darf es keine Unklarheiten geben, da hiervon die Anwendung des Datenschutzrechtes auch bei Forschungsvorhaben abhängt. Es sollte geregelt werden, über welche Sachverhalte eines Forschungsvorhabens aufzuklären ist, wenn Personen um die freiwillige Erteilung von Auskünften für ein Forschungsvorhaben gebeten werden. Darüber hinaus sollte deutlich gemacht werden, für welche Zwecke Auskünfte genutzt werden dürfen.

Ferner habe ich vorgeschlagen, die Vertragsbedingungen für Auftragnehmer der BASt, die für sie Forschungsvorhaben durchführen, um Regelungen zur Sicherung des Datenschutzes zu ergänzen. Dadurch soll der Schutz der Teilnehmer an einem Forschungsprojekt in diesen Fällen in gleicher Weise gewährleistet werden wie bei dessen Durchführung durch die BASt selbst. Im einzelnen geht es dabei um die Verpflichtung zum Hinweis auf die Freiwilligkeit der Teilnahme an einem Forschungsvorhaben, die Verwendung der Daten nur im Rahmen des Auftrags und die Beachtung aller übrigen für die BASt geltenden Datenschutzbestimmungen, z. B. über die Löschung der Daten. Aus dem gleichen Grund sollte der Auftragnehmer verpflichtet werden, sich der Kontrolle eines unabhängigen Datenschutzbeauftragten zu unterwerfen; eine solche Regelung sieht das neue hessische Datenschutzgesetz bereits vor. Eine entsprechende Ergänzung der Vertragsbedingungen halte ich insbesondere deshalb für erforderlich, weil der Kreis der potentiellen Auftragnehmer der BASt sehr heterogen ist, so daß nicht in jedem Fall die Kenntnis der datenschutzrechtlichen Verpflichtungen unterstellt werden kann.

Wie mir die BASt inzwischen mitgeteilt hat, wird sie in Kürze sowohl die angesprochenen Hausverfügungen als auch die Bedingungen für Forschungsverträge überarbeiten und hierbei meine Vorschläge berücksichtigen.

9.2 Forschungsvorhaben „Anonymisierung"

Der Lehrstuhl für Methoden der empirischen Sozialforschung und angewandte Soziologie der Universität Mannheim führt zusammen mit dem Statistischen Bundesamt unter Mitwirkung des Zentrums für Mikrodaten, einer Abteilung des Zentrums für Umfragen, Meinungen und Analysen (ZUMA), Mannheim, ein Forschungsprojekt mit der Bezeichnung „Entwicklung eines anonymisierten Mikrodatenfiles für wissenschaftliche Zwecke" durch. Ziel dieses Projektes, das vom Bundesminister für Forschung und Technologie finanziert wird, ist die Erarbeitung allgemeiner Regeln zur Beurteilung der Frage, ob ein Einzeldatensatz nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer Person zugeordnet werden kann. Nur unter dieser Voraussetzung dürfen nach der Vorschrift des § 16 Abs. 6 Bundesstatistikgesetz Einzelangaben, die für statistische Zwecke erhoben worden sind, vom Statistischen Bundesamt und den Statistischen Ämtern der Länder an Hochschulen oder sonstige Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung für die Durchführung wissenschaftlicher Vorhaben übermittelt werden.

Obwohl im Vordergrund der Untersuchung der Zugang der wissenschaftlichen Forschung zu statistischen Mikrodaten stehen, verspreche ich mir von diesem Projekt, in dessen begleitendem Beirat auch meine Dienststelle vertreten ist, neue Erkenntnisse zu der für alle Bereiche des Datenschutzrechts bedeutsamen Frage, wann Einzeldatensätze als hinreichend (faktisch) anonymisiert angesehen werden können. Das Projekt bietet auch Gelegenheit, im Dialog mit Wissenschaftlern Standards für die Datensicherung bei der Durchführung von wissenschaftlichen Vorhaben zu erarbeiten.

Das Projekt baut auf den Erkenntnissen auf, die in dem Forschungsvorhaben der Gesellschaft für Mathematik und Datenverarbeitung (GMD) mit der Bezeichnung „Konstruktion und Erprobung eines anonymisierten integrierten Mikrodatenfiles der bundesdeutschen Privathaushalte" gewonnen wurden. In mehreren Arbeitsschritten werden dabei zunächst verschiedene Wissenschaftsszenarien für die human- und gesellschaftswissenschaftliche Forschung entwickelt, um sodann eine operationale Definition des gesetzlichen Merkmals „unverhältnismäßig großer Aufwand an Zeit, Kosten und Arbeitskraft" für eine Reidentifizierung zu erarbeiten. Schließlich ist vorgesehen, anhand empirischer Untersuchungen die Schutzwirkung ausgewählter Anonymisierungsverfahren zu überprüfen und auf dieser Grundlage konkrete Anonymisierungsregeln aufzustellen. Die Ergebnisse dieses Projekts sollen im September 1989 vorgestellt werden.

9.3 Gentechnologie

Die Enquete-Kommission „Chancen und Risiken der Gentechnologie" des 10. Deutschen Bundestages hat in ihrem Anfang 1987 vorgelegten Schlußbericht (Bundestagsdrucksache 10/6775) zu den verschiedenen Anwendungsbereichen, Querschnittsthemen und Rechtsfragen der Gentechnologie Empfehlungen formuliert, die sich an den Deutschen Bundestag richten und deren Verwirklichung teilweise gesetzgeberische Maßnahmen erfordert. Für den Datenschutz sind insbesondere die Beratungen der Kommission zum Anwendungsbereich „Genomanalyse" von Interesse. Die Nutzung von gentechnischen Untersuchungsmethoden ist vorstellbar

- in der pränatalen Diagnostik,
- beim Neugeborenen-Screening (d. h. der Untersuchung Neugeborener auf bestimmte genetisch bedingte Entwicklungsstörungen oder Schäden),
- in der Arbeitsmedizin im Rahmen von Einstellungs-, Eignungs- oder Vorsorgeuntersuchungen,
- zur Risikobewertung im Versicherungswesen sowie

— im gerichtlichen Verfahren zur Überführung von Straftätern oder zum Vaterschaftsnachweis.

Einige dieser Anwendungen werden vereinzelt schon praktiziert.

In allen diesen Fällen können personenbezogene Informationen von hohem Aussagewert, aber auch äußerst sensiblen Inhalts entstehen, die zumindest teilweise zum inneren Kernbereich der Persönlichkeitssphäre gehören und aus deren Kenntnis sich weitreichende, möglicherweise existentielle Konsequenzen für den Betroffenen ergeben. Die Enquete-Kommission hat die Vor- und Nachteile solcher Anwendungen der Genomanalyse auch unter datenschutzrechtlichen Gesichtspunkten aufgezeigt und Handlungsbedarf des Gesetzgebers festgestellt. Die Datenschutzbeauftragten müssen diese Problematik aufgreifen, um im aktuellen Beratungsfall reagieren zu können. Zur speziellen Frage der Erhebung, Speicherung und Verwertung genetischer Analyseergebnisse für Zwecke der polizeilichen Prävention und der Strafverfolgung hat die Enquete-Kommission in ihrem Bericht ausdrücklich empfohlen, „daß sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder dieser Problematik annimmt und zu ihr Stellung nimmt".

Die Konferenz hat daraufhin eine Arbeitsgruppe unter meiner Federführung eingesetzt, die sich mit den genannten Anwendungsmöglichkeiten und ihrer datenschutzrechtlichen Bewertung befaßt. Die Verhandlungen erweisen sich als außerordentlich schwierig und werden nach meinem derzeitigen Eindruck — längerfristig — nicht ohne naturwissenschaftliche Sachkunde speziell auf dem Gebiet der Humangenetik auskommen. Es hat sich ferner gezeigt, daß eine datenschutzrechtliche Bewertung zum Teil davon abhängt, ob es methodisch möglich ist, gentechnische Untersuchungen auf bestimmte Fragestellungen, die sich aus dem jeweiligen Untersuchungszweck ergeben, zu beschränken und nicht erforderliche Überschußinformationen zu vermeiden. Dabei spielt auch die Feststellung des Bundesverfassungsgerichts im Volkszählungsurteil eine Rolle, wonach ein überwiegendes Allgemeininteresse an Eingriffen in das Recht auf informationelle Selbstbestimmung regelmäßig nur an Daten mit Sozialbezug „unter Ausschluß unzumutbarer intimer Angaben" bestehen wird.

Angesichts der faktischen Unsicherheiten, die ebenso wie gewisse ethische Vorfragen noch vor einer datenschutzrechtlichen Bewertung geklärt werden müssen, ist ein Zwischenbericht über die Erörterungen in der Arbeitsgruppe der Konferenz der Datenschutzbeauftragten derzeit noch nicht möglich. Ich werde daher den mit der Behandlung des Berichts der Enquete-Kommission befaßten Bundestagsausschüssen, soweit sie meine Beratung wünschen, auch nur vorläufige Überlegungen und Tendenzen mitteilen können.

Der Rechtsausschuß des Deutschen Bundestages hat zum Teilbereich „Genomanalyse im Strafverfahren" am 12. 10. 1988 eine öffentliche Anhörung durchgeführt, in der ich mich als Sachverständiger geäußert habe. Um anhand eines konkreten Anwendungsfeldes gentechnischer Untersuchungen die Schwierigkeit der Problematik aufzuzeigen, ist meine Stellungnahme vor dem Rechtsausschuß auszugsweise in der Anlage 7 abgedruckt.

10. Sozialwesen — Allgemeines

10.1 Gesetz über die Verwendung der Versicherungsnummer

Im Berichtszeitraum wurde das Erste Gesetz zur Änderung des Sozialgesetzbuches verabschiedet. Darin sind Regelungen über die Verwendung der bisherigen Rentenversicherungsnummer (§§ 18f, 18g, 95 SGB IV) vorgesehen, auf die ich bereits in früheren Tätigkeitsberichten (8. TB S. 29, 9. TB S. 47) eingegangen bin. Zu dem Gesetzentwurf habe ich schon im Vorfeld und während des Gesetzgebungsverfahrens gegenüber dem Bundesminister für Arbeit und Sozialordnung und in einer Anhörung des Ausschusses für Arbeit und Sozialordnung des Deutschen Bundestages Stellung genommen. Aus datenschutzrechtlicher Sicht war die gesetzliche Regelung überfällig, weil die Versicherungsnummer innerhalb und außerhalb des Sozialbereiches weitgehend beliebig verwendet werden konnte.

Die Versicherungsnummer ist nach ihrer Zusammensetzung ein eindeutiges, unverwechselbares und grundsätzlich nur einmal vorhandenes Zuordnungsmerkmal. Sie unterliegt als personenbezogenes Datum dem Sozialgeheimnis nach § 35 SGB I; ihre Weitergabe durch Sozialleistungsträger an Stellen außerhalb dieses Bereichs ist nur unter den Voraussetzungen der §§ 67 bis 77 SGB X zulässig. Gleichwohl reichten diese Regelungen nicht aus, um einer Gefahr der Ausweitung der Verwendung bis hin zu einem Identifikationsmerkmal im Sinne eines allgemeinen Personenkennzeichens wirksam zu verhindern. Da die Versicherungsnummer sowohl im Bereich der Privatwirtschaft wie auch in verschiedenen Bereichen der Verwaltung leicht bekannt und beliebig benutzt werden konnte, waren die Möglichkeiten einer Verknüpfung unterschiedlicher Dateien und damit die Zusammenführung personenbezogener Daten bis hin zur Bildung von Persönlichkeitsprofilen vorstellbar.

Durch das nunmehr verabschiedete Gesetz wird die Verwendung der Versicherungsnummer grundsätzlich auf den Bereich des Sozialwesens und insoweit eingeschränkt, als sie in diesem Zusammenhang zur gesetzlichen Aufgabenerfüllung erforderlich ist. Dabei werden die zulässigen Verwendungsmöglichkeiten näher konkretisiert. Dies geschah insbesondere durch die in § 18 f SGB IV vorgesehene, abgestufte Zulässigkeitsregelung nach folgenden Prinzipien:

1. Sozialversicherungsträger, ihre Verbände, ihre Arbeitsgemeinschaften, die Bundesanstalt für Arbeit, die Deutsche Bundespost, soweit sie mit der Berechnung oder Auszahlung von Sozialleistungen betraut ist, und die Künstlersozialkasse, dürfen die Versicherungsnummer nur erheben, speichern oder verwenden, soweit dies für die Erfüllung einer gesetzlichen Aufgabe nach diesem Gesetzbuch erforderlich ist. Diese Stellen dürfen die Versicherungsnummer für Zwecke der Prävention, der Rehabilitation und der Forschung, die dem Ziel die-

nen, gesundheitlichen Schäden bei Versicherten vorzubeugen oder diese zu beheben, grundsätzlich nur erheben, speichern oder verwenden, soweit ein einheitliche Ordnungsmerkmal zur personenbezogenen Zuordnung der Daten bei langfristigen Beobachtungen erforderlich ist und der Aufbau eines besonderen Ordnungsmerkmals mit erheblichem organisatorischen Aufwand verbunden wäre.

2. Andere in § 35 SGB I genannte Stellen wie die Träger der Sozialhilfe, die Versorgungsämter und Landesversorgungsämter, die Jugendämter und Landesjugendämter, Wohngeldstellen u. ä., die zwar auch Aufgaben nach dem Sozialgesetzbuch durchführen, aber keine Sozialversicherungsträger sind, dürfen die Versicherungsnummer nur erheben, speichern oder verwenden, soweit im Einzelfall oder in festgelegten Verfahren eine Offenbarung von Daten gegenüber den unter 1. genannten Stellen oder ihren Aufsichtsbehörden, für die Erfüllung einer Aufgabe nach diesem Gesetzbuch erforderlich ist.

3. Andere Behörden, Gerichte, Arbeitgeber oder Dritte wie auch Privatpersonen dürfen die Versicherungsnummer nur erheben, speichern oder verwenden, soweit dies für die Erfüllung einer gesetzlichen Aufgabe der bereits oben unter 1. erwähnten Stellen, wie der Sozialversicherungsträger und der Bundesanstalt für Arbeit, erforderlich ist, insbesondere bei Mitteilungen, im Rahmen der Beitragszahlung oder der Leistungserbringung einschließlich deren Abrechnung oder deren Erstattung. Die Verwendung der Versicherungsnummer ist hier in Teilbereichen, zum Beispiel dem Meldewesen in der Sozialversicherung, gesetzlich vorgeschrieben, in anderen Bereichen ist sie für die Korrespondenz im Rahmen der Aufgabenerfüllung erforderlich.

Die unter 2. und 3. aufgeführten befugten Verwender der Versicherungsnummer dürfen diese aber nicht zur Ordnung oder Erschließung von Dateien verwenden.

Ich gehe nach allem davon aus, daß die getroffene gesetzliche Regelung insbesondere durch die Bindung an den Erforderlichkeitsgrundsatz und die Aufgabenerfüllung nach dem Sozialgesetzbuch zu einer einschränkenden Verwendung der Versicherungsnummer in der künftigen Praxis führen wird. Dies gilt um so mehr, als im Rahmen des Gesetzgebungsverfahrens zum Gesundheitsreformgesetz auf meine Anregung hin die weitere Verwendung der Versicherungsnummer als Krankenversichertennummer ausgeschlossen und damit ihre mögliche Entwicklung zu einem allgemeinen Personenkennzeichen schon im Ansatz verhindert wurde.

10.2. Sozialversicherungsausweis

Gegen die gesetzliche Einführung des Sozialversicherungsausweises und die in diesem Zusammenhang vorgesehene Erweiterung der Meldepflichten für geringfügig Beschäftigte wurden von verschiedenen Seiten Bedenken erhoben. Die Bedenken richteten sich gegen die Eignung und Erforderlichkeit des Sozialversicherungsausweises für den angestrebten Zweck einer besseren Bekämpfung von Schwarzarbeit, aber auch gegen die vorgesehene Vergabe einer Versicherungsnummer an nicht versicherungspflichtige Beschäftigte und die Errichtung einer Zentraldatei über geringfügig Beschäftigte beim Verband der Rentenversicherungsträger in Würzburg (VDR).

Diese Bedenken habe ich geprüft, bin im Verlaufe meiner Beteiligung durch den Bundesminister für Arbeit und Sozialordnung indessen zu der Auffassung gelangt, daß angesichts der mit dem Entwurf verfolgten wesentlichen politischen Ziele die Erforderlichkeit der vorgesehenen Maßnahmen, aber auch deren grundsätzliche Eignung bejaht werden kann. Die Eignung des Sozialversicherungsausweises wird nach meinen Feststellungen auch durch das Fehlen eines Lichtbildes nicht wesentlich beeinträchtigt, so daß dieses im Hinblick auf den — bei Forderung eines Lichtbildes — erheblichen zusätzlichen Verwaltungs- und Kostenaufwand entbehrlich erscheint. Zur Identifizierung des Ausweisinhabers und für Abgleichs- und Verknüpfungszwecke reicht vielmehr die Versicherungsnummer aus. Ferner ist zu berücksichtigen, daß die beabsichtigte gesetzliche Regelung die Neuvergabe einer Versicherungsnummer an nicht versicherungspflichtige, geringfügig beschäftigte Arbeitnehmer nur in einer geringen Anzahl von Fällen zur Folge hat. Denn die Betroffenen besitzen häufig schon vorher, sei es aufgrund einer früheren versicherungspflichtigen Beschäftigung, sei es aufgrund einer Wehrdienstzeit, eines Erziehungsjahres oder einer Ausfallzeit (z. B. Schulbesuch), eine Versicherungsnummer.

Auch an einer Regionalisierung der Datei, die mir anfänglich als bessere Lösung erschien, halte ich nicht mehr fest; die Zentraldatei beim VDR bietet sowohl im Hinblick auf die Effizienz als auch die Transparenz und Kontrollierbarkeit ungleich bessere Bedingungen.

Von dieser Bewertung ausgehend habe ich jedoch noch Verbeserungen des Entwurfs unter datenschutzrechtlichen Gesichtspunkten vorgeschlagen und dem BMA im einzelnen folgende Änderungen und Ergänzungen des Gesetzentwurfs nahegelegt:

- Die Verwendung des Sozialversicherungsausweises sollte auf die gesetzlich vorgesehenen Zwecke beschränkt werden; eine Verwendung für andere Zwecke sollte ausdrücklich verboten und eine Verletzung dieses Verbots mit einem Bußgeld bedroht werden.

- Falls eine maschinenlesbare Gestaltung des Sozialversicherungsausweises beabsichtigt sein sollte, muß dies unmittelbar im Gesetz selbst geregelt werden.

- Bei der Datenstelle des VDR sollte für die Meldedaten über die geringfügigen Beschäftigungsverhältnisse (Beginn, Ende, Arbeitgeber, Entgelt usw.) außerhalb der Datei mit den Stammdaten eine besondere Datei geführt werden. Ferner sollten eine zweckentsprechende Löschungsfrist und die für diese Datei zugriffsberechtigten Stellen bestimmt werden.

— Ich habe ferner angeregt, Jugendliche im schulpflichtigen Alter (16 Jahre) von der Ausweispflicht ausnehmen und die Herausnahme von Beschäftigungen zu erwägen, die erfahrungsgemäß nicht von berufsmäßig tätigen Arbeitnehmern ausgeübt werden.

Ich gehe davon aus, daß ich Gelegenheit habe, meine Anregungen im Gesetzgebungsverfahren zur Geltung zu bringen.

10.3 Künstlersozialversicherungsgesetz

Das Künstlersozialversicherungsgesetz (KSVG) regelt insbesondere die Kranken- und Rentenversicherung der selbständig tätigen Künstler und Publizisten und die Abgabepflicht der Verwerter künstlerischer oder publizistischer Leistungen.

Im Rahmen der Novellierung des KSVG konnte ich in mehreren Gesprächen mit dem Bundesminister für Arbeit und Sozialordnung und durch Stellungnahmen gegenüber den zuständigen Bundestagsausschüssen folgende, aus datenschutzrechtlicher Sicht wesentliche Verbesserungen erreichen:

In § 11 Abs. 2 des KSVG werden die vom Betroffenen zu machenden Angaben in direkten Bezug zu den jetzt so konkret wie möglich umrissenen Aufgaben der Künstlersozialkasse gestellt. Eine solche, aus datenschutzrechtlicher Sicht gebotene Konkretisierung konnte auch für die Auskunftspflichten der Unternehmen, die künstlerische oder publizistische Werke verwerten, in § 29 des Gesetzes durchgesetzt werden.

Eine weitere datenschutzrechtliche Verbesserung wurde dadurch erreicht, daß in § 12 Abs. 1 KSVG die Verpflichtung der Künstler und Publizisten, ihr voraussichtliches Arbeitseinkommen zu melden, betragsmäßig auf die Höhe der Beitragsbemessungsgrenze in der Rentenversicherung begrenzt wurde. Darüber hinausgehende Einnahmen sind für die Versicherung ohne Bedeutung. Damit ist es erstmals gelungen, Einkommensangaben in der Sozialversicherung gesetzlich auf die für die Aufgabenerfüllung tatsächlich erforderliche Höhe zu begrenzen.

10.4. Schwangerenberatungsgesetz

Im Berichtsjahr habe ich mich auch mit dem vom BMJFFG vorgelegten Vorentwurf eines Gesetzes über die Beratung von Schwangeren (Schwangerenberatungsgesetz) befaßt. Das darin vorgesehene Beratungsangebot für Schwangere, dessen Annahme grundsätzlich freiwillig und nur in Einzelfällen zwingend vorgeschrieben ist, bringt es mit sich, daß die mit der Beratung betrauten Stellen Kenntnis von persönlichen und sachlichen Verhältnissen der Schwangeren erhalten, die weit in den sensiblen Kernbereich der Persönlichkeit reichen.

Aus datenschutzrechtlicher Sicht habe ich u. a. die folgenden, besonders bedeutsamen Forderungen gegenüber dem Bundesminister für Jugend, Familie, Frauen und Gesundheit geltend gemacht:

— Eine Aufzeichnung personenbezogener Daten zur Durchführung des Gesetzes darf nur mit schriftlicher Einwilligung der Betroffenen nach Aufklärung über den Verwendungszweck und ggf. den Datenempfänger erfolgen. Im Gesetz sollten auch möglichst kurze Aufbewahrungs- und Löschungsfristen für die bei der Beratung anfallenden Aufzeichnungen bestimmt werden. Dies sollte auch dann gelten, wenn es sich um Aufzeichnungen außerhalb von Dateien handelt.

— In das Gesetz selbst sollte der Anspruch der beratenen Frauen auf Auskunft über und Einsicht in die über sie geführten Akten oder Dateien aufgenommen werden.

— Im Hinblick auf den von den Beratungsstellen zu führenden Beratungsnachweis gehe ich davon aus, daß der vorgesehene Personenbezug nur dann aufrecht erhalten bleibt, wenn er aus zwingenden haushaltsrechtlichen Gründen unumgänglich ist.

Im übrigen habe ich mich auch mit datenschutzrechtlichen Aspekten der Meldung von Schwangerschaftsabbrüchen an das Statistische Bundesamt auseinandergesetzt und dazu Stellung bezogen (s. 8.2.9).

10.5 Adoptionsverhältnisse und Sozialwesen

Durch eine Eingabe wurde ich darauf aufmerksam, daß ein von der Bundesversicherungsanstalt für Angestellte ausgegebenes Antragsformular auf Feststellung von Zeiten der Kindererziehung nach dem Hinterbliebenenrenten- und Erziehungszeiten-Gesetz die Frage enthielt, ob eines der anspruchsberechtigenden Kinder ein Adoptivkind ist, und wenn ja, wer außer dem Antragsteller das Kind gegebenenfalls in den ersten zwölf Kalendermonaten nach der Geburt aufgezogen hat. Wie mir die BfA mitteilte, war hierfür die Überlegung maßgebend, daß regelmäßig die leiblichen Eltern das Kind unmittelbar nach der Geburt erziehen, während Adoptiveltern meist erst mit dem Zeitpunkt der Adoption zum Erzieher des Kindes werden. Aus diesem Grunde hatten die Sozialversicherungsträger es zunächst für notwendig gehalten, bei Adoptionsverhältnissen zu ermitteln, ab wann den Adoptiveltern Erziehungszeiten zustehen (§ 56 Abs. 3 Nr. 3 Sozialgesetzbuch I — SGB I —), möglicherweise auch aus einem vorangegangenen Pflegeverhältnis. Die Frage diente dem Zweck, einer Adoptivmutter oder einem Adoptivvater die gesetzlich zustehenden Kindererziehungszeiten — aber auch nur diese — zuzuerkennen. Zusätzlich hätte die Beantwortung der Frage Doppelanrechnungen vermeiden helfen können. Da hierdurch jedoch gegen das in § 1758 BGB normierte Ausforschungsverbot einer Adoption verstoßen worden wäre, hat der Bundesminister für Arbeit und Sozialordnung die Träger der gesetzlichen Rentenversicherung angewiesen, die Antragsformulare auf Feststellung von Zeiten der Kindererziehung umzugestalten. Dies ist inzwischen geschehen. In den zuständigen Gremien des Verbandes der Rentenversicherungsträger (VDR) kam die Bundesversicherungsanstalt für Angestellte (BfA) mit den anderen Trägern überein, daß im Antragsvordruck nicht mehr

nach Adoptionskindschaftsverhältnissen gefragt wird.

Neben der Neugestaltung des Vordrucks hat die BfA mit den anderen Rentenversicherungsträgern noch weitere Maßnahmen vereinbart, um dem Ausforschungsverbot des § 1758 BGB Rechnung zu tragen.

- Soweit in maschinell geführten Versicherungskonten früher die Tatsache einer Adoption gespeichert war, wird dieser Hinweis gelöscht.
- Gegenseitige Informationspflichten der Versicherungsträger sind in Adoptionsfällen aufgehoben. Hierdurch entfällt die Gefahr, daß den leiblichen Eltern Einzelheiten des Adoptionsverhältnisses bekannt werden können.
- Begehrt eine leibliche Mutter die Anrechnung von vor der Adoption liegenden Kindererziehungszeiten und verfügt nicht mehr über einen Geburtsnachweis, so fordern die Rentenversicherungsträger nur noch formlose Bescheinigungen an, die keine Rückschlüsse auf Einzelheiten des Adoptionsverhältnisses zulassen.

Wie mir mitgeteilt wurde, ist außerdem vorgesehen, in das Antragsformular einen Hinweis aufzunehmen, daß die Beantwortung der Frage „Familienname des Kindes zur Zeit der Geburt" bei Adoptivkindern entbehrlich ist.

In Fällen, in denen dem Versicherungsträger die Tatsache der Adoption bekannt geworden ist und eine doppelte Anrechnung von Erziehungszeiten vermieden werden kann, soll in Zukunft nur noch eine Bescheinigung des zuständigen Jugendamtes über den Adoptionszeitpunkt angefordert werden, in der kein Hinweis auf die leiblichen Eltern des Kindes enthalten ist.

Eine ähnliche Problematik ergibt sich auch bei der Durchführung des Bundeskindergeldgesetzes (BKGG) durch die Bundesanstalt für Arbeit. Die Meldebehörden übermitteln der Bundesanstalt für Arbeit im Rahmen eines Datenabgleichs (§ 3 der 2. BMeldDÜV vom 26. Juni 1984, BGBl. I S. 810) in automatisierter Form jährlich Daten aller Einwohner, für die auch Daten minderjähriger Kinder gespeichert sind. Diese Daten werden mit der Kindergelddatei verglichen; alle Kinder, deren Existenz so nachgewiesen ist, werden in der Datei entsprechend gekennzeichnet. Ergibt der Datenabgleich keinen „Treffer", muß geprüft werden, ob das Kindergeld zu Recht gezahlt wird.

Die Bundesanstalt für Arbeit hat in diesem Zusammenhang mitgeteilt, daß bei der Datenerhebung zur Durchführung des Bundeskindergeldgesetzes zwischen leiblichen und Adoptiveltern grundsätzlich kein Unterschied gemacht wird. Insbesondere wird die Frage nach einer Adoption aus den eventuell neben dem Datenabgleich zur Durchführung des Bundeskindergeldgesetzes erforderlichen Formularen nicht mehr gestellt.

Ich begrüße die Entscheidungen der Sozialleistungsträger, dem Adoptionsgeheimnis stärker Rechnung zu tragen.

11. Arbeitsverwaltung

11.1 Kontrolle eines Arbeitsamtes

Im Berichtsjahr habe ich eine Kontrolle bei einem Arbeitsamt durchgeführt, deren Schwerpunkt eine Prüfung des Einsatzes des computerunterstützten Ausbildungsvermittlungssystems COMPAS bildete. Das kontrollierte Arbeitsamt ist Modellarbeitsamt für dieses System. Die vom Arbeitsamt in einer Amtsverfügung festgelegten Regelungen zu „Datenschutz und Datensicherheit" konkretisieren ausführlich und präzise die Anforderungen des Sozialdatenschutzes auch in der Alltagsarbeit eines Arbeitsamtes.

Demgegenüber war bei den tatsächlichen Arbeitsabläufen folgendes zu bemängeln:

Sowohl bei den Einrichtungen der computerunterstützten Leistungsgewährung, coLei, wie auch bei denen der computerunterstützten Arbeitsvermittlung, coArb, verfügen die Tastaturen der Bildschirme mit angeschlossenem Drucker über die Funktionstaste „Hardcopy". Wird diese Taste gedrückt, so wird der augenblickliche Inhalt des Bildschirmes auf dem angeschlossenen Drucker auf jedem beliebigen Papier ausgedruckt. Meine grundsätzliche Auffassung zu diesem Problem habe ich unten unter Nr. 24.3 dargestellt und der Arbeitsverwaltung die dort dargestellte Verfahrensweise empfohlen. Die Bundesanstalt für Arbeit will dagegen weiterhin an allen Terminals die Hardcopyfunktion beibehalten. Nach ihrer Ansicht, die ich nicht teile, würde die von mir vorgeschlagene programmgesteuerte Druckausgabe und Protokollierung über den Zentralrechner einen nicht vertretbaren technischen Aufwand verursachen, zumal Hardcopies keine zusätzlichen Möglichkeiten des Datenmißbrauchs schafften. Ich werde mich weiter für eine datenschutzgerechte Lösung dieses Problems einsetzen.

Ich hätte es begrüßt, wenn eine bessere Sicherung des Rechenzentrums des Arbeitsamtes nach außen vorhanden wäre. Das Arbeitsamt liegt innerhalb einer engen Bebauung in der Innenstadt und der Gebäudeteil mit dem Rechenzentrum kann von den gegenüberliegenden Gebäuden eingesehen werden. Ich hatte daher zur Verbesserung der Raumsicherheit und als Schutz gegen denkbare Ausspähungen empfohlen, die Fenster mit durchwurf- und durchsichthemmendem Glas auszustatten. Die Arbeitsverwaltung hat mir mitgeteilt, daß für Rechenzentren in Obergeschossen bisher keine Sicherheitsverglasung vorgesehen sei. Zusätzliche Überlegungen zur äußeren Sicherung von Rechenzentren würden allerdings angestellt. Ich gehe davon aus, daß auch hier noch eine Lösung gefunden werden kann.

In einer Eingabe bin ich darauf hingewiesen worden, daß die Raumaufteilung in dem im Jahre 1986 bezogenen Neubau dritten Personen das Mithören vertraulicher Gespräche mit Arbeitsuchenden ermögliche. Der Bereich, um den es dabei geht, besteht aus drei kleinen Räumen, die jeweils eine Tür zu einer Wartezone haben und auf der gegenüberliegenden Seite offen auf einen gemeinsamen Gang münden (sog. Boxen). Hier werden Beratungsgespräche ge-

führt und Anträge für das Leistungsverfahren (coLei) aufgenommen.

Meine Mitarbeiter konnten sich davon überzeugen, daß in den Boxen die in den anderen Boxen geführten Gespräche tatsächlich mitgehört werden können. Weil in diesen Gesprächen zum Teil sehr sensible Daten von Arbeitsuchenden erfragt werden, habe ich empfohlen, diesen Raum in der Leistungsabteilung baulich zu verändern. Die Bundesanstalt für Arbeit ist meiner Empfehlung leider nicht gefolgt und hat erklärt, daß wegen des üblicherweise starken Andrangs in der Antragsannahmestelle stets mindestens 3 Bedienstete Gespräche mit Arbeitsuchenden führten. Dadurch sei der allgemeine Geräuschpegel so hoch, daß ein Mithören der Gespräche grundsätzlich nicht möglich sei. Gesprächsteile oder einzelne Worte seien nur bei deutlicher und lauter Aussprache aus der Nachbarbox vernehmbar.

Diese Darstellung entspricht nicht den Feststellungen meiner Mitarbeiter. Danach besteht vielmehr die konkrete Gefahr, daß wegen unzureichender baulicher Vorsorge das Sozialgeheimnis des § 35 SGB I verletzt wird. Ich werde diesem Problembereich weiter besondere Aufmerksamkeit widmen.

Im Aufgabenbereich „Anmeldung" in dem sich Arbeitsuchende arbeitslos melden, steht der Bediensteten, die das sogenannte Eingangsgespräch allein mit den Arbeitsuchenden führt, auch ein Terminal mit coLei-Zugriff zur Verfügung. Nach Vergabe der Stammnummer an den Arbeitsuchenden sind hier die gesamten Stammdaten und nach Bewilligung von Arbeitslosenhilfe/Arbeitslosengeld auch die sich darauf beziehenden Daten abrufbar. Ich habe empfohlen, daß hier nur der Stammdatensatz und gegebenenfalls das Datum der Zahlungsanweisung am Terminal angezeigt werden, da die übrigen Daten für die Tätigkeit der Anmeldekraft nicht erforderlich sind.

Die Bundesanstalt für Arbeit hat mir hierzu mitgeteilt, daß sie derzeit Überlegungen anstellt, Regelungen über den Zugriff auf Daten der jeweiligen Anwendungen zu treffen. Dabei werde auch entschieden, auf welche Daten die Anmelde- und Vermittlungsfachkräfte jeweils Zugriff erhalten und welche Zugriffe ihnen verwehrt werden sollen. Eine abschließende Entscheidung sei insoweit noch nicht getroffen.

11.2 Einkommensnachweise Unterhaltsverpflichteter im Leistungsverfahren

Für die Gewährung von Arbeitslosenhilfe durch die Bundesanstalt für Arbeit kann das Einkommen von Personen, die dem Antragsteller zum Unterhalt verpflichtet sind, von wesentlicher Bedeutung sein.

In meinem Zehnten Tätigkeitsbericht (S. 64) hatte ich mich mit der Frage befaßt, inwieweit die Bundesanstalt vorgelegte Ausfertigungen von Verträgen, aus denen dem Antragsteller oder Angehörigen Einkommen erwächst, in den Akten behalten darf. Mir wurde mitgeteilt, daß mit dem Bundesrechnungshof erörtert werden soll, welche Unterlagen bei den Akten der Arbeitsverwaltung zu verbleiben haben und welche nach Abschluß der Prüfung an die Antragsteller oder dessen Unterhaltsverpflichteten zurückgereicht werden können. Eine abschließende Antwort steht noch aus.

Zusätzlich zu dieser Frage hatte ich mich im Berichtszeitraum damit auseinanderzusetzen, ob und welche Unterlagen ein leistungsfähiger Unterhaltsverpflichteter, der seine Leistungsfähigkeit anerkennt, vorzulegen hat, insbesondere ob er sein genaues Einkommen in jedem Fall angeben muß. Der Umfang der durch die Arbeitsverwaltung zu erhebenden Daten muß so gering wie möglich bleiben. Die Bundesanstalt für Arbeit räumt ein, daß die Praxis der einzelnen Arbeitsämter, ja teilweise sogar einzelner Sachbearbeiter eines Amtes, unterschiedlich sei. Eine generelle Regelung dieser Problematik gebe es nicht. Vielmehr bleibe es jedem Sachbearbeiter überlassen, festzustellen, welche Unterlagen er für seine Entscheidung für nötig hält.

Ich bin der Auffassung, daß dann, wenn die Höhe des Einkommens nach allen Berechnungsmodalitäten eine Leistungsverpflichtung der Bundesanstalt für Arbeit ausschließt, ein genauer Einkommensnachweis nicht erforderlich ist. Ich habe daher angeregt, eine Erklärung, daß das Einkommen eine bestimmte Höhe übersteigt, als ausreichend anzuerkennen. In Zweifelsfällen könne die Erklärung durch das Finanzamt oder den Steuerberater bestätigt werden.

Die Arbeitsverwaltung hält dies nicht für ausreichend. Ich habe die Bundesanstalt für Arbeit aufgefordert, ihre derzeitige Praxis nochmals zu überprüfen.

11.3 Studie zur Arbeitslosigkeit

Der Bundesminister für Arbeit und Sozialordnung (BMA) hat mich um Beratung bei der Vorbereitung eines Forschungsvorhabens mit dem Thema „Arbeitssuchende, berufliche Mobilität und soziale Lage Arbeitsloser" gebeten. Mit dieser Studie sollen die individuellen, wirtschaftlichen und gesellschaftlichen Probleme Arbeitsloser untersucht sowie Erkenntnisse für den Vergleich mit einer ähnlichen Studie aus dem Jahre 1978 gefunden werden. Die hierzu notwendige Offenbarung von Sozialdaten der Bundesanstalt für Arbeit gegenüber dem mit dem Forschungsvorhaben beauftragten Sozialforschungsinstitut bedarf gemäß § 75 Sozialgesetzbuch X (SGB X) einer vorherigen Zustimmung des BMA.

Nach § 75 Abs. 1 Satz 2 SGB X ist eine Offenbarung dann nicht zulässig, wenn es zumutbar ist, die Einwilligung der Betroffenen nach § 67 SGB X einzuholen oder den Zweck der Forschung auf andere Weise zu erreichen. Zur Beurteilung der Zumutbarkeit ist vornehmlich auf die Interessen der in § 35 SGB I genannten Stellen sowie des Forschungsträgers abzustellen. Unter diesem Aspekt habe ich dem BMA empfohlen, dafür zu sorgen, daß die Betroffenen nicht durch vor ihrer Tür stehende Interviewer vor die vollendete Tatsache der Weitergabe ihrer Sozialdaten gestellt werden.

Der BMA hat daraufhin die Genehmigung nach § 75 SGB X nur unter strengen Auflagen erteilt. Die Bundesanstalt für Arbeit muß den Betroffenen zunächst

die Absicht der Offenbarung schriftlich mitteilen und sie zugleich auf die Möglichkeit hinweisen, der Offenbarung zu widersprechen. Sie darf dem Forschungsinstitut nur die Adressen solcher Arbeitsloser offenbaren, die nicht binnen 14 Tagen den Widerspruch schriftlich erklärt haben. Die Bundesanstalt für Arbeit wurde ferner verpflichtet, durch organisatorische Vorkehrungen sicherzustellen, daß die Arbeitsvermittler keine Kenntnis davon erhalten können, ob ein Arbeitsloser der Übermittlung seiner Daten widersprochen hat. Dazu gehört insbesondere, daß der Widerspruch nicht an das regional zuständige Arbeitsamt, sondern entweder an die Hauptstelle oder an das zuständige Landesarbeitsamt zu richten ist.

Die Mitarbeiter des Forschungsinstituts, denen von der Bundesanstalt für Arbeit mitgeteilte personenbezogene Daten zur Kenntnis kommen können, insbesondere die vorgesehenen Interviewer, sind von der Bundesanstalt für Arbeit nach Maßgabe des Verpflichtungsgesetzes (Artikel 42 des Einführungsgesetzes zum Strafgesetzbuch vom 2. März 1974, BGBl. 1974, S. 469) über die ihnen obliegenden Pflichten, insbesondere zur Wahrung des Sozialgeheimnisses, zu belehren und auf deren gewissenhafte Erfüllung zu verpflichten. Den Interviewern darf außer Name, Vorname, Anschrift und Telefonnummer kein weiteres Datum eines Interviewten offengelegt werden, insbesondere nicht der Umstand, ob er noch arbeitslos ist.

Dem Forschungsinstitut sowie der Bundesanstalt für Arbeit wurden besondere Pflichten zur Löschung und bei der Übermittlung der Daten auferlegt.

Des weiteren wurde festgelegt, daß die Untersuchungsergebnisse nur in einer Form veröffentlicht werden dürfen, die Rückschlüsse auf personenbezogene Daten befragter Arbeitsloser unmöglich macht.

Schließlich müssen die zu Befragenden in einem Begleitschreiben der Bundesanstalt für Arbeit über die Herkunft ihrer Daten, über die Erteilung der datenschutzrechtlichen Genehmigung und über die getroffenen Datenschutzmaßnahmen informiert werden.

Angesichts dieser umfassenden Auflagen habe ich gegen die Durchführung der Erhebung keine Bedenken. Bei Einhaltung der Auflagen durch die Bundesanstalt für Arbeit und durch das Forschungsinstitut wird dem Datenschutz hinreichend Rechnung getragen.

11.4 Regelungen zum Postversand

Mehrere Petenten haben mir die Frage gestellt, inwieweit datenschutzrechliche Anforderungen durch Versendeformen der Bundesanstalt für Arbeit verletzt werden.

Der von der Bundesanstalt an der Verschlußstelle für Briefdrucksachen benutzte Hinweis „hier offen" führt offenbar zu Mißverständnissen. Derartige Briefdrucksachen befanden sich in Umschlägen mit Klebepunkten oder Adhaesionsverschlüssen, waren also gar nicht offen. Der Hinweis auf dem Umschlag bedeutete nur, daß dieser für Prüfzwecke von der Post an dieser Stelle des Umschlags geöffnet werden sollte. Gleichwohl entstand bei den Empfängern der Eindruck, es liege eine offene Versendung vor. Es bereitete mir immer wieder Schwierigkeiten zu erläutern, weshalb die Kennzeichnung der Briefumschläge „hier offen" nicht besagt, daß der Brief tatsächlich offen ist. Die Bundesanstalt für Arbeit hat daher auf mein Drängen hin im Einverständnis mit dem Bundesminister für das Post- und Fernmeldewesen die Weisung erteilt, daß Briefumschläge an der fraglichen Stellen nunmehr mit dem Aufdruck „Nur für Postzwecke — Hier offen" zu versehen seien.

Des weiteren hatte ich mich mit der Frage der Verwendung von Postkartenvordrucken für Veränderungsmitteilungen an die Bundesanstalt für Arbeit zu befassen. In diesen Fällen bleibt es einem Leistungsempfänger zwar unbenommen, Veränderungsmitteilungen auf eine andere Weise als durch die Übersendung der von der Bundesanstalt für Arbeit ausgegebenen Vordrucke vorzunehmen oder die Postkarte in einen frankierten Umschlag zu stecken; die Leistungsempfänger werden aber häufig davon ausgehen, daß sie den übersandten Postkartenvordruck benutzen müssen. Ich habe die Bundesanstalt für Arbeit daher gebeten, den Leistungsempfängern diese Möglichkeit ausreichend deutlich zu machen. Die Bundesanstalt für Arbeit hat daraufhin in dem von ihr herausgegebenen „Merkblatt für Arbeitslose" die Ausführungen zur Mitwirkungspflicht der Arbeitssuchenden in diesem Sinne ergänzt. So heißt es nun auf Seite 17 des Merkblattes „Bitte benutzen Sie für eine schriftliche Mitteilung möglichst den Postkartenvordruck ‚Veränderungsmitteilung', den Sie von Ihrem Arbeitsamt erhalten haben. Das erleichtert die Bearbeitung. Sie können das Arbeitsamt selbstverständlich auch in anderer geeigneter Weise informieren." Dadurch ist eine ausreichende Information der Arbeitssuchenden gewährleistet.

Die Bundesanstalt für Arbeit hat darüber hinaus auf meine Initiative hin die Verwendung von Postkarten eingehend geregelt. Postkarten werden durch die Bundesanstalt für Arbeit nur noch dann eingesetzt, wenn keine sensiblen persönlichen Daten zu übermitteln sind. Unter Aspekten des Sozialdatenschutzes sensible Sachverhalte wie beispielsweise „Arbeitslosenhilfe für Ihren Sohn" dürfen daher in Zukunft nicht mehr auf Postkarten behandelt werden.

11.5 Gebührenfreiheit im Auskunftsverfahren

Nach der Datenschutzgebührenordnung vom 22. Dezember 1977, (BGBl. I Seite 3153) können Behörden und sonstige öffentliche Stellen für erteilte Auskünfte nach § 13 Abs. 4 BDSG Gebühren erheben. § 3 der Datenschutzgebührenordnung läßt Ausnahmen von der Gebührenpflicht zu. In Fällen einfacher Art sowie in Härtefällen kann von der Erhebung der Gebühr ganz oder teilweise abgesehen werden. Schon mit Rundschreiben an die obersten Bundesbehörden vom 30. März 1979 hat der Bundesminister des Innern angeregt, diese Ausnahmeregelung großzügig zu handhaben. Seitdem werden von Bundesbehörden keine Gebühren für Auskünfte mehr erhoben. Die Bundes-

anstalt für Arbeit hatte sich dieser Praxis zunächst jedoch nicht angeschlossen.

Da die Erhebung von Gebühren gerade für die Auskunft über Sozialdaten als unbefriedigend angesehen werden muß, hat die Bundesanstalt für Arbeit auf mein Drängen hin am 9. Juni 1988 die Weisung erteilt, Auskünfte aus in den Dienststellen dezentral geführten automatisch betriebenen Dateien in der Regel als Auskünfte einfacher Art zu behandeln. Solche Auskünfte sind deshalb künftig grundsätzlich gebührenfrei. Die Auskunft erfolgt dann in möglichst einfacher Form mündlich (Bildschirmeinsicht) oder formlos schriftlich (Übergabe eines Ausdrucks). Die Angaben sind — falls erforderlich — dem Auskunftssuchenden in ausreichender Weise zu entschlüsseln.

12. Krankenversicherung

12.1 Gesundheits-Reformgesetz

Das auch unter datenschutzrechtlichen Gesichtspunkten bedeutendste Gesetzgebungsvorhaben im Bereich des Sozialwesens war im Berichtszeitraum die Strukturreform des Gesundheitswesens durch das Gesundheits-Reformgesetz (GRG). Dieses regelt auch die Erhebung und Verarbeitung der schutzwürdigen Gesundheitsdaten von Millionen von Bundesbürgern und greift daher in deren verfassungsrechtlich garantiertes Recht auf informationelle Selbstbestimmung ein.

Im Vorfeld und während des Gesetzgebungsverfahrens hat der Bundesminister für Arbeit und Sozialordnung mich intensiv beteiligt, ebenso haben mich die Bundestagsausschüsse zu den Beratungen hinzugezogen. U. a. hatte ich als Sachverständiger in einer öffentlichen Anhörung Gelegenheit, meine Auffassung darzulegen.

Mit meinen Bemühungen habe ich vor allem zwei Ziele verfolgt, nämlich

- einmal den Umfang der Datenverarbeitung auf das unbedingt notwendige Maß zu beschränken und den Verwendungszweck der Daten für die Krankenkassen und die Kassenärztlichen/Kassenzahnärztlichen Vereinigungen so weit als möglich zu konkretisieren und
- zum anderen die Entstehung eines Leistungskontos für den Versicherten zu vermeiden, das unter dem Stichwort „Gläserner Patient" in die öffentliche Diskussion geraten war.

Auf der Basis dieser Zielvorstellungen konnte ich unter datenschutzrechtlichen Aspekten wesentliche Verbesserungen insbesondere in folgenden Punkten erreichen:

- Die vorgesehene Verarbeitung *versichertenbeziehbarer Daten* wurde eingeschränkt. Eine versichertenbeziehbare Abrechnung mit den Krankenkassen findet grundsätzlich nur bei den ärztlich verordneten Leistungen (Arzneien, Heil- und Hilfsmittel u. ä.) statt.
- Die *ärztlichen Leistungen* werden zwar von den Ärzten versichertenbezogen bei den Kassenärztlichen Vereinigungen abgerechnet, diese dürfen die ärztlichen Leistungen jedoch zum Zwecke der Abrechnung nicht versichertenbezogen erfassen und können sie daher auch nicht versichertenbezogen, sondern nur fallbezogen, an die Krankenkassen weiterleiten. Das Abrechnungsverfahren wurde ebenfalls in die gesetzliche Regelung einbezogen.
- Von den vorgesehenen *Wirtschaftlichkeitsprüfungen* dürfen die Prüfungen nach Durchschnittswerten und die nach Richtgrößen grundsätzlich nur arztbezogen durchgeführt werden. Versichertenbeziehbare Leistungs- und Gesundheitsdaten dürfen für Zwecke von Wirtschaftlichkeitsprüfungen nur erfaßt und auf maschinell verwertbaren Datenträgern verknüpft werden, soweit dies für die *Stichprobenprüfungen* erforderlich ist, die vierteljährlich zwei vom Hundert der Ärzte umfassen. Die Einbeziehung dieser Daten haben die Prüfgremien auf das für die Erreichung des Zieles der jeweiligen Prüfung erforderliche Maß zu beschränken. Der Versichertenbezug wird bei der Stichprobenprüfung lediglich durch die Krankenversichertennummer herstellbar. Eine Übermittlung der Diagnose auf elektronischen Datenträgern unterbleibt.
- Die Aufzeichnungen in Dateien sind zu *löschen*, sobald ihre Kenntnis für die Aufgabenwahrnehmung nicht mehr erforderlich ist, in der Regel spätestens nach zwei Jahren. Für Angaben über Leistungen, die zur Prüfung späterer Leistungsvoraussetzungen erforderlich sind, besteht eine Löschungsfrist von maximal zehn Jahren.
- Die Datenverarbeitung beim neu einzurichtenden *Medizinischen Dienst* wird ebenfalls an die konkret umschriebenen Aufgaben gebunden. Es dürfen nur Aktenhinweisdateien und insbesondere keine Gesundheitsdateien geführt werden. Die Weitergabe von medizinischen Unterlagen, die der Versicherte „freiwillig" seiner Krankenkasse überlassen hat, ist an seine Einwilligung gebunden. Personenbezogene Daten sind nach fünf Jahren zu löschen.
- Aufzeichnungen zum *Zwecke der Beitragsrückzahlung* im Rahmen entsprechender Modellvorhaben sind auf die Art und den Wert der zu berücksichtigenden Leistungen zu beschränken und zu beenden, sobald der Wert eines Monatsbeitrages zur Krankenversicherung erreicht ist; sie sind schließlich zu löschen, wenn sie für Zwecke der Beitragsrückzahlung nicht mehr benötigt werden.
- Versicherten- und Leistungsdaten der *Beschäftigten einer Krankenkasse* und ihrer mitversicherten Angehörigen dürfen Personen, die *kasseninterne Personalentscheidungen* treffen oder daran mitwirken können, nicht zugänglich sein und ihnen auch nicht offenbart werden. Damit ist eine von mir seit Jahren erstrebte Regelung erreicht (vgl. auch 9. TB S. 52).

Auf eine vergleichbare Abschottung der Mitarbeiterdaten zielt auch die Regelung für *Betriebskrankenkassen* ab, wonach Dienstvorgesetzte oder Angehörige der Personalverwaltung des Betriebes als Mitglied eines Selbstverwaltungsorganes bei einer Beratung oder Abstimmung nicht anwesend sein dürfen, wenn hierbei personenbezogene Daten von Mitarbeitern offengelegt werden. Ihnen darf insbesondere auch bei der Vorbereitung einer Beratung keine Kenntnis von solchen Daten gegeben werden.

Die jetzige Lösung entspricht zwar nicht meiner seit Jahren erhobene Forderung nach einem Totalausschluß von Personalentscheidungsträgern aus den Selbstverwaltungsorganen bei Betriebskrankenkassen (vgl. 10. TB S. 69). Die zukünftige Praxis wird zeigen müssen, ob die Praktizierung der dem Befangenheitsrecht nachempfundenen Regelung datenschutzrechtlichen Ansprüchen genügt.

- Die mitversicherten *Familienangehörigen* eines Mitgliedes erhalten einen eigenen Versichertenstatus. Dadurch wird diesen ein eigenständiges Recht auf informationelle Selbstbestimmung auch gegenüber dem Mitglied und damit eine datenschutzrechtliche Position eingeräumt, die ich gleichfalls schon seit längerem gefordert habe (vgl. 8. TB S. 31f.). Sie ist wichtig bei der selbständigen Geltendmachung von Leistungsansprüchen.
- Für *Forschungsvorhaben* dürfen versichertenbeziehbare Datenbestände nicht mehr verwendet werden. Personenbeziehbare Daten sind stets zu anonymisieren.
- Die *Verwendung der Rentenversicherungsnummer* als Krankenversichertennummer wird ab 1. 1. 1992 untersagt. Damit wird für die Krankenkassen ein eigenständiges Identifikationsmerkmal geschaffen und etwaigen Tendenzen, diese Nummer in Richtung eines allgemeinen Personenkennzeichens fortzuentwickeln, der Boden entzogen.
- Die konkrete inhaltliche und technische Ausgestaltung der *Krankenversicherungskarte* wird im Gesetz selbst geregelt.
- Gleiches gilt für den *Inhalt* der *Behandlungsscheine* (Krankenscheine, Vorsorge-Untersuchungsscheine). Diese sollen später durch die *Krankenversicherungskarte* ersetzt werden. Statt der bisherigen Angabe des Arbeitgebers oder des die Versicherungspflicht begründenden Verhältnisses (z. B. Arbeitslosengeldbezug) ist nunmehr die Krankenversichertennummer anzugeben. Damit ist ein weiteres datenschutzrechtliches Problem gelöst, auf das ich mehrfach in früheren Tätigkeitsberichten hingewiesen habe (vgl. 7. TB S. 51). Die Krankenversicherungskarte darf nur für den Nachweis der Berechtigung zur Inanspruchnahme von Leistungen im Rahmen der kassen- oder vertragsärztlichen Versorgung sowie für die Abrechnung mit den Leistungserbringern verwendet werden.
- Der unter Transparenzgesichtspunkten neu eröffnete *Anspruch auf Auskunft* über die Leistungsaufwendungen gegenüber den Krankenkassen schließt den allgemeinen Anspruch auf Auskunft über die Art der Erkrankung nicht aus. Ein gleicher Auskunftsanspruch wird auch gegenüber den Kassenärztlichen und Kassenzahnärztlichen Vereinigungen eingeräumt. Der Medizinische Dienst ist aufgrund des § 79 i. V. m. § 83 des Zehnten Buches des Sozialgesetzbuches zur Auskunft verpflichtet.
- In bezug auf die *Zentraldatei der Unfallversicherungsträger* wird klargestellt, daß die Schutzvorschriften des Sozialgesetzbuches, insbesondere dessen § 76 SGB X, auch für die Übermittlung von Gesundheitsdaten an die Zentraldatei gelten und daß auch diese dem Schutz des Sozialgeheimnisses unterliegt.
- Die versichertenbezogenen Angaben, die die *Krankenhäuser* und sonstigen Leistungserbringer den Krankenkassen übermitteln dürfen, sind im Gesetz ausdrücklich aufgeführt.
- Der Betrieb von Rechenzentren durch die Landesverbände wird auch nach dem GRG als *Auftragsdatenverarbeitung* der Krankenkassen qualifiziert. Diese bleiben damit Herr der Daten und sind auch weiterhin für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich.
- Zu den datenschutzrechtlichen Aspekten im Zusammenhang mit der Krankenhausstatistik vgl. oben 8.2.8.

Die dargestellten Verbesserungen haben es mir ermöglicht, nach Abschluß der Beratungen die Feststellung zu treffen, daß das Gesundheits-Reformgesetz den datenschutzrechtlichen Forderungen Rechnung trägt.

12.2 Offenbarung des Familieneinkommens

Durch eine Eingabe wurde mir bekannt, daß eine Krankenkasse das von der Versicherten im Rahmen eines Antrages auf Befreiung von der Entrichtung der Verordnungsblattgebühr (§ 182 a Reichsversicherungsordnung) mitgeteilte Familieneinkommen an eine Rehabilitationseinrichtung offenbart hatte, in der ein Kind der Versicherten stationär untergebracht war. Bei der Rehabilitationsstätte ging es um eine ganz andere Frage, nämlich, ob die Versicherte anteilig an Transportkosten für ihr Kind zu beteiligen war. Dafür war die Kenntnis des Einkommens nicht erforderlich. Die Krankenkasse hätte allenfalls mitteilen dürfen, daß eine Eigenbeteiligung der Versicherten an diesen Kosten zumutbar sei, nicht aber die Höhe des Familieneinkommens.

Ich habe diese unzulässige Offenbarung gem. § 20 Abs. 1 Bundesdatenschutzgesetz (BDSG) als Verstoß gegen § 35 Sozialgesetzbuch I i. V. m. §§ 67 ff. SGB X beanstandet. Die Krankenkasse hat die Unzulässigkeit der Datenübermittlung eingeräumt und Maßnahmen getroffen, die die Wiederholung eines solchen Vorgangs vermeiden sollen.

13. Rentenversicherung

13.1 Bundesversicherungsanstalt für Angestellte

— Durch eine Eingabe wurde mir bekannt, daß der Rentenbescheid eines Rentenanwärters mit den Daten über Rentenhöhe, Krankenversicherungsbeitrag usw. seinem Arbeitgeber übersandt worden war. Das Schreiben war nicht an die Personalstelle des Arbeitgebers adressiert. Auch ein besonderer Hinweis auf die Vertraulichkeit des Inhaltes war auf dem Umschlag nicht angebracht.

Die Bundesversicherungsanstalt für Angestellte (BfA) hat den Vorgang bestätigt und eingeräumt, daß eine Notwendigkeit für die Übersendung des Rentenbescheides an den Arbeitgeber nicht bestanden habe. Ich habe diese unzulässige Offenbarung von Sozialdaten gemäß § 20 Abs. 1 BDSG als Verstoß gegen § 35 SGB I beanstandet.

— Eine Petentin beschwerte sich darüber, daß ein Versichertenältester der Bundesversicherungsanstalt für Angestellte (BfA) nach einem Informationsgespräch anläßlich einer zufälligen Begegnung, in dem er auf die Möglichkeiten seiner Auskunfts- und Beratungstätigkeit hingewiesen hatte, ohne ihr Wissen ihren vollständigen Versicherungsverlauf bei der BfA angefordert und zu ihrer Überraschung bei einem späteren Gespräch präsentiert hatte.

Die Vertreterversammlung der BfA wählt im Rahmen der der BfA als rechtsfähiger Körperschaft des öffentlichen Rechts zustehenden Selbstverwaltung (§ 29 Abs. 2 Sozialgesetzbuch IV — SGB IV —) auch die Versichertenältesten (§ 39 Abs. 1 SGB IV). Die Versichertenältesten, deren Aufgaben in § 39 Abs. 3 SGB IV näher beschrieben sind, haben die Aufgaben, eine ortsnahe Verbindung des Versicherungsträgers mit den Versicherten und Leistungsberechtigten herzustellen und diese zu beraten. Sie üben ihre Tätigkeit im Rahmen eines öffentlich-rechtlichen (Ehren-)Amtsverhältnisses aus und nehmen ihre Aufgaben aufgrund des Gesetzes eigenständig wahr. Demgemäß vertritt die BfA zu Recht die Auffassung, daß der Versichertenälteste kein Dritter im Verhältnis zwischen dem Versicherten und der BfA ist; er muß vielmehr wie ein Mitarbeiter der BfA im Außendienst mit gleicher sachlicher Funktion behandelt werden. Wegen dieser Vergleichbarkeit wurde seitens der BfA auch die datenschutzrechtliche Konsequenz gezogen, daß die Versichertenältesten auf das Datengeheimnis nach § 5 BDSG zu verpflichten sind. Sie werden also im Sinne dieser Vorschrift als „bei der Datenverarbeitung beschäftigte Person" angesehen.

Daraus ergibt sich, daß die Zulässigkeit der Offenbarung von Sozialdaten an den Versichertenältesten nicht nach § 67 Nr. 1 SGB X zu beurteilen ist. Die Übersendung des Versicherungsverlaufes an den Versichertenältesten ist somit grundsätzlich keine unzulässige Offenbarung. Die BfA hat allerdings in den Geschäftsanweisungen für ihre Versichertenältesten bestimmt, die Anforderung von EDV-Ausdrucken über die gespeicherten Versicherungsdaten setze voraus, daß ein Versicherter um eine persönliche Beratung gebeten hat und mit der Anforderung der Ausdrucke einverstanden ist.

Auf meine Empfehlung beabsichtigt die BfA, das Verfahren zur Anforderung von EDV-Ausdrucken durch die Versichertenältesten dahin gehend zu ändern, daß dem Versichertenältesten ein EDV-Ausdruck nur noch dann durch die Auskunfts- und Beratungsstelle übersandt wird, wenn der betroffene Versicherte schriftlich erklärt hat, daß er mit der Anforderung einverstanden ist. Fordert ein Versichertenältester einen EDV-Ausdruck ohne Vorlage dieser Erklärung an, wird der betreffende Versicherungsverlauf (bzw. die Rentenauskunft) dem Versicherten direkt zugesandt. Mit der Einführung des unter Aspekten des Sozialdatenschutzes einwandfreien Verfahrens ist im ersten Quartal 1989 zu rechnen.

13.2 Landwirtschaftliche Alterskasse Hessen-Nassau

Im Berichtsjahr habe ich eine datenschutzrechtliche Kontrolle der Landwirtschaftlichen Alterskasse Hessen-Nassau durchgeführt. Die Landwirtschaftliche Alterskasse bildet mit der Landwirtwirtschaftlichen Krankenversicherung und der Landwirtschaftschaftlichen Berufsgenossenschaft eine Verwaltungsgemeinschaft. Durch diese besondere Organisationsform von Sozialversicherungsträgern entstehen datenschutzrechtliche Probleme, mit deren Lösung ich bisher noch nicht konfrontiert gewesen bin.

Die Struktur der Verwaltungsgemeinschaft, die einer weitgehenden Realunion der Träger der Landwirtschaftlichen Sozialversicherung entspricht, ist durch § 45 Abs. 1 des Gesetzes über die Krankenversicherung der Landwirte (KVLG) angeordnet. Nach dieser Vorschrift sind die Träger der Landwirtschaftlichen Krankenversicherung, der Landwirtschaftlichen Altershilfe und der Landwirtschaftlichen Unfallversicherung zu enger verwaltungsmäßiger Zusammenarbeit verpflichtet, damit die in diesen Einrichtungen Versicherten von Zuständigkeitsstreitigkeiten verschont werden und ihre nahtlose Betreuung in Angelegenheiten dieser drei Versicherungszweige erreicht wird. Die Verwaltungseinrichtungen der drei genannten Träger sollen so miteinander zusammenwirken, daß den Versicherten das Gefühl vermittelt wird, es mit *einer* Verwaltung zu tun zu haben. Die sachliche Zuständigkeit der einzelnen Träger für ihren jeweiligen Aufgabenbereich wird dadurch aber nicht berührt.

Angesichts dieser Organisationsform stand zunächst die Frage im Vordergrund, wer speichernde Stelle für die gesamten im Bereich der drei Versicherungsträger eingesetzten DV-Verfahren ist. Diese war dahingehend zu beantworten, daß jeder Versicherungsträger als speichernde Stelle für die rechtmäßig von ihm eingegebenen Daten anzusehen ist. Ich habe festgestellt, daß sämtliche Daten zentral gespeichert und den Benutzern im Dialog zur Abfrage bereitgestellt waren.

Alle drei Versicherungsträger konnten also im Zeitpunkt der Kontrolle theoretisch sowohl auf die eigenen Datenbestände als auch auf die der beiden anderen Versicherungsträger zugreifen. Es war im Rahmen des Kontrollbesuchs nicht eindeutig und im einzelnen zu klären, inwieweit jeder Versicherungsträger Zugriffsbeschränkungen unterlag. Da mit der Eigenschaft als speichernde Stelle für die im Zugriff befindlichen Daten auch die Verantwortung für die erforderlichen Maßnahmen zur Organisation von Datenschutz und Datensicherung verbunden ist, sind konkrete und dokumentierte Planung sowie Organisation der Zugriffsmöglichkeiten unverzichtbar. Da diese nicht vorhanden waren, habe ich eine Beanstandung gemäß § 20 Abs. 1 in Verbindung mit § 6 BDSG ausgesprochen.

Außerdem waren folgende Mängel zu beanstanden:

- Die gemäß § 79 Abs. 1 Sozialgesetzbuch X (SGB X) in Verbindung mit §§ 28, 29 BDSG einem Beauftragten für den Datenschutz obliegenden Aufgaben wurden in der LAK nur unzureichend wahrgenommen.
- Es fehlte eine Dienst- und Arbeitsanweisung mit Regeln und Richtlinien zur Organisation des Datenschutzes, die der Aufbau- und Ablauforganisation der LAK Rechnung tragen.
- Eine vollständige Übersicht gemäß § 15 Abs. 1 Nr. 1 BDSG, in der die Datenbank mit den Mitgliederdaten der LAK, der Berufsgenossenschaft und der Krankenkasse sowie die weiteren automatisiert betriebenen Dateien mit personenbezogenen Daten aufgeführt sind, war nicht vorhanden.
- Eine Veröffentlichung gemäß § 12 Abs. 1 sowie der Registermeldung gemäß § 19 Abs. 4 Satz 1 BDSG hat nicht stattgefunden.

Die Landwirtschaftliche Alterskasse Hessen-Nassau hat meine Beanstandungen und Anregungen aufgegriffen und mir zugesichert, für eine schnelle Verbesserung des Sozialdatenschutzes in ihrem Bereich zu sorgen.

Ich habe darüber hinaus dem Bundesminister für Arbeit und Sozialordnung empfohlen, meine Prüfergebnisse bei der Landwirtschaftlichen Alterskasse, soweit sie sich auf den Zusammenschluß der Landwirtschaftlichen Sozialversicherung in einer Verwaltungsgemeinschaft beziehen, auch für andere, ähnlich organisierten Sozialversicherungsträger auszuwerten.

13.3 Zusatzversorgungskasse der Deutschen Bühnen und der Deutschen Kulturorchester

Der Bundesminister für Arbeit und Sozialordnung hat mich zu einem inzwischen zurückgestellten Entwurf eines Theater- und Orchesterzusatzversorgungsgesetzes (TOZG) um Stellungnahme gebeten. Zur Vorbereitung dieser Stellungnahme, habe ich bei den Versorgungsanstalten der Deutschen Bühnen und Kulturorchester bei der Bayerischen Versicherungskammer einen Informationsbesuch durchgeführt. Er gab Anlaß für folgende Empfehlungen aus datenschutzrechtlicher Sicht:

- Der Lesezugriff sollte den Sachbearbeitern der Versorgungsanstalten nicht mehr auf den gesamten gespeicherten Datenbestand möglich sein, sondern auf die für die jeweilige Fachzuständigkeit erforderlichen Daten beschränkt werden.
- Zur Verbesserung der Datensicherheit sollten technische Ergänzungen, wie beispielsweise Abbruch der Verbindung nach Fehlversuchen, regelmäßige Paßworterneuerung, Organisation der Protokollauswertung, vorgenommen sowie Regelungen über Empfangsberechtigte und Vernichtung von Listenausdrucken und Mikrofiches getroffen werden.
- Eine Aufstellung der vorgesehenen Auswertungen und Listenausdrucke sollte erstellt werden.
- Medizinische Gutachten Versicherter sollten in verschlossenen Umschlägen in der Akte abgelegt und eine Öffnung des Umschlags protokolliert werden.
- Die im Ruhegeldantrag für den Fall der Einholung ärztlicher Gutachten vorgesehene pauschale Schweigepflichtentbindungserklärung sollte durch eine nach Zweck und Arzt jeweils konkretisierte Entbindungserklärung ersetzt werden.
- Die Versorgungsanstalten sollten eine Datenschutzanweisung erstellen.

Ich habe darüber hinaus empfohlen, in den oben erwähnten Gesetzentwurf die Vorschriften über den Sozialdatenschutz in der Weise aufzunehmen, daß § 35 Sozialgesetzbuch I (SGB I), und die §§ 25 und 60 bis 85 SGB X für entsprechend anwendbar erklärt werden. Die Vertreter der Versorgungsanstalten sowie der Bayerischen Versicherungskammer hielten diese Lösung für praktikabel. Der Bayerische Landesbeauftragte für den Datenschutz hat sich wegen seiner Zuständigkeit für die Bayerische Versicherungskammer an dem Schlußgespräch beteiligt.

14. Gesundheitswesen

14.1 Bundesgesundheitsamt

Auch in diesem Jahr habe ich im Bundesgesundheitsamt (BGA) Kontroll- und Informationsgespräche geführt, die von der geprüften Behörde leider so unzureichend vorbereitet waren, daß ich dies als Verstoß gegen die in § 19 Abs. 3 BDSG festgelegte Pflicht, den Bundesbeauftragten und seine Mitarbeiter bei der Erfüllung ihrer Aufgaben zu unterstützen, gemäß § 20 Abs. 1 BDSG beanstanden mußte.

In Sachfragen ergaben die Gespräche folgendes:

- Bei der erneuten Erörterung von Problemen der Erfassung und Auswertung unerwünschter Arzneimittelnebenwirkungen stand das Verfahren der Datenerfassung mit Hilfe der Berichtsbögen, die jeweils vom Arzt ausgefüllt und der Arzneimittelkommission der Deutschen Ärzteschaft übersandt werden, im Vordergrund. Von dort werden die Mitteilungen über die Arzneimittelnebenwirkungen dem BGA übermittelt. In Übereinstimmung

mit einigen Landesdatenschutzbeauftragten hatte ich bereits bei früherer Gelegenheit darauf hingewiesen, daß durch die in den Berichtsbögen übermittelten Daten (Initialien des Vor- und Zunamens, Geburtsdatum, Tätigkeit) eine hinreichende Anonymisierung der betroffenen Patienten nicht gewährleistet ist.

Es müßte zunächst geprüft werden, ob die Zahl der Verknüpfungsmerkmale in den Erfassungsbögen noch reduziert werden kann. Dabei muß — um Mehrfachmeldungen zu erkennen — natürlich sichergestellt sein, daß eine hinreichend sichere Identifizierung von paarigen Datensätzen möglich bleibt, ohne daß allerdings der einzelne Patient identifiziert werden kann. Sollte dies nicht möglich sein, so wäre als eine rechtlich vertretbare Lösung ein Treuhändermodell anzusehen, bei dem einer dritten Stelle nur die Aufgabe zukäme, anhand der bisher zur Feststellung der Identität von Patienten genutzten Daten (Initialen, Geburtsdatum, Tätigkeit) die Paarigkeit von Datensätzen zu prüfen. Eine Übermittlung der Daten an das BGA würde dann ohne diese Identitätsmerkmale erfolgen, der Treuhänder seinerseits würde nur die Identitätsmerkmale, aber keine sonstigen Patientendaten erhalten.

Dies setzt allerdings voraus, daß die Ärzte ihrer Berichtspflicht lückenlos nachkommen. Wie meine Mitarbeiter bei Einsichtnahme in verschiedene Erfassungsbögen festgestellt haben, ist dies nicht der Fall. Mehrfachmeldungen sind deshalb nicht ausgeschlossen. Damit ist auch eine korrekte Häufigkeitsschätzung aufgetretener unerwünschter Arzneimittelwirkungen derzeit nicht gewährleistet.

Ich verkenne nicht die medizinische Notwendigkeit, unerwünschte Wirkungen von Arzeimitteln festzustellen und zentral zu erfassen. Ich halte allerdings an meiner Auffassung fest, daß fundierte Ergebnisse nur erreicht werden können, wenn sowohl die Erfassungsvorschriften präzisiert als auch die Informationswege einheitlich gestaltet werden, damit Mehrfachmeldungen ausgeschlossen sind. Dieses Ziel kann nach meiner Auffassung nur durch eine Änderung von § 62 Arzneimittelgesetz (AMG) erreicht werden.

— Die im BGA geführten AIDS-Register wurden mit dem Leiter des AIDS-Zentrums eingehend erörtert. Dabei ergab sich folgendes Bild:

Die aufgrund der Laborberichtsverordnung verarbeiteten Daten führen deswegen nicht zu abgesicherten Fallzahlen, weil das in der Verordnung vorgeschriebene Verfahren keine Vorkehrungen zum Ausschluß von Doppelmeldungen enthält.

Ein Abgleich der aufgrund der Laborberichtsverordnung gespeicherten Daten mit dem Fallberichtsregister ist nach meinen Feststellungen zur Zeit nicht möglich. Das Bundesgesundheitsamt beabsichtigt indessen, sowohl das Fallberichtsregister wie auch die aufgrund der Laborberichtsverordnung gespeicherten Daten ab Januar 1989 auf Personalcomputer zu führen. Ich habe auf die besonderen Gefahren dieses Verfahrens hingewiesen und darum gebeten, es zu gegebener Zeit mit mir abzustimmen.

Soweit von Ärzten auf den Fallbögen Namen der Patienten angeben werden, habe ich empfohlen, die Bögen unmittelbar bei Eingang zu anonymisieren. Dies wurde zugesagt. Im Arbeitskreis AIDS der Datenschutzbeauftragten von Bund und Ländern wurde in diesem Zusammenhang folgende Übereinstimmung erzielt: Gibt der Arzt die Probe an das Labor mit dem Namen des Untersuchten weiter, um die Verwechslungsgefahr zu reduzieren, so ist die zusätzliche Weitergabe der in § 3 Abs. 1 Ziffer 4 bis 8 Laborberichtsverordnung vorgesehenen Angaben (u. a. Alter, Geschlecht, die ersten beiden Ziffern oder Postleitzahl des Wohnorts, Krankheitsbild) unzulässig. Gibt der Arzt die Proben nur mit einer Nummer an das Labor weiter, so darf er weitere Angaben übermitteln, soweit dadurch keine Identifizierung des Untersuchten möglich wird.

Nach meinen weiteren Feststellungen hat das BGA bislang die Namen der Ärzte als Suchkriterium mitgespeichert. Mir wurde zugesagt, die bisher gespeicherten Arztnamen zu löschen und künftig auf deren Speicherung zu verzichten.

Die Fallberichtsbögen werden sämtlich ohne Zeitbegrenzung aufbewahrt. Da sie erst kurze Zeit im BGA lagern, bestehen hiergegen derzeit noch keine Bedenken. Ich habe dem BGA jedoch empfohlen, zweckgemäße Aufbewahrungsfristen festzulegen.

14.2 HIV-Tests im öffentlichen Dienst

Am 16. 12. 1987 hat der Nationale AIDS-Beirat in seinem Votum zur HIV-Diagnostik darauf hingewiesen, daß ärztliche Untersuchungen auf HIV-Infektion nur mit Einwilligung des Patienten durchgeführt werden dürfen. Von begründeten Ausnahmefällen abgesehen, müsse die Einwilligung des Patienten auf der Aufklärung über Wesen, Bedeutung und Tragweite des Tests beruhen. Darüber hinaus stellte der Nationale AIDS-Beirat fest, daß ein HIV-Antikörpertest nicht obligatorischer Bestandteil der Tropentauglichkeits- und Rückkehruntersuchungen sei. Er solle empfohlen, aber ausschließlich auf freiwilliger und, falls gewünscht, auf anonymer Basis mit eingehender ärztlicher Beratung angeboten werden. Dieser Auffassung haben sich mittlerweile weitgehend Rechtswissenschaft und Ärzteschaft angeschlossen.

Ich hatte mich u. a. mit folgendem Problemfall zu befassen:

Im Bereich des Medizinischen Dienstes des Auswärtigen Amtes waren bis August 1987 HIV-Tests als Teil der Tropentauglichkeitsuntersuchung obligatorisch. Die Erforderlichkeit eines solchen Tests wurde darauf gestützt, daß eine HIV-Infektion die Tropentauglichkeit beeinflusse. Mit Rundschreiben vom 16. 10. 1985 waren die Bediensteten des Auswärtigen Amtes erstmals auf die Gefahren, die von AIDS ausgehen, und auf entsprechende Bluttests im Rahmen der Eignungsuntersuchungen (Tropentauglichkeitsuntersu-

chungen einschließlich Zwischen- und Rückkehruntersuchungen) hingewiesen worden. Schriftliche Einwilligungserklärungen zu solchen Tests sind den Betroffenen allerdings nicht abverlangt worden. Ein Großteil der untersuchten Personen war zwar auf die jeweils vorgesehene HIV-Untersuchung aufmerksam gemacht worden, dies war jedoch nicht gegenüber allen Bediensteten geschehen.

Ich habe das Auswärtige Amt aufgefordert, die seinerzeit ohne Kenntnis der Betroffenen erhobenen HIV-Untersuchungsergebnisse zu löschen oder deren weitere Aufbewahrung in den Unterlagen des Ärztlichen Dienstes von der Zustimmung des jeweiligen Betroffenen abhängig zu machen.

Mittlerweile habe ich — auch mit Unterstützung des BMJFFG und der Bundesärztekammer — erreichen können, daß die Betroffenen, die der durchgeführten HIV-Untersuchung nicht ausdrücklich zugestimmt hatten, zur Abgabe einer Erklärung darüber aufgefordert wurden, ob sie mit dem weiteren Verbleib der Ergebnisse in den Gesundheitsakten und im Laborbuch einverstanden sind. Das Auswärtige Amt hat zugesagt, das Untersuchungsergebnis zu löschen, falls die Zustimmung nicht ausdrücklich erteilt wird.

15. Sicherheitsbereich — Übergeordnete Probleme

15.1 Auskunft an Betroffene

Auch im abgelaufenen Jahr haben sich die Gerichte mit der Frage der Auskunftserteilung durch Nachrichtendienste an den Bürger befaßt. In zwei mir bekannt gewordenen Entscheidungen der Verwaltungsgerichte Berlin und Köln sind der Sache nach jeweils die Verfassungsschutzbehörden unterlegen.

In dem vom Verwaltungsgericht Köln entschiedenen Fall ging es um den Auskunftsanspruch eines Bundestagsabgeordneten, dessen personenbezogene Daten in dem sog. „Nachrückerbericht" des Bundesamtes für Verfassungsschutz über die Fraktion der GRÜNEN enthalten waren. Dieser Bericht war später in der Presse aufgetaucht. Das Verwaltungsgericht Köln verpflichtete das Bundesamt für Verfassungsschutz über den Antrag des Klägers, der Auskunft über weitere, in dem Bericht nicht enthaltene Daten verlangte, unter Beachtung der Rechtsauffassung des Gerichts neu zu entscheiden. Zur Begründung wird im wesentlichen ausgeführt, es spreche einiges dafür, daß die derzeitigen rechtlichen Grundlagen für die Datenverarbeitung durch das BfV den verfassungsrechtlichen Anforderungen nicht genügten. Noch sei allerdings der Übergangsbonus nicht abgelaufen. Solange sich die Nachrichtendienste aber nur auf den Übergangsbonus stützen könnten, müßten sie dem Bürger großzügiger Auskunft geben. Hierbei sei zwischen den verschiedenen Aufgabenbereichen des BfV zu differenzieren. Unterschiede seien etwa zwischen der Sicherheitsüberprüfung, der Spionage- und Terrorismusbekämpfung sowie der Extremismusbeobachtung zu machen. Bei letzterer könne die Auskunft dann verweigert werden, wenn die Informationen des BfV aus geschützten Quellen stammten oder konspirativ arbeitende Gruppen beträfen. Daß in derartigen Fällen die Auskunft verweigert werden könne, dürfe aber nicht dazu führen, daß aus Gründen einer allgemeinen Ausforschungsgefahr die Auskunft generell verweigert werde. Es komme vielmehr darauf an, daß in jedem Einzelfall geprüft werde, ob solche Gründe der Auskunftserteilung entgegenstünden oder nicht. Sei dies nicht der Fall, so sei regelmäßig Auskunft zu erteilen. Eine etwaige ablehnende Entscheidung über einen Auskunftsantrag sei soweit zu begründen und plausibel zu machen, daß der Betroffene soweit erforderlich Rechtschutz erlangen könne. Auch wenn dies im Ergebnis auf eine partielle Offenlegung des Erkenntnisstandes hinauslaufen könne, so sei dies im Hinblick auf Artikel 19 Abs. 4 GG hinzunehmen. Das Urteil ist noch nicht rechtskräftig.

Im Berichtsjahr haben BfV und MAD erfreulicherweise häufiger Auskunft erteilt als in früheren Jahren. Sind Daten von Personen lediglich aus Gründen der Sicherheitsüberprüfung gespeichert, so wird in der Regel die Auskunft hierüber erteilt. Ansonsten wird in Einzelfällen Auskunft gegeben, wenn der betreffende Bürger für sein Auskunftsverlangen besondere Umstände geltend machen kann und eine Ausforschungsgefahr erkennbar nicht besteht. Hierzu sind aber in der Regel zähe Verhandlungen mit dem BfV nötig. Hierdurch verzögert sich die Bearbeitung von Bürgerpetitionen oftmals um Wochen und Monate.

Ich bin der Auffassung, daß diese zeitraubende Prozedur kein Dauerzustand sein kann, sondern daß der Gesetzgeber Rechtsklarheit schaffen muß. Er sollte Vorgaben machen, die dem Geheimhaltungsinteresse der Nachrichtendienste ebenso gerecht werden wie dem Recht auf informationelle Selbstbestimmung der Bürger. Mit einem solchen Interessensausgleich verträgt sich ein pauschales Auskunftsverweigerungsrecht für die Nachrichtendienste, so wie es derzeit im Entwurf für ein neues BDSG enthalten ist, nicht.

15.2 Sicherheitsrichtlinien, erste Erfahrungen, offene Fragen

Die neuen Sicherheitsrichtlinien des Bundes (zum Inhalt vgl. 9. TB S. 56f., 10. TB S. 74f.) sind am 1. 5. 1988 in Kraft getreten. Wenngleich sie in einzelnen Fällen auch zu intensiveren Ermittlungen führen können, so hat sich doch insgesamt die Stellung der zu Überprüfenden spürbar verbessert. Überprüfungen ohne Wissen des Betroffenen sind nunmehr ausdrücklich untersagt. Die Richtlinien selbst sind veröffentlicht, so daß jedermann sich über den Ablauf des Verfahrens informieren kann. Im Bundesbereich wurde die Zahl der Sicherheitsüberprüfungen um ca. ein Drittel reduziert. Die Zahl des sog. Schlüsselpersonals, das einer besonders intensiven Überprüfung unterzogen wird, wurde noch stärker vermindert.

In einzelnen Detailfragen der Umsetzung der neuen Richtlinien befinde ich mich noch in der Diskussion mit dem Bundesminister des Innern.

Für die Sicherheitsüberprüfungen im Bereich der Privatwirtschaft fehlt es bislang an der Umsetzung der neuen Sicherheitsrichtlinien. Das BfV hat mir aber

mitgeteilt, daß bis zu einer entsprechenden Überarbeitung des hierfür maßgeblichen „Handbuchs Geheimschutz in der Wirtschaft" die neuen Richtlinien bereits analog angewandt werden. Auch der Bundesminister der Verteidigung und der Bundesnachrichtendienst arbeiten, wie mir bekanntgeworden ist, an einer Umsetzung der neuen Richtlinien für ihre speziellen Bereiche.

Die neuen Sicherheitsrichtlinien des Bundes haben trotz wesentlicher datenschutzrechtlicher Verbesserungen das Defizit einer fehlenden Rechtsgrundlage für die Sicherheitsüberprüfung nicht beseitigen können. Selbst wenn man — wie kürzlich die 3. Kammer des 2. Senats des Bundesverfassungsgerichts — in den hergebrachten Grundsätzen des Berufsbeamtentums oder in einfachgesetzlichen beamtenrechtlichen Vorschriften eine Rechtsgrundlage für die Abforderung des Erklärungsbogens vom Beamten sieht, so ist damit nur ein Teilaspekt der Sicherheitsüberprüfung, nicht aber alle weiteren hiermit verbundenen Eingriffe in das Recht auf informationelle Selbstbestimmung abgedeckt. Die mitunter langjährige Aufbewahrung der Unterlagen aus der Sicherheitsüberprüfung und ihre ständige Ergänzung und Aktualisierung bedürfen einer präzisen gesetzlichen Regelung. Soweit die Sicherheitsüberprüfung Arbeiter und Angestellte im öffentlichen Dienst oder in der Privatwirtschaft sowie die Angehörigen von Überprüften betrifft, scheidet das Beamtenrecht als Rechtsgrundlage ohnehin aus. In § 3 Abs. 2 des Bundesverfassungsschutzgesetzes ist lediglich die Mitwirkung des BfV an der Sicherheitsüberprüfung geregelt. Dies setzt voraus, daß das Verfahren als solches von einer anderen Stelle durchgeführt wird und ist schon deshalb kein Ersatz für eine verfassungsgemäße Rechtsgrundlage für deren Handeln. Die Bundesregierung hat ihre Absicht erklärt, ein Geheimschutzgesetz einzubringen. Bislang ist mir noch kein entsprechender Entwurf zugegangen. Ob es noch vor Ablauf dieser Legislaturperiode zu einer gesetzlichen Regelung kommen wird, ist ungewiß.

Daß auch bei den Bürgern zunehmend Zweifel und Unklarheiten über die rechtliche Zulässigkeit von Sicherheitsüberprüfungen entstehen, kann ich aus der wachsenden Zahl von Eingaben zu diesem Fragenkreis entnehmen. Nicht selten geben die Petenten zu erkennen, daß sie gegen die Sicherheitsüberprüfung als solche nichts einzuwenden haben, daß sie aber wissen möchten, was anschließend mit den bei dieser Gelegenheit gesammelten Daten geschieht.

Ich habe auch in diesem Jahr bei meinen Kontrollen wieder Fälle festgestellt, in denen Daten, die im Rahmen der Sicherheitsüberprüfung erhoben worden sind, an dritte Stellen übermittelt wurden, ohne daß auch nur nach dem Zweck gefragt wurde, zu dem die anfragende Stelle die Daten benötigte. In einem Falle wurden dabei Informationen über zwei eingeleitete polizeiliche Ermittlungsverfahren weitergegeben, die dem BfV für Zwecke der Sicherheitsüberprüfung vom BKA Jahre zuvor übermittelt worden waren. Über den Ausgang der Verfahren war dem BKA nichts bekannt, ein extremistischer Hintergrund der möglicherweise begangenen Straftaten wurde nicht mitgeteilt. Im Jahre 1988 hat das BfV diese Informationen an eine Landesbehörde für den Verfassungsschutz weiterübermittelt, ohne daß nachgefragt worden wäre, zu welchem Zweck die Daten dort benötigt wurden. Auch wurde das BKA nicht nach dem Ausgang des Ermittlungsverfahrens gefragt, obwohl eine interne Dienstvorschrift dies nach meiner Auffassung verlangt hätte. Inzwischen hatte das BKA bei sich diese Daten bereits gelöscht. Sie waren auch beim BfV nicht im Zusammenhang mit der Extremismusbeobachtung, sondern ausschließlich in der sog. Sicherheitsprüfungsakte gespeichert. Bei der Überprüfung, in deren Rahmen diese Daten gesammelt worden waren, handelte es sich im übrigen um eine sog. Dateianfrage (vgl. 4. TB, S. 29). Ich habe diese Datenübermittlung beanstandet.

Beim MAD habe ich im Rahmen einer Querschnittskontrolle (vgl. unten 21.1.2) festgestellt, daß das Ergebnis von Befragungen im Rahmen der Sicherheitsüberprüfung routinemäßig an den Verfassungsschutz weitergeleitet wird, wenn es für dessen Aufgabenerfüllung von Bedeutung sein könnte. Nach meinen Feststellungen wird hierbei der Einfachheit halber in der Regel eine Kopie des gesamten Befragungsberichts übersandt. Dabei werden nicht nur Daten über den Verdacht extremistischer Betätigung, sondern auch alle Informationen mitübermittelt, die im Rahmen der Befragung mit dem Betroffenen erörtert worden sind. In einem von mir beanstandeten Fall wurden beispielsweise Informationen über die familiären Verhältnisse des Betroffenen sowie über seine finanzielle Situation an das BfV übermittelt. Ich habe diese Übermittlungspraxis gegenüber dem Bundesminister der Verteidigung beanstandet.

Diese Beispielsfälle zeigen, daß die im Rahmen einer Sicherheitsüberprüfung gewonnenen Daten nicht schrankenlos für alle übrigen Aufgaben des Verfassungsschutzes verwendet werden dürfen. Diese Forderung liegt nicht nur im Interesse des Datenschutzes der Betroffenen, sondern auch der Sicherheitsüberprüfung selbst. Zu der angestrebten vertrauensvollen Zusammenarbeit mit dem zu Überprüfenden kann es nur dann kommen, wenn dieser sicher sein kann, daß die Informationen, die er für Zwecke der Sicherheitsüberprüfung hergibt, grundsätzlich nur für diesen Zweck und für die Spionageabwehr verwendet werden. Derzeit ist dies nicht sichergestellt.

16. Bundeskriminalamt

16.1 Bundeskriminalamt-Gesetz

Der Bundesminister des Innern hat mir im August 1988, gleichzeitig mit den Bundesressorts und den Ländern, den Entwurf eines „Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamt-Gesetz — BKAG)" mit der Bitte um Stellungnahme zugeleitet. Ich bin bei der Beurteilung des Entwurfs von folgenden Prämissen ausgegangen:

— Als bereichspezifische Regelung soll das Gesetz die Erfassung der Bürger durch die Sicherheitsorgane und den Informationsaustausch zwischen

diesen sowie mit anderen Stellen durch möglichst präzise Regelungen berechenbar machen und begrenzen.

- Im Konflikt zwischen dem Informationsbedürfnis der Behörden und dem Recht des einzelnen auf informationelle Selbstbestimmung sind Kompromisse notwendig.
- In den wesentlichen Fragen muß der Gesetzgeber zumindest die richtungsweisenden Grundsatzentscheidungen selbst treffen.

Meine dem Bundesminister des Innern mitgeteilte Position läßt sich wie folgt zusammenfassen:

1. Die Aufgabe des Bundeskriminalamtes, als Zentralstelle personenbezogene Daten zu sammeln und anderen Polizeibehörden zugänglich zu machen, ist auf die länderübergreifende und internationale Kriminalität zu begrenzen. Mit der Verwirklichung des Entwurfs würde eine weitgehende Zentralisierung der Datenhaltung ermöglicht, die mit der Kompetenzverteilung des Grundgesetzes (Artikel 73 Nr. 10, Artikel 87 Abs. 1 Satz 2) nicht vereinbar wäre.

   Das Gesetz sollte klarstellen, daß auch eine Speicherung beim BKA als Zentralstelle stets voraussetzt, daß die zuständige Polizeibehörde die Daten nach dem Strafverfahrensrecht oder dem Gefahrenabwehrrecht erheben und aufbewahren darf.

2. Der Verarbeitungszweck ist jeweils speziell festzulegen, je nachdem ob die Datei bzw. die Daten beispielsweise dem Aktennachweis, der Spurenauswertung, der Fahndung oder der Eigensicherung der Beamten dienen. Bei Daten aus der Anwendung besonderer Fahndungsmittel ist sicherzustellen, daß eine besonders enge Zweckbindung beachtet wird.

   Die Verarbeitung von Daten über nicht verdächtige Personen (Anzeigende, Zeugen, Hinweisgeber, Kontakt- und Begleitpersonen, Geschädigte, Gefährdete) ist durch einschränkende Regelungen der Speichervoraussetzungen und der Nutzung in engen Grenzen zu halten.

   Das Gesetz sollte auch Grundentscheidungen über die Dauer der Speicherung treffen.

3. Die Voraussetzungen für die Errichtung neuer Dateien sind zu definieren, differenziert nach dem jeweiligen Typ des Datei- oder Verarbeitungssystems (Aktennachweissystem, Falldatei, Recherchiersystem nach Art von PIOS, Erkennungsdienst, Haftdatei, Spurendokumentationssystem usw.).

4. Beim elektronischen Datenverbund sind nähere Regelungen des Zusammenwirkens von Bundes- und Landesbehörden erforderlich, damit auch bei gegenseitiger Verknüpfung, Änderung und Löschung von Daten stets klar bleibt, welche Stelle die datenschutzrechtliche Verantwortung trägt.

   Dienststellen, die keine polizeilichen Aufgaben haben, dürfen keinen Direktzugriff auf polizeiliche Datensammlungen erhalten; insbesondere sind Ermächtigungen an die Innenminister, solche on-line-Anschlüsse zuzulassen, abzulehnen.

5. Zur internationalen Harmonisierung sollte sich der Entwurf strikt an den Vorgaben der Datenschutzkonvention des Europarats und möglichst weitgehend auch an der Empfehlung des Europarats zur polizeilichen Datenverarbeitung orientieren.

   Dies betrifft beispielsweise den Grundsatz, daß Daten auf rechtmäßige Weise und nach Treu und Glauben beschafft sein müssen (Artikel 5 a der Konvention), den Grundsatz des besonderen Schutzes von Daten über die rassische Herkunft, politische Anschauungen oder religiöse und andere Überzeugungen und das Sexualleben (Artikel 6 der Konvention und Nr. 2.4 der Empfehlung) sowie den Grundsatz der abgeschotteten Verarbeitung von Daten, die zu administrativen Zwecken gesammelt wurden (Nr. 3.3 der Empfehlung).

   Vor einer Übermittlung ins Ausland ist unter Beteiligung der zuständigen Polizeibehörde festzustellen, ob schutzwürdige Belange des Betroffenen entgegenstehen. Die Übermittlung zu vorbeugenden Zwecken, also ohne Anforderung im Einzelfall, ist einschränkend zu regeln. Soweit irgend möglich muß sichergestellt sein, daß die Zweckbindung auch im Ausland beachtet wird.

16.2 Entwicklung der Datenverarbeitung beim Bundeskriminalamt

Der vom Innenausschuß des Deutschen Bundestages angeforderte Bericht der Bundesregierung über die Entwicklung der automatisierten Datenverarbeitung des Bundeskriminalamtes liegt noch nicht vor.

Im Berichtszeitraum wurde mir die Einrichtung von zehn weiteren SPUDOK-Dateien mitgeteilt. Sie dienen überwiegend der Sammlung und Auswertung von Erkenntnissen im Rahmen bestimmter Strafverfolgungsmaßnahmen, teilweise aber auch der Gefahrenabwehr (z. B. Datei, anläßlich der Tagung in Hannover über die europäische politische Zusammenarbeit, in der die Polizei zum Zwecke des Personenschutzes für Mitglieder von Verfassungsorganen des Bundes und deren ausländische Gäste vorübergehend auch personenbezogene Daten gespeichert hat). Sechs SPUDOK-Dateien wurden gelöscht. Damit betreibt das Bundeskriminalamt zur Zeit rund zwanzig SPUDOK-Dateien; die Schwerpunkte liegen weiterhin bei der Bekämpfung terroristischer Gewalttäter und krimineller Vereinigungen.

Über die Praxis der Speicherung „anderer Personen", also solcher Personen, denen keine strafbaren Handlungen vorzuwerfen sind, habe ich im Neunten Tätigkeitsbericht (S. 59) berichtet. Im Rahmen meiner datenschutzrechtlichen Prüfung bei der Abteilung Staatsschutz des Bundeskriminalamtes (vgl. unten 16.3) habe ich auch den Umfang der Speicherung „anderer Personen" in einer SPUDOK-Datei überprüft, die in einem Ermittlungsverfahren gegen eine politische Vereinigung von Ausländern betrieben wird. Dabei zeigte sich, daß das Bundeskriminalamt die Daten sämtlicher Personen gespeichert hat, deren Adressen bei einer Durchsuchung von Vereinsräumen bei-

spielsweise in Adressenlisten und Telefonnotizbüchern gefunden worden waren. Darunter waren auch die Adressen von Bundestagsabgeordneten, bekannten Wissenschaftlern und sogar die eines amtierenden Ministerpräsidenten eines Bundeslandes. Das Bundeskriminalamt hat die Speicherung damit begründet, daß einmal die betroffenen Personen möglicherweise noch dazu befragt werden müßten, aus welchem Anlaß ihre Personendaten in die Unterlagen der Vereinigung geraten seien, und zum anderen mit Hilfe der Speicherung Aufschlüsse über die Zielsetzung des Täters oder der Tätergruppe gewonnen, Zusammenhänge zu anderen Tätergruppen oder Ereignissen hergestellt oder Erkenntnisse über Vorgehensweisen des Täters oder der Tätergruppe gesammelt werden könnten. Ich halte es für erforderlich zu prüfen, ob der Kreis der zu speichernden Personen nicht vermindert werden kann. Der mit der Speicherung verbundene Eingriff ist nur dann gerechtfertigt, wenn die Angaben wirklich als Spuren in Betracht kommen, nicht aber schon dann, wenn lediglich theoretisch nicht ausgeschlossen werden kann, daß sie eventuell zu einer Spur werden könnten. Im konkreten Fall ist die Befragung der Betroffenen noch nicht abgeschlossen. Über die Löschung oder Aufrechterhaltung der Speicherung will das Bundeskriminalamt je nach Ergebnis der Befragung erst anschließend entscheiden.

Das Bundeskriminalamt beabsichtigt, die Errichtungsanordnungen für SPUDOK-Dateien entsprechend meinen Anregungen dahingehend zu ändern, daß die Daten von Personen, die als „andere Personen" gespeichert sind, nur im Rahmen der Zwecke verwendet werden dürfen, denen die SPUDOK-Anwendung dient. Eine anderweitige Verwertung, insbesondere in der Form der Übermittlung an Dritte, wird damit unzulässig sein.

Erstmals hat das Bundeskriminalamt im Berichtszeitraum automatisierte Dateien, die mittels Personalcomputer betrieben werden, zum besonderen Register gemäß § 19 Bundesdatenschutzgesetz gemeldet. In diesen Dateien werden auch personenbezogene Daten gespeichert. Eine inhaltliche Prüfung dieser DV-Anwendungen war mir im Berichtsjahr wegen der begrenzten Arbeitskapazität nicht möglich. Das Bundeskriminalamt beabsichtigt, durch Dienstanweisung zu regeln, wann und in welchem Umfang PC zur Aufgabenerfüllung der Dienststelle eingesetzt werden dürfen. Meine Beteiligung ist vorgesehen.

16.3 Kontrolle bei der Abteilung Staatsschutz des Bundeskriminalamtes

Zu Beginn des Berichtsjahres habe ich eine Querschnittskontrolle bei der Abteilung Staatsschutz des BKA durchgeführt, deren Schwerpunkte bei der Arbeitsdatei PIOS Innere Sicherheit (APIS) und bei der Datenspeicherung durch das Bundeskriminalamt im nachrichtendienstlichen Informationssystem (NADIS) lagen. Insgesamt habe ich dabei einen wesentlich besseren Eindruck als bei meiner ersten Querschnittskontrolle im Jahre 1982 gewonnen. Daran dürfte die in der Zwischenzeit erfolgte datenschutzrechtliche Schulung wesentlichen Anteil haben. Die Zahl der Kriminalakten und damit auch der in den Dateien erfaßten Personen hat sich etwa halbiert. Bei leichteren Straftaten wird nunmehr in der Regel eine dreijährige Aussonderungsprüffrist eingegeben, nach deren Ablauf die Daten zumeist gelöscht werden, wenn keine neuen Erkenntnisse hinzugekommen sind. Grundlage für die Anlegung einer Kriminalakte und die damit verbundene Speicherung in Dateien ist in aller Regel die Einleitung eines strafrechtlichen Ermittlungsverfahrens, d. h. zumindest der Verdacht einer Straftat.

Allerdings habe ich auch bei dieser Kontrolle wieder Mängel der Datenverarbeitung festgestellt und beanstandet. Sie beziehen sich in erster Linie auf die Handhabung der Datei APIS sowie auf die fortbestehende Praxis des BKA, Daten in NADIS zu speichern.

16.3.1 APIS

Über die mit der Einführung von APIS verbundenen datenschutzrechtlichen Probleme habe ich mehrfach berichtet (vgl. 9. TB S. 60ff. und zuletzt 10. TB S. 77f.).

In wesentlichen Punkten hat die Kontrolle die Befürchtungen bestätigt, die ich bei der Einführung von APIS hegte. Nach der Errichtungsanordnung werden nicht nur Staatsschutzdelikte im eigentlichen Sinn erfaßt, sondern — nach einer Art Auffangklausel — auch jede andere Straftat, wenn wegen des Motivs des Täters, seiner Verbindung zu einer Organisation oder wegen des Objekts, gegen das sich die Straftat richtet, zu vermuten ist, daß der Täter extremistische Ziele verfolgt. Die Klausel ist, wie ich festgestellt habe, weitgehend zum Regeltatbestand für die Speicherungen in APIS geworden. Auf sie werden ca. 80% der erfaßten Straftaten gestützt. Im übrigen sind nach meiner Schätzung ca. 75% aller in APIS gespeicherten Straftaten eher leichterer Art, wie z. B. Verdacht der Nötigung im Zusammenhang mit Demonstrationen, der Beleidigung von Politikern und der Sachbeschädigung in Form von Schmierereien oder durch Abschneiden der Zählnummer vom Volkszählungsbogen.

Die Mehrzahl dieser Fälle ist von den Landeskriminalämtern unter Anwendung der gemeinsamen APIS-Errichtungsanordnung eingegeben worden.

Ich habe dem Bundesminister des Innern empfohlen, die Errichtungsanordnung neu zu fassen und dabei sicherzustellen, daß „andere Straftaten" nur dann erfaßt werden, wenn sie von der Schwere her mit den benannten Staatsschutzdelikten vergleichbar sind, wenn sie überörtliche Bedeutung haben, wenn ihr verfassungsfeindlicher Charakter eindeutig festgestellt oder aufgrund klarer Indizien vermutet werden kann und wenn beim Täter Wiederholungsgefahr besteht.

Der Bundesminister des Innern hat in seiner Stellungnahme zu meinem Prüfbericht eine Änderung der Errichtungsanordnung abgelehnt. Er begründet dies im wesentlichen damit, meine Feststellungen zu den „anderen Straftaten" bestätigten, daß sich Staatsschutzkriminalität zum zahlenmäßig geringeren Teil

in den sog. „klassischen" Staatsschutzdelikten äußere und gerade deswegen die Aufnahme des Auffangtatbestandes zwingend geboten sei. Der Schwere der Straftat komme im Hinblick auf die generelle Zielsetzung des Meldedienstes in Staatsschutzsachen sowie der Datei APIS keine entscheidende Bedeutung zu. Auch auf die überörtliche Bedeutung der Straftat komme es nicht an, da dieses Kriterium für die Beurteilung der Motivationslage des Täters keine wesentliche Rolle spiele. Die besondere Feststellung einer Wiederholungsgefahr sei nicht notwendig, da die Diagnose „verfassungsfeindliche Zielsetzung" bereits die Wiederholungsgefahr beinhalte. Der BMI hat aber zugesagt, daß durch eine weitere intensive Schulung der APIS-Anwender eine verbesserte Handhabung der Errichtungsanordnung gewährleistet werden soll. Aufgrund der zwischenzeitlich gewonnenen Erfahrungen werde das BKA künftig besonders darauf achten, daß sich aus den Meldungen zumindest Rückschlüsse auf die in der Errichtungsanordnung genannten Speicherungsvoraussetzungen (Motivation, Organisationszugehörigkeit, Objektbezug) ergeben.

Weiter habe ich bemängelt, daß auch beim Vorliegen eines „klassischen" Staatsschutzdelikts Daten zu schematisch in APIS erfaßt werden. Dies ist insbesondere bei der Speicherung von Straftaten nach § 86a StGB in der Form des Verwendens von nationalsozialistischen Symbolen der Fall. Beispielsweise habe ich die Datenspeicherung in einem Fall beanstandet, in dem ein betrunkener Fußballfan im Vorbeigehen zwei Polizeibeamten „Sieg heil" zugerufen hatte, ebenso den Fall einer Person, die in der Halbzeitpause eines Bundesligaspiels die Hand zum „Deutschen Gruß" erhoben und „Sieg heil Deutschland" gerufen hatte, und den einer weiteren Person, die erfaßt war, weil an ihrem Fahrzeugschlüssel ein Anhänger mit Reichsadler und Hakenkreuz angebracht war. Das BKA hat inzwischen in den meisten dieser Fälle die Akten ausgesondert und die Speicherungen gelöscht. Eine Änderung der Erfassungsvorschriften hält der BMI aber auch insoweit nicht für notwendig und will statt dessen zukünftig im Rahmen von Schulungsmaßnahmen auf die Problematik hinweisen.

Ich habe auch den Passus der Errichtungsanordnung beanstandet, der vorsieht, daß Daten der sog. „L-Gruppe" auch über „andere Personen" gespeichert werden dürfen. Bei der „L-Gruppe" handelt es sich um Daten, mit denen das äußere Erscheinungsbild und das Verhalten von Personen dargestellt werden kann. Beispielsweise können Informationen wie „aalglatt", „arrogant", „besondere Eßgewohnheiten", „besondere Rauchgewohnheiten", „besondere sexuelle Gewohnheiten", „besondere Trinkgewohnheiten", erfaßt werden. Derartige Informationen sind der Sache nach erkennungsdienstliche Unterlagen, und es ist allenfalls zulässig, sie über Verdächtige und Beschuldigte zu speichern.

Der Bundesminister des Innern hat erwidert, er überarbeite derzeit den Datenkatalog der L-Gruppe; die meisten der von mir beanstandeten Einzelbegriffe würden gestrichen. Er sehe aber keine Notwendigkeit dafür, auf die Speicherung von Daten aus der L-Gruppe bei „anderen Personen" gänzlich zu verzichten. Beim Vorliegen besonderer kriminalistischer Gründe könne es zwingend geboten sein, bei einer „anderen Person" eine Personenbeschreibung zu erfassen, etwa weil dies die einzige Möglichkeit sei, die Person zu identifizieren. Auf meinen Hinweis, daß insoweit eine Rechtsgrundlage fehlt, ist der Bundesminister des Innern noch nicht eingegangen.

Generell habe ich die Auffassung vertreten, daß eine qualitative Verstärkung der Datenverarbeitung im Bereich des polizeilichen Staatsschutzes, wie sie durch die Einführung von APIS erfolgt ist, ohne ausdrückliche gesetzliche Grundlage nicht zulässig ist. Der Bundesminister des Innern hat hierzu ausgeführt, daß bis zur Schaffung bereichsspezifischer rechtlicher Grundlagen eine Übergangsfrist anerkannt werden müsse. In dieser Zeit dürfe nicht lediglich der bisherige Zustand übergangsweise beibehalten werden, sondern es seien diejenigen Maßnahmen gestattet, die „unerläßlich" seien. Erweise sich eine Maßnahme als „unerläßlich", so dürfe sie auch in der Übergangsfrist erstmalig durchgeführt werden. Dies treffe auf die Arbeitsdatei APIS zu.

Insgesamt erachte ich — trotz einiger zugesagter Verbesserungen — die Stellungnahme des BMI zu meinen Beanstandungen bezüglich APIS als nicht befriedigend. Die von mir schon seit Jahren geltend gemachten Befürchtungen hinsichtlich der Generalklausel über die Erfassung „anderer Straftaten" in APIS haben sich bestätigt. Es handelt sich nicht um neu entdeckte Schwachstellen, sondern um die wesentlichen Punkte der Diskussion über die APIS-Errichtungsanordnung in den vergangenen Jahren. Ich halte Schulungsmaßnahmen nicht für ausreichend, um die Mängel abzustellen.

16.3.2 NADIS

Einen weiteren Schwerpunkt der Kontrolle bildete die Speicherung von Daten durch das Bundeskriminalamt in NADIS. Diese Praxis hatte ich bereits wiederholt beanstandet (vgl. zuletzt 10. TB S. 77f.). Der Bundesminister des Innern hat meine Beanstandungen bislang stets zurückgewiesen, und das Bundeskriminalamt fährt fort, Daten in NADIS zu speichern. Der BMI begründet dies im wesentlichen damit, daß alle vom BKA in NADIS gespeicherten Fälle für die Verfassungsschutzbehörden relevant seien. Das BKA sei auf die Speicherung in NADIS nicht angewiesen, denn es verfüge über eigene Dateisysteme, in denen es die Speicherung vornehmen könnte. Die Speicherung in NADIS erfolge im Interesse der Informationsübermittlung an den Verfassungsschutz.

In früheren Stellungnahmen hatte der BMI die Relevanz der durch das BKA in NADIS gespeicherten Fälle für den Verfassungsschutz daraus abgeleitet, daß nur solche Fälle in NADIS gespeichert würden, die auch die Erfassungskriterien für APIS erfüllten; aus diesen ergebe sich die Verfassungsschutzrelevanz. Ich habe demgegenüber festgestellt, daß das BKA doppelt so viele Fälle in NADIS wie in APIS speichert. NADIS ist sozusagen die „Auffangdatei" für die Fälle, die die — ohnehin zu weiten — Voraussetzungen für die Erfassung in APIS nicht erfüllen (vgl. oben 16.3.1).

Dies betraf beispielsweise zwei Personen, die die Rede eines Staatssekretärs der Bayerischen Staatsregierung in einem Festzelt mit dem Zwischenruf „Heil-Gauleiter" gestört hatten. Eine andere Person hatte ein Verwarnungsgeld wegen Falschparkens bezahlt und auf dem begleitenden Anschreiben „mit deutschem Gruß" unterschrieben. Eine weitere Person rief in betrunkenem Zustand im Schützenzelt auf dem Münchener Oktoberfest „Sieg heil". Diese und weitere von mir aufgeführte Fälle wurden vom BKA nicht in APIS, wohl aber in NADIS gespeichert und damit an die Verfassungsschutzbehörden übermittelt.

Der BMI räumt nunmehr ein, daß in NADIS auch Fälle erfaßt werden, die nicht in APIS gespeichert sind. Im übrigen ist seine Auffassung in dieser Frage unverändert. Meine Feststellung, daß mehr als die Hälfte der von der Abteilung Staatsschutz des BKA erteilten konventionellen Auskünfte in dem von mir untersuchten Zeitraum an Verfassungsschutzbehörden gingen, hält der BMI für einen Beleg für die Notwendigkeit des engen Informationsaustauschs zwischen Polizei und Verfassungsschutz.

Die Speicherung von Daten durch die Abteilung Staatsschutz des BKA in der NADIS-Personenzentraldatei (NADIS-PZD) bedeutet, daß routinemäßig personenbezogene Daten übermittelt und gespeichert werden, ohne daß die jeweils verantwortliche Behörde die Zulässigkeit der konkreten Einzelmaßnahmen prüft. Eine solche Verfahrensweise ist mit dem geltenden Recht nicht vereinbar. Aber auch die Entwürfe für das Verfassungsschutzgesetz sowie für das BKA-Gesetz sehen keine einschlägige Rechtsgrundlage vor. Der Entwurf eines Verfassungsschutzgesetzes schließt im Gegenteil die Beteiligung anderer als Verfassungsschutzbehörden an NADIS-PZD ausdrücklich aus.

Weiterhin hatte ich bemängelt, daß für die Speicherung von BKA-Daten in NADIS eine Errichtungsanordnung fehlt, wie sie von den Dateienrichtlinien für alle Dateien des BKA vorgeschrieben wird. Der BMI ist der Ansicht, die Erwähnung des BKA in der Errichtungsanordnung für die NADIS-PZD der Verfassungsschutzbehörden als „Verbundteilhaber" sowie die Richtlinien für die kriminalpolizeilichen personenbezogenen Sammlungen (KpS-Richtlinien) seien eine ausreichende Grundlage für die Speicherung von Daten in NADIS-PZD. Nach meiner Auffassung ist dies nicht ausreichend, da die bloße Erwähnung als Verbundteilnehmer noch keine Regelung der Voraussetzungen bedeutet, unter denen Daten in NADIS-PZD gespeichert werden dürfen. Auch das BfV selbst hat für alle Abteilungen neben der NADIS-Errichtungsanordnung noch eigene Verkartungspläne mit detaillierten Regelungen, unter welchen Voraussetzungen welche Daten gespeichert werden dürfen. Die KpS-Richtlinien gelten generell für die gesamte konventionelle und automatisierte Datenverarbeitung des BKA und nicht nur für einzelne Dateien. Wären sie als Ersatz für Datei-Errichtungsanordnungen anzusehen, so hätten die zeitgleich verabschiedeten Dateienrichtlinien nicht für jede Datei eine eigene Errichtungsanordnung vorschreiben müssen. Gerade in einem so sensiblen Bereich wie dem polizeilichen Staatsschutz und im Hinblick auf die Beteiligung zweier Behörden mit unterschiedlichen Aufgaben halte ich eine innerdienstliche Vorschrift für unerläßlich, in der geregelt wird, welche Daten unter welchen Voraussetzungen vom BKA in welchen Dateien gespeichert werden dürfen.

16.3.3 Weitere Probleme

Gegenstand meiner Kontrolle war auch das konventionelle Meldewesen im Bereich des polizeilichen Staatsschutzes. Es ist im „Kriminalpolizeilichen Meldedienst in Staatsschutzsachen (KPMD-S)" geregelt. Der KPMD-S beschreibt die Tatbestände, bei deren Vorliegen eine Straftat als Staatsschutzdelikt an das BKA zu melden ist. Die Formulierungen stimmen mit der APIS-Errichtungsanordnung überein und wurden deshalb von mir als zu unpräzise kritisiert. Ich habe außerdem festgestellt, daß neben diesem Meldedienst weitere Meldeverpflichtungen und -praktiken bestehen, die zu Informationsflüssen an das BKA führen. Da es insoweit an genauen Regelungen fehlt, kann es vorkommen, daß Fälle, die nicht unter den KPMD-S „passen", — unter anderem Bezug — gleichwohl gemeldet werden. Ich kann nicht erkennen, welchen Sinn ein detailliert geregelter Meldedienst hat, wenn daneben weitere Meldewege bestehen, die zu einem weit größeren Meldevolumen führen. Insbesondere erscheint klärungsbedürftig, in welchem Verhältnis KPMD-S und sonstige Meldeverpflichtungen zueinander stehen und unter welchen Voraussetzungen kriminaltaktische Anfragen als Meldung eines Staatsschutzdelikts genutzt werden dürfen.

Nach Auffassung des BMI müsse es neben dem KPMD-S noch weitere Meldeverpflichtungen und -möglichkeiten geben. Er will aber künftig dafür Sorge tragen, daß Erkenntnisanfragen ohne Meldecharakter ausdrücklich als solche bezeichnet und dann entsprechend behandelt werden.

Ich habe in meinem Prüfbericht noch eine Reihe weiterer Mängel der Datenverarbeitung beim BKA kritisiert, die hier nicht im einzelnen dargestellt werden können. Die Stellungnahme des BMI ist für mich auch in diesen Punkten zumeist noch nicht befriedigend. Ich habe deshalb dem Bundesminister des Innern weitere Bedenken mitgeteilt und um erneute Stellungnahme gebeten.

17. Bundesgrenzschutz — Bewerbungsverfahren —

Im Jahr 1987 hatte ich das Verfahren der Einholung von Polizeiauskünften über Bewerber beim Bundesgrenzschutz beanstandet (10. TB S. 84). Der Bundesminister des Innern hat inzwischen mit den Innenministern der Länder vereinbart, das Verfahren in veränderter Form fortzuführen. Dabei soll es aber jedem Land freistehen, ob es sich daran beteiligen möchte. Die Auskunft wird von den Innenministern jetzt nicht mehr als Teil der Sicherheitsüberprüfung, sondern als Teil der Eignungsfeststellung verstanden und dementsprechend nicht mehr vom Geheimschutzbeauftragten, sondern von der Personalverwaltung eingeholt. Der Betroffene muß sich mit dieser Auskunftseinholung durch Unterschrift einverstanden erklären.

Seine Einwilligung ist, wie es in einem Erlaß des Bundesministers des Innern an die Grenzschutzkommandos heißt, von ihm „zu erwirken". Das Anfrageformular ist überarbeitet worden. Die Fragen nach dem Leumund, den wirtschaftlichen Verhältnissen und danach, ob der Bewerber die Gewähr bietet, jederzeit für die freiheitlich demokratische Grundordnung einzutreten oder sonstige Gründe gegen eine Einstellung in den Polizeidienst sprechen, sind durch die Frage ersetzt worden, ob „ansonsten aktenkundige Tatsachen darüber (vorliegen), daß der Bewerber in einer Weise polizeilich in Erscheinung getreten ist, die Zweifel an seiner Eignung für den Polizeidienst aufkommen lassen könnten". Nach wie vor werden die örtlichen Polizeidienststellen danach gefragt, ob über den Bewerber Erkenntnisse hinsichtlich eines gegen ihn geführten polizeilichen, staatsanwaltlichen oder gerichtlichen Ermittlungsverfahrens vorliegen.

Auch das neue Verfahren erscheint im Hinblick auf das Fehlen einer wirklich freiwilligen Einwilligung, die Grenzen des Fragerechts des Arbeitgebers und die Grundsätze des Jugendstrafverfahrens problematisch. Wegen des Schwergewichts bei den Ländern bin ich um eine Abstimmung mit den Landesbeauftragten für den Datenschutz bemüht.

18. Bahnpolizei

Der Vorstand der Deutschen Bundesbahn hat neue Regelungen zur Führung der Bahnhofsverbotskarteien erlassen. Er hat dabei meine Empfehlungen berücksichtigt. Vorausgegangen war folgender Vorgang:

Die Kölner Kriminalpolizei hatte im Rahmen von Ermittlungen in einem Mordfall im Homosexuellenmilieu von der Bahnpolizei Köln Zugang zu der dort geführten Bahnhofsverbotskartei erhalten und daraus die Personalien von über hundert Personen entnommen, von denen sie aufgrund entsprechender Eintragungen in der Kartei annahm, daß sie dem homosexuellen Milieu zuzurechnen sind; diese wurden dann zur Vernehmung vorgeladen. Daraufhin wurde der Vorwurf erhoben, die Bahnpolizei führe „Rosa Listen".

Bei einer Kontrolle vor Ort habe ich festgestellt, daß zahlreiche Karteikarten in der „Begründung" für eine Bahnhofsverweisung oder ein (für eine bestimmte Zeit laufendes) Bahnhofsverbot Formulierungen enthielten, die auf Homosexualität des Betroffenen hinwiesen, ohne daß dies zur Beschreibung des Verstoßes gegen die Bahnordnung erforderlich gewesen wäre. Die Weitergabe der Informationen, die die Kriminalpolizei für ihre Ermittlungen benötigte, war nicht zu beanstanden, wohl aber die Gewährung von Einsicht in die gesamte Kartei. Die neuen Regelungen entsprechen dieser Rechtslage. Es wird auch vorgeschrieben, daß in der Kartei nur noch eingetragen werden darf, durch welches Verhalten der Betroffene gegen die Bahnordnung verstoßen hat, und daß dabei Kürzel wie etwa „Stricher, Dirne, Homo, Schläger" zu unterlassen sind. Die Aufbewahrung wird auf maximal ein Jahr nach Ablauf des Bahnhofsverbots begrenzt. Die Einhaltung der Anordnung soll bei Gelegenheit kontrolliert werden.

19. Bundesamt für Verfassungsschutz

19.1 Entwurf eines Bundesverfassungsschutzgesetzes

Gegen Ende des Berichtsjahres hat die Bundesregierung im Rahmen des Entwurfs eines Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes auch einen Entwurf für ein neues Bundesverfassungsschutzgesetz beschlossen.

Dieser Entwurf enthält gegenüber einem vorausgegangenen Entwurf, zu dem ich eine ausführliche Stellungnahme abgegeben hatte, eine Reihe von Verbesserungen; insbesondere wurden Verschlechterungen gegenüber dem Koalitionsentwurf der letzten Legislaturperiode wieder rückgängig gemacht. Der neue Entwurf bietet eine geeignete Grundlage für die weiteren Beratungen, muß aber in wesentlichen Punkten noch geändert und ergänzt werden:

- Die Aufgabenbestimmung wird unverändert aus dem geltenden Recht übernommen. Ich rate dringend zu einer Präzisierung. Diese sollte einmal eine größere Normenklarheit erreichen, auf die die Rechtsprechung des Bundesverfassungsgerichts Wert legt; zum anderen halte ich sie für erforderlich, um den Verfassungsschutzbehörden klare Vorgaben dafür zu geben, in welchen Bereichen sie tätig werden dürfen. Das fordern nicht nur die Belange unserer Bürger, sondern auch die wohlverstandenen Interessen der Verfassungsschutzbehörden, wie die immer wieder auftretenden Konflikte um deren Aufgabenwahrnehmung zeigen.
- Die Befugnisregelungen wiederholen grundsätzlich lediglich das bereichsübergreifende Erforderlichkeitsprinzip. Eine bereichsspezifische Regelung erfordert aber gerade, soweit irgend möglich nach den verschiedenen Aufgaben zu differenzieren. Deshalb sollte z. B. das Recht, öffentlich geführte Register einzusehen auf Sachbereiche eingeschränkt werden, für die dies unerläßlich ist, wie z. B. die Spionageabwehr, die Terrorismusbeobachtung, die Vorbereitung von Partei- und Vereinsverboten.
- Die Regelung für die gemeinsamen Verbunddateien der Verfassungsschutzbehörden ist präzisierungsbedürftig. Unklar ist insbesondere, unter welchen Voraussetzungen Personen in Verbunddateien mit Textzusätzen oder mit weiteren, im Gesetz nicht definierten Datenfeldern gespeichert werden dürfen.
- Daten dürfen auch innerhalb des BfV nicht schrankenlos weitergegeben werden, was vor allem bei Daten bedeutsam ist, die im Rahmen von Mitwirkungsaufgaben erhoben werden (vgl. dazu auch Abschnitt 15.2).
- Die Regelung über nachrichtendienstliche Mittel legt nicht präzise fest, gegen wen sie gerichtet werden dürfen und welche Rechtseingriffe dabei erlaubt sind.
- Das Gesetz sollte die Voraussetzungen für die wesentlichen Schritte der Automatisierung bestim-

men. Dies wäre um so notwendiger, als auch beim BfV verstärkt neue Datenverarbeitungsverfahren zum Einsatz kommen (vgl. dazu auch 19.3 und 19.4).

- Auch für manuelle Datensammlungen, wie Karteien und Akten, sind einschränkende Regelungen, z. B. zum Minderjährigenschutz, erforderlich.

- Der Gesetzgeber muß für die Speicherfristen sowie für die Fristen zur Überprüfung der Erforderlichkeit von Dateien einen Rahmen vorgeben.

- Das Recht des Bürgers auf Auskunft sollte — mit den für die Aufgabenerfüllung der Verfassungsschutzbehörden unerläßlichen Einschränkungen — auch gegenüber diesen Behörden bestehen, bereichsspezifisch im Verfassungsschutzgesetz geregelt werden und die neuere Rechtsprechung berücksichtigen (vgl. dazu 19.1).

Ich hoffe, daß die parlamentarische Beratung Gelegenheit bieten wird, diese und weitere Gesichtspunkte zu erörtern und den Gesetzentwurf einer auch unter Gesichtspunkten des Datenschutzes guten Lösung zuzuführen.

19.2 Ergebnis der Kontrolle bei der Abteilung V

Im Jahre 1986 habe ich die Datenverarbeitung bei der für die Durchführung von Sicherheitsüberprüfungen zuständigen Abteilung V des BfV kontrolliert. Über die dabei festgestellten erheblichen datenschutzrechtlichen Mängel und die unbefriedigende Stellungnahme des Bundesministers des Innern hierzu habe ich im Zehnten Tätigkeitsbericht (S. 81 f.) berichtet. Im Vorfeld der Beratungen der Berichterstattergruppe des Innenausschusses des Deutschen Bundestages zum Achten und Neunten Tätigkeitsbericht haben weitere Gespräche mit dem Bundesminister des Innern und dem BfV in dieser Sache stattgefunden. Dabei konnten entscheidende datenschutzrechtliche Verbesserungen erreicht werden, so daß bei der Neukonzeption der Datenverarbeitung bei der Abteilung V des BfV nahezu allen meinen Bedenken Rechnung getragen wurde.

Die Einzelheiten dieser Verbesserungen können im Detail aus Geheimhaltungsgründen hier nicht dargestellt werden. Von besonderer Bedeutung sind aber folgende Gesichtspunkte:

- Der Katalog der Merkmale, die im Anschluß an die Überprüfungsergebnisse gespeichert werden dürfen, wurde erheblich reduziert. Die von mir besonders kritisierte Speicherung von Daten aus der engeren Persönlichkeitsphäre wurde eingestellt; die über Straftaten spürbar eingeschränkt.

- Für die Zukunft ist ausgeschlossen, daß belastende Informationen gespeichert werden, deren Sicherheitsrelevanz offengeblieben oder verneint worden ist, vielmehr muß eine definierte Relevanzstufe bejaht worden sein.

- Durch geeignete Maßnahmen soll die Speicherung falscher, sich widersprechender oder zeitlich nicht zuordenbarer Merkmale verhindert werden.

- Der Zugriff auf die belastenden Merkmale im Wege der Einzelabfrage wurde erheblich eingeschränkt. Die Voraussetzungen für Querschnittsauswertungen des gesamten Bestandes und das Verfahren ihrer Anordnung wurden erheblich verschärft.

- Über den Dateiinhalt wird grundsätzlich nichts an Dritte übermittelt.

- Im Zusammenhang mit den neuen Sicherheitsrichtlinien wird auch routinemäßig überprüft, welche Personen noch in sicherheitsempfindlicher Position tätig sind; Datensätze anderer Personen werden gelöscht.

- Das BfV hat mir darüber hinaus zugesagt, Anfang 1989 auch die Forderung aus meinem Prüfbericht zu erfüllen, in der Sonderdatei die Datensätze aller Personen zu löschen, die nur wegen einer Dateianfrage (siehe dazu 4. TB S. 29) erfaßt worden waren.

Nachdem auch in einer Reihe weiterer Fragen meinen datenschutzrechtlichen Vorstellungen Rechnung getragen wurde, konnte ich dem Vorsitzenden der Berichterstattergruppe im Innenausschuß des Deutschen Bundestages in einem gemeinsamen Schreiben mit dem BMI mitteilen, daß durch die beschlossenen Maßnahmen alle wichtigen Beanstandungen und Kritikpunkte aus meinem Prüfbericht zur Abteilung V in bezug auf die Spezialdatei ausgeräumt sind. Der Bundesminister des Innern hat in diesem Schreiben bestätigt, daß die Neuregelung auch die Sicherheitsbelange voll wahrt.

19.3 Neue Verkartungspläne und Weiterentwicklung der Datenverarbeitung beim BfV

Als Ergebnis meiner Kontrolle bei der Abteilung III wurde deren Verkartungsplan, in dem im einzelnen geregelt ist, unter welchen Voraussetzungen personenbezogene Daten in Dateien gespeichert werden dürfen, grundlegend überarbeitet. Einzelne Fragen, über die in den Erörterungen zwischen dem Bundesamt für Verfassungsschutz und mir kein Einvernehmen erzielt worden war, konnten im Rahmen der Beratungen im Innenausschuß des Deutschen Bundestages einer Klärung zugeführt werden (vgl. dazu 19.4).

Der Bundesminister des Innern hatte nach meiner Kontrolle bei der Abteilung III angekündigt, auch die Verkartungspläne der anderen Abteilungen des BfV so zu ändern, daß sie den Grundsätzen des neu gestalteten Verkartungsplans der Abteilung III im wesentlichen entsprächen. Bislang ist mir lediglich der Entwurf eines neuen Verkartungsplans der Abteilung VI (Beobachtung extremistischer Bestrebungen von Ausländern) zugegangen, den ich im Laufe des Jahres mit dem BMI und dem BfV beraten habe. Er orientiert sich im wesentlichen an den bei der Abteilung III erreich-

ten Ergebnissen. Ich beabsichtige, mir nach Inkrafttreten des neuen Verkartungsplans bei der Abteilung VI ein Bild von der dortigen Speicherpraxis zu verschaffen.

Im Laufe dieses Jahres sind mir mehrere Konzeptionen für neue Dateien und Datenverarbeitungsverfahren beim BfV zugegangen, die über die Möglichkeiten der NADIS-Personenzentraldatei (NADIS-PZD) hinausgehen. Es handelt sich um Dateien, zu denen nur die jeweilige Fachabteilung Zugriff hat. Zumeist wird dabei zu der Frage, welche Personen in diesen Spezialdateien erfaßt werden dürfen, auf die Verkartungspläne verwiesen. Ich habe den BMI darauf hingewiesen, daß nach meiner Auffassung zunächst die Verkartungspläne neu und restriktiver gestaltet werden müssen, bevor an die Einrichtung neuer Dateien und Verfahren herangegangen wird.

Durch eine Kontrolle bei der Abteilung Staatsschutz des BKA (vgl. 16.3) ist mir bekannt geworden, daß die NADIS-PZD Ende 1987 neu konzipiert worden ist. Nach meinem ersten Eindruck handelt es sich bei NADIS-PZD-Neu in erster Linie um eine Modernisierung des bestehenden Verfahrens, die datenschutzrechtlich keine größeren Probleme aufwirft. Meine weiteren Nachforschungen haben allerdings neue Erkenntnisse in bezug auf NADIS-PZD-Alt ergeben. Dieses wurde bisher als bloßes Aktennachweissystem bewertet, da immer wieder darauf hingewiesen worden war, daß es nur Personengrunddaten und Fundstellen enthalte. Ich habe jetzt festgestellt, daß darüber hinaus weitere Daten gespeichert werden konnten und in bestimmten Fällen auch tatsächlich gespeichert wurden.

Mit der Einführung von NADIS-PZD-Neu am 1. Oktober 1987 wurde die Speicherung derartiger Daten zwar nicht eingestellt, der Zugriff auf die betreffenden Daten jedoch auf die jeweils eingebende Stelle beschränkt. Zur sachlichen Begründung wird angeführt, die Speicherung der Daten sei zu Identifizierungszwecken erforderlich. Eine entsprechende Formulierung findet sich für Verbunddateien der Verfassungsschutzbehörden in § 4 Abs. 2 des Entwurfs eines Bundesverfassungsschutzgesetzes. Bei dessen Beratung wird zu prüfen sein, in welchem Umfang die Speicherung von Daten zu Identifizierungszwecken notwendig ist und wie gegebenenfalls eine entsprechende gesetzliche Ermächtigung begrenzt werden kann.

19.4 Konsequenzen aus früheren Kontrollen

Im Zuge der Beratung meines Achten und Neunten Tätigkeitsberichts im Innenausschuß des Deutschen Bundestages wurden auch noch offene Punkte aus meiner Prüfung bei der Abteilung III des BfV diskutiert. In diesem Zusammenhang konnte ich in Gesprächen mit dem BMI und dem BfV meine Vorstellungen größtenteils zur Geltung bringen.

Durch eine Ergänzung der entsprechenden Dienstvorschrift ist nunmehr ausdrücklich festgelegt, daß vor der Weiterübermittlung von Informationen zu überprüfen ist, ob diese überhaupt noch relevant sind. Bei Informationen, die älter als ein Jahr sind und dem BfV von einer anderen Stelle übermittelt wurden, soll vor einer Weiterübermittlung nach Möglichkeit eine ergänzende Auskunft eingeholt werden, wenn Anlaß besteht, an ihrer Richtigkeit oder Vollständigkeit zu zweifeln. Ich hatte in der Vergangenheit wiederholt festgestellt, daß unvollständige Informationen, z. B. über eingeleitete Verfahren oder Verdachtsfälle, weiterübermittelt wurden, ohne daß zuvor bei der ursprünglich meldenden Stelle nachgefragt worden wäre, ob sich der Verdacht bestätigt hat.

Ferner hatte ich früher bemängelt, daß in zusammenfassenden Lageberichten personenbezogene Daten enthalten waren, ohne daß dies in jedem Fall erforderlich war. Bei derartigen Lageberichten steht zum Zeitpunkt ihrer Abfassung nicht immer fest, an welche Empfänger sie übersandt werden. Ich habe in einzelnen Fällen auch festgestellt, daß solche Berichte ausländischen Nachrichtendiensten zugänglich gemacht worden sind. Durch eine Änderung der entsprechenden Dienstvorschrift des BfV ist nunmehr ausdrücklich klargestellt worden, daß personenbezogene Daten in Berichte des BfV für inländische und ausländische Behörden nur aufgenommen werden, wenn dies erforderlich ist und schutzwürdige Belange betroffener Personen dabei berücksichtigt sind. Ich gehe davon aus, daß es bei derartigen Berichten in der Regel genügt, wenn Personen ohne Namensnennung mit ihrer politischen Funktion beschrieben werden, so daß die Notwendigkeit der Aufnahme personenbezogener Daten in derartige Berichte die Ausnahme ist.

Ich konnte auch erreichen, daß Daten, die im Rahmen einer Sicherheitsüberprüfung erhoben worden sind, nur noch in geringerem Umfang an ausländische Nachrichtendienste übermittelt werden. Die Dienstvorschrift über die Beziehungen des BfV zu ausländischen Nachrichtendiensten wurde dahin ergänzt, daß Daten, die den Bereich der persönlichen Lebensführung betreffen, an diese nur noch für Zwecke der Sicherheitsüberprüfung und der Spionageabwehr übermittelt werden dürfen.

Das BfV wird von ausländischen Nachrichtendiensten nicht selten um Übermittlung von Informationen ersucht, die für eine dort durchzuführende Sicherheitsüberprüfung benötigt werden. Bei einer Sicherheitsüberprüfung nach deutschem Recht ist dem Betroffenen rechtliches Gehör zu gewähren, falls seine Ermächtigung zum Umgang mit Verschlußsachen abgelehnt werden soll. Dies ist nicht in allen Ländern so, an deren Nachrichtendienste das BfV Daten zum Zwecke der Sicherheitsüberprüfung übermittelt.

Nach meiner Auffassung wäre es notwendig, daß das BfV entweder auf der Gewährung von rechtlichem Gehör durch die dortigen Behörden besteht oder aber selbst dem Betroffenen rechtliches Gehör gewährt, wenn es belastende Daten über ihn an einen ausländischen Nachrichtendienst übermittelt. Immerhin konnte ich nunmehr erreichen, daß das BfV alle ausländischen Nachrichtendienste angeschrieben und sie gebeten hat, entsprechend den Regelungen in der Bundesrepublik Deutschland den Betroffenen rechtliches Gehör zu geben, wenn ihre Ermächtigung zum Umgang mit Verschlußsachen aufgrund von Informationen abgelehnt werden soll, die vom BfV übermittelt

worden sind. Es bleibt abzuwarten, ob dies eine ausreichende Maßnahme ist, um die schutzwürdigen Belange der Betroffenen zu gewährleisten.

20. Bundesnachrichtendienst

20.1 Einrichtung von Dateien

Der Präsident des Bundesnachrichtendienstes hat mit Zustimmung des Staatssekretärs beim Bundeskanzler eine Weisung für die Einrichtung personenbezogener Dateien beim BND gegeben, an deren Vorbereitung ich beteiligt war. Danach bedürfen die Einrichtung neuer und die Erweiterung bestehender Dateien mit personenbezogenen Daten einer förmlichen Einrichtungsanordnung des Präsidenten, die dieser nach Zustimmung durch den Staatssekretär beim Bundeskanzler erteilt. Die Weisung zielt darauf ab, daß die datenschutzrelevanten Aspekte im Entscheidungsverfahren besonders beachtet werden. Die praktische Anwendung werde ich überprüfen.

20.2 Gesetz über den Bundesnachrichtendienst

Mitte Oktober hat mir der Staatssekretär beim Bundeskanzler den Entwurf eines Gesetzes über den Bundesnachrichtendienst zugeleitet. Aus der Sicht des Datenschutzes ist es zu begrüßen, daß die Bundesregierung nunmehr vorgesehen hat, auch die informationsverarbeitende Tätigkeit des Bundesnachrichtendienstes in einem eigenen Gesetz zu regeln. In meiner Stellungnahme zu dem Gesetzentwurf habe ich insbesondere auf folgende Punkte hingewiesen:

Die begrüßenswerte Klarstellung, daß der Bundesnachrichtendienst auf innenpolitischem Gebiet nicht tätig wird, sollte durch einschränkende Regelungen zur Informationserhebung, -speicherung und -nutzung konkretisiert werden. Zur Verwirklichung des Zweckbindungsgrundsatzes sollte das Gesetz nähere Vorgaben enthalten. Auch im Rahmen der außen- und sicherheitspolitischen Berichterstattung sollte sich die Verwendung personenbezogener Angaben am Grundsatz der Erforderlichkeit und Eignung orientieren. Der Entwurf verweist in großem Umfang auf den Entwurf des Bundesverfassungsschutzgesetzes, zu dem ich gesondert Stellung genommen habe (vgl. 19.1).

21. Verteidigung

21.1 Militärischer Abschirmdienst

21.1.1 MAD-Gesetz

Das Kabinett hat Ende des Berichtsjahres den Entwurf für ein MAD-Gesetz beschlossen. Ich begrüße es ausdrücklich, daß damit die Arbeit des MAD erstmals umfassend gesetzlich geregelt werden soll. Für den MAD ist es besonders wichtig, daß darüber hinaus eine bereichsspezifische Rechtsgrundlage für die Sicherheitsüberprüfung geschaffen wird. Mit rund 200 000 Sicherheitsüberprüfungen pro Jahr ist der MAD zum weit überwiegenden Teil auf diesem Gebiet tätig. Die auf der Grundlage von Sicherheitsüberprüfungen vorgenommenen Speicherungen gehen in die Millionen. Die einschlägigen Bestimmungen des MAD-Gesetzentwurfs reichen indessen nicht aus, da sie keine Regelung darüber enthalten, wer in eine Sicherheitsüberprüfung einbezogen werden darf, wer für die Durchführung der Sicherheitsüberprüfung zuständig ist, welche informationellen Eingriffe in diesem Zusammenhang zulässig sind und was mit den erhobenen Daten geschehen kann. Insbesondere fehlt eine Regelung, die eine schrankenlose Weitergabe dieser Daten auch innerhalb des MAD und der Nachrichtendienste ausschließt.

Mir wurde der Entwurf für ein MAD-Gesetz vor der Kabinettvorlage zur Kenntnisnahme übersandt. Ich habe die Gelegenheit genutzt und eine Stellungnahme abgegeben. Daraufhin wurde der Gesetzentwurf in einem für mich zentralen Punkt überarbeitet. Der Wortlaut schließt jetzt — dies ist erfreulich — eindeutig aus, daß beim MAD erneut Datensammlungen nach der Art der von mir beanstandeten und inzwischen vernichteten „Basiskartei Zersetzung" (vgl. 7. TB S. 81) entstehen dürfen.

In einigen weiteren Punkten sind meine Vorstellungen bislang aber nicht berücksichtigt worden. Es geht dabei insbesondere darum, daß das MAD-Gesetz nur wenige eigenständige Regelungen enthält, während vor allem bei den Datenverarbeitungsbefugnissen zumeist pauschal auf das Verfassungsschutzgesetz verwiesen wird. Die gewählte komplizierte Verweisungstechnik macht es dem Bürger schwer zu erkennen, welche Daten der MAD bei welcher Gelegenheit über ihn verarbeiten darf.

Aber auch inhaltlich habe ich Zweifel, ob der MAD wirklich sämtliche Befugnisse haben muß, die den Verfassungsschutzbehörden zustehen sollen. In der Begründung zum Entwurf wird darauf verwiesen, daß der MAD im Geschäftsbereich des Bundesministers der Verteidigung Funktionsträger des Verfassungsschutzes sei. Allerdings gilt dies nur mit Einschränkungen. Die Beobachtung verfassungsfeindlicher Bestrebungen obliegt dem MAD beispielsweise nur dann, wenn diese sich unmittelbar gegen Dienststellen oder Einrichtungen im Geschäftsbereich des BMVg richten und von Personen aus diesem Bereich ausgehen. Es ist nicht zwingend, aus der Ähnlichkeit der Aufgaben darauf zu schließen, daß die gleichen Befugnisse zur Verfügung stehen müssen. Vielmehr ist zu berücksichtigen, daß das Operationsgebiet des MAD anders strukturiert ist als das der Verfassungsschutzbehörden. Im militärischen Bereich besteht ein stark ausgebildetes Meldewesen, das dem MAD einen beträchtlichen Informationszugang garantiert. Hinzu kommt, daß der MAD mit dem Mittel der förmlichen Befragung viel leichter Daten beim Betroffenen erheben kann als die Verfassungsschutzbehörden. Bei Verdachtsfällen wird davon regelmäßig Gebrauch gemacht.

Daß die pauschale Übernahme der Befugnisse der Verfassungssungsschutzbehörden für den MAD nicht geboten ist, zeigt sich etwa bei der Registereinsicht. Ich bin der Auffassung, daß eine umfassende Befugnis

zur Einsicht in alle Register der Verwaltung für die Erfüllung aller Aufgaben schon bei den Verfassungsschutzbehörden nicht erforderlich ist. Dies gilt um so mehr für den MAD, der sich im wesentlichen nur mit Angehörigen der Bundeswehr befaßt. Über diese bestehen im Verteidigungsbereich umfangreiche Dateien, aus denen der MAD Informationen erhalten kann. Auch in einigen weiteren Punkten halte ich den Gesetzentwurf noch für überarbeitungs- und präzisierungsbedürftig.

21.1.2 Datenschutzrechtliche Kontrolle beim MAD

Im Berichtsjahr habe ich eine Querschnittskontrolle beim Amt für den MAD durchgeführt. Schwerpunkte waren die Nachprüfung der Einhaltung früher gemachter Zusagen und die Datenverarbeitung im Abwehrbereich „Verfassungsfeindliche Kräfte" . Dazu kamen einzelne Aspekte der Datenverarbeitung bei den anderen Abteilungen. Nach meinem Gesamteindruck beschränkt sich der MAD nunmehr auf Bundeswehrangehörige, so daß Datensammlungen nach der Art der „Basiskartei Zersetzung" (vgl. dazu 7. TB S. 80f.) nicht mehr betrieben werden. Eine Reihe von mir empfohlener Verbesserungen wurde umgesetzt. Die Aufgeschlossenheit gegenüber dem Datenschutz ist beim MAD nach wie vor ausgeprägt. Gleichwohl habe ich wiederum einige Mängel beanstandet und neue Maßnahmen zur Verbesserung des Datenschutzes vorgeschlagen.

Der Bundesminister der Verteidigung hat mir kurz vor der Fertigstellung dieses Tätigkeitsberichts eine erste Stellungnahme zugehen lassen. Er hat darin die Berechtigung meiner Einzelbeanstandungen anerkannt und die Löschung der entsprechenden Datensätze mitgeteilt. Zu einer Reihe von Fragen erwarte ich noch die ergänzende Stellungnahme des Bundesministers der Verteidigung.

Als Konsequenz aus meiner Kontrolle im Jahre 1982 prüft eine Arbeitsgruppe des MAD alle Akten und die darauf beruhenden Dateispeicherungen. Allerdings ist diese Arbeitsgruppe personell unzureichend ausgestattet. Nach eigenen Berechnungen benötigt sie bis zur Beendigung der Bereinigungsarbeiten noch acht bis zehn Jahre. Dies kann ich nicht akzeptieren. Auch der Bundesminister der Verteidigung hält den zeitlichen Ablauf der Bereinigungsarbeiten für unbefriedigend. Er hat Maßnahmen angekündigt, die die Bereinigung so beschleunigen sollen, daß in spätestens zwei Jahren sämtliche Altfälle des MAD überprüft und unzulässige Speicherungen korrigiert sind. Dieser Zeitraum ist auch nach meinen Vorstellungen noch vertretbar.

Nach der derzeit gültigen zentralen Weisung für seine Arbeit wie auch auch nach dem Entwurf für ein MAD-Gesetz müssen für ein Tätigwerden des MAD drei Voraussetzungen kumulativ vorliegen:

- Es muß sich um geheimdienstliche Tätigkeiten für eine fremde Macht oder Bestrebungen und Tätigkeiten handeln, die gegen die freiheitlich demokratische Grundordnung oder den Bestand und die Sicherheit des Bundes gerichtet sind.
- Sie müssen unmittelbar gegen die Bundeswehr gerichtet sein.
- Sie müssen von Angehörigen der Bundeswehr oder anderen im Geschäftsbereich des Bundesministers der Verteidigung beschäftigten Personen ausgehen.

Ich habe 1988 die im Abwehrbereich „Verfassungsfeindliche Kräfte" (VfK) in einem bestimmten Zeitraum angelegten Ermittlungsvorgänge überprüft und statistisch ausgewertet. Dabei stellte sich heraus, daß am Beginn der Ermittlungen in ca. vier Fünfteln der Fälle keine konkret unmittelbar gegen die Bundeswehr gerichteten extremistischen Handlungen vorlagen. Ausgangspunkt der Bearbeitung waren vielmehr in fast jedem zweiten Fall Informationen, die im Rahmen einer Sicherheitsüberprüfung angefallen, im übrigen in der Regel Informationen, die dem MAD von anderen Sicherheitsbehörden übermittelt worden waren. Zumeist handelt es sich dabei um Hinweise auf eine extremistische Betätigung von Bundeswehrangehörigen.

Die Ermittlungen des MAD haben in fast jedem zweiten aller Fälle ergeben, daß der Verdacht extremistischer Bestrebungen widerlegt bzw. ausgeräumt werden konnte. In etwa einem Viertel der Fälle ist es letztlich offengeblieben, ob der Verdacht zutraf oder nicht. Lediglich im verbleibenden Viertel ergaben die Recherchen, daß sich die Person in einer extremistischen Organisation betätigte. Diese Betätigung hatte aber nur in seltenen Fällen etwas mit der Bundeswehr zu tun. Zum großen Teil handelte es sich um die Mitgliedschaft in einer Organisation, deren Tätigkeit gegen die freiheitlich demokratische Grundordnung gerichtet und die von den Verfassungsschutzbehörden als Beobachtungsobjekt eingestuft ist. Im Ergebnis fehlte es bei der weit überwiegenden Zahl der von mir insgesamt ausgewerten Fälle objektiv an der Voraussetzung einer „unmittelbar gegen die Bundeswehr gerichteten Bestrebung". Gleichwohl war stets, wenn im Ermittlungszusammenhang auch gegen eine der Wehrüberwachung unterliegende Person ermittelt wurde, eine Speicherung in der Personenzentraldatei des MAD veranlaßt worden. Bei Bestätigung des Verdachts einer extremistischen Betätigung, auch wenn diese sich nicht unmittelbar gegen die Bundeswehr richtete, wurde eine fünfjährige Speicherung verfügt, bei Ausräumung des Verdachts sogar zehn Jahre, was besonders unverhältnismäßig erscheint.

Ich habe den Bundesminister der Verteidigung aufgefordert, diese Regelungen zu überprüfen. Auch wenn man akzeptiert, daß der MAD als Nachrichtendienst bereits beim Verdacht, daß eine unmittelbar gegen die Bundeswehr gerichtete extremistische Bestrebung vorliegen könnte, tätig wird, so dürfen seine Ermittlungen jedenfalls dann, wenn sie die Unzuständigkeit des MAD ergeben haben, nicht zu einer mehrjährigen Speicherung in den Dateien des MAD führen. Ich habe vorgeschlagen, statt dessen die (ursprünglich) meldende Stelle davon zu unterrichten, daß der Verdacht entkräftet wurde. Im übrigen halte ich eine Speicherung derartiger Fälle höchstens nur bis zum Ende der aktiven Bundeswehrzeit des Betreffenden für zulässig. Der Bundesminister der Verteidigung hat angekündigt, daß er die entsprechenden innerdienst-

lichen Vorschriften ändern und mich dabei beteiligen will.

Überprüft wurde auch, unter welchen Voraussetzungen beim MAD Operationen mit nachrichtendienstlichen Mitteln durchgeführt werden. Aufgrund einiger Beispielsfälle habe ich den Eindruck, daß die Schwelle für den Einsatz nachrichtendienstlicher Mittel — auch gemessen am MAD-Gesetzentwurf — manchmal zu niedrig angesetzt wird. Ich bin der Auffassung, daß der Einsatz nachrichtendienstlicher Mittel einen besonders schweren Eingriff bedeutet, der nur unter besonderen Voraussetzungen in Betracht kommen kann. Dies gilt für den MAD umso mehr, als er für seine Tätigkeit derzeit keine gesetzliche Grundlage hat. Zudem hat der MAD durch die Einbettung in die Bundeswehr objektiv bessere Möglichkeiten des Nachrichtenzugangs als andere Nachrichtendienste, so daß ein Rückgriff auf nachrichtendienstliche Mittel seltener notwendig ist. Ich habe deshalb vorgeschlagen, die innerdienstlichen Vorschriften für den Einsatz nachrichtendienstlicher Mittel im Hinblick auf den MAD-Gesetzentwurf zu revidieren und die Praxis des Einsatzes nachrichtendienstlicher Mittel vorerst einzuschränken. Der Bundesminister der Verteidigung hat auch insoweit angekündigt, die entsprechenden Vorschriften unter meiner Beteiligung zu überarbeiten. Zu einer Reihe weiterer Punkte meines Prüfvermerks, wie etwa zur Anwesenheit von Mitarbeitern des Verfassungsschutzes bei Befragungen durch MAD-Angehörige, zur Beachtung des Postgeheimnisses und zum Modus der Berechnung der Speicherfristen liegt noch keine Äußerung vor.

Ich habe auch die Frage der Zweckbindung von Daten aufgeworfen, die der MAD im Rahmen der Sicherheitsüberprüfung erhebt. Anlaß hierzu bot die Praxis des Abwehrbereichs „Verfassungsfeindliche Kräfte", immer dann einen eigenen Ermittlungsvorgang anzulegen und eigene — d. h. zusätzliche — Speicherungen in der Personenzentraldatei vorzunehmen, wenn im Rahmen einer Sicherheitsüberprüfung im Auftrag der hierfür zuständigen Abteilung I eine Person befragt wurde. Eigene Vorgänge des Abwehrbereichs „Verfassungsfeindliche Kräfte" werden in solchen Fällen auch dann angelegt, wenn der Betroffene seine Mitgliedschaft in einer extremistischen Organisation selbst angegeben hat oder wenn die Ermittlungen ergeben haben, daß ein extremistischer Verdacht nicht besteht. Der BMVg hat die Änderung dieser Praxis zugesagt.

Wie bereits erwähnt (vgl. 15.2), habe ich Fälle beanstandet, in denen Daten aus der Sicherheitsüberprüfung, die die private und familiäre Sphäre des Betroffenen betrafen, an andere Sicherheitsbehörden übermittelt worden sind. Dabei handelt es sich nicht um Einzelfälle. Vielmehr verpflichtet die Arbeitsvorschrift des MAD ausdrücklich dazu, daß Informationen, die für andere Nachrichtendienste „von Interesse sein könnten", diesen zu übermitteln. Der Bundesminister der Verteidigung hat die Berechtigung meiner Beanstandungen in den Einzelfällen anerkannt und eine Überarbeitung der Arbeitsvorschrift angekündigt, vertritt allerdings weiterhin die Auffassung, daß Daten aus der Sicherheitsüberprüfung grundsätzlich für alle Zwecke des MAD und des Verfassungsschutzes verwendet werden dürften. Er beruft sich dabei auf die Sicherheitsrichtlinien des Bundes.

21.1.3 Neukonzeption der Merkmalspeicherung

Auch beim MAD werden, vergleichbar mit der unter 19.2 erwähnten Spezialdatei des BfV, Erkenntnisse aus Sicherheitsüberprüfungen in Form von Merkmalen gespeichert. Bei einer Überprüfung dieser Merkmalspeicherung im Jahre 1982 hatte ich erhebliche datenschutzrechtliche Mängel beanstandet (vgl. dazu 5. TB, S. 95 ff.). Meine Kritik hatte sich vor allem gegen solche Merkmale gerichtet, die die Privat- und Intimsphäre betrafen.

In Verhandlungen mit dem BMVg habe ich erreicht, daß auf die Speicherung derartiger Merkmale auch bei der Neukonzeption verzichtet wird. Darüber hinaus wurden u. a. folgende Verbesserungen erzielt:

- Der Zweck der Merkmalspeicherung wurde definiert. Der Zugriff darf nur noch im Rahmen dieser Zweckbestimmung erfolgen. Nicht alle Abwehrbereiche des MAD erhalten Zugriff auf alle Merkmalsgruppen. Der differenzierte Zugriff wird sowohl technisch als auch auf dem Befehlswege sichergestellt.
- Merkmale dürfen in Zukunft nur noch gespeichert werden, wenn sie sicherheitsrelevant sind, mit hoher Wahrscheinlichkeit zutreffen und durch Akten belegt sind. Bei früheren Kontrollen hatte ich festgestellt, daß Merkmale gespeichert waren, obwohl eine oder mehrere dieser Voraussetzungen nicht vorlagen.
- Die Entscheidung über die Speicherung von Merkmalen ist in einigen Fällen dem Dezernatsleiter vorbehalten.
- Recherchen und Querschnittsabfragen in diesem Datenbestand sind nur durch das Amt für den MAD selbst zulässig. Derartige Auswertungen dürfen nur durch die für Sicherheitsüberprüfungen und für die Spionageabwehr zuständigen Abteilungen, nicht aber durch die nachgeordneten MAD-Einheiten erfolgen.
- Gespeicherte Merkmale, die mit der Neukonzeption nicht übereinstimmen, werden gelöscht.

Ich habe dem Bundesminister der Verteidigung mitgeteilt, daß gegen die Neukonzeption jetzt keine datenschutzrechtlichen Bedenken mehr bestehen.

21.2 Wehrpflichtige und Soldaten

Im Berichtszeitraum habe ich zwei Kreiswehrersatzämter, vier Dienststellen des Bundesministers der Verteidigung in den USA und das Sozialwissenschaftliche Institut der Bundeswehr kontrolliert und beraten. Ein Schwerpunkt war hierbei die technische und organisatorische Datensicherung. Über die wichtigsten Ergebnisse der Kontrollen und Beratungen berichte ich nachfolgend im einzelnen.

Weiterhin haben sich regelmäßige Besprechungen beim Bundesminister der Verteidigung bewährt, in denen Probleme aus Eingaben zu diesem Geschäftsbereich sowie Fragen der Durchsetzung datenschutzrechtlicher Forderungen diskutiert und — wenn möglich — Lösungen zugeführt werden. Bei den Eingaben bildet nach wie vor der Umgang mit Gesundheits-Unterlagen einen Schwerpunkt der Besorgnisse der Betroffenen.

21.2.1 Musterung in Verbindung mit der Eignungs- und Verwendungsprüfung

Der Bundesminister der Verteidigung erprobt in drei Kreiswehrersatzämtern zum Teil schon seit 1985, ob sich die Musterung und die Eignungs- und Verwendungsprüfung (EVP) der Wehrpflichtigen, d. h. die Prüfung auf ihre Eignung für bestimmte Verwendungen bei der Bundeswehr nach § 20 a des Wehrpflichtgesetzes (WPflG), *an einem Tag* durchführen lassen (s. auch 9. TB S. 65 f.). Mit der Zusammenfassung der beiden unterschiedlichen Verfahren sollen Zeit und Kosten der Wehrpflichtigen, der Arbeitgeber und der Bundeswehr eingespart werden. Ich habe den Ablauf der Erprobung in einem der drei Kreiswehrersatzämter kontrolliert. Hierbei habe ich einen Verstoß gegen § 20 a Abs. 1 Satz 1 WPflG festgestellt, den ich beanstandet habe:

In dem von mir kontrollierten Kreiswehrersatzamt wurde nach der Aufnahme der Personalien für die Musterung gemeinsam mit dem jeweiligen Wehrpflichtigen der sog. EVP-Personalbogen ausgefüllt, der über die unmittelbaren Belange der Musterung hinausgehende Fragen u. a. nach bestimmten Vorkenntnissen (z. B. Fernmeldekenntnisse) oder nach dem Hobby des Wehrpflichtigen enthält; diese Angaben sind für den Wehrpsychologen von Bedeutung. Der größte Teil der für einen Tag geladenen Wehrpflichtigen wurde anschließend gemustert und — bei Feststellung der Wehrdienstfähigkeit im Musterungsbescheid — sodann auf die Eignung für bestimmte Verwendungen bei der Bundeswehr überprüft.

Einige Wehrpflichtige wurden jedoch — nach Erklärung ihrer Einwilligung — bereits Tests der Eignungs- und Verwendungsprüfung unterzogen, *bevor* das Ergebnis der Musterung feststand. Ergab die — am selben Tage durchgeführte — Musterung, daß diese Wehrpflichtigen „vorübergehend nicht wehrdienstfähig" oder „nicht wehrdienstfähig" waren (§ 8 a Abs. 1 WPflG), wurden die im Rahmen der Eignungs- und Verwendungsprüfung angefallenen Unterlagen unverzüglich vernichtet.

Das Ausfüllen der sog. EVP-Personalbogen bereits im Zusammenhang mit der Erhebung der Personalien für die Musterung und die Durchführung von Tests für die Eignungs- und Verwendungsprüfung bei noch nicht gemusterten Wehrpflichtigen widersprechen § 20 a Abs. 1 Satz 1 WPflG. Nach dieser Vorschrift dürfen nur solche Wehrpflichtige einer Eignungs- und Verwendungsprüfung unterzogen werden, „die nach dem Musterungsbescheid *wehrdienstfähig* sind". Damit soll sichergestellt werden, daß die Erhebung und die Verarbeitung der besonders schützenswerten Daten aus der Eignungs- und Verwendungsprüfung nur bei Wehrpflichtigen erfolgen, bei denen dies auch erforderlich ist. Der Verstoß gegen § 20 a Abs. 1 Satz 1 WPflG wird durch eine Einwilligungserklärung der noch nicht gemusterten Wehrpflichtigen nicht geheilt. Der Gesetzgeber hat den Kreis der Wehrpflichtigen, die einer Eignungs- und Verwendungsprüfung unterzogen werden dürfen, eindeutig begrenzt. Dementsprechend ist schon die Frage der Bundeswehrverwaltung an die noch nicht gemusterten Wehrpflichtigen nach einer Einwilligung in eine vorgezogene Eignungs- und Verwendungsprüfung unzulässig. Ebensowenig können die Betroffenen die Entscheidung des Gesetzgebers in § 20 a Abs. 1 WPflG mit ihrer Einwilligungserklärung außer Kraft setzen.

Eine Antwort des Bundesministers der Verteidigung auf meine gegen Ende des Jahres 1988 ausgesprochene Beanstandung lag mir zum Zeitpunkt der Erstellung dieses Berichts noch nicht vor. Ich gehe jedoch davon aus, daß das Verfahren in dem kontrollierten Kreiswehrersatzamt zwischenzeitlich so geändert wurde, daß nur noch wehrdienstfähige Wehrpflichtige einer Eignungs- und Verwendungsprüfung unterzogen werden. Dies wurde mir bereits während der Kontrolle zugesagt.

21.2.2 Sozialwissenschaftliches Institut der Bundeswehr — Umfrage „Soldaten als Mandatsträger"

Das Sozialwissenschaftliche Institut der Bundeswehr (SOWI) hat Ende 1987/Anfang 1988 im Auftrag des Bundesministers der Verteidigung unter Soldaten, die ein politisches Mandat ausüben, eine Umfrage durchgeführt. Von den Ergebnissen erhofft sich die Bundeswehr u. a. „mehr Verständnis für die Doppelfunktion von Soldat und Mandat in der Bundeswehr und in der Öffentlichkeit". Die Befragung erfolgte mit einem umfangreichen Fragenkatalog (68 Fragen), der an die Privatadresse der Betroffenen geschickt wurde. Die Beantwortung der Fragen war freigestellt.

Die Umfrage wurde in der Öffentlichkeit zum Teil heftig angegriffen. Es wurde behauptet, sie sei verfassungswidrig und die zugesicherte Anonymität könne nicht eingehalten werden, da die Namen der Befragten jederzeit leicht rekonstruiert werden könnten. Vor diesem Hintergrund bin ich von mehreren Seiten, auch vom Wehrbeauftragten des Deutschen Bundestages, um eine datenschutzrechtliche Beurteilung gebeten worden und habe das SOWI bei einem Besuch vor Ort in Fragen des Datenschutzes insbesondere zur Umfrage „Soldaten als Mandatsträger" und deren Auswertung beraten.

Da die Datenerhebung zu diesem Zeitpunkt bereits abgeschlossen war, konnten Empfehlungen für die notwendige vorausgehende *Information der Befragten* über den Zweck der Erhebung, deren Durchführung und die spätere Verarbeitung der erhobenen Daten nur noch mit Blick auf mögliche künftige Befragungen gegeben werden. Um dem Betroffenen für eine freiwillige Teilnahme an einer Erhebung die bestmögliche Entscheidungsgrundlage zu geben, sollte ihm mehr noch als bisher transparent gemacht werden, für welche Aufgaben/Zwecke seine Daten

benötigt werden und wie diese verarbeitet werden sollen.

Für die datenschutzrechtliche Beurteilung der genannten Umfrage ist wesentlich, welche Anforderungen an den Umgang mit den Original-Erhebungsbogen, an die automatisierte Datei „Mandatsträger", in der bestimmte Daten aus diesen Bogen gespeichert werden, und an die Auswertung des Materials zu stellen sind:

Die Sammlung der *Original-Erhebungsbogen* ist eine Datei im Sinne des § 2 Abs. 3 Nr. 3 BDSG. Sie ist besonders schützenswert, weil sie sog. Überzeugungsdaten (politische Anschauungen und Überzeugungen) enthält. Die technischen und organisatorischen Maßnahmen zu ihrer Sicherung nach § 6 BDSG müssen somit einen hohen Standard aufweisen. Das SOWI ist meinen Empfehlungen zu einer sicheren Aufbewahrung der Original-Erhebungsbogen gefolgt.

Die Original-Erhebungsbogen sind zu vernichten, sobald die zur automatisierten Speicherung vorgesehenen Daten erfaßt und die geplanten Auswertungen abschließend festgelegt sind. Zukünftig sollen Auswertungen so rechtzeitig festgelegt werden, daß die Original-Antwortbelege nach der Übernahme plausibler Daten auf maschinenlesbare Träger vernichtet werden können. Zum Zeitpunkt der Fertigstellung dieses Berichts waren die Original-Erhebungsbogen noch nicht vernichtet, weil noch nicht feststand, welche Angaben und handschriftlichen Ergänzungen in diesen Bogen auf welche Weise bei den Auswertungen berücksichtigt werden. Aufgrund der hohen Bedeutung der Studie kann dies akzeptiert werden.

Ich sehe einen weiteren Konflikt: Das Bundesarchiv — Militärarchiv — beansprucht die erhobenen Daten, obwohl die Befragten bei ihrer Einwilligung in die Erhebung nicht darauf hingewiesen wurden, daß ihre Antworten grundsätzlich unbefristet beim Bundesarchiv aufbewahrt werden können.

Die *automatisierte Datei „Mandatsträger"* wird im Rechenzentrum der Bundeswehr (RzBw) in München geführt. Das SOWI ist mit dem RzBw über eine Standleitung verbunden. Mängel bei der Datenverarbeitung konnte ich nicht feststellen; ich habe jedoch einige grundsätzliche Empfehlungen zur Verbesserung der Zugriffssicherheit gegeben, die allerdings nur zusammen mit dem Bundesministerium der Verteidigung realisiert werden können (siehe auch unten 21.2.4).

Zur Wahrung des informationellen Selbstimmungsrechts der Befragten habe ich auch unter Berücksichtigung der grundrechtlich geschützten Interessen von Wissenschaft und Forschung (Art. 5 GG), namentlich für die Auswertung der Studie über die Mandatsträger, Empfehlungen gegeben. Da es sich bei den Befragten um eine kleine Gruppe von Personen handelt, die dazu noch besonders schützenswerte Daten (Überzeugungen, Bekenntnisse) offenbart haben, müssen die vorliegenden Rohdaten sowohl formal als auch inhaltlich äußerst sorgfältig behandelt werden, bevor Ergebnisse in die Studie eingehen. So wird es z. B. bei der Bildung von Gruppen, über die die Studie Aussagen treffen soll, wie auch bei Betrachtung der Zahl derjenigen, die den jeweiligen Gruppen zuzuordnen sind, darauf ankommen, daß die Betroffenen nicht bestimmbar sind, die Studie also tatsächlich nur anonyme Aussagen trifft.

Grundlage für empirische Untersuchungen in der Bundeswehr ist der Erlaß „Empirische Untersuchungen zur Einstellungs-, Meinungs- und Verhaltensforschung in der Bundeswehr" (VMBl 1980 S. 523). Dieser Erlaß ist noch vor dem Volkszählungsurteil des Bundesverfassungsgerichts ergangen. Aufgrund dieser Entscheidung sind an die Verarbeitung personenbezogener Daten höhere Anforderungen zu stellen. Ich habe dem BMVg empfohlen, den Erlaß zu präzisieren und den Anforderungen des Volkszählungsurteils anzupassen. Dies wurde mir zugesagt.

21.2.3 Umgang mit Gesundheitsunterlagen

Bereits seit mehreren Jahren versuche ich zu erreichen, daß für die verschiedenen Arten von Gesundheitsunterlagen entsprechend dem Grad ihrer Sensibilität differenzierende Aufbewahrungsvorschriften geschaffen werden (s. 10. TB S. 86). Der Bundesminister für Jugend, Familie, Frauen und Gesundheit hat mir hierzu lediglich mitgeteilt, es bestünden keine Bedenken, vom ärztlichen Standesrecht abweichende Regelungen zu treffen. Diese Aussage reicht jedoch nicht aus, um bei der Aufbewahrung von Gesundheitsunterlagen Interessen militärischer Einsatzbereitschaft, ärztliche Pflichten sowie Rechte und schutzwürdige Belange der Betroffenen in einen angemessenen Ausgleich zu bringen. Ich gehe davon aus, daß vom Bundesminister der Verteidigung noch im Laufe des Jahres 1989 für seinen Bereich Regelungen entwickelt werden, die unterschiedliche Aufbewahrungsfristen festlegen sollen. Wesentliches Unterscheidungsmerkmal soll dabei sein, ob es sich um Gesundheitsunterlagen handelt, die als Gutachten zu werten sind, oder um Unterlagen, die für Behandlungen notwendig sind (z. B. laufende Eintragungen in der Gesundheits-Karte). Über dieses Ergebnis konnte ich dem Verteidigungsausschuß des Deutschen Bundestages in seiner Sitzung am 9. November 1988 berichten.

Ebenfalls zugesagt wurde mir, daß der Vordruck „Gesundheitliche Vorgeschichte", der von jedem Wehrpflichtigen im Rahmen der Musterung gemeinsam mit dem Musterungsarzt ausgefüllt und vom Betroffenen unterschrieben wird, datenschutzgerechter gestaltet wird. So soll für den Betroffenen aus dem Vordruck zu entnehmen sein, aufgrund welcher Rechtsvorschrift ihm die Fragen zu seiner gesundheitlichen Vorgeschichte gestellt werden und an wen die Durchschriften des Vordrucks gehen. Auch soll der Betroffene unterrichtet werden, daß die Frage nach Geschlechtskrankheiten nicht auch AIDS umfaßt. Zu letzterem Problem besteht, wie ich Fragen einer Schülerbesuchergruppe eines Abgeordneten in meinem Hause entnehmen konnte, eine gewisse Verunsicherung.

Auch die sog. Ladungskarte mit der der Wehrpflichtige aufgefordert wird, Gesundheitsunterlagen zur Musterung mitzubringen, soll datenschutzgerecht gestaltet werden. Sie enthält bisher keine Information

darüber, daß der Betroffene grundsätzlich selbst entscheiden kann, ob er diese Unterlagen dem Musterungsarzt überläßt. Wenn er sie dem Musterungsarzt überläßt und später Widerspruch gegen das Musterungsergebnis einlegt, werden diese Unterlagen Bestandteil des anschließenden Verwaltungsverfahrens. Das bedeutet aber, daß Unterlagen, die beim Musterungsarzt noch dem Schutz des Arztgeheimnisses unterliegen, den ärztlichen Bereich verlassen und im Verwaltungsbereich wie Verwaltungsunterlagen behandelt werden. Es ist nicht anzunehmen, daß ein Wehrpflichtiger diese möglichen Konsequenzen erkennt. Ich halte entsprechende Hinweise für notwendig, damit der Betroffene bewußt bestimmen kann, wie er sein Recht auf informationelle Selbstbestimmung wahrnehmen möchte. Die vom BMVg zugesagte datenschutzrechtliche Verbesserung bedingt allerdings, daß an die Stelle der — bereits jetzt textlich überfrachteten — Ladungskarte (Postkarte) ein größeres Blatt tritt, das dann im Umschlag versandt werden muß.

21.2.4 Sicherheit in der automatisierten Datenverarbeitung am Beispiel von WEWIS

Wie oben (21.2) erwähnt, bildeten technische und organisatorische Maßnahmen nach § 6 BDSG einen Schwerpunkt meiner Kontrollen und Beratungen. Die Übernahme meiner Vorschläge zu Verbesserungen bei Online-Zugriffen auf zentrale DV-Verfahren erwies sich wiederholt deshalb als schwierig, weil sicherheitsorientierte Software im Bereich des Bundesministers der Verteidigung zentral verantwortet und programmiert wird. Diese Regelung hat zwar unbestreitbare Vorteile. Es wirkt sich aber nachteilig aus, daß jede Änderung allein schon im Hinblick auf die Beteiligung mehrerer Organisationsebenen erheblichen Aufwand erfordert. Auch lassen sich für einen bestimmten Bereich angemessene Maßnahmen dann nur schwer umsetzen, wenn damit grundsätzlich jeweils alle anderen zu einem Schutz-Rahmen gehörenden Anwendungen ebenfalls diesem höheren Aufwand an Sicherheit unterworfen werden, ohne daß dies geboten wäre. Höherer Aufwand an Sicherheit bedeutet dann z. B. für alle betroffenen Anwender einen höheren Zeitbedarf, bevor sie bei der Eröffnung des Dialogs die Kontrollen bis zu ihrer Anwendung passiert haben.

Meine Empfehlungen für das Wehrersatzwesen-Informationssystem (WEWIS) beziehen sich insbesondere auf eine anwenderfreundlichere Dialogeröffnung, auf Informationen an den Anwender, die ihm helfen, seine Verantwortung für eine sichere Datenverarbeitung besser wahrzunehmen, auf die Bindung von Terminals an Funktionen oder auf die sog. TIME-OUT-Funktion:

Bei umständlicher und deshalb zeitaufwendiger *Dialogeröffnung* sorgt der Benutzer, wenn er erst einmal bis zu seiner Anwendung durchgekommen ist, erfahrungsgemäß dafür, daß ihm diese Anwendung möglichst lange ungestört zur Verfügung steht. Eine beliebte Methode zur Vermeidung des „TIME-OUT" (s. u.) ist, in kurzen Abständen immer wieder auf die Tastatur zu drücken; für den Rechner bedeutet dies, der Benutzer ist im Rahmen seiner Berechtigungen noch aktiv. Auf diese Art und Weise bleiben Terminals häufig über den ganzen Arbeitstag aktiviert, so daß es einem Dritten leicht gemacht wird, unbefugt auf Daten zuzugreifen. Der Bundesminister der Verteidigung hat zugesagt, meine Anregungen aufzugreifen.

Jeder Benutzer sollte grundsätzlich wissen, wie das *Sicherheitskonzept* gestaltet ist, und welche Hinweise auf der sog. Begrüßungsseite für ihn wichtig sind, damit er überprüfen kann, ob jemand unter seiner Berechtigung unbefugt gearbeitet hat. Hierzu sollten Datum und Uhrzeit seines letzten Zugriffs und ggf. auch Paßwortfehlversuche unter seiner Benutzerkennung angezeigt werden. Diese Begrüßungsseite sollte nicht nur, wie häufig üblich, kurz gezeigt werden und dann selbsttätig verschwinden; der Anwender sollte vielmehr nur durch eigene Aktion (z. B. durch die nächste planmäßige Eingabe) einen neuen Bildschirminhalt aufrufen können.

Die *Bindung von Terminals an Funktionen* ist eine Maßnahme, die ich seit Jahren im gesamten Bereich der Bundesverwaltung immer wieder fordere. So einleuchtend das Argument ist, daß jemand bei Ausfall eines Terminals seine Berechtigungen von einem anderen Terminal aus nutzen können muß, so wenig ist mit diesem Konzept allgemeiner Flexibilität der Sicherheit gedient. Terminals sollten an Funktionen gebunden werden, wenn aufgrund ihrer Vielzahl ohnehin nicht *alle* Terminals notwendig sind, um bei Ausfall *eines* Terminals ausweichen zu können. Dies gilt vor allem, wenn die Terminals großflächig verteilt sind. Auf jeden Fall sollten jedoch zumindest diejenigen Terminals eindeutig an Benutzerkennungen und das dazugehörige Paßwort gebunden werden, von denen aus sicherheitsrelevante Funktionen wahrgenommen werden, die mit der Systemtechnik (z. B. Betriebssystem, Netzwerksteuerung, Sicherheits-Software) zusammenhängen.

Die sog. *TIME-OUT-Funktion* sollte früher dazu dienen, den zentralen Rechner von der Dialogbereitschaft mit nicht aktiven Terminals zu entlasten. Deshalb wurde nach einer jeweils festgelegten Zeit der Inaktivität eines Terminals die logische Verbindung zum Rechner abgebrochen mit der Folge, daß der Benutzer zur Weiterarbeit den Dialog völlig neu beginnen mußte. Dieses Verfahren hat zugleich einen Sicherheitswert, weil dadurch das Risiko verringert wurde, daß ein Unbefugter die Abwesenheit des befugten Benutzers nach einiger Zeit dazu verwenden konnte, die begonnene Arbeit „fortzusetzen". Weil das Entlastungsargument bei der heute weit größeren Leistungsfähigkeit der zentralen Rechner kaum noch bedeutsam ist, kann der Sicherheitswert der TIME-OUT-Funktion jetzt auch so genutzt werden, daß der Benutzer nach einer Zeitspanne der Inaktivität lediglich sein Paßwort neu eingeben muß, um mit der Arbeit dort fortzufahren, wo er sie unterbrochen hatte. Weil dies wesentlich einfacher ist, als den Dialog neu aufzubauen, sind damit auch kürzere TIME-OUT-Spannen zumutbar, wodurch der Sicherheitswert erhöht wird.

Im Zusammenhang mit meinen beim Bundesminister der Verteidigung durchgeführten Kontrollen habe ich

im Laufe des Berichtsjahres erstmalig auch das sog. *Hardcopy-Problem* aufgegriffen. An Terminals, denen ein Drucker angeschlossen ist, kann durch Betätigung einer bestimmten Taste ein Ausdruck dessen bewirkt werden, was gerade auf dem Bildschirm gezeigt wird. Dieser Ausdruck wird üblicherweise als Hardcopy bezeichnet. Die Erstellung einer Hardcopy kann nicht kontrolliert werden. Wegen der generellen Bedeutung dieses Problems, habe ich hierzu im Kapitel Datensicherung näheres ausgeführt (s. unten 24.3).

Der Bundesminister der Verteidigung hat seine Bereitschaft erklärt, meine Anregungen so weit wie möglich umzusetzen, eine abschließende Stellungnahme lag mir zum Zeitpunkt der Fertigstellung dieses Berichts noch nicht vor.

22. Wirtschaftsverwaltung

22.1 Bundesamt für Wirtschaft

22.1.1 Kontrolle des Amtes

Die Kontrolle der Einhaltung der Vorschriften des Datenschutzes beim Bundesamt für Wirtschaft (BAW), die bereits 1987 begonnen worden war und erhebliche Mängel zutage gefördert hatte, habe ich abgeschlossen. Meiner Beanstandung (10. TB, S. 86 ff.) hat das Bundesamt inzwischen abgeholfen. Die festgestellten Mängel, insbesondere die unzureichende organisatorische Sicherstellung des Datenschutzes und das Fehlen der Übersicht gemäß § 15 Abs. 1 BDSG, sind beseitigt worden. Das Bundesamt hat im Zuge der internen Reorganisation des Datenschutzes eine vorbildliche Übersicht über seine Datenverarbeitung erstellt. Es ist jetzt möglich, anhand dieser Aufzeichnungen rasch einen Überblick über die Aufgaben zu erlangen, zu deren Erfüllung das Bundesamt personenbezogene Daten speichert oder sonst verarbeitet, und sich über die Einzelheiten dieser Verarbeitung zu unterrichten. Auf die Bedeutung des Datenschutzes bei der Erledigung der Aufgaben des Amtes, die grundlegenden Regelungen des Bundesdatenschutzgesetzes und die sich daraus ergebenden Pflichten sind alle Bediensteten mit einer umfassenden Hausverfügung hingewiesen worden. Das Bundesamt hat außerdem sichergestellt, daß die Meldepflichten zur Gewährleistung der Aktualität der Dateienübersicht eingehalten werden und der dateimäßige Umgang mit personenbezogenen Daten nicht ohne Beteiligung des für den Datenschutz zuständigen Beamten erfolgt. Bei einigen speziellen Fragen der automatisierten Datenverarbeitung habe ich das Bundesamt weiter beraten, so bei der Organisation der Paßwortverwaltung und dem Einsatz von Arbeitsplatzcomputern. Außerdem habe ich angeregt, zur Vermeidung von Mißbräuchen die Nutzung des umfangreichen Archivs des Bundesamtes durch entsprechende Anweisungen zu regeln.

22.1.2 Förderung der Unternehmensberatung

In meinem Zehnten Tätigkeitsbericht (S. 87) habe ich über die Datenverarbeitung im Rahmen der Förderung von Unternehmensberatungen für kleine und mittlere Unternehmen durch das Bundesamt für Wirtschaft berichtet.

Hierbei ging es zunächst um die Speicherung von Angaben über den am Subventionsverhältnis rechtlich unbeteiligten Unternehmensberater im Bundesamt. Ich habe diese Datenspeicherung, für die eine gesetzliche Verarbeitungsgrundlage fehlt und die ohne Einwilligung des Beraters erfolgt, kritisiert.

Der Bundesminister für Wirtschaft ist inzwischen weitgehend auf meine Anregungen eingegangen. Ein geändertes Förderungsverfahren und ihm zugrundeliegende neugefaßte Richtlinien, welche voraussichtlich im Herbst 1989 in Kraft treten sollen, können zukünftig als datenschutzrechtlich hinreichende Grundlage für die im Bundesamt vorgenommene Datenspeicherung gelten. So wird der Unternehmensberater künftig um seine Einwilligung zur Speicherung seiner personenbezogenen Daten gebeten. In dieser Einwilligung wird klargestellt, daß die Datenspeicherung der Überprüfung der vom Berater zu erfüllenden Förderungsvoraussetzungen dient; die Einwilligung erstreckt sich auch darauf, daß das Bundesamt die Angaben mit anderen Förderungsanträgen vergleichen darf. Konsequenz einer verweigerten Einwilligung kann eine Verzögerung der Antragsbearbeitung sein, keineswegs aber der Ausschluß von der Förderung.

Außer der Speicherung der Beraterdaten habe ich es in meinem Zehnten Tätigkeitsbericht (S. 87) für datenschutzrechtlich bedenklich gehalten, daß der antragstellende Unternehmer nicht die Möglichkeit erhält, seinen Antrag unmittelbar beim Bundesamt einzureichen, vielmehr gezwungen ist, die Förderung über eine Leitstelle — das sind Verbände des Handels, des Handwerks und der Industrie sowie deren Untergliederungen — einzureichen. Damit erhält eine dritte Stelle, in der in aller Regel Berufskollegen oder Konkurrenten vertreten sind, Kenntnis vom Antrag und von Interna des Betriebes. Der Bundesminister für Wirtschaft hat sich bereiterklärt, in den neugefaßten Richtlinien dem antragstellenden Unternehmer die Wahl der Leitstelle, insbesondere auch einer branchenfremden, freizustellen. Insofern ist die Zusicherung des Bundesministers hervorzuheben, dem Antrag ein Verzeichnis aller Leitstellen sowie weiterer als Erfüllungsgehilfen bezeichneter Stellen, die ebenfalls die Antragsprüfung vornehmen können, mit ihren Anschriften beizufügen. Sichergestellt ist auch, daß die Antragsunterlagen nicht länger als ein Jahr nach der Entscheidung über die Förderung bei der Leitstelle verbleiben. Dieses Verfahren konnte ich akzeptieren.

22.1.3 Datenübermittlung an Verwertungsgesellschaften

Ein Importeur von Bild- und Tonaufzeichnungsgeräten hatte mich darauf aufmerksam gemacht, daß eine Durchschrift des Formularsatzes, die als Einfuhrkon-

trollmeldung vom Zollamt dem Bundesamt für Wirtschaft (BAW) übersandt wird, von diesem über das Deutsche Patentamt gemäß § 20a des Gesetzes über die Wahrnehmung von Urheberrechten und verwandten Schutzrechten an Verwertungsgesellschaften wie die GEMA weitergeleitet wird.

Die Verwertungsgesellschaften haben mir mitgeteilt, daß sie nicht alle auf den übersandten Durchschriften enthaltenen Angaben für ihre Aufgaben benötigen. Dies gilt insbesondere für Informationen über „Lieferbedingungen", „Verkehrszweig an der Grenze", „Verfahren", „Besondere Vermerke/vorgelegte Unterlagen/Bescheinigungen und Genehmigungen" sowie „Statistischer Wert", die für entbehrlich gehalten werden.

Die Verwertungsgesellschaften erhalten somit zahlreiche — auch personenbezogene — Daten, deren Übermittlung zur Wahrnehmung ihres Vergütungsanspruchs nicht erforderlich ist. Dies ist datenschutzrechtlich unzulässig.

Der Bundesminister für Wirtschaft hat zugesagt, bei der nächsten Änderung der Außenwirtschaftsverordnung die Datenübermittlung auf das erforderliche Maß zu beschränken und dem durch ein neues Durchschreibeverfahren Rechnung zu tragen.

Die in Aussicht genommene Umgestaltung des Weiterleitungsverfahrens von Einfuhrkontrollmeldungen an die Verwertungsgesellschaften genügt datenschutzrechtlichen Anforderungen.

22.2 Bundesaufsichtsamt für das Versicherungswesen

Gegenstand einer Datenschutzkontrolle beim Bundesaufsichtsamt für das Versicherungswesen waren der allgemeine Umgang mit personenbezogenen Daten bei der Erledigung der Fachaufgaben des Amtes sowie die automatisierte Datenverarbeitung. Besondere Mängel oder Mißstände habe ich dabei nicht feststellen können. Es haben sich jedoch in einigen Bereichen der Aufgabenwahrnehmung durch das Amt Fragen ergeben, zu denen ich zunächst den Bundesminister der Finanzen um eine Stellungnahme gebeten habe.

So ist z. B. die rechtliche Grundlage für die Sammlung von Daten über Vorstandsmitglieder von Versicherungsunternehmen noch nicht endgültig geklärt. Das Versicherungsaufsichtsgesetz sieht für diesen Personenkreis zwar eine Eignungsbeurteilung vor, ehe einem Unternehmen die Erlaubnis zum Geschäftsbetrieb erstmalig erteilt wird. Es enthält jedoch keine ausdrückliche und normenklare Bestimmung über die Sammlung von Daten zum Zweck der Beurteilung einmal bestellter oder später neu eintretender Vorstandsmitglieder. Der weiteren Prüfung bedarf ferner, ob und in welchem Umfang das Bundesaufsichtsamt zur Erfüllung seiner Aufgaben personenbezogene Angaben über Außendienstmitarbeiter von Versicherungsunternehmen benötigt.

Im Zusammenhang mit der Datenschutzkontrolle habe ich das Bundesaufsichtsamt in einer Reihe von Fragen des Datenschutzes in der privaten Versicherungswirtschaft beraten und versucht, auf eine intensivere Zusammenarbeit des Amtes mit den gemäß §§ 30, 40 BDSG für die Datenschutzaufsicht in der Privatwirtschaft zuständigen Behörden der Länder hinzuwirken. Dies ist vom Bundesaufsichtsamt sehr kooperativ aufgenommen worden. In Gesprächen, die inzwischen mit Vertretern von Aufsichtsbehörden geführt worden sind, hat das Amt eine gegenseitige Unterrichtung in allen Fragen zugesagt, die für den Datenschutz in der privaten Versicherungswirtschaft von Bedeutung sind.

Die Stellungnahme des Bundesministers für Finanzen hat mich erst nach Redaktionsschluß dieses Berichtes erreicht, so daß ich darauf nicht mehr näher eingehen konnte.

22.3 Oberprüfungsamt für die höheren technischen Verwaltungsbeamten

Durch einen Hinweis wurde ich darauf aufmerksam gemacht, daß das Oberprüfungsamt regelmäßig die Namen und Wohnorte erfolgreich geprüfter Kandidaten für den höheren technischen Verwaltungsdienst an Fachzeitschriften zum Zweck der Veröffentlichung übermittelt, ohne zuvor die Einwilligung der Betroffenen einzuholen. Diese Übermittlung erfolgt auf Initiative der Fachpresse. Die Veröffentlichung der Angaben liegt wegen ihrer Werbewirkung in aller Regel im Interesse der Betroffenen. Es kann gleichwohl nicht ausgeschlossen werden, daß im Einzelfall Absolventen diese Veröffentlichung nicht wünschen, weil sie, aus welchen Gründen auch immer, allein über die Bekanntgabe des Prüfungserfolgs entscheiden wollen. Um dieses Selbstbestimmungsrecht der Betroffenen zu wahren, wird das Oberprüfungsamt zukünftig erst dann entsprechende Daten an Fachzeitschriften übermitteln, wenn die Betroffenen dieser Übermittlung nicht widersprochen haben. Auf das Widerspruchserfordernis wird bei der Übersendung des Prüfungszeugnisses besonders hingewiesen.

Das Oberprüfungsamt hat sich zur Einholung einer Einzeleinwilligung, die ich zunächst befürwortet habe, nicht entschließen können, weil es dann die Datenübermittlung wegen des anderenfalls erforderlichen Verwaltungsaufwandes hätte einstellen müssen. Die gewählte Widerspruchslösung halte ich im Hinblick auf die typische Interessenlage aller Beteiligten datenschutzrechtlich indessen noch für akzeptabel, um die Verletzung schutzwürdiger Belange geprüfter Kandidaten ausschließen zu können.

23. Nicht-öffentlicher Bereich

23.1 Zuständigkeiten und Berichtspflicht des BfD

Die im Bericht des Vorjahres vorausgeschickten kritischen Feststellungen zur Situation des Datenschutzes im sogenannten nicht-öffentlichen Bereich (10. TB, S. 88f.) haben in der Privatwirtschaft große Resonanz gefunden. In den Stellungnahmen, die mich zu diesem Berichtsteil überwiegend aus Kreisen von be-

trieblichen Datenschutzbeauftragten erreicht haben, wurden diese Bemerkungen häufig als unzutreffend zurückgewiesen.

Im Gespräch mit Vertretern aus verschiedenen Wirtschaftsbereichen habe ich inzwischen versucht, auf ein besseres Verständnis dieses Berichtsteils hinzuwirken und Kritikpunkte zu konkretisieren. Ich werde, wo immer sich die Gelegenheit bietet, weiterhin bemüht sein, die Sensibilität für die Belange der Bürger bei der Verarbeitung ihrer personenbezogenen Daten durch private Stellen zu verstärken. So habe ich auch auf der 12. Datenschutzfachtagung der in der Gesellschaft für Datenschutz und Datensicherung zusammengeschlossenen betrieblichen Datenschutzbeauftragten dargelegt, in welchem Maße das Recht auf informationelle Selbstbetimmung auch in den Bereich privatwirtschaftlicher Datenverarbeitung hineinwirkt. Ich werde weiter beobachten, wie sich die Überzeugung von der Bedeutung dieses Bürgerrechts im Bereich der Wirtschaft entwickelt.

In Reaktionen auf den angesprochenen Teil des 10. Tätigkeitsberichts wurde meine Berechtigung in Frage gestellt, über die Entwicklungen des Datenschutzes in der Privatwirtschaft zu berichten. Ich leite diese Zuständigkeit aus meiner Aufgabe ab, die Einhaltung der Datenschutzbestimmungen bei den der Staatsaufsicht des Bundes unterliegenden öffentlichrechtlichen Wettbewerbsunternehmen zu kontrollieren (§ 19 Abs. 1 BDSG) und auf die Zusammenarbeit mit den Aufsichtsbehörden hinzuwirken, denen die Kontrolle des Datenschutzes in der Privatwirtschaft obliegt (§ 19 Abs. 5 BDSG). Neben diesen gesetzlichen Aufgaben besteht außerdem der Auftrag des Deutschen Bundestages (Plenarprotokoll 10/85 vom 20. September 1984, Bundestags-Drucks. 10/1719), wonach ich „auch über wesentliche Entwicklungen im nicht-öffentlichen Bereich unabhängig von der Kompetenzlage" berichten soll, damit „das Parlament auch über diesen Bereich, der in der künftigen Entwicklung für den Bürger von immer größerer Bedeutung sein wird, unterrichtet ist". Diesem Auftrag werde ich im Rahmen der mir zur Verfügung stehenden — personell beschränken — Möglichkeiten weiterhin zu entsprechen versuchen.

23.2 Kreditwirtschaft

23.2.1 Teilnahme von Inkasso-Unternehmen am SCHUFA-Kreditinformationssystem

Über die Funktionsweise und die datenschutzrechtlichen Probleme beim Betrieb des Kreditinformationssystems der SCHUFA habe ich in den vergangenen Jahren ausführlich berichtet (8. TB S. 52ff.; 9. TB S. 68ff.; 10. TB S. 89ff.). Letzter noch offener Punkt bei der datenschutzrechtlichen Reform dieses Systems war dessen Nutzung durch Inkasso-Unternehmen.

Nach der Rechtsprechung des Bundesgerichtshofs (vgl. das sog. SCHUFA-Urteil vom 19. 9. 1985) hat sich die Datenübermittlung durch die SCHUFA auf solche Stellen zu beschränken, die als Kreditgeber ein berechtigtes Interesse haben, über die Kreditwürdigkeit einer Person zum Zweck der Bonitätsbeurteilung unterrichtet zu werden. An Inkasso-Unternehmen, die naturgemäß kein Interesse an solchen Angaben haben, darf die SCHUFA deshalb grundsätzlich keine Daten übermitteln. Inkasso-Unternehmen erhalten von der SCHUFA gleichwohl im Rahmen eines sog. „Suchdienstes" Adreßdaten. Diese Datenübermittlung beleuchtet einen Aspekt des Kreditinformationssystems, der bisher noch wenig Aufmerksamkeit gefunden hat und der gegenwärtig weder in der sog. SCHUFA-Klausel noch dem dazu erschienenen Merkblatt erläutert wird. Seine Besonderheit liegt darin, daß die Inkasso-Unternehmen Daten nicht zur Bonitätsbeurteilung, sondern zur Ermittlung des aktuellen Aufenthalts von Personen erhalten. Dies erfolgt in der Weise, daß der SCHUFA ein Suchauftrag erteilt wird, wenn eine Person unter der letzten dem Inkasso-Unternehmen bekannten Anschrift nicht mehr ermittelt werden kann. Die SCHUFA erfüllt den Suchauftrag, indem sie den ihr übermittelten Personendatenstammsatz mit ihrem Datenbestand vergleicht. Soweit dieser Abgleich noch nicht zur Ermittlung der aktuellen Anschrift führt, wird dieser Datensatz zusammen mit dem Merkmal Suchauftrag (SU) gespeichert. Wird später, etwa bei Neueröffnung eines Girokontos, von einem anderen Vertragspartner der SCHUFA ein übereinstimmender Personendatenstammsatz neu gemeldet, erhält der Suchauftraggeber automatisch die dazugehörige neue Anschrift. Im Kreditbereich soll durch dieses Verfahren sichergestellt werden, daß ein Schuldner, der sich seinen Zahlungsverpflichtungen u. a. dadurch entzieht, daß er seinen Aufenthalt wechselt, stets wieder zur Verantwortung gezogen werden kann, wenn seine Daten erneut wegen eines Kreditgeschäfts an die SCHUFA übermittelt werden.

Die Öffnung dieser Ermittlungsmöglichkeit auch für die Inkasso-Unternehmen ist wegen der damit verbundenen Erweiterung des Geschäftszwecks der SCHUFA datenschutzrechtlich nur zulässig, wenn die Betroffenen hierüber hinreichend informiert werden. Außerdem müssen die Betroffenen bei Unterzeichnung der SCHUFA-Klausel mit diesem Zweck einverstanden sein. Dies muß auch für die bei der SCHUFA bereits erfaßten Altkunden von Kreditinstituten gelten. Die SCHUFA-Klausel, die die Grundlage für die Übermittlung von Daten über die Aufnahme und vertragsgemäße Abwicklung einer Geschäftsverbindung durch das jeweilige Kreditinstitut an die SCHUFA ist und die zugleich auch die Grundlage für die Speicherung dieser Daten durch die SCHUFA darstellt, muß deshalb erneut geändert und um den Zweck der Aufenthaltsermittlung für Inkasso-Aufgaben erweitert werden. Dies gilt auch für das SCHUFA-Merkblatt. Der Zentrale Kreditausschuß, die Vereinigung der Spitzenverbände des Kreditgewerbes, hat jetzt einen entsprechenden Vorschlag gemacht. Es ist daran gedacht, in der SCHUFA-Klausel auch die Übermittlung von Adreßdaten an die Inkasso-Unternehmen ausdrücklich zu nennen.

Für die Zulässigkeit der einzelnen Suchanfrage bei der SCHUFA und die Übermittlung aktueller Adreßdaten ist sodann entscheidend, ob das Inkasso-Unternehmen ein berechtigtes Interesse an der Kenntnis dieser Daten hat und schutzwürdige Belange der Betroffenen nicht entgegenstehen (vgl. im einzelnen § 32

BDSG). Im Zweifel ist hierzu eine sorgfältige Einzelfallabwägung erforderlich, wobei es für das berechtigte Interesse auch darauf ankommt, daß die Forderung wirklich besteht und der Suchauftrag nicht etwa zur Durchsetzung von Forderungen genutzt wird, die sich später als sittenwidrig erweisen. Das Inkasso-Unternehmen muß hierauf achten. Außerdem erscheint ein Suchdienstauftrag erst angebracht, wenn zuvor eine Melderegisteranfrage ergebnislos geblieben ist.

Als Gegenleistung für den Suchdienst übermitteln die InkassoUnternehmen Negativmerkmale an die SCHUFA und zwar ohne Rücksicht darauf, ob diese Daten aus Kreditverhältnissen oder aus anderen Rechtsverhältnissen stammen. Voraussetzung für die Zulässigkeit dieser Übermittlung ist die Kreditrelevanz dieser Daten. Abgesehen davon, daß die Forderung, auf die sich die Merkmale beziehen, überhaupt bestehen muß, ist die Übermittlung nur zulässig, wenn die Zahlungsunwilligkeit oder Zahlungsunfähigkeit des Schuldners feststeht. Die Entscheidung bedarf einer sorgfältigen Einzelfallabwägung.

Die Erweiterung des SCHUFA-Systems auf Inkasso-Unternehmen rückt erneut die mit der Eigenauskunft gemäß § 34 Abs. 1 BDSG verbundenen Probleme in den Blick, die ich in den letztjährigen Berichten (9. TB S. 68ff.; 10. TB S. 89ff.) dargelegt habe. Nachdem die Handelsauskunfteien Eigenauskünfte erteilen, ohne ein Entgelt zu verlangen, kommt die leider auch im Novellierungsentwurf zum BDSG wieder vorgesehene Möglichkeit der Erhebung einer Auskunftsgebühr praktisch ausschließlich der SCHUFA zugute. Die Gründe, die gegen eine Kostenpflicht der Auskunft sprechen — nach Angabe der Bundes-SCHUFA betragen die Auskunftsgebühren bei den einzelnen SCHUFA-Gesellschaften 8,— bis 12,— DM — habe ich in der Vergangenheit ausführlich dargelegt; sie bestehen fort.

23.2.2 Entwurf eines Verbraucherkreditgesetzes

Der Bundesminister der Justiz bereitet gegenwärtig auf der Grundlage der Richtlinie der Europäischen Gemeinschaften zur Angleichung der Rechts- und Verwaltungsvorschriften über den Verbraucherkredit den Entwurf eines Verbraucherkreditgesetzes vor. Dieser Entwurf soll den Verbraucherschutz bei Kredit-, Kreditvermittlungs- und Ratenkaufverträgen regeln. Er sieht jedoch, ebenso wie die Richtlinie, keine Regelungen über den Umgang mit personenbezogenen Daten bei der Eingehung und Abwicklung derartiger Verträge vor. Wenn auch die Richtlinie solche Bestimmungen nicht ausdrücklich fordert, sollte jedoch die Gelegenheit genutzt werden, einen erfahrungsgemäß außerordentlich sensiblen Bereich der privatwirtschaftlichen Datenverarbeitung zum Nutzen sowohl der beteiligten Verbraucher wie auch der Kreditgeber bereichsspezifisch präzise gesetzlich zu regeln. Wünschenswert erscheint mir dies vor allem deshalb, weil die Verarbeitung von Verbraucherdaten im Bereich der Kreditwirtschaft und des Versand- und Abzahlungshandels inzwischen derartig unübersichtlich und kompliziert geworden ist, daß selbst Experten Mühe haben, Außenstehenden zu erläutern, welche Daten über die Aufnahme oder Abwicklung einer Kreditverbindung unter welchen Umständen von welchen Stellen zu welchen Zwecken gespeichert oder an andere Stellen übermittelt werden.

Eine spezialgesetzliche Regelung muß aber auch aus folgendem Grunde angestrebt werden. Für den Verbraucher ist es unbefriedigend, daß seine Einwilligung zur Übermittlung von Daten über die Aufnahme und vertragsgemäße Abwicklung eines Kredits an ein Kreditinformationssystem — auf der dortigen Speicherung beruht letztlich jeder weitere Datenverarbeitungsschritt — im Grunde nur eine Formalität darstellt; denn ohne die Abgabe dieser Erklärung, die überall in gleicher Weise von ihm verlangt wird, erhält er nirgendwo Kredit. Eine normenklare gesetzliche Übermittlungsgrundlage würde eher verstanden und akzeptiert werden als der in die Form einer Einwilligung gekleidete faktische Zwang zur Abgabe von Konsenserklärungen. Für die Kreditwirtschaft ist es unbefriedigend, daß etwa die Zulässigkeit der Verarbeitung von Negativdaten, die im Laufe eines Kreditverhältnisses anfallen, anhand der unbestimmten Generalklauseln des BDSG beurteilt werden muß, also immer eine Einzelfallabwägung mit einem verbleibenden Rest von Unsicherheit erforderlich ist. Eine Einzelfallabwägung ist andererseits mit den gerade im Massengeschäft eingeführten extrem formalisierten Kreditvergabe- und -abwickungsverfahren unter organisatorischen wie wirtschaftlichen Gesichtspunkten nur schwer zu vereinbaren. Die Kreditwirtschaft hat zudem immer wieder erfahren müssen, daß trotz des Aufwandes, der im Zusammenhang mit der SCHUFA-Klausel gegenüber dem Betroffenen erforderlich war und ist, das Verfahren immer wieder neue Fragen und rechtliche Unsicherheit birgt; sie erfährt dies jetzt erneut (vgl. oben 26.2.1).

Der entscheidende Grund für die Notwendigkeit, die Datenverarbeitung bei Kreditgeschäften mit Endverbrauchern gesetzlich zu regeln, ist jedoch die Bedeutung, die die Kreditinformation sowohl für den Betroffenen als auch für das wirtschaftliche Leben insgesamt hat. Schon heute kommen praktisch keine Kontoeröffnung, kein Abzahlungs- oder Versandhandelskauf und erst recht kein Ratenkredit ohne die Abfrage eines entsprechenden Bonitätsprofils und die sich daran anschließende laufende Bonitätskontrolle zustande. Bereits jede Ausgabe einer Kreditkarte zieht die Beobachtung der Kreditwürdigkeit des Betroffenen nach sich. Es ist für den Bürger deshalb gerade auch angesichts der schon für die nahe Zukunft prognostizierten explosionsartigen Zunahme von Kartenzahlungssystemen immer wichtiger, die Folgen genau kennen und berücksichtigen zu können, die sein wirtschaftliches Handeln für sein eigenes Kreditprofil und damit für seinen zukünftigen wirtschaftlichen Handlungsspielraum als Verbraucher hat. Unter den Bedingungen unserer modernen Industrie- und Dienstleistungsgesellschaft sind Erhebung, Speicherung, Übermittlung und sonstige Verarbeitung von Angaben über die Kreditwürdigkeit für die persönliche und wirtschaftliche Entfaltungsfreiheit so wesentlich, daß die Chance, diese Informationsverarbeitung mit dem Verbraucherkreditgesetz wegweisend zu regeln, unbedingt ergriffen werden sollte.

Gesetzliche Bestimmungen könnten sich dabei im wesentlichen an den Vereinbarungen orientieren, die zwischen den obersten Aufsichtsbehörden für den Datenschutz und der Kreditwirtschaft unter meiner Beteiligung vereinbart worden sind, nachdem der Bundesgerichtshof mit dem sog. SCHUFA-Urteil vom 19. September 1985 das bis dahin praktizierte Verfahren des Informationsaustauschs zwischen den am Verbraucherkredit beteiligten Stellen beanstandet hatte, weil dessen Grundlage, die SCHUFA-Klausel, mit wesentlichen Grundgedanken des Datenschutzes nicht in Einklang zu bringen war. Wie die mit dem Anschluß von Inkasso-Unternehmen an das SCHUFA-System zusammenhängenden Probleme zeigen, ist zunächst vor allem regelungsbedüftig, zu welchen Zwecken bei welchen Verbraucherkreditgeschäften Daten erhoben werden dürfen. Durch klare Übermittlungsregelungen muß sichergestellt werden, wann welche der am Abschluß oder der Durchführung eines Kreditgeschäfts beteiligten Stellen über welche Daten des Betroffenen verfügen und wozu sie genutzt werden dürfen. Ebenso müssen Umfang und Dauer der zulässigen Speicherung bestimmt werden. Der Auskunftsanspruch des Betroffenen ist umfassend und kostenlos zu gewährleisten. Vor Mißbrauch der Auskunft zu unzulässigen Zwecken ist der Betroffene zu schützen. Eine Reihe von Problemen, die in der Praxis nach wie vor zu Schwierigkeiten führen, wie etwa die Frage, unter welchen Umständen die Rücknahme der Einwilligung durch den Betroffenen — der sog. Widerspruch zur SCHUFA-Klausel — an die beteiligten Stellen weitergemeldet werden darf, würde bei einer gesetzlichen Regelung des Verfahrens entfallen. Einzelne Pflichten sowohl der Kreditgeber als auch des Kreditinformationssystems, etwa die zur Identitätsprüfung zur Vermeidung von Verwechslungsfällen, ließen sich exakt bestimmen.

23.2.3 Neue Karten-Zahlungssysteme

Häufig werde ich von Bürgern oder durch die Medien nach den datenschutzrechtlichen Risiken der neuen Kartenzahlungssysteme befragt. Dabei wird befürchtet, daß Daten über die Persönlichkeit und das individuelle Verbrauchsverhalten der Betroffenen gesammelt und anschließend automatisiert ausgewertet werden könnten, ohne daß die Betroffenen Einfluß darauf hätten. Daß solche Befürchtungen nicht aus der Luft gegriffen sind, zeigt etwa der Prospekt eines Marketingunternehmens, der Kartenzahlungssysteme als Dienstleistung anbietet und in dem es heißt: „Zunächst einmal müssen Sie Ihren Kunden kennenlernen. Das heißt, Sie benötigen Informationen über seinen Wohnort, seinen Beruf, seine Interessen, seine Bedürfnisse, sein Kauf- und Auswahlverhalten." Einer regionalen Datenschutzaufsichtsbehörde liegt zudem gegenwärtig der Entwurf eines Vertrages vor, mit dem sich ein Marketingunternehmen durch Betreiber von Kartenzahlungssystemen die Befugnis einräumen lassen will, personenbezogene Daten über das Kaufverhalten von Karteninhabern auch für eigene Zwecke auszuwerten. Dabei ist auch an eine kartenübergreifende personenbezogene Auswertung gedacht; dies bedeutet, daß das Einkaufsverhalten einer Person auch bei Benutzung unterschiedlicher Kreditkarten ausgewertet werden soll.

In der Tat werden nirgendwo in der privaten Wirtschaft zukünftig die Möglichkeiten, umfassende Käuferprofile herzustellen, so einfach sein wie bei den Besitzern der Daten, die bei kartengestützten Geschäften anfallen. Die Entwicklung von Kartenzahlungssystemen bedarf deshalb bei der außerordentlich raschen Zunahme der Stellen, bei denen mit Hilfe solcher Karten gezahlt werden kann, besonders aufmerksamer Beobachtung. Zu diesem Zweck und um gegebenenfalls datenschutzrechtliche Empfehlungen für Kartenzahlungssysteme und deren sozialverträgliche Gestaltung geben zu können, hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder einen Arbeitskreis eingerichtet, der sich vor allem mit Fragen der Automatisierung des Zahlungsverkehrs befaßt.

23.3 Versicherungswirtschaft

23.3.1 Schweigepflichtentbindungsklauseln

In den Tätigkeitsberichten der vergangenen Jahre (zuletzt 10. TB S. 91) habe ich ausführlich über die datenschutzrechtlichen Defizite bei der Verwendung von Schweigepflichtentbindungsklauseln vor allem der privaten Kranken- und Unfallversicherung berichtet. Über eine datenschutzgerechte Neufassung dieser Klauseln werden bereits seit mehreren Jahren Gespräche zwischen den obersten Aufsichtsbehörden für den Datenschutz, dem Bundesaufsichtsamt für das Versicherungswesen und den Verbänden der Versicherungswirtschaft geführt, an denen ich mich im abgelaufenen Jahr wiederum beteiligt habe. Erstmals ist es bei diesen Verhandlungen jetzt zu einer Einigung über eine Neufassung der Schweigepflichtentbindungsklausel in Krankenversicherungsverträgen gekommen.

Die neue Klausel (vgl. Anlage 8) ist in mehrfacher Hinsicht zu begrüßen. Sie macht schon vom Aufbau her deutlich, daß die Entbindung der Ärzte und sonstigen verpflichteten Personen von ihrer Schweigepflicht gegenüber der Versicherung zu zwei unterschiedlichen Zwecken erfolgt: Zum einen zur — ggf. auch rückwirkenden — Beurteilung des Risikos durch den Versicherer bei Vertragsabschluß und zum anderen zur Beurteilung seiner Leistungspflicht in einem konkreten Abrechnungseinzelfall. Im Gegensatz zur alten Klausel, die eine Unterscheidung der Erklärungszwecke nicht kennt, kann der Betroffene aus der Neufassung jetzt unschwer ersehen, warum eine Erklärung zur Entbindung von der Schweigepflicht von ihm überhaupt verlangt wird. Der Geltungsumfang dieser Erklärung ist inhaltlich exakt bestimmt, der Adressatenkreis ist abschließend aufgezählt.

Zur Risikobeurteilung darf das Versicherungsunternehmen, wenn dies erforderlich ist, Ärzte, Zahnärzte, Angehörige anderer Heilberufe und Angehörige von Krankenanstalten, Gesundheitsämtern sowie von Kranken-, Lebens- und Unfallversicherern nach dem Gesundheitszustand des Betroffenen befragen, der den Abschluß eines Versicherungsvertrags beantragt

hat. Diese Personen sind von ihrer Schweigepflicht entbunden, wenn sie den Betroffenen in den letzten zehn Jahren vor der Antragstellung untersucht oder behandelt haben. Weiter zurückliegende Behandlungen sollen zukünftig in die Risikoprüfung nicht mehr einbezogen werden. Zu dieser Prüfung ist das Versicherungsunternehmen allerdings auf der Grundlage der Erklärung nur in den ersten fünf Jahren nach der Antragstellung berechtigt. Nur in diesem Rahmen darf das Versicherungsunternehmen dem Verdacht auf eine verschwiegene Vorerkrankung nachgehen, ohne den Betroffenen hierüber erneut unterrichten zu müssen. In der alten Klausel war hierfür keinerlei Beschränkung vorgesehen. Will das Versicherungsunternehmen später als fünf Jahre nach Antragstellung den Gesundheitszustand des Versicherten zum Zeitpunkt der Antragstellung überprüfen, muß es hierfür eine neue Schweigepflichtentbindungserklärung bei ihm einholen.

Der Umfang der Schweigepflichtentbindung zum Zweck der Beurteilung der Leistungspflicht bezieht sich, anders als früher, präzise auf die Prüfung der Leistungspflicht im jeweiligen Abrechnungseinzelfall. Das Versicherungsunternehmen soll in der Lage sein zu klären, ob die zur Begründung eines Erstattungsanspruchs vorgelegten Unterlagen authentisch sind und für die erbrachten Leistungen eine Erstattungspflicht nach dem vereinbarten Tarif besteht. Nur zu diesem Zweck darf es, immer bezogen auf den in Rede stehenden Abrechnungsfall, anfragen. Dem entspricht es, daß die Adressaten der Klausel nur noch diejenigen Angehörigen von Heilberufen und Krankenanstalten sind, die in den vorgelegten Abrechnungsunterlagen genannt werden oder die an der Heilbehandlung beteiligt waren. Die neue Klausel umfaßt nicht mehr — wie früher — eine darüber hinausgehende Erhebung und Offenbarung von Gesundheitsdaten. Zur Verhütung von Versicherungsmißbrauch durch verschwiegene Doppelversicherungen dürfen Mitarbeiter anderer Krankenversicherer danach befragt werden, ob für den Versicherten dort Krankenversicherungsverträge bestehen. Der Umfang der Schweigepflichtentbindung zur Beurteilung der Leistungspflicht orientiert sich damit insgesamt an den Auskunftsobliegenheiten, die der Versicherungsnehmer nach dem Versicherungsvertragsgesetz und den Allgemeinen Krankenversicherungsbedingungen gegenüber seinem Versicherungsunternehmen hat. Zugleich wird für den Versicherungsnehmer klargestellt, daß bei der Überprüfung eines künftigen Leistungsanspruchs eine gesonderte Befreiungserklärung nicht mehr eingeholt werden wird. Gegen diese unbeschränkte, andererseits inhaltlich klar eingegrenzte Zukunftswirkung dieses Teiles der Klausel haben die obersten Aufsichtsbehörden für den Datenschutz keine Einwände mehr erhoben.

Mit der Einigung auf den neuen Wortlaut der Klausel ist es endlich gelungen, den Umgang mit personenbezogenen Daten in einem außerordentlich sensiblen Bereich der Privatwirtschaft auf eine neue Grundlage zu stellen, die die schutzwürdigen Belange der Betroffenen berücksichtigt und zugleich Raum für berechtigte Kontroll- und Informationswünsche der Versicherungswirtschaft läßt. Die Verbände der Versicherungswirtschaft haben zugesagt, die Verwendung der neuen Klausel umgehend beim Bundesaufsichtsamt für das Versicherungswesen zur Genehmigung vorzulegen. Das Bundesaufsichtsamt, das an den Verhandlungen beteiligt war, hat die Genehmigung der neuen Klausel in Aussicht gestellt. Die Aufsichtsbehörden für den Datenschutz werden kontrollieren, ob dann auch entsprechend der neuen Vorgabe verfahren wird, was nach den Zusagen der Versicherungswirtschaft bei allen Krankenversicherungsverträgen ab sofort der Fall sein soll.

23.3.2 Datenverarbeitungsklausel und zentrale Dateien in der Versicherungswirtschaft

In den Gesprächen zwischen der Versicherungswirtschaft und den Datenschutzaufsichtsbehörden konnte die seit langem ausstehende datenschutzrechtliche Überarbeitung der Datenverarbeitungsklausel mit einer weitgehenden Einigung wesentlich vorangetrieben werden.

Mit der Datenverarbeitungsklausel (zuweilen wird auch von „Datenschutzklausel" oder „Datenschutzermächtigungsklausel" gesprochen) erklärt der Betroffene sein Einverständnis damit, daß die Versicherungsunternehmen personenbezogene Vertragsdaten an andere Stellen übermitteln. Bei diesen handelt es sich neben Rückversicherern vor allem um eine Reihe von Versicherungsfachverbänden, bei denen — in der Regel zum Zweck der Verhütung von Versicherungsmißbrauch — zentrale Datensammlungen oder Hinweissysteme geführt werden. Solche zentralen Dateien gibt es in den Sparten Rechtsschutzversicherung, Unfallversicherung, Kfz-Haftpflichtversicherung, Sachschadenversicherung, Lebensversicherung und Transportversicherung. Die gegenwärtig noch verwendete alte Klausel, über deren Schwächen ich berichtet habe (vgl. 9. TB S. 70, 10.TB S. 91), war von den Datenschutzaufsichtsbehörden insbesondere deshalb kritisiert worden, weil sie die Datenverarbeitungsvorgänge, in die mit der Klausel eingewilligt wird, nicht hinreichend transparent macht. Der Betroffene kann die Reichweite seiner Einwilligung anhand der geltenden Klausel nicht genau abschätzen. Auch zusammen mit einem Merkblatt zur Datenverarbeitung, das interessierten Versicherungsnehmern auf besondere Anforderung von den Versicherungsunternehmen zur Verfügung gestellt wird, ist dies allenfalls Experten möglich.

Die außerordentlich schwierigen Verhandlungen zwischen Versicherungswirtschaft und Datenschutzbehörden führten zu einer Neufassung der Klausel, die allerdings immer noch sehr abstrakt formuliert ist. Deshalb soll künftig der Betroffene besser als bisher durch das Merkblatt informiert werden, und zwar schon vor Abgabe seiner Einwilligungserklärung, ohne daß es einer besonderen Anforderung bedarf. Der Betroffene kann jetzt aus dem überarbeiteten Merkblatt (vgl. Anlage 9) anhand von Beispielen erfahren, in welchem Umfang und zu welchen Zwecken der Versicherer Daten über ihn speichert und an Rückversicherer oder andere Gesellschaften übermittelt. Die bestehenden zentralen Dateien der Versicherungswirtschaft werden ebenfalls, wenn auch nur skizzenhaft, unter Hinweis auf den Verarbeitungs-

zweck erläutert. Außerdem wird deutlich gemacht, in welcher Weise innerhalb einer Versicherungsgruppe Daten in gemeinsamen Datensammlungen dieser Gruppe verarbeitet werden. Damit kann zukünftig von einer auf hinreichender Information beruhenden Einwilligung ausgegangen werden.

Die Gespräche zwischen Versicherungswirtschaft und Datenschutzbehörden sollen im Jahr 1989 fortgesetzt werden, um eine Reihe noch offener Fragen im Zusammenhang mit den zentralen Dateien, vor allem im Bereich der Kfz-Haftpflicht und Sachschadensversicherer, datenschutzrechtlich befriedigend zu lösen. An den Gesprächen werde ich mich weiter beteiligen. Dabei werde ich auch die Frage noch einmal ansprechen, ob die in der Datenverarbeitungsklausel vorgesehenen Möglichkeit einer Weitergabe von Gesundheitsdaten an selbständige Vertreter nicht noch besser gelöst werden kann.

23.4 Wohnungsvermietung

Wie verschiedentlich bereits in der Vergangenheit (vgl. 4. TB S. 45, 5. TB S. 105) haben sich die Aufsichtsbehörden der Länder im Berichtsjahr erneut mit Fragen der Datenverarbeitung und des Datenschutzes bei der Vermietung von Wohnraum beschäftigt.

Datenschutzrechtlich problematisch ist insbesondere die Verwendung von Fragebögen, die betroffenen Mietbewerbern in vielen Fällen vor Vertragsabschluß vor allem durch Großvermieter vorgelegt werden. Häufig werden hierin Angaben verlangt, die tief in die Privatsphäre eingreifen, ohne daß sie für das Mietverhältnis erforderlich sind. Der Betroffene kann sich der Beantwortung dieser Fragen nur dadurch entziehen, daß er in Kauf nimmt, als Mietbewerber abgelehnt zu werden. Das Verlangen solcher Großvermieter kann daher dazu führen, daß die schwierige Lange von Wohnungssuchenden mißbräuchlich ausgenutzt wird. Der für das Mietrecht zuständige Bundesminister der Justiz hat dies bereits im Jahre 1982 eingeräumt. Zu einer befriedigenden, die Praxis umgestaltenden Klärung des Fragerechts von Vermietern durch die Rechtsprechung ist es jedoch bislang entgegen den Erwartungen der Bundesregierung nicht gekommen. Ich halte es aus diesem Grunde für notwendig, erneut zu prüfen, ob der Umfang des Fragerechts des Vermieters gesetzlich geregelt werden sollte.

Die Datenschutzaufsichtsbehörden hatten außerdem den Versuch eines Unternehmens zu beurteilen, nach dem Muster des Kreditinformationssystem SCHUFA bundesweit ein Vermieterinformationssystem einzuführen. In diesem Informationssystem sollten eine Fülle von Angaben über Mieter (u. a.: Staatsangehörigkeit, Höhe des Einkommens, Pünktlichkeit der Mietzahlungen) gespeichert und zum Abruf durch andere Vermieter bereitgehalten werden. Das Unternehmen wollte seinen Datenbestand außerdem durch die Einspeicherung sämtlicher Schuldnerverzeichnisse erweitern.

Die Aufsichtsbehörden stehen solchen Vorhaben nicht zuletzt wegen der möglichen Auswirkungen auf die Betroffenen mit äußerster Skepsis gegenüber. Sie halten eine Speicherung auf der Grundlage der Generalklauseln des 3. und 4. Abschnitts des BDSG allenfalls dann für gerechtfertigt, wenn nur gesicherte Daten gespeichert werden; Daten über Mietrückstände dürfen also nur dann gespeichert werden, wenn die Schuld rechtskräftig festgestellt ist. Der Versuch des in Rede stehenden Unternehmens, Informationen über Mieter als vermarktbares Produkt anzubieten, zeigt, wie schnell es — gerade auch im Hinblick auf die Verwendung von Mieterfragebögen — in diesem Wirtschaftsbereich zu Gefährdungen schutzwürdiger Belange der Betroffenen kommen kann. Deshalb sollten die Grenzen solcher Informationssysteme bereichsspezifisch gesetzlich eindeutig bestimmt werden.

24. Datensicherung

Als letzte von allen Vorschriften des BDSG traten am 1. Januar 1979 die Datensicherungsvorschriften (§ 6 und die Anlage zu § 6 Abs. 1 Satz 1) in Kraft. Auch zehn Jahre danach sind diese Vorschriften noch längst nicht bei jeder automatisierten Verarbeitung personenbezogener Daten realisiert. Zwar gibt es im Bereich der zentralen DV-Verfahren eine deutliche Tendenz zu Verbesserungen; durch die Einführung von dezentraler, individueller Datenverarbeitung — meist unter Verwendung von Personalcomputern — sind aber neue Risiken entstanden, denen bislang oft nicht oder nur unzureichend begegnet wird. Auch für diesen Bereich gibt es aber inzwischen technische Hilfen zur Datensicherung, und weil für Personalcomputer von ganz unterschiedlichen Seiten mehr Sicherheit gefordert wird (siehe unten 24.2), ist mit Fortschritten zu rechnen.

Welche Verbesserungen der Datensicherheit möglich sind, zeigen z. B. die Vorschläge, die ich dem Bundesminister der Verteidigung für das Wehrersatzwesen-informationssystem (WEWIS) unterbreitet habe. Sie beziehen sich auf

- eine anwenderfreundliche Dialogeröffnung, die den Benutzer mit möglichst wenig Formalitäten belastet und die Sicherheitsanforderungen wirksam, aber ohne unnötigen Aufwand einbezieht,
- Informationen an den Anwender, die ihm helfen können, seine Verantwortung für eine sichere Datenverarbeitung besser wahrzunehmen,
- die Bindung von Terminals an Funktionen, die zwar die Flexibilität der Benutzung einschränkt, dafür aber die Sicherheit dadurch erhöht, daß besonders sicherheitsrelevante Eingaben nur über solche Terminals erfolgen können, bei denen der Ort der Aufstellung eine zusätzliche Kontrolle garantiert, und
- die sogenannte TIME-OUT-Funktion, durch die nach einer — einstellbaren — Zeit der Nicht-Benutzung eines Terminals erneut eine Berechtigungsprüfung erzwungen wird, was eine gewisse Sicherheit dagegen bietet, daß eingeschaltete Terminals während einer Arbeitspause des Berechtigten unbefugt genutzt werden.

Ich bin überzeugt, daß die Empfehlungen auch für andere dialogorientierte DV-Verfahren gelten können (siehe auch 21.2.4).

Als Problem für alle Maßnahmen zur Datensicherung erweist sich immer wieder, daß die richtigen Maßnahmen stets nur aus den näheren Umständen der jeweiligen Datenverarbeitung und nicht aus einem allgemein gültigen Rezept abgeleitet werden können. Deshalb müssen jeweils die tatsächlichen besonderen Verhältnisse festgestellt und danach die erforderlichen Maßnahmen ausgewählt werden. Dabei entsteht auch ständiger Organisationsbedarf, z. B. um die den einzelnen Benutzern zur Verfügung gestellten Zugriffsmöglichkeiten stets den Erfordernissen der rechtmäßigen Aufgabenerfüllung anzupassen und um die tatsächliche Nutzung vergebener Zugriffsberechtigungen zu kontrollieren.

Typisch für solche Daueraufgaben ist auch die Notwendigkeit, bei Datenübermittlungen auf Fernschreibleitungen stets den möglichen und zur Sicherheit im Fernschreibdienst auch erforderlichen Kennungsvergleich durchzuführen. Geschieht dies nicht, kann nach der Neuvergabe alter Fernschreibnummern der neue Inhaber Nachrichten erhalten, die für den Vorgänger bestimmt sind. Der Bundesminister des Innern, den ich auf dieses Risiko hingewiesen habe, hat in seinem Geschäftsbereich dafür gesorgt, daß dieser Vergleich regelmäßig vorgenommen wird; er hat auch die anderen Ressorts gebeten, in ihrem Bereich auf die Notwendigkeit des Kennungsvergleichs hinzuweisen.

Deutlich erkennbare Fortschritte haben im Berichtsjahr die zentralen Bemühungen der Bundesverwaltung um mehr Datensicherheit gemacht. Sie führten — koordiniert vom Interministeriellen Ausschuß für die Sicherheit in der Informationstechnik (ISIT) — insbesondere zur Definition der Anforderungen an sichere DV-Systeme und zur Formulierung von Kriterien zur praktischen Beurteilung von DV-Systemen. Abgesehen von dem unmittelbaren Beitrag, den diese Bemühungen zur Datensicherheit in der Zukunft leisten, dürften sie auch auf die Motivation in den datenverarbeitenden Stellen zur weiteren Verbesserung der Datensicherheit ausstrahlen.

24.1 Hacker-Erfolge

In Abständen, die in der letzten Zeit anscheinend immer kürzer werden, berichten die Medien über spektakuläre Fälle, in denen Unbefugte durch das planmäßige Ausnutzen von Sicherheitsmängeln in großen Datenverarbeitungssystemen Veränderungen oder Störungen vorgenommen und zum Teil auch erhebliche Schäden angerichtet haben. Bei den angegriffenen Systemen handelt es sich in der Regel um Datenverarbeitungsanlagen, die über große Netze vielen Tausend unterschiedlichen Benutzern zugänglich sind.

Die Angreifer sind, soweit sie bekannt wurden oder aus den Ergebnissen auf sie geschlossen werden konnte, im wesentlichen nach zwei Methoden vorgegangen. Die eine Methode ist das mehr oder minder systematische Ausprobieren von Eingaben mit dem Ziel, daß eine dieser Eingaben vom System so interpretiert wird, als habe dieser Benutzer besondere Rechte (Privilegien) bei der Arbeit mit dem System. Diese erschlichenen Rechte werden dann zu unerlaubten, meist störenden Aktivitäten mißbraucht. Vom „Herumhacken" auf der Tastatur zum Ausprobieren der Eingaben wurde die Bezeichnung „Hakker" abgeleitet. Sie wird heute auch benutzt für die Anwender der zweiten Methode, bei der ein berechtigter Benutzer seine Rechte — oft ohne sie durch Tricks zu erweitern — in schädlicher Weise nutzt. Dies geschieht z. B. dadurch, daß er an andere Teilnehmer im Netz die Aufforderung schickt, ein in derselben Nachricht enthaltenes Programm ablaufen zu lassen, das neben seinen planmäßigen, dem Anwender bekannten Wirkungen heimlich auch Störungen verursacht (Prinzip des trojanischen Pferdes). Oder man nutzt die Berechtigung, selbstgeschriebene Programme ablaufen zu lassen, um durch solche Programme in andere Programme Abschnitte einzufügen, die wiederum bei jeder Ausführung des so geänderten Programms den hinzugefügten Abschnitt in weitere Programme einbringen (Prinzip des Virus). Oder man schafft ein Programm, daß „nichts weiter" tut, als sich selbst in möglichst viele andere, über ein Datennetz erreichbare Computer zu schreiben, um sich von dort aus ebenso in andere oder auch schon einmal betroffene Computer zu schreiben und so weiter. Computernetze sind zwar nicht planmäßig für solche „Spielereien" ausgelegt. Wenn es aber gelingt, durch das Ausnutzen von Sicherheitsmängeln dieses Prinzip in die Praxis umzusetzen, so kann — wie im Herbst 1988 in den USA geschehen — binnen einiger Stunden ein Netz von mehreren Tausend Computern so vollständig ausgelastet sein, daß für sinnvolle Arbeit keine Kapazität mehr verfügbar und das System dadurch blockiert ist.

Weil dem Erfindungsreichtum hier kaum Grenzen gesetzt sind, ist damit zu rechnen, daß einzelne Benutzer ihre speziellen Fähigkeiten in immer neuen Variationen und Kombinationen an Datenverarbeitungssystemen ausprobieren. Dabei kann man sich aber keineswegs darauf verlassen, daß es — wie in den bekannt gewordenen Fällen — das ganze Ziel der Täter ist, lediglich durch eine spektakuläre „Leistung" aufzufallen. Es ist vielmehr damit zu rechnen, daß schon jetzt dieselben Schwächen auch von anders motivierten Tätern, die gerade unentdeckt bleiben wollen, zu anderen Zwecken (z. B. Ausspähung) ausgenutzt werden. Dadurch kann auch der Datenschutz nachhaltig beeinträchtigt werden.

In der Bundesverwaltung sind mir derartige Fälle bisher nicht bekannt geworden. Dies liegt zum einen wohl daran, daß die in der Bundesverwaltung betriebenen Netze in der Regel für sehr spezielle Aufgaben, wie z. B. die bloße Abfrage von Datenbeständen, eingesetzt werden. Sie bieten ihren Benutzern deshalb nur sehr spezielle Funktionen, insbesondere nicht die Funktion, selbstgeschriebene Programme ausführen zu lassen. Auch benutzen viele Bundesbehörden, die vernetzt arbeiten, dafür Standleitungen. Standleitungen sind für den allgemeinen Nachrichtenverkehr nicht zugänglich (nicht anwählbar) und verhindern deshalb einen Angriff von nicht zugelassenen (be-

kannten) Benutzern. Ein weiterer Grund dürfte sein, daß diese Netze nicht auch große Benutzergruppen aus dem Forschungs-, Universitäts- und Studentenbereich haben. Eine Garantie für Unangreifbarkeit ist das jedoch nicht. Denn die Schwächen, die von den Hackern ausgenutzt werden, sind zum Teil technisch, zum Teil organisatorisch bedingt, weit verbreitet und nicht ohne weiteres zu beseitigen:

- Die heute benutzten Betriebssysteme (die stets benötigte Basis-Software) sind in ihren wesentlichen Teilen in einer Zeit entstanden, in der das Hacker-Problem unbekannt war. Die Systemphilosophie ist ausgerichtet auf Effizienz im Sinne von Geschwindigkeit, Leistungsfähigkeit, nicht aber auf Sicherheit gegen Angriffe.
- Die Betriebssysteme sind untereinander inkompatibel. Dadurch ist die Zusammenarbeit ohnehin schon schwierig und man verzichtet deshalb auf zusätzliche Erschwernisse durch Sicherungsmaßnahmen, so daß Lücken in der Überwachung der Sicherheit bleiben.
- Systemverwalter und auch Benutzer sind oft von einem geradezu unverantwortlichen Leichtsinn. Dies ist der Hauptgrund für Fälle erfolgreichen Eindringens. Immer wieder kommt es z. B. vor,
  - daß Vornamen (des Benutzers), der Name des Herstellers oder andere naheliegende und deshalb leicht zu erratende Zeichenfolgen als Paßwort benutzt werden,
  - daß Paßworte über eine nicht vertretbar lange Zeit nicht verändert werden oder
  - daß aus Sicherheitsgründen abgewiesene Eingaben nicht beachtet werden und ein Angreifer deshalb ungestört beliebig viele Versuche unternehmen kann.
- Weil die Paßworte schon zur Berechtigungsprüfung verfügbar sein müssen, ist ihr Schutz gegen unberechtigte Zugriffe schwierig und oft unzureichend. Auch das heute mögliche kryptographische Verschlüsseln bietet dann keine sichere Lösung, wenn das Verschlüsselungsverfahren und der benutzte Schlüssel so verfügbar sind, daß ein Unbefugter beliebige Probeläufe zur Paßwortsuche durchführen kann.
- In praktisch allen Systemen sind Benutzer zugelassen, deren Name ihrer Stellung in der Benutzerhierarchie entspricht (z. B. „Admin", „Root" für einen besonders hoch priviligierten Administrator bzw. sicherheitsrelevante Basisfunktionen) und es gibt Benutzernamen wie „System" oder „Guest". Die damit aufrufbaren Funktionen sind schon vom Lieferanten eingerichtet und mit einem Paßwort geschützt, gelegentlich aber weltweit einheitlich mit seinem Firmennamen. Wenn diese Paßwörter nicht sofort bei der Betriebsaufnahme geändert werden, muß man dies als grobe Fahrlässigkeit bezeichnen. Es ist jedem Systemverwalter anzuraten, die Tabelle der zugelassenen Benutzer daraufhin einmal kritisch zu überprüfen.
- Fast nie wissen die berechtigten Benutzer, an wen sie sich wenden sollen, wenn sie einen Hinweis auf mögliche Sicherheitslücken oder Sicherheitsverletzungen entdeckt haben.

Einige der hier genannten Schwächen und Versäumnisse lassen sich mit durchaus vertretbarem Aufwand beheben. Selbst wenn damit keine absolute Sicherheit erreicht wird, so können doch durchaus wirksame Schranken aufgebaut werden, und schon wenige richtig eingesetzte Überwachungsmaßnahmen können die Entdeckung von Sicherheitsverletzungen so erleichtern, daß ein Angreifer auch im Erfolgsfall daraus nicht lange Nutzen ziehen kann. Ein gutes Mittel dazu ist, daß jeder berechtigte Benutzer zum Beginn jedes Kontaktes mit dem System darüber informiert wird, welche Aktivitäten seit der letzten Information unter seiner Berechtigung durchgeführt wurden. Damit kann die Nutzung seiner Berechtigung durch andere Benutzer zwar nicht verhindert, aber doch wahrscheinlich bald entdeckt werden.

Eine Daueraufgabe für die Systemverantwortlichen ist es dagegen, sich bei jeder Änderung neu über die tatsächlich gegebenen Zugriffs- und Angriffsmöglichkeiten zu informieren und über die Abwehrmaßnahmen oder die bewußte Inkaufnahme des durch diese Maßnahmen nicht abgedeckten Risikos zu entscheiden.

24.2 Personalcomputer am Arbeitsplatz

Die Verarbeitung personenbezogener Daten auf Personalcomputern bleibt weiterhin problematisch, weil im allgemeinen wenig getan wird, um den besonderen Risiken beim Einsatz dieser Geräte als Arbeitsplatzcomputer (APC) entgegenzuwirken. Die Risiken liegen darin, daß die wesentlichen Sicherungskomponenten, die sich bei Großrechenanlagen aus der Arbeitsteilung beim Erbringen einer Serviceleistung für die Anwender beinahe von selbst ergeben, hier fehlen: Das Vier-Augen-Prinzip, die Funktionstrennung, kontrollierte Auftragsverfahren, die Programmfreigabe durch die Fachabteilung und die Beteiligung des Datenschutzbeauftragten an der Verfahrensentwicklung.

Anders als die Großrechenanlage ist der Personalcomputer als der persönliche Computer eines Benutzers entwickelt worden. Auch beim Einsatz am Arbeitsplatz verfügt der Benutzer deshalb selbst (und meist uneingeschränkt) über die Anlage und die Datenträger: Er ist Auftraggeber und Auftragnehmer in einer Person, er verfügt über Betriebssystem und Programme, er verarbeitet die Daten und verwendet die Ergebnisse. Weil es dabei keine Arbeitsteilung mehr gibt, müssen die einzelnen Arbeitsschritte auch nicht mehr besonders aufeinander abgestimmt und organisiert werden, und so überläßt man es gern dem Benutzer selbst, die Arbeit mit „seinem" APC zu organisieren. So alleingelassen, sieht der Benutzer häufig nur seine eigene, aktuelle Aufgabenerfüllung. Deshalb entwickelt er in aller Regel Lösungen, die lediglich seine eigenen Belange berücksichtigen, und übersieht häufig, daß auch andere Aspekte, insbesondere solche des Datenschutzes, zu bedenken sind.

Die Folgen dieses Mangels an übergreifender Organisation hat der Bundesrechnungshof in seiner am 24. März 1988 herausgegebenen „Mitteilung über die Orientierungsprüfung Datensicherung am Arbeitsplatz beim Einsatz von Arbeitsplatzcomputern (APC) bei ausgewählten obersten Bundesbehörden und Behörden des nachgeordneten Bereichs" deutlich geschildert: Es fehlen die für einen ordnungsgemäßen Betrieb erforderlichen Sicherheitsvorkehrungen und der Einsatz ist oft unwirtschaftlich. Die Systeme sind wegen Mängeln in der Organisation nicht beherrschbar, die korrekte Aufgabenerfüllung kann nicht gewährleistet werden. Das entspricht auch meinen Erfahrungen aus Datenschutzkontrollen: Oft werden die gesetzlichen Meldepflichten — z. B. zum Datenschutzregister gem. § 19 Abs. 4 BDSG — beim Einsatz von APC nicht erfüllt, die datenschutzrechtliche Zulässigkeit der Verarbeitung personenbezogener Daten nicht geprüft, die gesetzlich geforderten Sicherungsmaßnahmen unterlassen, und die Behörden können die Verantwortung für die tatsächlich stattfindende Datenverarbeitung oft schon deswegen nicht wahrnehmen, weil die in § 15 BDSG vorgeschriebene Übersicht darüber nicht existiert (siehe auch 6.6 und 2.4).

Da die beschriebenen Versäumnisse nicht nur im Bereich der Bundesverwaltung, sondern auch in den Landesverwaltungen (wie übrigens ähnlich im nichtöffentlichen Bereich) vorkommen, hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz am 10. Oktober 1988 in einem Beschluß darauf hingewiesen, daß Datensicherheit und Ordnungsmäßigkeit der Verarbeitung personenbezogener Daten beim Einsatz kleinerer Datenverarbeitungsanlagen, vor allem von persönlichen Computern (PC) besondere Probleme bereiten. Im Hinblick darauf hat die Konferenz eine Reihe von Empfehlungen gegeben (s. Anlage 4).

Auch die oben erwähnte Prüfungsmitteilung des Bundesrechnungshofs enthält Hinweise zur Verbesserung des APC-Einsatzes und betont dabei auch die Notwendigkeit, die Benutzer umfassend zu schulen.

Während es vor einigen Jahren, als die ersten Personalcomputer angeboten wurden, kaum ausreichende technische Unterstützung zur Lösung des Sicherheitsproblems gab, hat sich die Lage insoweit deutlich gebessert. Es gibt heute eine Reihe von Softwareprodukten zur PC-Sicherung, von denen einige sehr wirksam durch passende Hardwarezusätze verstärkt werden können.

Derartige Software hat im wesentlichen folgende Eigenschaften:

- Es wird eine Benutzeranmeldung mit Benutzername und Paßwort gefordert.
- Es erfolgt eine lückenlose Menüsteuerung; dadurch können nur planmäßige Programme, nicht etwa „selbstgemachte" eingesetzt werden.
- Der Benutzer hat keinen Zugang zur Betriebssystemebene und kann dadurch die Menüsteuerung nicht umgehen.
- Das Laden eines (anderen) Betriebssystems wird verhindert (durch Einbau einer Steckkarte oder auch durch Software).
- Es wird ein Protokoll der Benutzeraktivitäten (Logdatei) geführt.
- Alle Dateien werden kryptographisch verschlüsselt und sind damit nur für die planmäßig vorgesehene Verarbeitung verfügbar.

Nach diesen sehr wirksamen Prinzipien hat z. B. die Deutsche Bundesbahn ihre örtliche Personaldatenverarbeitung mit APC organisiert.

Es sind inzwischen Angebotsverzeichnisse für PC-Sicherheitssoftware erschienen, mit denen sich jeder Benutzer einen Marktüberblick verschaffen und die für ihn geeignete Software auswählen kann.

Es soll jedoch nicht verkannt werden, daß mit der passenden Auswahl und Anschaffung von Sicherheitssoftware nur die *Möglichkeiten* zur Problemlösung verbessert werden. Die Lösung selbst erfordert immer auch Organisationsmaßnahmen. Für die Sicherung gilt genau wie für Fragen der datenschutzrechtlichen Zulässigkeit und des wirtschaftlichen Einsatzes, daß zunächst zu klären ist, wer mit welchem Gerät welche Daten mit welchem Ziel verarbeiten soll. Erst wenn darüber Klarheit besteht, hat es Sinn, Maßnahmen zur Erreichung und Sicherung des gewünschten Zustandes durchzuführen.

Nun ist es gewiß schwierig, schon vor dem Einsatz von APC — und das heißt oft: ohne Erfahrung — alle Festlegungen zu treffen. Deshalb ist es verständlich, daß man den einzelnen Benutzern zunächst freie Hand lassen möchte, schon weil ja häufig niemand weiß, was man eigentlich vorschreiben könnte. Aber auch und vielleicht gerade bei einer solchen Art der APC-Einführung ist es geboten, jeden Benutzer auf die einschlägigen Vorschriften hinzuweisen, weil sonst nicht nur gegen Datenschutzvorschriften, sondern leicht auch gegen Vorschriften zur Kassen- und Abrechnungssicherheit verstoßen werden kann. Außerdem ist das Risiko, unwirtschaftlich zu arbeiten, bei einer solchen Vorgehensweise extrem hoch und kann nur durch begleitende Betreuung in erträglichen Grenzen gehalten werden. Im übrigen ist daran zu erinnern, daß mittlerweile an verschiedenen Stellen für eine Reihe von Aufgaben, die mit APC unterstützt werden können, schon brauchbare Verfahren erarbeitet wurden, so daß es oft wirtschaftlicher ist, sich erst einmal umzuhören, bevor man Arbeitszeit und Geld für eine Eigenentwicklung aufwendet.

Wie immer aber APC eingeführt werden, stets ist es geboten — und in § 15 BDSG auch gesetzlich vorgeschrieben — von Anfang an eine Übersicht über die tatsächlich stattfindende Verarbeitung personenbezogener Daten zu haben und damit die Zulässigkeit und Ordnungsmäßigkeit der einzelnen Verfahren zu kontrollieren. Dies ist eine Organisationsaufgabe, deren Erfüllung erst einmal Aufwand verlangt, aber auch geeignet ist, überflüssigen Aufwand zu vermeiden. Die gesetzliche Verpflichtung dazu ergibt sich auch aus Nr. 10 (Organisationskontrolle) der Anlage zu § 6 Abs. 1 Satz 1 BDSG.

Um über meine zwangsläufig nur seltenen stichprobenartigen Kontrollen hinaus Erkenntnisse darüber zu erlangen, mit welchen Mitteln die obersten Bundesbehörden die dringende Aufgabe angehen, beim APC-Einsatz den Datenschutz zu gewährleisten, und auch um dabei besser beraten und Erfahrungen vermitteln zu können, habe ich im Oktober 1988 eine entsprechende Umfrage begonnen. Die ersten darauf eingegangenen Antworten zeigen, daß dieses Problem sehr ernst genommen wird und die notwendigen Regelungen in zum Teil recht detaillierter Form erlassen wurden oder bald erlassen werden. Es wird darauf ankommen, solche Regelungen allgemein zu schaffen und in die Praxis umzusetzen. Ich werde dem in der nächsten Zeit besondere Aufmerksamkeit widmen.

Bessere Übersicht und mehr Sicherheit beim Einsatz von APC sind auch deswegen erforderlich, weil zum einen diese heute sehr leistungsfähigen Geräte oft schon von mehreren Benutzern zu unterschiedlichen Zwecken genutzt werden. Hier kommt es darauf an, die notwendige Zusammenarbeit der Benutzer zu regeln und jedem Benutzer nur die Aktivitäten zu ermöglichen, die in seiner Zuständigkeit liegen. Zum anderen gibt es eine gewisse Tendenz, die Zusammenarbeit der APC untereinander durch Vernetzung zu fördern. Wenn dabei nicht Transparenz über die Verarbeitungen und die technischen Möglichkeiten im Netz besteht und keine ausreichenden Sicherheitsvorkehrungen getroffen werden, können leicht zwei gegensätzliche Eigenschaften von APC zu einem erheblichen Risiko führen: Einerseits kann ein APC wegen seiner hohen Leistungsfähigkeit in der Hand eines geschickten Benutzers in einem Datennetz leicht zu einem wirksamen Angriffsinstrument werden, dem aber andererseits in Sicherheitsfragen wenig geschulte APC-Benutzer kaum etwas entgegensetzen können, um die Daten vor einem solchen Angriff zu sichern und die Funktionsfähigkeit der Programme zu gewährleisten. Spätestens bei einer Vernetzung führt also das jetzt beim APC-Einsatz häufig gegebene Organisations- und Sicherheitsdefizit zu offenkundig untragbaren und nicht mehr beherrschbaren Risiken.

24.3 Hardcopy

Bei verschiedenen Kontrollen im Berichtsjahr habe ich festgestellt, daß die Bildschirmarbeitsplätze zur Nutzung zentraler DV-Verfahren zunehmend auch mit Druckausgabegeräten ausgestattet sind. Diese dezentralen Drucker werden aber nicht nur dazu genutzt, zentral gesteuerte Ausgaben der gespeicherten Informationen direkt zur Verfügung zu stellen, sondern um bei Bedarf für den Sachbearbeiter das festzuhalten, was sonst nur vorübergehend auf dem Bildschirm steht. Dazu dient die sogenannte Hardcopy-Funktion: Wird die dafür bestimmte Taste gedrückt, so druckt der Drucker den aktuellen Inhalt des Bildschirms in der dort gezeigten Anordnung auf das eingelegte Papier.

Diese einfache Funktion birgt deswegen Risiken, weil eine Protokollierung dabei nicht stattfindet und deshalb solche Ausdrucke beliebig erzeugt und auch leicht mitgenommen werden können. Außerdem können bewußt oder unbewußt auch falsche Angaben ausgedruckt werden, z. B. wenn eine Hardcopy erzeugt wird, nachdem eine Datenanzeige aus dem zentralen DV-Verfahren durch Änderungen oder Ergänzungen über die Tastatur partiell verändert wurde. Gerade weil Computerausdrucke im allgemeinen für so richtig gehalten werden, daß sie nicht einmal mehr unterschrieben werden müssen, liegt hier eine Gefahr. Deshalb ist es geboten, diese einfache und nützliche Arbeitsunterstützung kritischer als oft noch üblich zu betrachten. Zumindest bei der Verarbeitung besonders schützenswerter Daten sollte der Einsatz von Hardcopy-Geräten oder -Funktionen dadurch ersetzt werden, daß jeder von den Benutzern des Verfahrens voraussichtlich benötigte Ausdruck vom Programm vorgegeben und seine Herstellung prüfbar protokolliert wird (siehe auch 11.1 und 21.2.4).

25. Entwicklung des allgemeinen Datenschutzrechts

25.1 Novellierung des Bundesdatenschutzgesetzes

In meinem Zehnten Tätigkeitsbericht (10. TB S. 97) habe ich über den Referentenentwurf eines Artikelgesetzes zur Neufassung des Bundesdatenschutzgesetzes und zur Änderung des Verwaltungsverfahrensgesetzes berichtet und eine summarische datenschutzrechtliche Bewertung dieses Entwurfs vorgenommen. Eine ins einzelne gehende Stellungnahme habe ich im Frühjahr gegenüber dem Bundesminister des Innern abgegeben. Die von mir zu zahlreichen Regelungen des Entwurfs formulierte Kritik und meine Anregungen zu seiner Verbesserung im Sinne des Datenschutzes sind jedoch in keinem bedeutsamen Punkt aufgegriffen oder berücksichtigt worden. Inzwischen hat die Bundesregierung den Entwurf eines Artikelgesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes verabschiedet, in dem außer den genannten Entwürfen auch die Entwürfe der sog. Sicherheitsgesetze — Bundesverfassungsschutzgesetz, MAD-Gesetz, BND-Gesetz — zusammengefaßt wurden.

Die Neuregelungen des Bundesdatenschutzgesetzes und des Verfassungsschutzgesetzes sowie eine erstmalige Regelung der Rechtsgrundlagen für den MAD und den BND sind überfällig. Es ist dringend zu wünschen, daß die Gesetzentwürfe vom Bundestag gründlich beraten und noch in dieser Legislaturperiode verabschiedet werden. Dies liegt nicht nur im Interesse der Bürger, sondern auch in dem der Behörden, die Klarheit darüber haben müssen, welche Konsequenzen sich aus der Rechtsprechung des Bundesverfassungsgerichts zum Recht auf informationelle Selbstbestimmung ergeben.

Auch die SPD-Fraktion hat inzwischen ihre eigenen Vorstellungen von einer Anpassung des BDSG an die verfassungsrechtlichen Vorgaben konkretisiert und den Entwurf eines Bundesinformationsschutzgesetzes eingebracht.

Der Regierungsentwurf knüpft inhaltlich ohne große Änderungen an die Entwürfe aus der 10. Legislaturperiode (Drucksachen 10/4737 und 10/5343) an, so daß ich zur Konzeption auf die Bewertungen in meinem Neunten und Zehnten Tätigkeitsbericht (9. TB S. 75ff., 10. TB S. 97ff.) Bezug nehmen kann, die insgesamt weiter Gültigkeit haben. Ich sehe deshalb auch von einer detaillierten Stellungnahme zum Regierungsentwurf im Rahmen dieses Tätigkeitsberichts ab, wobei ich davon ausgehe, bei den parlamentarischen Beratungen Gelegenheit zur Äußerung zu erhalten. An dieser Stelle möchte ich lediglich Ausführungen zu den mir besonders wichtig erscheinenden Punkten machen.

Der Entwurf enthält eine Reihe von erfreulichen Verbesserungen. So wird klargestellt, daß Datenschutz nicht nur Schutz vor Mißbrauch ist, sondern den Bürger vor Verletzungen seines Persönlichkeitsrechtes schützen soll. Andere Regelungen entsprechen immer wieder erhobenen Forderungen der Datenschutzbeauftragten, so z. B.

- die Regelung nicht nur der Speicherung und sonstiger technischer Verarbeitung personenbezogener Daten, sondern auch ihrer sonstigen Nutzung,
- die Anerkennung der Zweckbindung für personenbezogene Daten,
- die Abschaffung der Entgeltpflicht für die Auskunft über die eigenen Daten und die Ausdehnung der Auskunft auf Herkunft und Empfänger der Daten im öffentlichen Bereich,
- die Pflicht zur Löschung der Daten, die für den Speicherungszweck nicht mehr erforderlich sind,
- die Klarstellung, daß besondere Amtsgeheimnisse der Kontrolle durch den Bundesbeauftragten nicht entgegengehalten werden können, und
- die Verstärkung der Befugnisse der Aufsichtsbehörden für den nicht-öffentlichen Bereich und der Stellung der betrieblichen Datenschutzbeauftragten.

Es kann aber nicht verkannt werden, daß der Entwurf — teilweise auch konzeptionell — Mängel aufweist, die die Gewährleistung des Bürgerrechts auf informationelle Selbstbestimmung beeinträchtigen.

25.1.1 Eingeschränkter Anwendungs- und Geltungsbereich

Ein konzeptioneller Mangel des Regierungsentwurfs ist die Aufspaltung des allgemeinen Datenschutzrechts in Bestimmungen über die Datenverarbeitung in Dateien und Bestimmungen über den aktenmäßigen Umgang mit personenbezogenen Daten. Dabei soll der Anwendungsbereich des BDSG strikt auf die Dateiverarbeitung beschränkt bleiben, während Bestimmungen über die Aktenverarbeitung in das Verwaltungsverfahrensgesetz aufgenommen werden sollen. Diese Trennung ist rechtssystematisch nicht verständlich, weil das Recht auf informationelle Selbstbestimmung für jeden Umgang mit personenbezogenen Daten unabhängig von der Verarbeitungsform gilt und deshalb *allgemeine* Regelungen zu seiner Konkretisierung und seinem Schutz in *einem* Gesetz zusammengefaßt werden sollten. Für den betroffenen Bürger macht es keinen Unterschied, ob etwa unzulässig erhobene Daten in Dateien gespeichert oder in Akten erfaßt werden und ob eine unzulässige Übermittlung etwa aus einer Akte oder einer Datei heraus erfolgt. Erklärbar ist diese Trennung nur durch das Bemühen, eine entscheidende Konsequenz für die Verwirklichung des Rechts auf informationelle Selbstbestimmung, nämlich die externe Datenschutzkontrolle, auf die Dateiverarbeitung zu beschränken und den Bereich der Aktenverarbeitung davon möglichst auszunehmen.

Infolge der Aufsplitterung des allgemeinen Datenschutzrechts auf BDSG und Verwaltungsverfahrensgesetz bleiben zudem weite Bereiche der Datenverarbeitung außerhalb von Dateien datenschutzrechtlich ungeregelt, weil hierauf auch das Verwaltungsverfahrensgesetz keine Anwendung findet, nämlich die Datenverarbeitung bei der Strafverfolgung und der Verfolgung von Ordnungswidrigkeiten sowie bei der Post. Dasselbe gilt für die Datenverarbeitung in Akten bei den Finanzbehörden, für die offenbar Sonderregelungen in der Abgabenordnung geschaffen werden sollen (s.u. 25.2). Ungeregelt bleibt damit auch die Datenverarbeitung außerhalb von Dateien im Bereich der gesamten Privatwirtschaft.

Der Anwendungsbereich des Gesetzes wird ferner durch unzureichende Definitionen von Schlüsselbegriffen des Datenschutzrechts geschmälert. So ist insbesondere der Dateibegriff nicht mehr zeitgemäß und deshalb als entscheidende Voraussetzung für die Gewährung von Datenschutz verfehlt. Die inzwischen erreichte Datenverarbeitungstechnologie — etwa Videoaufzeichnungen, optische Speichermedien und moderne Bürokommunikationssysteme — findet darin keine ausreichende Berücksichtigung. Die Möglichkeit, gespeicherte Daten nach bestimmten Merkmalen ordnen oder umordnen zu können, kann heute kein Anknüpfungspunkt mehr für den Dateibegriff sein. Es kommt vielmehr auf die erleichterte Zugriffs- und Auswertungsmöglichkeit an, die das eigentliche Risiko der Datenverarbeitung darstellt. Es besteht beispielsweise auch dann, wenn ein Anwender, der sich den Beschränkungen des Gesetzes entziehen will, die Möglichkeit des für ihn uninteressanten Umordnens von Daten durch spezifische Techniken ausschließt oder wenn in der Textverarbeitung die gespeicherten Texte zwar nach verschiedenen Kriterien zugreifbar sind, das Umordnen jedoch ausgeschlossen ist, weil dafür kein Bedarf besteht. Neu definiert wurde auch der Begriff „personenbezogenes Datum". Nach dem Regierungsentwurf sind darunter künftig nur noch Einzelangaben „in einer Datei" zu verstehen. Die allgemein eingeführte datenschutzrechtliche Terminologie wird damit an einem ganz zentralen Punkt aufgegeben, ohne daß daraus die erforderlichen Konsequenzen gezogen werden. Eine ganze Reihe von Gesetzen enthält den Begriff „personenbezogene Daten" in einem Sinn, der unzweifelhaft auch Angaben außerhalb von Dateien erfaßt; eine Änderung dieser Gesetze ist nicht vorgesehen.

25.1.2 Unzureichende Verarbeitungsregelungen

Abweichend von inzwischen novellierten Landesdatenschutzgesetzen fehlt im Entwurf eine Regelung über die *Erhebung* personenbezogener Daten. Gleichwohl wird an einigen Stellen des Entwurfs auf den Erhebungszweck Bezug genommen. Eine Vorschrift über die Datenerhebung findet sich lediglich im Entwurf des Verwaltungsverfahrensgesetzes, wo „das Beschaffen" personenbezogener Informationen geregelt wird. Erklärbar wird der Verzicht auf eine Erhebungsvorschrift im BDSG allein aus der Erwägung, den Anwendungsbereich dieses Gesetzes ausnahmslos und strikt auf die *dateigebundene Datenverarbeitung* zu begrenzen. Dieser Ansatz wird jedoch den verfassungsrechtlichen Vorgaben, die mit der Gesetzesnovelle umgesetzt werden sollen, nicht gerecht, denn das Recht auf informationelle Selbstbestimmung betrifft essentiell gerade die Preisgabe von Daten durch den Betroffenen, also die Datenerhebung. Sie ist der erste Schritt und die Voraussetzung für jede nachfolgende Datenverarbeitung.

Die in den Entwurf aufgenommene Regelung über die Verwendung von Daten ist insofern nicht gelungen, als sie sich, wie in den Vorentwürfen, auf die Verwendung personenbezogener Daten „unmittelbar" aus Dateien beschränkt. Ich habe das bereits in meinem Zehnten Tätigkeitsbericht (10. TB S. 98) im einzelnen kritisiert. Zwar wird jetzt in der Begründung des Entwurfs erläutert, daß damit auch die Nutzung von Computerausdrucken, Listen und ähnlichen Arbeitsunterlagen gemeint sei, die aus der Datei hergestellt werden, aber den Dateibegriff nicht selbst erfüllen. Dann aber ist zu fragen, weshalb im Gesetzestext eine Formulierung gewählt wird, die leicht eine gegenteilige Auslegung ermöglicht. Jedenfalls wird an dieser Einschränkung besonders deutlich, wie sehr der Entwurf — an den Möglichkeiten moderner Datenverarbeitungstechniken vorbei — bemüht ist, den Anwendungsbereich des Gesetzes zu begrenzen.

Ebenso wie gegenüber hoheitlichen Eingriffen bedarf das Recht des Bürgers auf informationelle Selbstbestimmung auch im Bereich der *privatwirtschaftlichen Datenverarbeitung* effektiven Schutzes. Die Verarbeitungsregelungen für den nichtöffentlichen Bereich sind im Regierungsentwurf jedoch trotz einzelner Verbesserungen insgesamt eher zu Lasten des Betroffenen verschlechtert worden. Die Generalklauseln des jetzigen 3. und 4. Abschnitts sind neu gefaßt worden. Die Möglichkeiten zur Verarbeitung personenbezogener Daten werden dabei in einigen Bereichen gegenüber dem geltenden Recht erweitert. Die Zulässigkeit der Datenverarbeitung soll grundsätzlich weiterhin von einer Interessenabwägung durch die datenverarbeitende Stelle abhängig gemacht sein, ohne daß die Abwägungskriterien — berechtigte Interessen der datenverarbeitenden Stelle und schutzwürdige Interessen der Betroffenen — konkretisiert oder zumindest Orientierungspunkte für eine derartige Konkretisierung gegeben werden. Die Generalklauseln, die im öffentlichen Bereich wegen des Vorrangs bereichsspezifischer Vorschriften auf vielen Gebieten eine geringere Rolle spielen, führen deshalb hier weiterhin zu vermeidbaren Auslegungsunsicherheiten. Der Entwurf berücksichtigt außerdem nicht, daß die Einwilligung in wichtigen Wirtschaftsbereichen erfahrungsgemäß nur eine unzulängliche Verarbeitungsgrundlage darstellt, wenn sie in Rechtsverhältnissen abgegeben wird, bei denen die Verarbeitungsbedingungen kraft einseitiger Regelungsmacht von der wirtschaftlich stärkeren Vertragsseite festgelegt werden. Zusammen mit dem Fehlen bereichsspezifischer Datenschutzbestimmungen etwa im Zivil- oder Wirtschaftsverwaltungsrecht führt dies in manchen Bereichen der Privatwirtschaft im Vergleich mit dem öffentlichen Bereich zu einem materiellen Datenschutzdefizit für den Betroffenen.

Unbefriedigend ist schließlich die vorgesehene Bestimmung über die Verarbeitung und Nutzung personenbezogener Daten für die *wissenschaftliche Forschung*. Der Versuch, mit nur einer Bestimmung alle Aspekte des Umgangs mit personenbezogenen Daten zu Forschungszwecken zu erfassen, ist — vielleicht zwangsläufig — nicht geglückt. Die Unsicherheit darüber, wann diese Forschungsklausel gilt, beginnt bereits mit der Frage, was als „Wissenschaftliche Forschung" anzusehen ist. Eine normenklare und deshalb verläßliche Grundlage für den Umgang mit personenbezogenen Daten in der Forschung ist aber notwendig.

25.1.3 Mangelhafte Ausprägung der Rechte des Bürgers

Mit dem Regierungsentwurf soll zugunsten des Betroffenen erstmals ein verschuldensunabhängiger *Schadenersatzanspruch* in das BDSG eingeführt werden. Der Betroffene soll Schäden, die er erleidet, weil personenbezogene Daten bei dem „Betrieb einer automatisierten Datenverarbeitungsanlage unrichtig oder nach Überwindung automatisierter Sicherungseinrichtungen Unbefugten zugänglich werden", geltend machen können, ohne den Nachweis eines Verschuldens der speichernden Stelle führen zu müssen. Bei Schäden, die durch Eingabe- oder Bedienungsfehler oder etwa durch eine unzulässige Übermittlung infolge mangelhafter Datenverarbeitungsorganisation entstehen, muß der Betroffene dagegen weiterhin auf der Grundlage des allgemeinen Schadenersatzrechts ein Verschulden der datenverarbeitenden Stelle nachweisen. Schäden dieser Art dürften ungleich häufiger sein als etwa das nur schwer vorstellbare „automatische Unrichtigwerden" eines Datums. Der Schadenersatzanspruch ist deshalb in der vorgesehenen Form nur von begrenztem Wert für den Betroffenen. Um wirklich effektiv zu sein, müßte er stärker differenziert und für die genannten Fälle durch einen Schadensersatzanspruch mit Beweislastumkehr hinsichtlich des Verschuldens ergänzt werden.

Der Regierungsentwurf sieht für die Verfassungsschutzbehörden, den BND, den MAD und „andere Behörden des BMVg" weiterhin ein pauschales *Auskunftsverweigerungsrecht* ohne Begründungszwang vor. Er berücksichtigt damit nicht die inzwischen zu dieser Frage ergangene Rechtsprechung, die auf verfassungsrechtlichen Grundlagen (Art. 19 Abs. 4 GG) basiert. Die im Entwurf vorgesehene Möglichkeit, die Auskunft in diesen Fällen an den BfD zu erteilen, beschreibt das gegenwärtig zwischen mir und den Sicherheitsbehörden praktizierte Verfahren. Doch

dieses ist unbefriedigend, weil auch meine Mitteilung an den Betroffenen diesen über den Erkenntnisstand der jeweiligen Sicherheitsbehörde im Unklaren lassen muß. Das verstärkt vermutlich in der Mehrzahl gerade der Fälle, in denen keine Angaben über den Betroffenen gespeichert sind, dessen Befürchtungen, doch vom Verfassungsschutz registriert worden zu sein und daraus Nachteile zu erleiden. Über die verfassungsrechtlichen Zweifel an diesem Verfahren habe ich in meinen Tätigkeitsberichten wiederholt berichtet.

Im nicht-öffentlichen Bereich wird die Anspruchsgrundlage für ein *Auskunftsentgelt* aufrechterhalten, soweit Daten geschäftsmäßig für fremde Zwecke gespeichert werden und der Betroffene die Auskunft zu wirtschaftlichen Zwecken nutzen kann. Da die Handelsauskunfteien Auskünfte an Betroffene schon aus Akzeptanzgründen kostenlos erteilen, kommt diese Bestimmung inzwischen praktisch ausschließlich der SCHUFA zugute. Damit bleibt die Auskunft, die dort mit weitem Abstand am häufigsten eingeholt wird, auch zukünftig in der Praxis weiter kostenpflichtig.

25.1.4 Einschränkung der Datenschutzkontrolle

Über die vorgesehenen Einschränkungen meiner Kontrollkompetenz habe ich in den vorangegangenen Tätigkeitsberichten (9. TB S. 78, 10. TB S. 99) im einzelnen berichtet. Diese Ausführungen gelten im vollen Umfang auch für den neuen Regierungsentwurf. Zu einer erheblichen Einschränkung meiner Kontrollbefugnis gegenüber der bisherigen Praxis führt die Neuregelung vor allem deshalb, weil keinerlei Kontrolle im Bereich der Datenerhebung vorgesehen ist. Würde diese Regelung Gesetz, so könnte ich eine große Zahl von Eingaben, die ausschließlich die Datenerhebung betreffen — Beispiele dafür enthält der Abschnitt 1.1 — nicht mehr bearbeiten, wenn dazu eine Kontrolle notwendig ist. Die Kontrolle im Bereich der Datenverarbeitung hat nach dem Entwurf grundsätzlich nur die Verarbeitung oder Nutzung „in oder unmittelbar aus Dateien" zum Gegenstand. Außerhalb der Dateiverarbeitung wird meine Kontrollbefugnis auf eine anlaßbezogene Einzelfallprüfung beschränkt, was keinen Fortschritt darstellt, weil sie mir in den meisten Fällen bisher schon zugestanden wurde. Die Bundesbehörden müssen nach dem Wortlaut des Entwurfs zudem dem Bundesbeauftragten Auskunft nur noch zu Fragen geben, die mit seiner Kontrolltätigkeit in Zusammenhang stehen; es wird damit zweifelhaft, ob solche Auskünfte bei der ebenso bedeutsamen Beratungstätigkeit des Bundesbeauftragten oder bei Eingaben von Bürgern, wenn der Bundesbeauftragte diese nicht zum Anlaß einer Kontrolle macht, zu erteilen sind. Es wird an dieser Stelle augenfällig, wie sehr der Entwurf bemüht ist, eine unabhängige Datenschutzkontrolle, der das Bundesverfassungsgericht erhebliche Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung beimißt, möglichst eng zu begrenzen.

Die Rundfunkanstalten des Bundes, Deutschlandfunk und Deutsche Welle, werden auch hinsichtlich ihrer Verwaltungstätigkeit von jeglicher Kontrolle durch den Bundesbeauftragten für den Datenschutz freigestellt. Diese Privilegierung der Medien, für deren journalistisch redaktionelle Tätigkeit von den Vorschriften des Gesetzes nur die über die Datensicherung gelten, geht weiter als die der Gerichte, deren Verwaltungstätigkeit der Datenschutzkontrolle in vollem Umfang unterliegt.

Ob und in welchem Umfang die Freistellung karitativer und erzieherischer, den öffentlich-rechtlichen Religionsgesellschaften zugeordneter Einrichtungen des privaten Rechts von der staatlichen Datenschutzkontrolle nach Art. 140 GG in Verbindung mit Art. 137 der Weimarer Verfassung wirklich geboten ist, sollte im Hinblick auf die Rechtslage in vergleichbaren staatlichen oder kommunalen Einrichtungen (z. B. Kindergärten, Krankenhäuser, Schulen) noch einmal geprüft werden.

Im Ergebnis entspricht der Entwurf — trotz anzuerkennender Verbesserungen — auf die ich oben hingewiesen habe, nicht den Erwartungen. Er erweckt insbesondere gegenüber vergleichbaren Länderregelungen den Eindruck einer Besorgnis vor zu viel Datenschutz und vor der Kontrolltätigkeit des Bundesbeauftragten. Es ist dringend zu wünschen, daß die bestehenden Mängel im Laufe des Gesetzgebungsverfahrens noch behoben werden.

25.2 Bereichsspezifische Datenschutzvorschriften für die Finanzverwaltung

Der Bundesminister der Finanzen hat mir gegen Ende des Berichtsjahres einen Gesetzentwurf bereichsspezifischer Datenschutzvorschriften im Anwendungsbereich der Abgabenordnung zur Stellungnahme zugeleitet. Mit dem Entwurf sollen das von der Finanzverwaltung anzuwendende Datenschutzrecht, das sich aus dem Bundesdatenschutzgesetz und den Landesdatenschutzgesetzen zum Teil unterschiedlich ergibt, vereinheitlicht und darüber hinaus für den Anwendungsbereich der Abgabenordnung *ausschließlich* und abschließend geltende Datenschutzvorschriften geschaffen werden.

Eine umfassende Bewertung wird mir erst nach Kontakten mit den Landesbeauftragten für den Datenschutz möglich sein, die der Entwurf in gleicher Weise berührt wie mich. Bereits jetzt weise ich darauf hin, daß der Entwurf hinter dem Standard des Bundesdatenschutzgesetzes wie auch des neuen Regierungsentwurfs für ein Bundesdatenschutzgesetz erheblich zurückbleibt. Als Beispiele nenne ich:

— Nach dem Entwurf des BMF soll die Speicherung und Veränderung geschützter Daten zulässig sein, soweit diese der Erfüllung der den Finanzbehörden durch Rechtsvorschrift übertragenen Aufgaben *„dienen"*. Nach § 9 Abs. 1 des Bundesdatenschutzgesetzes (BDSG) ist demgegenüber präzise nachvollziehbar und sachgerecht festgelegt, daß das Speichern und Verändern personenbezogener Daten zulässig ist, wenn es zur rechtmäßigen Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben *„erforderlich ist"*. Der Regierungsentwurf für ein Bundesdatenschutzgesetz hat diesen allgemein anerkannten Grundsatz

des Datenschutzrechts übernommen und im übrigen noch weiter verstärkt. Die Fassung des Entwurfs des BMF würde mit dem Wort „dienen" zu einer nicht vertretbaren und mit der Rechtsprechung des Bundesverfassungsgerichts nicht vereinbaren Aufweichung des Datenschutzes im Bereich der Abgabenordnung führen. Die in der Speicherung und Veränderung personenbezogener Daten liegenden Einschränkungen einer verfassungsrechtlich geschützten Rechtsposition sind nur zulässig, soweit sie zum Schutz öffentlicher Interessen unerläßlich sind, nicht schon dann, wenn sie solchen lediglich „dienen".

- Nach § 21 BDSG kann sich jedermann an den Bundesbeauftragten für den Datenschutz wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch Behörden oder sonstige öffentliche Stellen des Bundes in seinen Rechten verletzt zu sein. Der Regierungsentwurf für ein Bundesdatenschutzgesetz sieht darüber hinaus noch vor, daß dieses Recht dem Bürger auch hinsichtlich „der Verwendung ihn betreffender Informationen außerhalb von Dateien", also auch in Akten, zusteht; dies soll künftig ausdrücklich auch im Anwendungsbereich des Steuergeheimnisses gelten. Der Gesetzentwurf des BMF enthält demgegenüber *keine* entsprechende Regelung. Damit nimmt er den Betroffenen im Rahmen der Abgabenordnung das Recht, den Bundesbeauftragten für den Datenschutz anzurufen, um sich gegen mögliche Verletzungen seines Rechts auf informationelle Selbstbestimmung zu wehren. Dies ist angesichts der vom Bundesverfassungsgericht betonten Bedeutung der unabhängigen Datenschutzbeauftragten nicht hinnehmbar.

- Nach dem Entwurf des BMF dürfen dem Bundesbeauftragten für den Datenschutz geschützte Daten „nur offenbart werden, soweit der Betroffene eingewilligt oder nach vorheriger schriftlicher Benachrichtigung durch den Bundesbeauftragten für den Datenschutz unter Hinweis auf diese Folge einer Offenbarung nicht widersprochen hat". Die Finanzbehörde darf dem Bundesbeauftragten für den Datenschutz für diesen Zweck Namen und Anschrift des Betroffenen offenbaren. Da meine Kontrolltätigkeit dem Schutz der Bürger dient, habe ich selbstverständlich nicht die Absicht, Kontrollen gegen den erkennbaren Willen eines Betroffenen durchzuführen. Von entscheidender Bedeutung ist dabei aber, wie der Wille des Betroffenen festgestellt werden soll. Gegen ein Widerspruchsrecht des Betroffenen wäre nichts einzuwenden, wenn dies so ausgestaltet ist, daß dadurch in der Praxis nicht Kontrollen der Datenverarbeitung einer Behörde schlechthin verhindert oder unzumutbar erschwert werden. Eine Regelung, die mich zur vorherigen Befragung aller Betroffenen nach ihrer Einwilligung oder einem etwaigen Widerspruch verpflichtet, ist nicht akzeptabel. Bei Kontrollen im Bereich der Steuer- und Zollfahndung würde ein solches Verfahren auch kaum im Interesse der Finanzbehörden liegen.

Ich habe dem Bundesminister der Finanzen bereits meine grundsätzlichen Bedenken vorgetragen; hierauf hat er sein Interesse an eingehenden Gesprächen, insbesondere über die oben angesprochenen Punkte mitgeteilt.

26. Ausland und Internationales

26.1 Europarat

Die internationale Harmonisierung des Datenschutzes mit dem Instrument der Datenschutzkonvention des Europarats schreitet beständig fort, wenn auch festgestellt werden muß, daß die Entwicklung — verglichen mit den ursprünglichen Erwartungen und der anhaltenden Dynamik in der Technologie und Anwendung der automatisierten Datenverarbeitung — außerordentlich schleppend verläuft. Zwar haben inzwischen neunzehn von einundzwanzig Mitgliedern des Europarats die Konvention gezeichnet (außer der Schweiz und Liechtenstein), doch liegt die Anzahl der Mitgliedsstaaten, die die Konvention ratifiziert, d. h. verbindlich gemacht haben, immer noch bei nur acht (Österreich, Frankreich, Bundesrepublik Deutschland, Luxemburg, Norwegen, Spanien, Schweden, Großbritannien). Unter diesen Ländern befindet sich überdies eines, bei dem fraglich ist, ob derzeit die Voraussetzungen für eine Ratifikation vorliegen, da es kein Datenschutzgesetz besitzt. Von dem mit der Konvention verfolgten Ziel, in Europa — und möglichst darüber hinaus — einen definierten Mindeststandard des Datenschutzes zu garantieren und im gleichen Zuge spezifische Behinderungen des grenzüberschreitenden Datenverkehrs auszuschließen, sind wir damit nach wie vor weit entfernt.

Wenn es gleichwohl beim grenzüberschreitenden Datenverkehr mit oder zwischen Nicht-Vertragsstaaten keine größeren Probleme gegeben hat, so dürfte das daran liegen, daß die Gesetzesanwender der Frage, ob im Empfängerland ein gleichwertiger Datenschutz besteht, ausweichen. Für die Betroffenen bedeutet dies, daß ihre Daten in der Praxis vielfältig auch dann ins Ausland übermittelt werden, wenn sie dort keine Auskunfts- und Berichtigungsrechte haben, keine besonderen Vorschriften gegen eine zweckfremde Verwendung und Weitergabe ihrer Daten bestehen und auch eine Löschung nach einer bestimmten Zeit nicht gesichert ist. Die Aufsichtsbehörden haben nur in wenigen Ländern und nur in seltenen Fällen grenzüberschreitende Datenübermittlungen untersagt oder beanstandet. Diese Zurückhaltung ist insofern verständlich, als eine negative Entscheidung in der Regel nur mit einer abstrakten rechtlichen Schlechterstellung begründet werden kann. Konkrete Mißbrauchsfälle im Empfängerland sind zwar nicht auszuschließen, aber meist nicht bekannt. Für die Notwendigkeit der Übermittlung werden dagegen in aller Regel konkret bezifferbare wirtschaftliche Interessen des Datenempfängers oder der übermittelnden Stelle geltend gemacht. Wenn die Bedenken allerdings immer wieder zurückgestellt werden, so kommt es in den Empfängerländern nicht zu dem offensichtlich notwendigen Handlungsdruck. Im Interesse einer zügigeren internationalen Verbreiterung des Datenschutzes könnte sich daher eine Überprüfung der Entscheidungspraxis empfehlen.

Symptomatisch für die Konsequenzen eines international nicht abgestimmten Datenschutzes ist folgender Vorgang: Ein schweizerisches Unternehmen bestellte bei einer deutschen Kreditauskunftei eine Auskunft über einen Bundesbürger. Die formularmäßig geforderte Darlegung eines berechtigten Intesses entsprechend § 32 Abs. 2 BDSG lehnte das Unternehmen ab, da dies dem schweizerischen Datenschutz widerspreche. Es ist im übrigen nicht bekannt, ob die Auskünfte verweigert worden sind; Beschwerden schweizerischer Firmen sind freilich nicht bekannt geworden.

Unproblematisch ist die grenzüberschreitende Datenübermittlung aber auch zwischen Vertragsstaaten nicht. Die Ratifikation der Europaratskonvention setzt zwar voraus, daß der ratifizierende Staat das in der Konvention definierte Datenschutzniveau in seiner Rechtsordnung realisiert hat. Ob diese Voraussetzung gegeben ist, bestimmt der betreffende Staat aber selbst. Eine Überprüfung durch Organe des Europarats ist nicht vorgesehen. Von den Regierungen der Vertragsstaaten, einschließlich der Bundesregierung, ist nicht bekannt, daß sie überprüft haben, ob die anderen Vertragsstaaten die Voraussetzungen der Ratifikation tatsächlich erfüllen. Auch wissenschaftliche Untersuchungen zu diesem Thema liegen nicht vor. Dabei enthält die Konvention mehrere unbestimmte Begriffe und weitgehende Ausnahmeklauseln, die in sehr unterschiedlicher Weise verstanden werden können. Solche Überprüfungen erscheinen aber dringend notwendig. Der Mechanismus der Konvention besteht, vereinfacht ausgedrückt, darin, daß eine Übermittlung zwischen Vertragsstaaten wie eine Übermittlung im Inland zu behandeln ist. Eine Übermittlung kann insbesondere nicht mehr mit der Begründung verboten werden, der Datenschutz im Empfängerland sei nicht ausreichend. Mit der Ratifikation der Konvention durch die beteiligten Staaten soll diese Frage ein für allemal beantwortet sein. Da es in der Bundesrepublik ein besonderes Prüfungs- oder Genehmigungsverfahren für die grenzüberschreitende Datenübermittlung nicht gibt, müssen sich die datenverarbeitenden Stellen darauf verlassen können, daß die Vertragsstaaten tatsächlich das von der Datenschutzkonvention geforderte Schutzniveau realisiert haben. Entsprechende Untersuchungen könnte die Bundesregierung veranlassen. Die österreichische Bundesregierung hat in diesem Sinne durch Verordnung förmlich festgestellt, in welchen Ländern ein im Verhältnis zum österreichischen Recht gleichwertiger Datenschutz besteht.

Eine Möglichkeit, der Frage der korrekten Befolgung der Konvention nachzugehen, bietet grundsätzlich auch der Beratende Ausschuß nach Artikel 18 bis 20 der Konvention, der u. a. Vorschläge zur Fortentwicklung des Inhalts der Konvention machen und auf Antrag einer Vertragspartei zu Fragen der Anwendung der Konvention Stellung nehmen soll. Ihm gehören Vertreter der Regierungen der Vertragsstaaten an. Er hat bisher zweimal getagt und dabei u. a. Berichte der Vertragsstaaten über die jeweilige nationale Umsetzung der Konvention entgegengenommen. Des weiteren sollen die nationalen Erfahrungen bei der Anwendung der Konventionsregelung über den grenzüberschreitenden Datenverkehr ausgewertet werden.

Mir erscheint allerdings zweifelhaft, ob der Beratende Ausschuß für eine Überprüfung der Ratifikationsvoraussetzungen geeignet ist. Mit der Ratifikation hat jeder Vertragsstaat völkerrechtlich verbindlich erklärt, daß seine nationale Gesetzgebung den Anforderungen der Konvention entspricht. Mit Selbstkritik ist danach nicht zu rechnen. Auch eine Kritik gegenüber den anderen Vertragsstaaten wird anscheinend als untunlich betrachtet. Selbst die Ratifikation durch einen Staat, der kein Datenschutzgesetz hat, hat bei den anderen Vertragsstaaten zu keinen erkennbaren Reaktionen geführt. Auch werden die Berichte der nationalen Datenschutzinstitutionen nicht ausgetauscht. Angesichts dieser Gegebenheiten besteht zur Zeit wenig Aussicht, daß der Beratende Ausschuß zur Effektivität der Konvention wesentliches beitragen wird.

Ich rege an, die Wirksamkeit der Europaratskonvention zu überprüfen. Es droht die Gefahr, daß diese ein Dokument des guten Willens bleiben wird, das praktisch vielfach folgenlos bleibt.

26.2. Entwicklung des Datenschutzes im Ausland

Die Anzahl der Länder mit einer nationalen Datenschutzgesetzgebung ist im Berichtsjahr von elf auf vierzehn gestiegen und hat sich damit erstmals seit Jahren wieder deutlich erhöht. Aber auch inhaltlich werden neue Wege beschritten. Aus der historischen Entwicklung erklärbare Grenzen des Anwendungsbereichs, die jedoch dem Schutz des Rechtsguts abträglich sind, werden zunehmend abgebaut. Daneben geht die Suche nach der besten Methode weiter, wie die sehr abstrakten Datenschutzgrundsätze in konkrete Handlungsvorgaben für die verschiedenen Lebensbereiche umgesetzt werden können. Für die Bundesrepublik Deutschland bedeutet dies, daß nur eine konsequente Fortentwicklung des Datenschutzrechts ausreicht, um im internationalen Vergleich einen Platz in der Spitzengruppe zu halten.

Das zu Jahresbeginn in Kraft getretene finnische Datenschutzgesetz enthält mehrere Regelungen, die auch für die Novellierung des Bundesdatenschutzgesetzes vorbildlich sein könnten. Dazu zählen beispielsweise die Vorschriften zur Sicherung der Datenqualität, zur Bestimmung und Einhaltung des Verarbeitungszwecks, zur Rechenschaft über Datenquellen, zum grenzüberschreitenden Datenverkehr und zur Benachrichtigung des Betroffenen über bei der Direktwerbung verwendete personenbezogene Daten sowie bei Kreditentscheidungen.

Das niederländische Gesetz (zum Inhalt vgl. 10. TB, S. 100) konnte zum Jahresende endlich verabschiedet werden. Von der Überlegung, die Registrierungskammer — entsprechend der britischen Lösung — in ein strukturschwaches Gebiet zu legen, hat man wieder Abstand genommen und einem Standort am Regierungssitz den Vorzug gegeben. Die Niederlande befassen sich auch mit bereichsspezifischer Datenschutzgesetzgebung auf den Gebieten der polizei-

lichen Datenverarbeitung, der Bevölkerungsregister und der Verwendung von Sozialversicherungs- und Steuernummern. Außerdem ist die Ratifizierung der Europaratskonvention eingeleitet.

Das im Juli verabschiedete irische Datenschutzgesetz folgt weithin den Vorgaben der Datenschutzkonvention des Europarats. Als Besonderheit ist zu erwähnen, daß der unabhängige Datenschutzbeauftragte die Befolgung des Gesetzes bei den datenverarbeitenden Stellen auch mit Hilfe von Zwangsbefugnissen durchsetzen kann. Der Datenschutzbeauftragte hat auch die Aufgabe, die branchenweise self regulation, d. h. die Entwicklung von branchenspezifischen Regelungen durch die Angehörigen bestimmter Berufe oder Geschäftszweige, zu unterstützen. Er kann solche Regelungen in einem förmlichen Verfahren allgemeinverbindlich machen. Darüber hinaus können solche Regelungen durch Zustimmungsakt des Parlaments Gesetzeskraft erhalten.

In Australien wurde im November mit dem Privacy Act 1988 erstmals ein Datenschutzgesetz auf nationaler Ebene parlamentarisch verabschiedet. Die Provinz New South Wales hatte schon 1975 mit dem Privacy Committee Act den Datenschutz in einer mit den europäischen Gesetzen vergleichbaren Weise geregelt und zur Kontrolle das Privacy Committee installiert. Kernstück des neuen Gesetzes sind die elf Privacy Principles, die im wesentlichen an die Grundsätze der Europaratskonvention und der OECD-Leitlinien anschließen. Von besonderem Interesse ist der Anwendungsbereich des Gesetzes. Es bezieht sich auf „personal information" d. h. Angaben über bestimmte oder bestimmbare natürliche Personen. Auf eine automatisierte Verarbeitung, auf das Vorliegen einer Datei oder auf eine andere besondere Organisationsform kommt es nicht an. Generalklauselartige Ausnahmen, die zu den Schwachstellen mancher Datenschutzgesetze gehören, werden strikt vermieden. Statt dessen können Gesetzesadressaten, die glauben, aufgrund ihrer spezifischen Aufgabenstellung die gesetzlichen Anforderungen nicht erfüllen zu können, beim Privacy Commissioner eine Befreiung von bestimmten Vorschriften beantragen. Australien widerlegt damit die verbreitete Ansicht, ein umfassender, auch die aktenmäßige Verarbeitung einbeziehender Anwendungsbereich müsse zwangsläufig zu einer Verwässerung der materiellen Grundsätze führen. Außerdem hat das australische Modell den Vorzug, daß es zu Befreiungen von Datenschutzgrundsätzen nur insoweit führt, als dafür eine konkrete Notwendigkeit dargetan ist. Zugleich reduziert das Gesetz den bürokratischen Aufwand, der mit dem in Europa verbreiteten Lizensierungsverfahren verbunden ist.

Das Interesse am Datenschutz hat jetzt auch in Amerika wieder deutlich zugenommen. Der in den USA im Berichtsjahr verabschiedete Computer Matching and Privacy Protection Act of 1988 (Public Law 100—503) befaßt sich mit dem Abgleich von Verwaltungsdateien zu dem Zweck, Hinweise auf einen ungerechtfertigten Bezug von Sozialleistungen oder andere Unregelmäßigkeiten zu gewinnen. Das Gesetz zielt vor allem darauf ab, die verfahrensmäßigen Rechte der betroffenen Bürger zu schützen und sie davor zu bewahren, daß die Ergebnisse eines Dateienabgleichs zum Wegfall von Leistungen führen, ohne daß sie Gelegenheit zur Stellungnahme haben. In der Vergangenheit war es infolge fehlerhafter und inaktueller Daten sowie unrichtiger „Treffer" zu zahlreichen Fehlentscheidungen mit teilweise schwerwiegenden sozialen Folgen gekommen. Das neue Gesetz verlangt von jeder an einem Matching-Programm beteiligten Behörde die Bildung eines Data Integrity Board (Ausschuß für Datenintegrität), der die Vereinbarungen zum Datenabgleich und deren Anwendung überprüft und dem Office of Management and Budget jährlich zu berichten hat. Das Gesetz selbst verpflichtet die Verwaltungsbehörden, die Anforderungen des Datenschutzes und der Datensicherheit vorab im einzelnen festzulegen und vor einer Sachentscheidung den Betroffenen Gelegenheit zur Stellungnahme während einer Äußerungsfrist von 30 Tagen zu geben. Das Gesetz regelt damit wesentliche Fragen des Verwaltungsverfahrens, hat aber, indem es der Datenqualität dient und vor unbefugter Datenverarbeitung wie auch vor spezifischen Risiken der automatisierten Verarbeitung schützt, auch ganz wesentlich Datenschutzcharakter.

Im Oktober hat der Kongreß außerdem den Video Privacy Protection Act (Senate 2361) verabschiedet. Er schützt die Entleiher und Käufer von Video-Aufnahmen vor einer Weitergabe personenbeziehbarer Angaben darüber, welche Aufnahmen sie gekauft oder geliehen haben. Kundenadressen dürfen zwar weiterhin verliehen werden, aber nur, nachdem jedem Kunden Gelegenheit zum Widerspruch gegeben wurde, und auch dann nur ohne Bezeichnung oder Beschreibung der gekauften oder entliehenen Titel. Eine Bestimmung, die auch Daten über das Leihverhalten bei Bibliotheken unter besonderen Schutz stellen sollte, wurde dagegen vom Repräsentantenhaus mit Rücksicht auf die Interessen der Strafverfolgung nicht verabschiedet. Auslöser dieser Gesetzesinitiative war die Zeitungsveröffentlichung einer Liste von Videokassetten, die angeblich der Kandidat für den obersten Gerichtshof Robert Bork genutzt haben sollte.

26.3 Datenschutz bei inter- und supranationalen Organisationen

Der Europarat und die OECD, die sich seit rund zwei Jahrzehnten um eine Verankerung des Datenschutzes im internationalen Zusammenhang bemühen, haben den Datenschutz jetzt auch für den eigenen Organisationsbereich förmlich institutionalisiert.

Die OECD hat „Grundsätze für den Schutz der Privatsphäre bei der Errichtung und Verwendung personenbezogener Dateien" aufgestellt, die Empfehlungscharakter haben. Sie orientieren sich inhaltlich an den OECD-Leitlinien vom 23. September 1980 (BAnz. Nr. 215 vom 14. November 1981) und enthalten darüber hinaus organisatorische Regelungen, etwa dahin gehend, daß eine Verknüpfung zwischen verschiedenen personenbezogenen Dateien nur von wenigen Führungspersonen angeordnet werden darf. Außerdem wurde eine besondere Kommission eingerichtet. Sie besteht mehrheitlich aus Bediensteten der OECD, die von deren Organisationseinheiten vorgeschlagen und vom Generalsekretär ernannt werden, in der Aus-

übung ihrer Funktion aber unabhängig sind. Die Kommission soll zu Beschwerden von Mitarbeitern Stellung nehmen und den Generalsekretär in Datenschutzfragen beraten.

Die vom Generalsekretär des Europarats erlassene „Regelung eines Datenschutzsystems für personenbezogene Dateien im Europarat", die sich inhaltlich an die Grundsätze der Datenschutzkonvention des Europarats anlehnt, hat dagegen bindenden Charakter und umfaßt gleichermaßen automatische wie manuell betriebene Datensammlungen. Personenbezogene Daten dürfen danach nur erhoben, gespeichert und verwendet werden, wenn dies der Durchführung notwendiger interner Verwaltungsmaßnahmen oder der Erfüllung der in den Statuten niedergelegten Funktionen dient. Ein Datenschutzbeauftragter wird vom Beratenden Ausschuß nach Artikel 18 der Datenschutzkonvention auf der Grundlage einer Vorschlagsliste des Generalsekretärs gewählt. Er soll Beschwerden Betroffener nachgehen, auf Wunsch des Generalsekretärs zu Fragen der Anwendung der Datenschutzregelung Stellung nehmen und kann sich jederzeit an den Generalsekretär wenden.

Für die Europäischen Gemeinschaften ist eine verfahrensmäßige und institutionelle Verankerung des Datenschutzes noch viel dringlicher, da sie durch Verwaltung und Normsetzung in weit größerem Umfang als die genannten Organisationen eine personenbezogene Datenverarbeitung und -nutzung veranlassen — und zwar nicht nur in der eigenen Organisation, sondern auch bei den Mitgliedsstaaten. Über verschiedene Bereiche, die datenschutzrechtliche Probleme aufwerfen, habe ich vor vier Jahren berichtet und empfohlen, daß die Bundesregierung Initiativen zur Verankerung des Datenschutzes auf EG-Ebene ergreifen möge (7. TB S. 95f.). Über entsprechende Aktivitäten der Bundesregierung oder der Organe der Europäischen Gemeinschaften ist mir nichts bekannt geworden. Ich erneuere deshalb meinen Appell.

26.4 Internationale Zusammenarbeit im Sicherheitsbereich (Schengener Übereinkommen)

Der Bundesminister des Innern strebt an, parallel zum Abbau der Grenzkontrollen in Europa intensivere Formen der Zusammenarbeit zwischen den Sicherheitsbehörden zu erreichen. Auf die Notwendigkeit, in diesem Zusammenhang auch den Datenschutz auszubauen und auf eine internationale Ebene zu stellen, habe ich hingewiesen (8. TB S. 39f.). Ausgehend von meinen Anregungen hat die Bundesregierung den EG-Partnern im Rahmen der Verhandlungen über Ausgleichsmaßnahmen beim Abbau der Grenzkontrollen die Vereinbarung bestimmter datenschutzrechtlicher Mindeststandards vorgeschlagen (Stellungnahme der Bundesregierung zum Achten Tätigkeitsbericht vom 27. 8. 1986 S. 46f.).

Seit längerer Zeit laufen zwischen den Partnern des Schengener Übereinkommens (Frankreich, Benelux-Staaten, Bundesrepublik) Verhandlung mit dem Ziel, im Sinne derartiger Ausgleichsmaßnahmen übergreifende Informationssysteme zur Unterstützung von bestimmten Aufgaben in den Bereichen der Grenzkontrolle, der Polizei und des Asylwesens zu errichten. Entsprechende völkerrechtliche Verträge sind in Vorbereitung. Dabei sind auch wichtige Fragen des Datenschutzes zu entscheiden.

26.5 Zusammenarbeit der Datenschutz-Kontrollinstanzen

Die internationale Datenschutzkonferenz, die 1988 in Norwegen stattfand, befaßte sich mit aktuellen Problemen. Bei der Entwicklung der Telekommunikation wurde auf bedeutsame Konsequenzen für den Datenschutz infolge der Internationalisierung von Planungsentscheidungen und der Privatisierung von Leistungsträgern hingewiesen. Unter den technischen Aspekten interessierte die Frage der Steuerbarkeit der Anruferidentifikation im diensteintegrierenden Telefonnetz. Auf dem Gesundheitssektor wurde der Umgang mit Angaben über eine HIV-Infektion erörtert. Ich referierte über Datenschutzprobleme bei der Strukturreform des Gesundheitswesens in der Bundesrepublik Deutschland. Aus Schweden wurde über eine Neuregelung berichtet, die Datenschutzfragen bei der dv-gestützten steuerlichen Buchprüfung klärt, insbesondere die Art und Weise der Nutzung der dabei erlangten personenbezogenen Daten.

Zehn Jahre nachdem der damalige Bundesbeauftragte Prof. Bull zur Gründung der Internationalen Datenschutzkonferenz nach Bonn eingeladen hat, wird die Bundesrepublik Deutschland im Jahre 1989 wieder Gastgeber der Konferenz sein. Sie soll Ende August im zeitlichen Zusammenhang mit der Internationalen Funkausstellung in Berlin stattfinden. Der Deutsche Bundestag hat freundlicherweise Konferenzräume im Reichstagsgebäude zur Verfügung gestellt. Thematischer Schwerpunkt werden die Internationalisierung des Datenverkehrs und die damit verbundenen Anforderungen an den Datenschutz sein.

27. Bilanz

Ebenso wie dieser Bericht behandelte auch mein Zehnter Tätigkeitsbericht eine Reihe von Einzelfragen, zu denen noch nicht über annehmbare Ergebnisse berichtet werden konnte. Darunter befinden sich auch schwierige Rechtsprobleme, die nur durch die Schaffung neuer oder durch wesentliche Änderungen bestehender Rechtsvorschriften gelöst werden können. Die nachfolgende Zusammenstellung zeigt, daß bei vielen der damals offenen Fragen eine sinnvolle Lösung noch immer aussteht. In anderen Fällen sind dagegen in Zusammenarbeit mit den Behörden befriedigende Ergebnisse erreicht worden.

1. Auf das Fehlen einer Rechtsgrundlage für die zwangsweise ärztliche Untersuchung der Asylbewerber habe ich hingewiesen (10. TB S. 15). Der Bundesminister für Jugend, Familie, Frauen und Gesundheit hat mir mitgeteilt, daß die Schaffung der notwendigen Rechtsgrundlagen derzeit in Fachgremien der Länder beraten wird, siehe Nr. 2.1.2 in diesem Bericht.

2. Zur Vermeidung der Mehrfachvergabe von Seriennummern für Personalausweise und Pässe habe ich dem Bundesminister des Innern empfohlen, entsprechenden Einfluß auf das Herstellungsverfahren bei der Bundesdruckerei zu nehmen (10. TB S. 16 f.). Inzwischen sind dort wirksame Maßnahmen zur Vermeidung der Auslieferung von Ausweisen mit bereits vergebenen Seriennummern getroffen, siehe dazu Nr. 2.3 in diesem Bericht.

3. Im Zusammenhang mit der beabsichtigten Novellierung des Waffengesetzes hatte ich angeregt, Auskünfte von anderen Behörden nicht mehr ohne Wissen des Antragstellers einzuholen (10. TB S. 18). Eine Anhörung vor dem Innenausschuß des Deutschen Bundestages gab mir Gelegenheit, diesen Vorschlag zu erläutern; eine Entscheidung steht noch aus.

4. Für die Aufbewahrung von Unterlagen über die Gewissenprüfung anerkannter Kriegsdienstverweigerer habe ich die Festlegung kurzer Aufbewahrungsfristen gefordert (10. TB S. 19). Der Bundesminister für Jugend, Familie, Frauen und Gesundheit hat das Bundesamt für den Zivildienst angewiesen, zunächst Vernichtungsfristen einzuhalten, die meinen Vorstellungen weitgehend entgegenkommen, und über die Erfahrungen zu berichten, siehe dazu Nr. 2.5.1 in diesem Bericht.

5. Auf die Notwendigkeit, in den Arbeitsberichten der Zivildienstleistenden weniger Angaben über Einzelheiten aus der individuellen Betreuung Hilfsbedürftiger zu verlangen, habe ich hingewiesen (10. TB S. 19 f.). Eine Übernahme der sinnvollen Regelungen für die individuelle Schwerstbehindertenbetreuung auch für den Bereich der Mobilen Sozialen Hilfsdienste ist noch immer nicht erfolgt, siehe dazu Nr. 2.5.2 in diesem Bericht.

6. Zur Verbesserung des Datenschutzes im Bundeszentralregistergesetz habe ich Empfehlungen gegeben (10. TB S. 21 f.). In einem ersten Arbeitspapier hat der Bundesminister der Justiz meine Anregungen im wesentlichen aufgegriffen, siehe dazu Nr. 3.1 in diesem Bericht.

7. Gegen die Praxis, bei Pfändungs- und Überweisungsbeschlüssen, die gleichartig und mit Sammeladressierung versandt werden, jedem einzelnen Empfänger unnötig Kenntnis von allen anderen Empfängern zu geben, habe ich Bedenken geltend gemacht (10. TB S. 23 f.). Eine die Interessen der Betroffenen, z. B. als Patienten eines Facharztes, hinreichend berücksichtigende Reaktion des Bundesministers der Justiz liegt noch nicht vor, siehe dazu Nr. 3.4 in diesem Bericht.

8. An der Zulässigkeit von an die Finanzämter zu richtenden Kontrollmitteilungen über Honorarzahlungen privater Stellen, die Zuwendungen aus dem Bundeshaushalt erhalten, habe ich Zweifel angemeldet (10. TB S. 25). Der Bundesminister der Finanzen ist meinen Bedenken gefolgt, siehe dazu Nr. 4.1 in diesem Bericht.

9. Über meine Beteiligung an dem Entwurf einer Steuerdaten-Abruf-Verordnung habe ich berichtet (10. TB S. 25 f.). Die Erörterungen mit dem Bundesminister der Finanzen sind noch nicht abgeschlossen, siehe dazu Nr. 4.2 in diesem Bericht.

10. Auf die Notwendigkeit, eine organisatorische und personelle Trennung zwischen den Beihilfestellen und der übrigen Personalverwaltung gesetzlich zu regeln, habe ich hingewiesen (10. TB S. 27). Die interministerielle Arbeitsgruppe zur Neuregelung des Personalaktenrechts ist dem nur zum Teil gefolgt und hält es für ausreichend, die personelle Trennung in das Ermessen der jeweiligen Dienststelle zu stellen, siehe dazu Nr. 5.2 in diesem Bericht.

11. Wegen der zunehmenden Automatisierung der Personaldatenverarbeitung habe ich das Fehlen einer bereichsspezifischen Regelung des Arbeitnehmerdatenschutzes bedauert (10. TB S. 28). Ein Referentenentwurf dazu liegt immer noch nicht vor.

12. In der Auseinandersetzung darüber, ob eine Personalakte dem Petitionsausschuß des Deutschen Bundestages auch dann vollständig vorgelegt werden darf, wenn der Bedienstete nicht der Petent ist, habe ich die Ansicht vertreten, daß sich die Vorlage auf die für die Petition relevanten Teile beschränken soll (10. TB S. 29). In dieser Auffassung wurde ich inzwischen durch einen dazu ergangenen Beschluß des OVG Münster bestätigt, das Hauptverfahren ist jedoch noch nicht erledigt.

13. Gegen die Speicherung von Telefonverbindungsdaten in automatisierten Telefon-Nebenstellenanlagen der Bundesbehörden habe ich Bedenken geäußert (10. TB S. 30 f.). In dem neuen Entwurf der Dienstanschlußvorschriften, der voraussichtlich im Jahr 1989 in Kraft treten wird, hat der Bundesminister der Finanzen eine Verkürzung der Zielnummer für Privatgespräche um zwei Stellen und bei besonderen Einrichtungen, wie z. B. Personalvertretungen, einen vollständigen Verzicht auf Einzelgesprächsdaten vorgesehen, siehe dazu Nr. 5.3 in diesem Bericht.

14. Auf erhebliche Schwierigkeiten bei der Zusammenarbeit mit dem Bundesminister für das Post- und Fernmeldewesen habe ich hingewiesen (10. TB S. 35). Im Laufe des Berichtsjahres zeichneten sich deutliche Verbesserungen ab, siehe dazu Nr. 6. in diesem Bericht.

15. Gegenüber dem Bundesminister für das Post- und Fernmeldewesen habe ich das häufige Versäumen der Pflicht beanstandet, automatisierte Dateien bei mir zum Register anzumelden (10. TB S. 35 f.). Maßnahmen zur Verbesserung der Erfassung der Dateien, der Führung der Übersicht und der Erfüllung der Meldepflicht sind eingeleitet.

16. Gegen die Speicherung von Verbindungsdaten aus der Vermittlung von Autotelefongesprächen habe ich Bedenken geltend gemacht (10. TB S. 36 f.). Eine Kontrolle dieses Verfahrens hat meine Bedenken verstärkt und zu einer Beanstan-

dung geführt, siehe dazu Nr. 6.2 in diesem Bericht.

17. Auf Sicherungsmängel bei der Verarbeitung der Daten aus der Vergabe und Benutzung von Telefon-Buchungskarten habe ich hingewiesen (10. TB S. 38). In seiner Stellungnahme hat mir der Bundesminister für das Post- und Fernmeldewesen mitgeteilt, daß Verbesserungen vorgenommen werden sollen.

18. Über Bearbeitungsfehler im Bildschirmtextdienst, die zur unzulässigen Übermittlung von Teilnehmerdaten an Informationsanbieter führten, habe ich berichtet (10. TB S. 41). Dieses Verfahren wurde so geändert, daß der Teilnehmer vorher informiert wird, wodurch Beeinträchtigungen schutzwürdiger Belange der Teilnehmer praktisch ausgeschlossen werden.

19. Das Fehlen einer ausreichenden Rechtsgrundlage für die von der Deutschen Bundespost geführte Sperrdatei, in der nicht mehr zum Postgirodienst zugelassene ehemalige Postgirokunden aufgenommen sind, habe ich kritisiert (10. TB S. 42f.). Der Bundesminister für das Post- und Fernmeldewesen hat datenschutzrechtliche Verbesserungen bislang von der Klärung der künftigen Gestaltung der Postbankdienste im Rahmen der Neustrukturierung des Post- und Fernmeldewesens abhängig gemacht.

20. Auf die Möglichkeit, daß aus Statistiken des Kraftfahrt-Bundesamtes gelegentlich auch Einzelangaben über einen Betroffenen entnommen werden können, habe ich hingewiesen (10. TB S. 44). Das Kraftfahrt-Bundesamt hat inzwischen die statistischen Auswertungen über Nutzfahrzeuge, bei denen dieses Problem besonders häufig auftrat, durch Zusammenfassung zu größeren Gruppen so umgestellt, daß ein Personenbezug ausgeschlossen ist.

21. Für die vom Kraftfahrt-Bundesamt aus Sicherheitsgründen vorgenommene Auslagerung von Magnetbandkopien habe ich Verbesserungen gefordert (10. TB S. 44). Trotz verschiedener Bemühungen zeichnet sich dafür noch immer keine befriedigende Lösung ab.

22. Auf die Notwendigkeit, noch in der laufenden Legislaturperiode eine normenklare gesetzliche Regelung für die Datenverarbeitung des Verkehrszentralregisters zu schaffen, habe ich hingewiesen (10. TB S. 46). Der Bundesminister für Verkehr hat mir im Oktober mitgeteilt, daß er nach einer ersten Beteiligung der Länder jetzt einen Referentenentwurf erstellen wird und eine Verabschiedung noch in dieser Legislaturperiode anstrebt.

23. Die Initiative des Bundesministers für Verkehr, die jetzt noch unzureichende gesetzliche Regelung für die Verarbeitung von Fahrerlaubnisdaten zu verbessern, habe ich begrüßt (10. TB S. 47 f.). Der Bundesminister für Verkehr hat mir mitgeteilt, daß er eine entsprechende Novellierung des Straßenverkehrsgesetzes in der laufenden Legislaturperiode anstrebt.

24. Auf die Verantwortung der Zentrale der Deutschen Bundesbahn für die Gewährleistung des Datenschutzes durch technische und organisatorische Maßnahmen bei den einzelnen Fachdiensten habe ich hingewiesen (10. TB S. 48). Die Deutsche Bundesbahn hat jetzt ihren Organisationsbereich mit einer Untersuchung zur besseren Umsetzung datenschutzrechtlicher Vorschriften beauftragt.

25. Gegen die Erhebung der Verbundpaßnummer bei Fahrgastbefragungen durch einen Verkehrsverbund, an dem die Deutsche Bundesbahn beteiligt ist, habe ich Bedenken geltend gemacht, weil damit in Verbindung mit den gesammelten Verbundpaßanträge ein Personenbezug hergestellt werden konnte (10. TB S. 50). Die zuständige Aufsichtsbehörde hat mir zu Beginn des Berichtsjahres mitgeteilt, daß die Anträge nunmehr unmittelbar nach der Ausgabe der Verbundpässe vernichtet werden.

26. Gegen die Aufnahme detaillierter Nachweise über das Einkommen Unterhaltsverpflichteter in die beim Arbeitsamt geführten Leistungsakten des unterhaltsberechtigten Arbeitslosenhilfeempfängers habe ich Bedenken geltend gemacht (10. TB S. 64). Der Bundesminister für Arbeit und Sozialordnung hat mit dem Bundesrechnungshof Gespräche aufgenommen, um hier eine Verbesserung zu erzielen, siehe dazu Nr. 11.2 in diesem Bericht.

27. Für die Verwahrung von Gutachten des Psychologischen Dienstes der Arbeitsverwaltung habe ich besondere Schutzmaßnahmen gefordert (10. TB S. 64. f.). Die Bundesanstalt für Arbeit hat mir dazu mitgeteilt, daß diese Gutachten künftig in besonderen Ordnern beim jeweils zuständigen Arbeitsvermittler unter Verschluß genommen werden, und daß diese sinnvolle Regelung im Rahmen der Bearbeitung auch auf die psychologischen Gutachten angewendet wird, die sich — noch — in der Vermittlungsdatei befinden.

28. Über Bemühungen zur Verringerung der Datenschutzrisiken, die sich aus einer engen personellen Verflechtung zwischen Betriebskrankenkasse und Unternehmensleitung ergeben können, habe ich berichtet (10. TB S. 69). Im Rahmen des Gesundheitsreformgesetzes wurde dafür eine Kompromißlösung gefunden, die zu einer Verbesserung des Sozialdatenschutzes der Versicherten beitragen wird, siehe dazu Nr. 12.1 in diesem Bericht.

29. Auf die Notwendigkeit, für die Durchführung der Sicherheitsüberprüfungen bald eine einwandfreie gesetzliche Regelung zu schaffen, habe ich hingewiesen (10. TB S. 74 f.). Ein Entwurf dazu ist mir im Berichtsjahr nicht zugegangen.

30. Das sehr restriktive Verhalten der Nachrichtendienste bei der Auskunftserteilung an betroffene Bürger habe ich kritisiert (10. TB S. 75 f.). Im Berichtsjahr hat sich diese Situation etwas verbessert, ohne daß schon von einer befriedigenden Praxis gesprochen werden könnte, siehe dazu Nr. 15.1 in diesem Bericht.

31. Die Einspeicherung von Daten durch das Bundeskriminalamt in das nachrichtendienstliche Informationssystem (NADIS) der Verfassungsschutzbehörden habe ich beanstandet (10. TB S. 77 f.). Auch eine erneute Beanstandung, die aufgrund neuer Prüfungsergebnisse erfolgte, hat keine Änderung dieser Praxis bewirkt, siehe dazu Nr. 16.3.2 in diesem Bericht.

32. Zweifel am Nutzen und damit an der Erforderlichkeit der Speicherung von Hinweisen auf AIDS-Erkrankungen in Polizei-Informationssystemen habe ich deutlich gemacht (10. TB S. 78 f.). Die Innenministerkonferenz hat die Speicherung solcher Hinweise in das Ermessen der Länder bzw. der beteiligten Stellen des Bundes gestellt, mit der Folge, daß die Mehrzahl der Länder auf diese Speicherung verzichtet, das Bundeskriminalamt und der Bundesgrenzschutz bislang aber noch daran festhalten.

33. Das vom Bundeskriminalamt durchgeführte Verfahren zur Besucherkontrolle habe ich beanstandet (10. TB S. 79). Die zugesagte Neuregelung der Besucherkontrolle steht noch aus.

34. Die Regelung, nach der hinsichtlich der Zugriffe der lediglich für Verwaltungszwecke des Bundeskriminalamtes geführte Vorgangsnachweis Personen (VNP) genauso behandelt wird wie eine kriminalpolizeiliche Sammlung, habe ich kritisiert (10. TB S. 80 f.). Diese Verwendung wird fortgesetzt.

35. Für die Speicherungspraxis des Bundesamtes für Verfassungsschutz im Zusammenhang mit der Sicherheitsüberprüfung habe ich weitreichende Änderungen gefordert (10. TB S. 81 f.). Der Bundesminister des Innern hat dem Rechnung getragen, siehe dazu Nr. 19.2 in diesem Bericht.

36. Den Verzicht auf die Speicherung von Daten über Asylbewerber im Grenzaktennachweis (GAN) habe ich für die Fälle empfohlen, in denen sie nur deshalb erfolgt, weil der Asylsuchende ohne Paß bzw. ohne Aufenthaltserlaubnis eingereist ist (10. TB S. 83). Da die Grenzschutzdirektion nunmehr für alle im Grenzaktennachweis erfaßten Akten nach einem Jahr eine materielle Prüfung der Erforderlichkeit der weiteren Aufbewahrung vorsieht, erscheint die Speicherung hinnehmbar.

37. Einen Verstoß gegen tragende Grundsätze des Jugendstrafrechts bei der Überprüfung von Bewerbern beim Bundesgrenzschutz habe ich beanstandet (10. TB S. 84). Auch das jetzt geänderte Verfahren ist nicht unproblematisch, siehe dazu Nr. 17. in diesem Bericht.

38. Über Erwägungen des Bundesministers der Verteidigung, beim MAD die Speicherung von Merkmalen aus der Intimsphäre wieder aufzunehmen, habe ich berichtet (10. TB S. 85). Der Bundesminister der Verteidigung hat inzwischen entschieden, auf diese Speicherung auch weiterhin zu verzichten, siehe dazu Nr. 21.1.3 in diesem Bericht.

39. Auf Probleme bei der Behandlung der Anträge auf Förderung von Unternehmensberatungen für kleine und mittlere Unternehmen habe ich hingewiesen (10. TB S. 87). Der Bundesminister für Wirtschaft hat meine Anregungen weitgehend aufgenommen, siehe dazu Nr. 22.1.2 in diesem Bericht.

40. Die ohne Einwilligung des Betroffenen erfolgende Übermittlung von SCHUFA-Daten an Inkasso-Unternehmen habe ich kritisiert (10. TB S. 89 f.). Die Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich und die Kreditwirtschaft haben sich inzwischen auf eine diese Übermittlung erlaubende Änderung der SCHUFA-Klausel geeinigt, siehe dazu Nr. 23.2.1 in diesem Bericht.

41. Auf die Notwendigkeit, möglichst bald die von der Versicherungswirtschaft verwendeten Klauseln zur Datenverarbeitung und zur Entbindung von der Schweigepflicht sachgerecht neu zu fassen, habe ich hingewiesen (10. TB S. 91). Inzwischen wurden von den Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich und der Versicherungswirtschaft dafür neue Klauseln erarbeitet, siehe dazu Nr. 23.3 in diesem Bericht.

Bonn, den 27. Januar 1989

Dr. Einwag

Anlage 1 (zu 1.4)

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 14./15. März 1988 in Mainz

Polizeiliche Datenverarbeitung bis zum Erlaß bereichsspezifischer gesetzlicher Regelungen

Eines der dringendsten datenschutzrechtlichen Anliegen ist die Schaffung bereichsspezifischer Grundlagen für die Datenverarbeitung der Sicherheitsbehörden. Dies gilt ebenso für die Nachrichtendienste. Schon seit Jahren haben die Datenschutzbeauftragten entsprechende Forderungen erhoben. Spätestens seit dem „Volkszählungsurteil" des Bundesverfassungsgerichts vom 15. 12. 1983 ist das gesetzliche Regelungsdefizit offenbar. So hat der Bayerische Verfassungsgerichtshof in einer Entscheidung vom 9. 7. 1985 bezogen auf die polizeiliche Datenverarbeitung hervorgehoben, es sei geboten, daß der Gesetzgeber die Materie regele, die bisher Gegenstand der „Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen (KpS)" ist.

Mit der Erhebung, Speicherung und Weitergabe personenbezogener Daten greift die Polizei in die Grundrechte der Betroffenen ein, ohne daß dafür immer die verfassungsrechtlich gebotenen gesetzlichen Grundlagen vorhanden sind. So haben schon einige Gerichte die polizeiliche Datenverarbeitung zum Zwecke vorbeugender Straftatenbekämpfung bis zum Erlaß bereichsspezifischer gesetzlicher Grundlagen für unzulässig erklärt. Gleichwohl kommen die gesetzgeberischen Initiativen zur Behebung dieses Zustandes nur äußerst schleppend voran.

Allerdings hat das Bundesverfassungsgericht dem Gesetzgeber in der Vergangenheit Übergangsfristen zur Beseitigung von Regelungsdefiziten zugebilligt, wenn damit eine sonst eintretende Funktionsunfähigkeit staatlicher Einrichtungen vermieden werden kann, die der verfassungsmäßigen Ordnung noch ferner stünde als der bisherige Zustand.

Dabei ist auf folgendes hinzuweisen:

1. Übergangsfristen können ihrer Natur nach nicht unbegrenzt in Anspruch genommen werden. Das Bundesverfassungsgericht hat ausdrücklich darauf hingewiesen, daß sie dann nicht mehr anerkannt werden können, wenn der Gesetzgeber eine Neuregelung ungebührlich verzögert.

2. Während der Übergangsfrist reduziert sich die Befugnis zu Eingriffen auf das, was für die geordnete Weiterführung eines „funktionsfähigen Betriebes" unerläßlich ist. Es ist mithin unzulässig und mit den vom Bundesverfassungsgericht festgestellten reduzierten Befugnissen unvereinbar, bereits bestehende Datenverarbeitungsabläufe noch auszuweiten, etwa durch den Aufbau neuer Datenbanken oder die Ausschöpfung neuer technischer Möglichkeiten, soweit die Eingriffe in die Rechte der Betroffenen damit eine neue Qualität erreichen.

3. Besondere Zurückhaltung hat sich die Polizei dort aufzuerlegen, wo Eingriffe in das informationelle Selbstbestimmungsrecht noch weitere Grundrechte betreffen.

3.1 Die Feststellungen von Personalien, damit verbundene Datenabgleiche und Speicherungen sowie Film- und Videoaufnahmen sind anläßlich von öffentlichen Versammlungen während der Übergangszeit nur dann als zulässig anzusehen, wenn Anhaltspunkte dafür vorliegen, daß strafbare Handlungen begangen werden.

3.2 Die Nutzung technischer Hilfsmittel zur verdeckten Datenerhebung durch Lauschangriffe in Wohnungen muß grundsätzlich ausgeschlossen sein.

4. Der Einsatz von verdeckten Ermittlern und V-Leuten sowie langfristige Observationen und polizeiliche Beobachtung dürfen nur zugelassen werden, wenn konkrete Anhaltspunkte für bestimmte schwere Straftaten bestehen. Es muß festgelegt werden, wer diese Maßnahmen anordnen darf, wie die anfallenden Erkenntnisse verwertet werden dürfen und wann die Betroffenen zu unterrichten sind.

5. Im Hinblick auf die von den Verfassungsgerichten für die Übergangszeit geforderte Beschränkung auf das, was für die geordnete Weiterführung eines „funktionsfähigen Betriebs" unerläßlich ist, erinnern die Datenschutzbeauftragten an ihre früheren Beschlüsse zur polizeilichen Datenverarbeitung. Danach sind künftig insbesondere folgende Datenverarbeitungsvorgänge zu unterlassen:

   - Speicherung diskriminierender personenbezogener Hinweise in polizeilichen Informationssystemen;
   - Speicherung (ehemals) verdächtiger Personen zu Zwecken vorbeugender Straftatenbekämpfung ohne verantwortbare kriminologische Prognose;
   - Speicherung von Daten über Personen, bei denen eine Anklageerhebung mangels öffentlichen Interesses abgelehnt wurde;
   - Speicherung von Daten über Kinder, die der Begehung einer Straftat verdächtigt werden;
   - Weitergabe von Informationen, die mit speziellen polizeilichen Befugnissen erhoben wurden, an andere als Polizeidienststellen.

Anlage 2 (zu 1.4)

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 6. Juni 1988 zur

Neufassung des Bundesdatenschutzgesetzes

Die Datenschutzbeauftragten stellen mit Bedauern fest, daß der vorliegende Entwurf einer Neufassung des Bundesdatenschutzgesetzes im wesentlichen die gleichen Mängel aufweist wie der entsprechende Entwurf der 10. Legislaturperiode des Deutschen Bundestages. Diese Mängel haben die Datenschutzbeauftragten bereits in ihrer Entschließung vom 14. März 1986 aufgezeigt.

Die Datenschutzbeauftragten halten es insbesondere für verfehlt, das allgemeine Datenschutzrecht aufzusplittern in ein streng auf die Datenverarbeitung in Dateien bezogenes Bundesdatenschutzgesetz und ein den Datenschutz in Akten regelndes Verwaltungsverfahrensgesetz, das weite und wichtige Verwaltungsbereiche (z. B. Finanzverwaltung und Sozialverwaltung) ebensowenig erfaßt wie die Strafverfolgung, und dessen Einhaltung sich überdies weitgehend der Datenschutzkontrolle entzieht.

Die Datenschutzbeauftragten stellen ferner fest, daß bei der Vorbereitung des Entwurfs ihre Empfehlungen sowie die zwischenzeitlich von einigen Bundesländern erlassenen, in wesentlichen Punkten vorbildlichen Neuregelungen des Datenschutzes nahezu unberücksichtigt geblieben sind.

Die Datenschutzbeauftragten verkennen nicht, daß auch der jetzige Entwurf einige Verbesserungen gegenüber dem geltenden Recht aufweist. Insgesamt jedoch werden die in der Begründung des Entwurfs genannten Ziele der beabsichtigten Weiterentwicklung des Bundesdatenschutzgesetzes nicht erreicht:

- Die Anpassung an die Grundsätze des Urteils des Bundesverfassungsgerichts vom 15. 12. 1983 zum Volkszählungsgesetz ist in mehrfacher Hinsicht nicht gelungen: so enthält der Entwurf keine ausdrückliche Regelung der Datenerhebung, obwohl gerade diese den Bürgern unmittelbar belastet; die geplante Regelung im Verwaltungsverfahrensgesetz reicht nicht aus. Auch erfährt der Grundsatz der Zweckbindung zu weitgehende Ausnahmen und die Transparenz der Datenverarbeitung, insbesondere das Recht des Betroffenen auf Auskunft, bleibt hinter verfassungsrechtlichen Anforderungen zurück.
- Dem technologischen Fortschritt auf dem Gebiet der Informations- und Kommunikationstechnik (z. B. Arbeitsplatzcomputer, neue optische Speichermedien, Videoaufzeichnungen, Telekommunikation und Vernetzung) wird der Entwurf nicht gerecht. Der im Entwurf verwandte Dateibegriff und die Beibehaltung des bisherigen Katalogs technischer und organisatorischer Datensicherungsmaßnahmen vernachlässigen die technische Entwicklung.
- Die Kontrollbefugnis des Bundesbeauftragten für den Datenschutz wird insgesamt eingeschränkt, insbesondere durch den Ausschluß systematischer Kontrollen bei der Erhebung und Verwendung personenbezogener Informationen außerhalb von Dateien. Keinesfalls kann eine Einschränkung der Kompetenz der Landesbeauftragten durch den Bundesgesetzgeber hingenommen werden.
- Die Datenschutzvorschriften für den nichtöffentlichen Bereich orientieren sich nicht an dem Grundsatz der Zweckbindung und räumen unvertretbare Verarbeitungsprivilegien ein.

Der Entwurf entspricht daher nicht den Erwartungen an ein zeitgemäßes Datenschutzrecht als Ausprägung des verfassungsrechtlich garantierten Rechts des Bürgers auf informationelle Selbstbestimmung. Dieses Recht ist erst jüngst durch das Bundesverfassungsgericht in seiner Entscheidung vom 9. März 1988 bestätigt worden. Dort heißt es:

„In dieses Recht wird nicht nur dann eingegriffen, wenn der Staat vom einzelnen die Bekanntgabe persönlicher Daten verlangt oder diese der automatisierten Datenverarbeitung zuführt . . . Das Recht auf informationelle Selbstbestimmung schützt vielmehr wegen seiner persönlichkeitsrechtlichen Grundlage generell vor staatlicher Erhebung und Verarbeitung personenbezogener Daten und ist nicht auf den jeweiligen Anwendungsbereich der Datenschutzgesetze des Bundes und der Länder oder datenschutzrelevanter Sonderregelungen beschränkt."

Die Konsequenz daraus muß eine möglichst lückenlose und präzise Regelung des Datenschutzes sein, um Rechtssicherheit für Bürger und Verwaltung herzustellen.

Anlage 3 (zu 1.4)

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 6. Juni 1988 zum

Entwurf eines Gesetzes zur Strukturreform im Gesundheitswesen (Gesundheits-Reformgesetz — GRG)

Die Konferenz der Datenschutzbeauftragten stellt fest, daß es in Verhandlungen zwischen dem Bundesbeauftragten für den Datenschutz und dem Bundesminister für Arbeit und Sozialordnung gelungen ist, eine Reihe von Forderungen des Datenschutzes im Regierungsentwurf gegenüber den Vorentwürfen zu verwirklichen.

Gleichwohl halten die Datenschutzbeauftragten eine Verbesserung des Persönlichkeitsschutzes der Krankenversicherten im weiteren Gesetzgebungsverfahren vor allem in den folgenden Punkten für notwendig:

1. *Erfassung medizinischer Daten und Grundsatz des geringstmöglichen Eingriffs*

   Die im Zusammenhang mit Leistungen der gesetzlichen Krankenversicherung vorgesehene automatisierte Verarbeitung von Daten der Versicherten, Ärzte und Zahnärzte darf der Gesetzgeber wegen des damit verbundenen gravierenden Eingriffs in das Selbstbestimmungsrecht der Versicherten nur zulassen, wenn damit tatsächlich auch die erklärten Ziele des Gesetzgebungsvorhabens gefördert, namentlich ein wesentlicher Beitrag zur Kostendämpfung geleistet werden kann, und sich dies nicht auch durch weniger einschneidende Maßnahmen erreichen läßt. So würde es für die Erstellung von Statistiken, die für die Bewertung und Beeinflussung des Leistungsgeschehens wichtig sind, genügen, einen anonymisierten Transparenzbestand zu bilden. Darüber hinaus wäre zu fragen, ob es nicht ausreicht, statt der vorgesehenen versichertenbezogenen umfassenden Datenspeicherung nur die rechtlichen und organisatorischen Voraussetzungen zur Überprüfung von Einzelfällen festzulegen.

2. *Festlegung des Verwendungszwecks personenbezogener Daten*

   Gegen die Nutzung personenbezogener Daten, soweit sie für die Überprüfung der Abrechnung medizinischer Leistungen und zur Kontrolle der Wirtschaftlichkeit erforderlich ist, bestehen keine grundsätzlichen Bedenken. Nach der Rechtsprechung des Bundesverfassungsgerichts muß der Verwendungszweck erhobener Daten vom Gesetzgeber normenklar festgelegt werden. Für Kassenärztliche Vereinigungen und für den Medizinischen Dienst fehlt es im Gesetzentwurf an einer Festlegung des Verwendungszwecks. Der Gesetzentwurf stellt außerdem nicht sicher, daß Daten der Krankenkassen nur für deren Zwecke verwendet werden. Eine Verwendung medizinischer Daten über den eigentlichen Aufgabenbereich der Krankenkassen, der Kassenärztlichen Vereinigungen und des Medizinischen Dienstes hinaus darf wegen der besonderen Sensibilität der Daten nur für eng umschriebene Ausnahmefälle zugelassen werden. Die allgemeinen Offenbarungsvorschriften des SGB X lassen eine zu weitgehende Nutzung durch Dritte zu.

   Dies gilt um so mehr, als die im Entwurf bereits einbezogene technische Entwicklung (maschinenlesbare Datenträger, Krankenversicherungskarte) immer mehr dazu führen wird, daß die versicherungsbezogenen Krankheitsdaten in maschinenlesbarer Form und damit vielfältig verwertbar vorliegen werden.

   Die Konferenz begrüßt die Verbesserungsvorschläge der Ausschüsse des Bundesrates.

3. *Vereinbarungen der Verbände*

   Der Gesetzentwurf überläßt die Regelungen der Abrechnung der kassenärztlichen Versorgung einschließlich der dafür erforderlichen Datenübermittlung den Vereinbarungen der Verbände der Krankenkassen und Kassenärztlichen Vereinigungen. Verschiedene Vereinbarungen greifen nachhaltig in das informationelle Selbstbestimmungsrecht der Versicherten ein, ohne daß diese — insbesondere als Pflichtversicherte — eine Wahlmöglichkeit hätten. Das betrifft z. B. Festlegungen über den Inhalt von Rezepten und Krankenscheinen, die Einbeziehung Dritter zu Prüfzwecken, Meldung von Behinderungen an die Krankenkassen.

   Da der Gesetzgeber nach der Rechtsprechung des Bundesverfassungsgerichts alles Wesentliche selbst regeln muß, reicht es nicht aus, die Regelungsbefugnis an die Verbände zu delegieren. Vielmehr müßte der Umfang der Eingriffe in das informationelle Selbstbestimmungsrecht und der Mindestinhalt der datenschutzrechtlichen Regelungen konkreter als bisher gesetzlich festgelegt werden. Das gilt auch für die Voraussetzungen zur Einführung maschinenlesbarer Krankenversicherungskarten. Darüber hinaus wäre klarzustellen, daß die Verarbeitung und Nutzung personenbezogener Daten für andere als die im Gesetz genannten Fälle nicht durch Vereinbarung vorgesehen werden kann. Der Gesetzgeber sollte überdies ein Verfahren vorsehen, in dem die Wahrung der Rechte der Patienten bei Erlaß solcher Vereinbarungen überprüft wird (z. B. Genehmigungsvorbehalt; eine Genehmigung dürfte nur erteilt werden,

wenn in den Vereinbarungen die Forderungen des Datenschutzes der Versicherten angemessen berücksichtigt sind).

Der Inhalt der Vereinbarungen ist dem Betroffenen auf Verlangen zugänglich zu machen.

4. *Medizinischer Dienst*

Im Hinblick auf die Schutzwürdigkeit der beim Medizinischen Dienst anfallenden Krankheitsdaten sind gesetzliche Regelungen erforderlich über

- Art und Umfang der zu verarbeitenden Daten
- Zweckbestimmung und Verwendungsmöglichkeit (etwa im Bereich des Sozialmedizinischen Dienstes der Rentenversicherungsträger)
- Vermeidung einer med. Zentraldatei
- Informationsrechte der Betroffenen
- Einschränkung der Offenbarungsbefugnisse gegenüber Dritten
- Löschungszeitpunkte

Die Konferenz begrüßt auch hier die in diese Richtung zielenden Vorschläge der Ausschüsse des Bundesrates.

5. *Auskunftsanspruch*

Wegen der zentralen Bedeutung des Auskunftsanspruchs ist im Gesetzestext deutlich klarzustellen, daß auf Verlangen des Versicherten Auskunft über Leistungen und Kosten sowie nach Maßgabe des § 83 SGB X auch über die Diagnose zu erteilen ist. Der Auskunftsanspruch darf nicht durch Satzung beschränkt werden. Der Anspruch muß auch gegenüber dem Medizinischen Dienst bestehen.

6. *Aufbewahrungsfristen*

Der verfassungsrechtliche Verhältnismäßigkeitsgrundsatz gebietet, die Speicherungsdauer personenbezogener Daten auf das erforderliche Maß zu begrenzen. Hierzu sind konkret bestimmte Aufbewahrungsfristen unerläßlich.

Im Gesetzentwurf ist bisher nur bei den Krankenkassen eine nach Jahren festgelegte Frist für die Aufbewahrung von Daten über Leistungsvoraussetzungen (z. B. Art der Erkrankung, Arbeitsunfähigkeitszeiten) vorgesehen. Die Speicherungsdauer für andere Daten bei Krankenkassen und Kassenärztlichen Vereinigungen (z. B. verordnete Medikamente, ärztliche Leistungen, Überweisungen, Abrechnungsunterlagen) ist im Gesetzentwurf nicht konkret befristet. Nach dem Grundsatz der Normenklarheit und dem Wesentlichkeitsgebot des Bundesverfassungsgerichts hat der Gesetzgeber hier selbst eine bestimmte Aufbewahrungsfrist festzulegen.

Die Konferenz begrüßt auch hier die in diese Richtung zielenden Vorschläge der Ausschüsse des Bundesrates. Sie weist jedoch darauf hin, daß die Aufbewahrungsfrist jeweils am Tage der jeweiligen Leistungsgewährung beginnen muß.

7. *Zentrale Krankheitsdatei der Unfallversicherungsträger*

Der Gesetzentwurf räumt den Unfallversicherungsträger die Möglichkeit ein, eine zentrale Krankheitsdatei einzurichten.

Angesichts der schon früher diskutierten vielfältigen datenschutzrechtlichen Probleme zentraler Krankheits- und Gefährdungsregister muß der Gesetzgeber jedoch gleichzeitig mit der Erlaubnis zur Einrichtung dafür sorgen, daß für solche Register ausreichende rechtliche und organisatorische Schutzvorkehrungen wirksam werden. Vorzusehen ist insbesondere eine Einwilligung des Betroffenen in die Speicherung seiner Daten.

Sicherzustellen ist ferner:

- die Verantwortlichkeit für die gespeicherten Daten (speichernde Stelle)
- Art und Umfang der zu speichernden Daten
- die konkrete Zweckbestimmung der Daten in dem betreffenden Register
- Zugriffsrechte

Sicherzustellen ist schließlich, daß die Patientendaten nicht aus dem durch § 35 SGB I geschützten Bereich (Sozialgeheimnis) herausgelöst werden.

Anlage 4 (zu 1.4 und 24.2)

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission RheinlandPfalz vom 10. Oktober 1988

Datensicherheit beim Einsatz kleinerer Datenverarbeitungsanlagen

Beim Einsatz kleinerer Datenverarbeitungsanlagen, vor allem von persönlichen Computern (PC), bereiten die Datensicherheit und die Ordnungsmäßigkeit der Verarbeitung personenbezogener Daten besondere Probleme. Im Hinblick auf diese Probleme geben die Datenschutzbeauftragten des Bundes und der Länder folgende Empfehlungen:

1. Vor jeder Entscheidung, ob für die Arbeiten eines Aufgabengebiets ein PC oder eine sonstige kleine Datenverarbeitungsanlage eingesetzt werden kann, muß geprüft werden, ob die dabei erzielbare Datensicherheit ausreichend ist. Bei dieser Prüfung müssen insbesondere die Empfindlichkeit der Daten und der Grad der Verbindlichkeit der Verarbeitungslogik berücksichtigt werden. Die Verarbeitung personenbezogener Daten mit einem automatisierten Verfahren, das keine angemessene Datensicherheit bietet, verstößt gegen die Datenschutzgesetze.

2. Eine speichernde Stelle hat auch bei der Verarbeitung personenbezogener Daten auf einem PC oder einer sonstigen kleineren Datenverarbeitungsanlage die technischen und organisatorischen Maßnahmen zu treffen, die je nach Art der zu schützenden Daten geeignet sind, die Datensicherheit zu gewährleisten. Sofern die Datensicherheit mit den verfügbaren Maßnahmen nicht in dem erforderlichen Umfang gewährleistet werden kann, muß auf den Einsatz des PC oder der kleineren Datenverarbeitungsanlage verzichtet werden.

   Um die Datensicherheit zu gewährleisten, sind insbesondere die dem neuesten Stand entsprechenden technischen Maßnahmen zu treffen. Weisungen sollten schriftlich erfolgen und in einer Dienstanweisung zusammengefaßt werden. Durch Kontrollen der Arbeitsdurchführung ist sicherzustellen, daß alle Vorschriften und Weisungen befolgt werden.

3. Die Hersteller von Hard- und Software werden aufgefordert, für kleinere Datenverarbeitungsanlagen einschließlich der persönlichen Computer Verfahren zu entwickeln und bereitzustellen, die einen Betrieb dieser Geräte mit einem Maß an Datensicherheit ermöglichen, das demjenigen großer Rechenzentren entspricht. Vor allem müssen Hilfsmittel verfügbar gemacht werden, die es einer datenverarbeitenden Stelle ermöglichen,

   - ohne organisatorisch strukturiertes Rechenzentrum und damit auch ohne Funktionstrennungen bei der Arbeitsabwicklung,
   - ohne organisatorische Trennung zwischen Anwendung und Durchführung der automatisierten Datenverarbeitung und
   - trotz Verzichts auf Detailkenntnisse der automatisierten Datenverarbeitung bei Vorgesetzten und der für die Revision zuständigen Organisationseinheit

   sicherzustellen, daß bei der Verarbeitung auf der eingesetzten Datenverarbeitungsanlage eine verbindlich vorgeschriebene Verarbeitungslogik eingehalten wird. Dazu ist es unter anderem erforderlich, Verfahren bereitzustellen, die gewährleisten, daß Programme ausschließlich in der freigegebenen Fassung zum Ablauf kommen. Systemprogramme und Anwendungsprogramme könnten dazu mit einem geeigneten kryptografischen Verfahren versiegelt werden, wodurch Manipulationen erkennbar würden.

   Für persönliche Computer und sonstige Datenverarbeitungsanlagen sollten zur Datensicherheit Systemprogramme und systemnahe Programme mit einem an der Ausstattung großer Anlagen orientierten Leistungsumfang zur Verfügung gestellt werden. Wesentliche der Datensicherheit dienende Komponenten sollten in das Betriebssystem integriert werden, um Manipulationen und Umgehungsmöglichkeiten zu erschweren.

Anlage 5 (zu 1.4 und 4.2)

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission RheinlandPfalz vom 10. Oktober 1988 zum

Entwurf einer Steuerdaten-Abruf-Verordnung — StDAV — (Stand 9. 6. 1988)

Die Konferenz begrüßt es, daß der Bundesminister der Finanzen bei der Vorbereitung einer Steuerdaten-Abruf-Verordnung einigen vom Bundesbeauftragten für den Datenschutz einvernehmlich mit den Landesbeauftragten für den Datenschutz und der Datenschutzkommission Rheinland-Pfalz ausgesprochenen Empfehlungen für eine datenschutzrechtliche Verbesserung gefolgt ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz erhebt jedoch ernste Bedenken gegen die nach dem derzeitigen Entwurf weiterhin vorgesehene Einrichtung von automatisierten Datenabrufverfahren für die obersten Finanzbehörden und für die Oberfinanzdirektionen. Die Einführung solcher Datenabrufverfahren bedeutet, daß bei den Oberfinanzdirektionen, den obersten Finanzbehörden der Länder und beim Bundesminister der Finanzen zentrale Abrufmöglichkeiten geschaffen werden können, die diesen Behörden einen unmittelbaren automatisierten Zugriff auf Steuerdaten der Finanzämter ihres Zuständigkeitsbereiches ermöglichen.

Solche zentralen Datenabrufmöglichkeiten sind für die Erfüllung der Aufgaben der Aufsichtsbehörden nicht erforderlich. Bei etwaigen Verfahren im Rahmen der Aufsicht sind ohnehin die Akten heranzuziehen. Von diesen Aufsichtsbehörden sind bei der Bearbeitung von steuerlichen Einzelfällen in aller Regel auch keine Entscheidungen unter Zeitdruck zu treffen.

Von der Einrichtung solcher Datenabrufverfahren ist kein ins Gewicht fallender Rationalisierungseffekt zu erwarten. Solche Verfahren können aber dazu führen, daß dem besonderen Steuergeheimnis unterliegende Daten auf sehr einfache Weise Personen bekannt werden, die sie für die Erfüllung ihrer Aufgaben nicht benötigen. Dem gilt es vorzubeugen. Die Datenschutzkonferenz schlägt daher vor, in dem Entwurf der Steuerdaten-Abruf-Verordnung automatisierte Datenabrufverfahren für Oberfinanzdirektionen und oberste Finanzbehörden nicht vorzusehen.

Anlage 6 (zu 6.1)

Stellungnahme im Rahmen der öffentlichen Anhörung durch den Ausschuß für das Post- und Fernmeldewesen des Deutschen Bundestages

Probleme des Datenschutzes im Zusammenhang mit dem Entwurf eines Gesetzes zur Neustrukturierung des Post- und Fernmeldewesens und der Deutschen Bundespost

1. *Vorbemerkung*

Die Regelung des Datenschutzes bei der Deutschen Bundespost als einem der größten Verarbeiter personenbezogener Daten in der Bundesrepublik Deutschland hat herausragende Bedeutung: Viele der angebotenen Dienstleistungen sind für die meisten Bürger unverzichtbar und mit einer Speicherung und Verarbeitung ihrer Daten verbunden. Eine Verletzung schutzwürdiger Belange von Bürgern hätte deshalb beträchtliche Breitenwirkung. Sie muß durch datenschutzgerechte Regelungen und datenschutzbewußtes Verwaltungshandeln vermieden werden. Das gilt auch für die Verarbeitung der Personaldaten der über 500 000 Bediensteten der Deutschen Bundespost. Die Regelungen und Vorkehrungen der DBP zur Durchsetzung des Datenschutzes können darüber hinaus Signalwirkung und Vorbildfunktion für andere Bereiche der öffentlichen Verwaltung, möglicherweise auch für den nicht-öffentlichen Bereich besitzen.

Von besonderer Bedeutung ist aus der Sicht des Datenschutzes die Verarbeitung von *Kundendaten im Bereich der Telekommunikationsdienstleistungen* der DBP. Das liegt vor allem daran, daß hier bereits jetzt in außerordentlich großem Umfange personenbezogene Daten verschiedener Art — neben den zur Durchführung des Dienstes erforderlichen Rahmendaten zum Teil auch die Nachrichteninhalte selbst — gespeichert und verarbeitet werden. Durch die als Folge der Strukturreform erwartete Erhöhung der Angebotsvielfalt vor allem in den Wettbewerbsbereichen der Telekommunikation ist mit einem schnellen Anwachsen des Volumens der verarbeiteten personenbezogenen Daten sowie der Zahl der angebotenen neuen Dienste zu rechnen. Dabei wird sich die bereits jetzt erkennbare Integration der (konventionellen) automatisierten Datenverarbeitung und der Telekommunikation fortsetzen und verstärken.

Diese beabsichtigte und von vielen erwartete Entwicklung erhöht die Risiken für schutzwürdige Belange der Bürger und verlangt daher vom Datenschutz nicht nur eine Sicherung des erreichten Schutzniveaus, sondern eine der Entwicklung entsprechende Anpassung und Weiterführung.

2. *Notwendigkeit und Qualität der bereichsspezifischen Datenschutzregelungen*

Den dargelegten Erfordernissen können die Auffangvorschriften des Bundesdatenschutzgesetzes (BDSG) nicht genügen. Vielmehr sind im Hinblick auf die Ziele des Poststrukturgesetzes bereichsspezifische Datenschutzvorschriften insbesondere im Bereich der Telekommunikation, aber auch für die anderen Postdienste erforderlich, die den jeweiligen Besonderheiten des Dienstes Rechnung tragen und den konkreten Schutzbedarf berücksichtigen.

Dies leistet der Entwurf nur unzureichend: Zwar ermächtigt Artikel 1 § 26 Abs. 2 die Bundesregierung, Vorschriften zum Schutz personenbezogener Daten der am Post- und Fernmeldeverkehr Beteiligten zu erlassen. Die Vorschrift verlangt dabei u. a. die „Berücksichtigung der berechtigten Interessen des jeweiligen Unternehmens" (§ 26 Abs. 2 Satz 1). Diese Forderung bedeutet, daß die Bindung der Datenverarbeitung an die Erforderlichkeit *zur Aufgabenerfüllung* — wie sie im BDSG für den öffentlichen Bereich vorgesehen ist — nicht mehr alleiniger Maßstab für die Zulässigkeit der Datenverarbeitung sein soll. In diesem Zusammenhang ist darauf hinzuweisen, daß das Bundesverfassungsgericht auch bei der Prüfung dieses Maßstabes die Interessen der öffentlichen Verwaltung nicht unberücksichtigt läßt. Es ist z. B. anerkannt, daß der einzelne organisatorische und verfahrensrechtliche Vorkehrungen nicht verlangen kann, die mit einem erheblichen, vernünftigerweise nicht zu beanspruchenden Mehraufwand verbunden sind. Wenn gleichwohl der von der Rechtsprechung sehr weit ausgelegte unbestimmte Rechtsbegriff des „berechtigten Interesses" als Maßstab eingeführt wird, kann die Datenverarbeitung erheblich ausgeweitet werden.

Auch besteht eine *Verpflichtung* der Bundesregierung zum Erlaß von Datenschutzvorschriften nur für den Telefondienst. Für die übrigen Telekommunikationsdienste wird deren Erlaß grundsätzlich in das Ermessen der Bundesregierung gestellt. Eine Verpflichtung besteht nur insoweit, als es um die Erhebung und Verarbeitung personenbezogener Daten „zur Sicherung der Richtigkeit des Leistungsentgelts, zur Störungsbeseitigung und zur Verhinderung mißbräuchlicher Verwendung" geht (vgl. § 26 Abs. 2 Satz 2) — und somit in erster Linie zur Wahrung der Interessen der Unternehmen und weniger der der Betroffenen. So fehlt z. B. die Verpflichtung, Vorkehrungen zu treffen, die den Schutz von Nachrichteninhalten — z. B. im Bildschirmtext — sicherstellen.

Für den *Postdienst* und den *Postbankdienst* besteht zumindest aus dieser Vorschrift keinerlei Ver-

pflichtung zum Erlaß von bereichsspezifischen Datenschutzvorschriften.

Ich halte es daher für dringend geboten, die Vorschriften des Artikels 1 § 26 in dem Sinne umzugestalten, daß die Bundesregierung zum Erlaß von Rechtsverordnungen zum bereichsspezifischen Schutz personenbezogener Daten verpflichtet wird, die zumindest das Schutzniveau des Bundesdatenschutzgesetzes erreichen. Sowohl hinsichtlich der materiellen Zulässigkeits- als auch der Sicherungsanforderungen müssen die zu erlassenden Vorschriften den jeweils aktuellen Entwicklungsstand berücksichtigen, z. B. bezüglich der notwendigen technischen und organisatorischen Sicherungsmaßnahmen.

3. *Schutzminderung durch Privatisierung*

Artikel 3 Nr. 1 des Gesetzes ändert § 1 des Fernmeldeanlagengesetzes dahingehend, daß das bisherige Ausschließlichkeitsrecht des Bundes, Fernmeldeanlagen zu errichten und zu betreiben, auf eindeutig festgelegte Aufgaben beschränkt, die übrigen Dienste und Leistungen aber dem Wettbewerb geöffnet werden. Insbesondere in letzterem Bereich wird infolge dieser Regelung ein schneller und starker Zuwachs sowohl bei bestehenden Diensten als auch hinsichtlich künftiger Telekommunikationsformen erwartet. Für die privaten Anbieter solcher Dienste gelten jedoch nicht die Datenschutzvorschriften für den öffentlichen Bereich, die eine strikte Bindung der Datenverarbeitung an die gesetzliche Aufgabenzuweisung der betreffenden Stelle vorsehen. Nach den statt dessen geltenden Datenschutzvorschriften für den nicht-öffentlichen Bereich, die von der im Wirtschaftsleben bestehenden Vertragsfreiheit ausgehen, wird die Datenverarbeitung in erster Linie durch den Vertragszweck begrenzt; sie sind deshalb weniger restriktiv. Dies wirkt zugleich auch als Datenschutzminderung für die Teilbereiche der Post, die mit privaten Anbietern im Wettbewerb stehen, denn für sie gelten nach § 7 Abs. 1 BDSG zum Teil die gleichen Vorschriften. Damit ergibt sich bei den Anbietern insgesamt eine datenschutzrechtliche Aufspaltung in

- öffentliche Stellen der *Post*, die nicht im Wettbewerb stehen; für diese gelten die §§ 7—21 BDSG und die bereichsspezifischen Datenschutzvorschriften für die Post,
- öffentliche Stellen der *Post*, die mit privaten Anbietern im Wettbewerb stehen; für sie gelten die §§ 15—27 BDSG sowie ebenfalls die bereichsspezifischen Datenschutzvorschriften für die Post, und
- *private Anbieter* von Telekommunikationsdienstleistungen, für die die §§ 22—30 BDSG gelten.

Hinsichtlich der *Qualität des Datenschutzes* führt dies dazu, daß es *unterschiedliche Klassen von Teilnehmern* gibt: diejenigen, die (in den ersten beiden Gruppen) als Postkunden den Schutz der Kontrollvorschriften des zweiten Abschnittes des BDSG — Kontrolle durch den Bundesbeauftragten für den Datenschutz — sowie der nur für die Post geltenden bereichsspezifischen Vorschriften in Anspruch nehmen können, und diejenigen, die Kunden eines privaten Anbieters sind, der diesen Vorschriften nicht unterliegt. Für letztere gelten z. B. auch nicht so wichtige bereichsspezifische Vorschriften wie die Verpflichtung der Postbediensteten zur Wahrung des Fernmeldegeheimnisses (§ 10 Fernmeldeanlagengesetz) oder die Datenschutzvorschriften der Telekommunikationsordnung (§ 449ff.). Soweit bereichsspezifische Regelungen fehlen, ergeben sich auch materiellrechtliche Unterschiede zwischen den in den ersten beiden Anstrichen genannten Stellen.

Ob diese datenschutzrechtliche Teilung der Teilnehmer am Fernmeldeverkehr durch die in Artikel 1 § 26 Abs. 2 vorgesehenen Rechtsverordnungen zumindest teilweise beseitigt werden kann, ist unklar. Die genannte Vorschrift dürfte nämlich nicht für den Fernmeldeverkehr gelten, der über Anlagen abgewickelt wird, die von Privaten eingerichtet und unterhalten werden. Probleme könnten deshalb z. B. im Bereich des Mobilfunks auftreten, in dem voraussichtlich auch Leistungen von Privaten angeboten werden.

Bezüglich der Gesamtheit der Telekommunikationsdienstleistungen führt der Gesetzentwurf zu einem datenschutzmäßigen Rückschritt gegenüber dem geltenden Recht, der sich mit zunehmendem Ausbau der Wettbewerbsbereiche erweitert. Dies kann vermieden werden, wenn für die von Privaten angebotenen Telekommunikationsdienstleistungen Vorgaben gemacht werden, die sicherstellen, daß in diesen Bereichen der Standard des Datenschutzes grundsätzlich demjenigen bei den öffentlichen Stellen der Deutschen Bundespost, die nicht im Wettbewerb stehen, entspricht.

4. *Tragfähigkeit und hinreichende Bestimmtheit der Verordnungsermächtigung*

Als neue Verordnungsermächtigung tritt anstelle des § 14 des Postverwaltungsgesetzes der Artikel 1 § 26 des Entwurfs. Schon in bezug auf die Verordnungsermächtigung des § 14 des Postverwaltungsgesetzes habe ich wiederholt Zweifel geltend gemacht, ob sie auch eine auf die Dauer ausreichende Rechtsgrundlage für die Einführung völlig neuartiger Dienste bietet, die die Kommunikationsbeziehungen der Bürger wesentlich verändern können. Dabei wurde auf die Wesentlichkeitstheorie des Bundesverfassungsgerichts (BVerfGE 49, S. 126) Bezug genommen, wonach der „*Gesetzgeber* . . . in grundlegenden normativen Bereichen, zumal im Bereich der Grundrechtsausübung, . . . alle wesentlichen Entscheidungen selbst zu treffen" hat (vgl. meinen 8. TB 6.2.2 S. 20, 9. TB 8.2. S. 31 und 10. TB 8.5 S. 42). Geht man davon aus, daß der Bürger staatlichem Handeln im Bereich der Deutschen Bundespost besonders häufig begegnet, und berücksichtigt man ferner, daß der Bürger sich dem vielfach kaum entziehen kann, so wird man die Frage stellen müssen, ob Eingriffe in das informationelle Selbstbestimmungsrecht in diesem Bereich nicht einer *gesetzlichen* Regelung bedürfen. Eine

solche muß nicht alle Einzelheiten der personenbezogenen Datenverarbeitung bei der Inanspruchnahme von Postdiensten festlegen. In besonders wichtigen Fragen sollte sie aber konkrete und präzise Vorgaben für die notwendigen Ausführungsvorschriften enthalten. So rechnete die DBP noch bei der Einführung von Bildschirmtext (Btx) mit mehreren Millionen privater Nutzer. Daher wäre es möglicherweise bereits für Btx geboten gewesen, diesen neuen Dienst durch gesetzgeberische Entscheidung auszugestalten, wie es dann ja auch die Länder durch Staatsvertrag getan haben. Andere Dienste, für die wegen ihrer möglichen erheblichen Auswirkungen für die Betroffenen ähnliche Überlegungen angestellt werden können, sind der Fernwirkdienst Temex und das diensteintegrierende Datennetz ISDN. Beispielhaft für Fragen, die dabei gesetzgeberisch geregelt werden müßten, sind die folgenden:

- In welchen Diensten dürfen auch ohne die ausdrückliche Einwilligung der Teilnehmer Rahmendaten der Kommunikation (Wer mit wem, wann, wie lange. .?) erfaßt und gespeichert werden und welche Nutzungen dieser Daten sind erlaubt?
- Unter welchen Umständen dürfen Inhalte der Kommunikation für betriebliche Zwecke der DBP geprüft oder verarbeitet werden?
- Für die Teilnahme an welchen Diensten darf die Aufnahme bestimmter Daten in ein öffentliches Verzeichnis verlangt werden?

Ich halte es deshalb für geboten, gesetzlich festzulegen, welchen Regelungsgehalt die Rechtsverordnungen sowohl für die öffentlichen als auch für die pivaten Unternehmen enthalten sollen. In diesem Zusammenhang könnten auch Rahmenbedingungen für die Verarbeitung von Telekommunikationsdaten in privaten Nebenstellenanlagen vorgegeben werden, soweit dafür ein Bedarf besteht.

5. *Begriffliche Schwierigkeiten*

Dem raschen technischen Wandel folgen Recht und Rechtsprache erfahrungsgemäß nur langsam. Dadurch entsteht die Gefahr, daß Inkongruenzen zwischen technischen Sachverhalten, dem Sprachgebrauch und den einschlägigen Rechtsvorschriften zu Schutzlücken für die betroffenen Bürger führen. So wird z. B. im Bundesdatenschutzgesetz der Begriff des Speicherns für einen solchen technischen Vorgang benutzt, der als Festhalten von Daten für die weitere Verwendung erfolgt. Insbesondere im Bereich der neuen Telekommunikationsdienste gibt es jedoch Speicherungen, die — wie z. B. die Verbindungsdaten bei Telefongesprächen in digitalen Vermittlungsstellen — lediglich der Herstellung und Aufrechterhaltung der Verbindung dienen und oftmals kurze Zeit dauern, trotzdem aber z. B. gegen unbefugte Kenntnisnahme zu schützen sind. Das Recht auf informationelle Selbstbestimmung fordert, daß auch solche temporären Speicherungen angemessen zu schützen sind. Insbesondere müssen die Zulässigkeit der Speicherung, deren Dauer sowie die notwendigen Schutzmaßnahmen dem Kontrollrecht des Bundesbeauftragten für den Datenschutz unterliegen.

Das Bundesdatenschutzgesetz verwendet den Begriff der „speichernden Stelle" für diejenige Stellen, die die inhaltliche Verantwortung für eine bestimmte Verarbeitung personenbezogener Daten trägt. Auch in den neuen Telekommunikationsnetzen kann mit diesem Begriff sinnvoll gearbeitet werden. Voraussetzung ist jedoch, daß die Verantwortungszuweisungen auch die Fälle, in denen — wie z. B. bei Bildschirmtext — häufig die tatsächliche Gewalt über die Speichermedien bei einer anderen Stelle liegt als die Verantwortung für den Inhalt der Daten, datenschutzrechtlich sinnvoll regeln. Das ist mit dem vorhandenen begrifflichen Instrumentarium durchaus möglich.

Der unterschiedliche Sprachgebrauch von Begriffen wie „Telekommunikationsdienste", „Fernmeldedienste" oder „Neue Medien" könnte Unklarheiten über die Reichweite von Rechtsvorschriften hervorrufen, wenn nicht eindeutig definiert wird, welche Dienste einschließlich der damit verbundenen Datenverarbeitungen darunter jeweils zu verstehen sind.

Anlage 7 (zu 9.3)

Stellungnahme zu den Fragen für die öffentliche Anhörung im Rechtsausschuß zum Thema „Genomanalyse im Strafverfahren" am 12. Oktober 1988 (Auszug)

II.

1. *Genomanalyse zum Identitätsnachweis*

1.1 *Art der Daten*

Im Mittelpunkt der bisherigen Diskussion steht nach meinem Eindruck die Nutzung der Genomanalyse zum *Identitätsnachweis* im Strafverfahren. Dabei dienen genomanalytisch gewonnene Daten dem Nachweis, daß bestimmte vorgefundene Spuren (Blutreste, Sperma, Hautreste, Haarwurzeln) von einer bestimmten Person herrühren.

Unter Gesichtspunkten des Datenschutzes wesentlich ist die schon im Bericht der Enquete-Kommission „Chancen und Risiken der Gentechnologie" (unter Empfehlungen C 6., S. XV) getroffene Aussage, daß es sich um Tatsachen handelt, die *„persönlichkeitsneutral"* sind, also über die Funktion eines individuellen Unterscheidungsmerkmals hinaus keine Aussagen über irgendwelche Persönlichkeitsmerkmale wie Krankheit, Krankheitsanlagen und sonstige biologisch bestimmte Dispositionen enthalten. Das Vorstellungsbild vom „genetischen Fingerabdruck", an das die Kommission (a. a. O., C 6.2.3.6.1, S. 175) anknüpft, erscheint insoweit gerechtfertigt.

Die Genomanalyse hat gegenüber herkömmlichen Untersuchungen zum Identitätsnachweis im Strafverfahren offenbar Vorteile. Konnten nach Darstellung der Kommission bislang Analysen zur Identifizierung eines Blutrestes höchstens nur an Zellen durchgeführt werden, die nicht älter als ein halbes Jahr sind, kann eine Genomanalyse dagegen noch an bis zu zwei Jahre altem Material durchgeführt werden (a. a. O., C 6.2.3.6.1, S. 175). Dazu kommt deren höhere Zuverlässigkeit. Während — wie ich einem Aufsatz von Steinke entnehme — bei weniger selektiven Blutgruppen nach herkömmlicher Blutgruppenbestimmung jeder 2.000-ste Mensch mit „gleicher" Blutgruppe als Spurenverursacher in Frage kommen kann (anders bei einigen „stark selektiven Blutgruppen", NJW 1987, S. 2914), soll bei genomanalytischen Befunden ein Singularitätsverhältnis von eins zu vielen Millionen bestehen, teilweise wird von einem Verhältnis eins zu einer Billion gesprochen (vgl. Sternberg-Lieben, NJW 1987, S. 1242). Dies ist auch datenschutzrechtlich von Interesse. Auch unter Gesichtspunkten des Datenschutzes ist nämlich das Verfahren vorzuziehen, das eine größere Richtigkeit der erhobenen Daten gewährleistet.

1.2 *Risiken — Grundrechtseingriff und Grundrechtsgefährdung*

Eine Entscheidung für die Anwendung der Genomanalyse zum Identitätsnachweis im Strafverfahren kann allerdings nicht ohne Berücksichtigung der mit diesem Verfahren verbundenen Risiken für schutzwürdige Belange des Betroffenen erfolgen. Das Hauptrisiko besteht offenbar darin, daß die Grenzlinie zwischen „persönlichkeitsneutraler" Datenerhebung (dem „genetischen Fingerabdruck") einerseits und der Gewinnung von „Befunden über verborgene Krankenheiten oder genetisch bedingte Persönlichkeitsmerkmale" andererseits nicht eingehalten wird oder gar nicht eingehalten werden kann. Es ist zu wünschen, daß die Antworten auf die Frage 5 des Fragenkataloges die Möglichkeiten für die Einhaltung dieser Grenzlinie eindeutig klären. Es muß angestrebt werden, solche Untersuchungsverfahren zu ermitteln, die die oben genannte Voraussetzung erfüllen. Nur solche dürfen durch den Gesetzgeber zugelassen werden.

Können solche Verfahren gefunden werden — was nach einem ersten Eindruck möglich erscheint —, so ist dafür zu sorgen, daß Möglichkeiten eines Mißbrauchs ausgeschlossen werden. Mißbräuche könnten z. B. sein:

- Überschreitung des Untersuchungsauftrages durch den Untersuchenden
- Weitergabe der Blutprobe als Material für weitere genetische Untersuchungen an andere, nicht mit der Strafverfolgung befaßte Stellen
- die Übermittlung des Befundes an Unbefugte.

Die Mißbrauchsgefahren sind allerdings kein Spezifikum der Genomanalyse (Sternberg-Lieben, a. a. O., S. 1244). Eine ähnliche Mißbrauchsgefahr wohnt bereits heute jeder Blutprobe inne. Diese kann mit herkömmlichen Mitteln zur Feststellung noch nicht erkennbarer Krankheitsbilder mißbraucht werden. Eindringliches Beispiel wäre eine HIV-Untersuchung einer für Zwecke des Täterschaftsnachweises gewonnenen Blutprobe.

Gleichwohl muß davon ausgegangen werden, daß die im Falle eines Mißbrauchs eintretende Grundrechts*gefährdung* stärker ist als bei herkömmlichen Untersuchungsmethoden, weil mehr und noch intimere Daten gewonnen werden können. Deshalb ist es notwendig, noch wirksamere Vorkehrungen gegen Mißbrauch

als bei herkömmlichen Untersuchungsmethoden zu treffen. Als solche kommen in Betracht: Es dürfen nur Institute zugelassen werden, die besondere nach Beratung durch Fachleute festzulegende Voraussetzungen zur Durchführung der Genomanalyse erfüllen. Die genomanalytische Untersuchung in einem Institut sollte unter einem Personencode stattfinden, den nur der Auftraggeber zu entschlüsseln in der Lage ist. Zu den erforderlichen Sicherungen durch Rechtsvorschriften wird unter 1.3 Stellung genommen.

1.3 *Rechtsgrundlagen*

1.3.1 *Notwendigkeit*

Für die Beantwortung der Frage, ob die vorhandenen Rechtsgrundlagen für eine Anwendung der Genomanalyse im Strafverfahren ausreichen, ist von Bedeutung, ob und inwieweit bei der Genomanalyse zum Identitätsnachweis personenbezogene Daten im Sinne des § 2 Abs. 1 BDSG erhoben werden.

Für Zwecke des Identitätsnachweises bedarf es — wie bei herkömmlichen Verfahren — eines Vergleichs, eines Vergleichs nämlich zwischen Informationen, die bei der Tat zurückgelassen wurden, und solchen, die beim Tatverdächtigen gewonnen werden. Daß bei der Genomanalyse von Material, das beim Tatverdächtigen erhoben wurde, personenbezogene Daten erhoben werden, liegt auf der Hand. In Bezug auf die „Genformel" einer am Tatort gesicherten Spur vertritt Steinke (NJW 1987, S. 2914) die Auffassung, es handele sich nicht um ein personenbezogenes, sondern um ein „anonymisiertes Formeldatum". Für diese Auffassung spricht, daß, die Bezugsperson festzustellen, gerade erst das Ziel vergleichender Untersuchungen ist. Gleichwohl liegt auch in diesem Fall ein latenter Personenbezug vor. Es erfolgt nämlich eine Erhebung zu dem Zwecke, diesen Personenbezug später offenbar zu machen. Dabei muß auch im Auge behalten werden, daß diese Daten in der Regel im Zusammenhang mit den Ermittlungen zu einem bestimmten Tatgeschehen, d. h. zu weiteren Daten über den Verdächtigen stehen. Auch ohne eine Vergleichsuntersuchung kann es im Zuge weiterer Ermittlungen oder eines Geständnisses zu einer Verdichtung des Personenbezuges kommen. Deshalb liegt auch bei der Untersuchung von Tatortspuren im Wege der Genomanalyse ein Eingriff in das Recht auf informationelle Selbstbestimmung (Schutzbereich des Artikel 2 Abs. 1 i.V.m. Artikel 1 Grundgesetz) vor.

Eingriffe in das Recht auf informationelle Selbstbestimmung sind nur im überwiegenden Allgemeininteresse aufgrund eines Gesetzes zulässig.

1.3.2 *Rechtsgrundlage vorhanden?*

Die unter 8 a des Fragenkataloges des Rechtsausschusses gestellte Frage, ob es für die Genomanalyse zum Identitätsnachweis im Strafverfahren, namentlich für die Nutzung des sog. genetischen Fingerabdrucks zur Feststellung der Täterschaft bzw. Entlastung des Beschuldigten, und für die damit verbundenen Datenerhebungen bereits eine hinreichende Rechtsgrundlage gibt, wird in der vorhandenen Literatur unterschiedlich beantwortet. Sternberg-Lieben (a. a. O., S. 1243f.) sieht in der geltenden Strafprozeßordnung eine hinreichende Rechtsgrundlage. Er räumt hierbei freilich ein, daß es sich bei der gentechnischen Analyse „noch nicht um eine Standardmaßnahme handelt". Für ihn sind gleichwohl — gestützt auf § 81 a Abs. 1 Satz 2 StPO — lediglich die „Auswirkungen auf den körperlichen Zustand des Beschuldigten" ausschlaggebend; insofern sieht er — „anders als etwa bei dem Gen-Transfer in somatische Zellen" keine Bedenken.

Kritischer ist die Enquete-Kommission (a. a. O., 6.2.3.6.2, S. 176): Sie weist darauf hin, daß in § 81 a StPO die Art der Untersuchungen nicht geregelt ist, die an entnommenen Blutproben durchgeführt werden dürfen. Die bestehende Rechtslage, daß zur Aufklärung von verfahrenserheblichen Tatsachen jede technisch mögliche Untersuchung gedeckt ist, mag — nach Auffassung der Kommission — für die bisher üblichen Untersuchungstechniken hinzunehmen sein. Ihr erscheint zwar die Verwendung von genomanalytischen Testmethoden, die genau nur die verfahrensrelevanten Tatsachen, also etwa die Herkunft von Tatspuren, feststellen, aber ansonsten „gleichsam persönlichkeitsneutral sind und keine weitere Ausforschung des genetischen Schicksals und der genetischen Anlagen des Betroffenen beinhalten", als unbedenklich. Bezüglich der Rechtslage sieht sie im Vergleich zu herkömmlichen Untersuchungstechniken gleichwohl eine „andere Situation" (a. a. O., S. 176). Ob eine Genomanalyse auf § 81 a StPO gestützt werden könne, sei „fraglich" (S. 175).

Ich neige der Auffassung zu, daß es sich bei der Genomanalyse nicht nur um eine Verfeinerung kriminalistischer Untersuchungsmethoden handelt (so aber Sternberg-Lieben, a. a. O., S. 1244), vielmehr liegt ein „qualitativer Sprung" im Methodenbereich vor. Deshalb reicht der geltende § 81 a StPO nicht aus.

Eine gesetzliche Regelung ist im übrigen schon deshalb geboten, weil es mit Blick auf die größeren Gefährdungen, auf die oben hingewiesen wurde, differenzierender Gewährleistungen gegen Mißbrauch bedarf.

Die unter 8 c des Fragenkataloges des Rechtsausschusses gestellte Frage, ob es neuer gesetzlicher Regelungen bedarf, wird von mir ausdrücklich bejaht.

1.3.3 *Inhalt einer gesetzlichen Neuregelung*

a) Die Zulässigkeitsvoraussetzungen genomanalytischer Untersuchungen von Tat- und

Tatortspuren sowie vergleichender genomanalytischer Untersuchungen zum Identitätsnachweis für Zwecke der Strafverfolgung sollten in der Strafprozeßordnung normenklar bestimmt werden. Hierbei sollten Untersuchungen, die diese Zweckbegrenzung überschreiten, namentlich eine Erhebung von Befunden über verborgene Krankheiten oder genetisch bedingte Persönlichkeitsmerkmale, gesetzlich untersagt und mit Strafe bedroht werden.

Der Gesetzgeber sollte das oder die — allein — zulässigen Untersuchungsverfahren ausdrücklich benennen.

b) Genomanalytische Untersuchungen zum Identitätsnachweis sollten nur zugelassen werden, wenn sie zur Identifizierung des Täters oder zur Entlastung des Beschuldigten bzw. zur Klärung der Frage, ob eine bestimmte Spur einem bestimmten Opfer zuzuordnen ist, erforderlich sind.

c) Die in Frage 7 des Rechtsausschusses angesprochene Problematik, ob ein bestimmter Verfahrensstand festgelegt werden sollte, von welchem an die Vergleichsuntersuchung zulässig sein soll, ist keine Besonderheit genomanalytischer Untersuchungen. Sie berührt die allgemeine Frage, unter welchen Voraussetzungen ein Verfahrensbeteiligter als Beschuldigter angesehen werden kann. Restriktive Sonderregelungen für die Genomanalyse zum Identitätsnachweis halte ich insoweit nicht für erforderlich.

d) Was die unter 7 a und b sowie 8 aa und 8 bb des Fragenkataloges des Rechtsausschusses gestellten Fragen nach den Anordnungsbefugnissen anbelangt, so empfehle ich, es bei der geltenden Rechtslage zu belassen, die in §§ 81 a Abs. 2 und 81 c Abs. 5 StPO im Falle des körperlichen Eingriffs, d. h. der Entnahme von Blutproben zur Vergleichsuntersuchung, nicht aber für die Untersuchung von Tatortspuren im Regelfalle die richterliche Anordnung vorsieht. Schon nach gegenwärtig gefestigter Rechtsauffassung (vgl. z. B. Baumbach, StPO, Anmerkung 27 zu § 81 a) muß die Anordnung den Eingriff und die durch ihn festzustellenden Tatsachen bezeichnen. Die Anordnung sollte außerdem das Untersuchungsinstitut und die Untersuchungsmethode nennen. Auch wenn dies schon jetzt herrschender Meinung entspricht, sollte eine entsprechende gesetzliche Klarstellung getroffen werden.

e) Die Sicherheit der Aufbewahrung und des Transportes von Tat- bzw. Tatortspuren sowie von Blutproben gegenüber einem unbefugten Zugriff muß — unabhängig von den Anordnungen über die Verwendung des Materials — neu überdacht, möglicherweise auch gesetzlich geregelt werden.

f) Es sollte gesetzlich bestimmt werden, daß mit genomanalytischen Untersuchungen zum Identitätsnachweis nur Institute betraut werden dürfen, die unter Kriterien der Zuverlässigkeit — auch im Sinne des Datenschutzes — hierfür durch die Justizminister/-senatoren zugelassen sind. In Anlehnung an Empfehlungen der Enquete-Kommission (a. a. O., S. 177) sollte geprüft werden, ob hierfür nur gerichtsmedizinische Institute (nur staatliche?) in Betracht kommen sollten. Unter dem Gesichtspunkt technisch-organisatorischer Maßnahmen zur Gewährleistung der Datensicherheit (§ 6 BDSG) empfehle ich, notwendige Vorkehrungen festzulegen.

g) Bezüglich der in Frage 9 c des Fragenkataloges des Rechtsausschusses gestellten Frage nach notwendigen Regelungen über den Verbleib der Befunde, bin ich der Auffassung, daß die untersuchende Stelle gesetzlich verpflichtet werden sollte, nach Abschluß der Untersuchung alle Unterlagen über die genomanalytischen Befunde an die ermittelnde Staatsanwaltschaft, mit deren Zustimmung auch an die ermittelnde Polizei, zu übergeben. Die Polizeibehörde sollte verpflichtet werden, nach Abschluß der Ermittlungen alle Unterlagen an die zuständige Staatsanwaltschaft weiterzuleiten.

h) Eine Aufbewahrung des Untersuchungsmaterials über den rechtskräftigen Abschluß des Strafverfahrens hinaus sollte untersagt werden.

i) Zu der unter 9 b des Fragenkataloges gestellten Frage der Speicherung bin ich der Auffassung, daß eine Speicherung genomanalytischer Befunde für ein bestimmtes Verfahren (SPUDOK) unter den gleichen Voraussetzungen zulässig sein sollte, wie die Speicherung anderer identifizierender Erkenntnisse, z. B. daktyloskopischer Angaben.

2. *Genomanalyse zur Unterstützung von Fahndungsmaßnahmen*

Es ist vorstellbar, daß die Genomanalyse auch ein geeignetes Hilfsmittel zur Gewinnung von Fahndungsansätzen bietet. So könnte mit ihrer Hilfe unter Umständen Merkmale des äußeren Erscheinungsbildes wie „männlich" oder „weiblich", „Augenfarbe", „Hautfarbe" bestimmt werden. Wenn es Verfahren geben sollte, die lediglich äußerlich erkennbare Merkmale feststellen, hätte ich gegen eine entsprechende genomanalytische Untersuchung keine grundsätzlichen Bedenken. Es müßte sichergestellt sein, daß keine Erkenntnisse über äußerlich nicht erkennbare Persönlichkeitsmerkmale wie Krankheit, Krankheitsanlagen und sonstige biologisch bestimmte Dispositionen gewonnen werden.

Ich empfehle für den Fall, daß es eine Untersuchungsmethode gibt, die die isolierte Feststellung solcher Merkmale des äußeren Erscheinungsbildes unter Ausschluß von Überschuß-

informationen ermöglicht, eine gesetzliche Grundlage für solche Untersuchungen zu schaffen. Dabei sollte hinsichtlich der Zulässigkeit nach der Schwere der in Frage stehenden Straftat differenziert werden. Außerdem wäre in jedem Falle eine richterliche Anordnung vorzuschreiben, die konkret die zu treffenden Feststellungen nennen muß.

Die Sicherungen gegen Mißbrauch müßten ebenso streng sein wie bei der Genomanalyse zum Identitätsnachweis (vgl. oben unter 1.).

Anlage 8 (zu 23.3.1)

Schweigepflichtentbindungsklauseln in Versicherungsverträgen

Krankenversicherung

Mir ist bekannt, daß der Versicherer — soweit hierzu ein Anlaß besteht — Angaben über meinen Gesundheitszustand und bei anderen Krankenversicherern auch Angaben über frühere oder bestehende oder beantragte Versicherungsverträge zur Beurteilung der Risiken eines von mir beantragten Vertragsabschlusses überprüft. Zu diesem Zweck befreie ich Ärzte, Zahnärzte, Angehörige anderer Heilberufe sowie Angehörige von Krankenanstalten und Gesundheitsämtern, die mich in den letzten zehn Jahren vor Antragstellung untersucht, beraten oder behandelt haben, von ihrer Schweigepflicht — und zwar auch über meinen Tod hinaus — und ermächtige sie, dem Versicherer die erforderlichen Auskünfte zu erteilen. Dies gilt auch für Angehörige anderer Kranken-, Lebens- und Unfallversicherer, mit denen ich bisher in Vertragsbeziehungen stand oder stehe. Diese Ermächtigung endet fünf Jahre nach Antragstellung.

Mir ist ferner bekannt, daß der Versicherer zur Beurteilung seiner Leistungspflicht auch Angaben überprüft, die ich zur Begründung etwaiger Ansprüche mache oder die sich aus von mir eingereichten Unterlagen (z. B. Rechnungen, Verordnungen) sowie von mir veranlaßten Mitteilungen eines Krankenhauses oder von Angehörigen eines Heilberufes ergeben. Auch zu diesem Zweck befreie ich die Angehörigen von Heilberufen oder Krankenanstalten, die in den vorgelegten Unterlagen genannt sind oder die an der Heilbehandlung beteiligt waren, von ihrer Schweigepflicht; dabei hat die Geltendmachung eines Leistungsanspruches die Bedeutung einer Schweigepflichtentbindung für den Einzelfall. Von der Schweigepflicht entbinde ich auch zur Prüfung von Leistungsansprüchen im Falle meines Todes. Die Schweigepflichtentbindung für die Leistungsprüfung bezieht sich auch auf die Angehörigen von anderen Kranken- und Unfallversicherern, die nach dort bestehenden Versicherungen befragt werden dürfen.

Diese Erklärung gebe ich auch für meine mitzuversichernden Kinder sowie die von mir gesetzlich vertretenen mitzuversichernden Personen ab, die die Bedeutung dieser Erklärung nicht selbst beurteilen können.

Unfallversicherung

Mir ist bekannt, daß der Versicherer — soweit hierzu ein Anlaß besteht — Angaben über meinen Gesundheitszustand, auch über frühere Erkrankungen oder Unfälle, und über frühere, bestehende oder beantragte Versicherungsverträge bei anderen Unfall-, Kranken- oder Lebensversicherern zur Beurteilung der Risiken eines von mir beantragten Vertrages überprüft. Zu diesem Zweck befreie ich Ärzte, Zahnärzte, Angehörige anderer Heilberufe sowie Angehörige von Krankenanstalten und Gesundheitsämtern, die mich in den letzten zehn Jahren vor Antragsstellung untersucht, beraten oder behandelt haben, von ihrer Schweigepflicht — und zwar auch über meinen Tod hinaus — und ermächtige sie, dem Versicherer die erforderlichen Auskünfte zu erteilen. Dies gilt auch für Angehörige anderer Kranken-, Lebens- und Unfallversicherer, mit denen ich bisher in Vertragsbeziehungen stand oder stehe. Diese Ermächtigung endet fünf Jahre nach Antragstellung.

Mir ist ferner bekannt, daß der Versicherer zur Beurteilung seiner Leistungspflicht auch Angaben überprüft, die ich zur Begründung etwaiger Ansprüche mache oder die sich aus von mir eingereichten Unterlagen (z. B. Bescheinigungen, Atteste) sowie von mir veranlaßten Mitteilungen eines Krankenhauses oder von Angehörigen eines Heilberufes ergeben. Auch zu diesem Zweck befreie ich die Angehörigen von Heilberufen oder Krankenanstalten, die in den vorgelegten Unterlagen genannt sind oder die an der Heilbehandlung beteiligt waren, von ihrer Schweigepflicht; dabei hat die Geltendmachung eines Leistungsanspruches die Bedeutung einer Schweigepflichtentbindung für den Einzelfall. Von der Schweigepflicht entbinde ich auch zur Prüfung von Leistungsansprüchen im Falle meines Todes. Die Schweigepflichtentbindung für die Leistungsprüfung bezieht sich auch auf die Angehörigen von anderen Unfall-, Kranken- oder Lebensversicherern, die nach dort bestehenden Versicherungen befragt werden dürfen. (1)

Diese Erklärung gebe ich auch für meine mitzuversichernden Kinder sowie die von mir gesetzlich vertretenen mitzuversichernden Personen ab, die die Bedeutung dieser Erklärung nicht selbst beurteilen können. (2)

(1) Dieser Absatz entfällt bei Unternehmen, die sich in jedem Leistungsfall eine Einzelfallentbindungserklärung geben lassen.

(2) Dieser Absatz entfällt bei Unternehmen, die keine Unfallverträge abschließen, in der Kinder oder andere Personen als Mitversicherte eingeschlossen werden.

Lebensversicherung

Ich ermächtige den Versicherer, zur Nachprüfung und Verwertung der von mir über meine Gesundheitsverhältnisse gemachten Angaben alle Ärzte, Krankenhäuser und sonstigen Krankenanstalten, bei denen ich in Behandlung war oder sein werde, sowie andere Personenversicherer über meine Gesundheitsverhältnisse bei Vertragsabschluß zu befragen; dies gilt für die Zeit vor der Antragsannahme und die nächsten

drei Jahre nach der Antragsannahme. Der Versicherer darf auch die Ärzte, die die Todesursachen feststellen,und die Ärzte, die mich im letzten Jahr vor meinem Tode untersuchen oder behandeln werden, sowie Behörden — mit Ausnahme von Sozialversicherungsträgern — über die Todesursachen oder die Krankheiten, die zum Tode geführt haben, befragen.

Insoweit entbinde ich alle, die hiernach befragt weren, von der Schweigepflicht auch über meinen Tod hinaus.

Anlage 9 (zu 23.3.2)

Merkblatt zur Datenverarbeitung

Versicherungen können heute ihre Aufgaben nur noch mit Hilfe der elektronischen Datenverarbeitung erfüllen. Nur so lassen sich Vertragsverhältnisse korrekt, schnell und wirtschaftlich abwickeln; auch bietet die EDV einen besseren Schutz der Versichertengemeinschaft vor mißbräuchlichen Handlungen als die bisherigen manuellen Verfahren. Die Verarbeitung der uns bekanntgegebenen Daten zu Ihrer Person wird durch das Bundesdatenschutzgesetz (BDSG) geregelt. Danach ist die Datenverarbeitung zulässig, wenn das BDSG oder eine andere Rechtsvorschrift sie erlaubt oder wenn der Betroffene eingewilligt hat. Das BDSG erlaubt die Datenverarbeitung stets, wenn dies im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses geschieht oder soweit es zur Wahrung berechtigter Interessen der datenverarbeitenden Stelle erforderlich ist und schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden.

Unabhängig von dieser im Einzelfall vorzunehmenden Interessenabwägung und im Hinblick auf eine sichere Rechtsgrundlage für die Datenverarbeitung ist in Ihren Versicherungsantrag eine Einwilligungserklärung nach dem BDSG aufgenommen worden. Daneben setzt auch die Übermittlung von Daten, die, wie z. B. beim Arzt, einem Berufsgeheimnis unterliegen, eine spezielle Erlaubnis des Betroffenen (Schweigepflichtentbindung) voraus. In der Lebens-, Kranken- und Unfallversicherung ist daher im Antrag auch eine Schweigepflichtentbindungsklausel enthalten. Beide Klauseln sind allen Versicherungsgesellschaften vom Bundesaufsichtsamt für das Versicherungswesen nach sorgfältiger Prüfung der Interessen der Versicherungsnehmer und nach Abstimmung mit den Datenschutz-Aufsichtsbehörden der Länder genehmigt worden. Die Versicherer verwenden — soweit nicht Besonderheiten einzelner Versicherungssparten Abweichungen erfordern — gleichlautende Texte. Das dient der Klarheit und Übersichtlichkeit.

Im folgenden wollen wir Ihnen einige wesentliche Beispiele für die Datenverarbeitung nennen.

1. *Datenspeicherung bei Ihrem Versicherer*

Wir speichern Daten, die für den Versicherungsvertrag notwendig sind. Das sind Ihre Angaben im Antrag und versicherungstechnische Daten, wie Kundennummer (Partnernummer) und Beitrag, Abrechnung mit Vermittlern, sowie erforderlichenfalls die Angaben eines Dritten, z. B. eines Sachverständigen oder eines Arztes. Bei einem Versicherungsfall speichern wir Ihre Angaben zum Schaden und ggf. auch Angaben von Dritten, wie z. B. den vom Arzt ermittelten Grad der Berufsunfähigkeit oder die Feststellung Ihrer Reparaturwerkstatt über einen Kfz-Totalschaden.

2. *Datenübermittlung an Rückversicherer*

Im Interesse seiner Versicherungsnehmer wird ein Versicherer stets auf einen Ausgleich der von ihm übernommenen Risiken achten. Deshalb geben wir in vielen Fällen einen Teil der Risiken an Rückversicherer im In- und Ausland ab. Diese Rückversicherer benötigen ebenfalls entsprechende versicherungstechnische Angaben von uns, wie Versicherungsnummer, Beitrag, Art des Versicherungsschutzes und des Risikos und Risikozuschlags, sowie im Einzelfall auch Ihre Personalien. Soweit Rückversicherer die Risiko- und Schadenbeurteilung übernehmen, werden ihnen auch die dafür erforderlichen Unterlagen zur Verfügung gestellt.

In einigen Fällen bedienen sich die Rückversicherer weiterer Rückversicherer, denen sie ebenfalls entsprechende Daten übergeben.

3. *Datenübermittlung an andere Versicherer*

Nach dem Versicherungsvertragsgesetz hat der Versicherte bei Antragstellung, jeder Vertragsänderung und im Schadenfall dem Versicherer alle für die Einschätzung des Wagnisses und die Schadensabwicklung wichtigen Umstände anzugeben. Hierzu gehören z. B. frühere Krankheiten und Versicherungsfälle oder Mitteilungen über gleichartige andere Versicherungen (beantragte, bestehende, abgelehnte oder gekündigte). Um Versicherungsmißbrauch zu verhindern, eventuelle Widersprüche in den Angaben des Versicherten aufzuklären oder um Lücken bei den Feststellungen zum entstandenen Schaden zu schließen, kann es erforderlich sein, andere Versicherer um Auskunft zu bitten oder entsprechende Auskünfte auf Anfragen zu erteilen.

Auch sonst bedarf es in bestimmten Fällen (§§ 59, 67 Versicherungsvertragsgesetz sowie bei Teilungsabkommen) eines Austausches von personenbezogenen Daten unter den Versicherern. Dabei werden Daten des Betroffenen weitergeben, wie Name und Anschrift, Kfz-Kennzeichen, Art des Versicherungsschutzes und des Risikos oder Angaben zum Schaden, wie Schadenshöhe und Schadentag.

4. *Zentrale Hinweissysteme der Fachverbände*

Bei Prüfung eines Antrags oder eines Schadens kann es notwendig sein, zur Risikobeurteilung, zur weiteren Aufklärung des Sachverhalts oder zur Verhinderung von Versicherungsmißbrauch Anfragen an den zuständigen Fachverband bzw. an andere Versicherer zu richten oder auch entsprechende Anfragen anderer Versicherer zu beantworten. Dazu werden bei einigen Fachverbänden zentrale Datensammlungen geführt bzw. bestehen zentrale Hinweissysteme.

Solche Datensammlungen bzw. Hinweissysteme gibt es beim Verband der Haftpflichtversicherer, Unfall-

versicherer, Autoversicherer und Rechtsschutzversicherer (HUK-Verband), beim Verband der Lebensversicherungs-Unternehmen, beim Verband der Sachversicherer, beim Deutschen Transport-Versicherungsverband sowie beim Verband der Privaten Krankenversicherung. Die Aufnahme in diese Datensammlungen/Hinweissysteme erfolgt lediglich zu Zwecken, die mit der jeweiligen Datei verfolgt werden dürfen, also nur soweit bestimmte Voraussetzungen erfüllt sind. Beispiele:

- Rechtsschutzversicherer — Aufnahme von Vertragskündigungen gem. § 19 ARB, um bei der Antragsprüfung Vorversicherungen aufzudecken.
- Unfallversicherer — Meldung verschwiegener anderweitiger Versicherungen oder sonstiger anzeigepflichtiger Umstände, um Mißbrauchshandlungen aufzudecken.
- Kfz-Versicherer — Registrierung von auffälligen Schadensfällen und Kfz-Diebstählen sowie von Personen, bei denen der Verdacht des Versicherungsmißbrauchs besteht. Zweck: Risikoprüfung, Schadensaufklärung und -verhütung.
- Sachschadenversicherer — Aufnahme von Schäden und Personen, wenn Brandstiftung vorliegt oder wenn aufgrund des Verdachts des Versicherungsmißbrauchs der Vertrag gekündigt wird und bestimmte Schadenssummen erreicht sind. Zweck: Risikoprüfung, Schadensaufklärung, Verhinderung weiteren Mißbrauchs.
- Lebensversicherer — Aufnahme von Sonderrisiken (z. B. Ablehnung des Risikos bzw. Annahme mit Beitragszuschlag
  - aus versicherungsmedizinischen Gründen,
  - aufgrund der Auskünfte anderer Versicherer,
  - wegen verweigerter Nachuntersuchung; Aufhebung des Vertrages durch Rücktritt oder Anfechtung seitens des Versicherers, Ablehnung des Vertrages seitens des Verischerungsnehmers wegen geforderter Beitragszuschläge. Zweck: Risikoprüfung.
  - Transportversicherer — Aufnahme von auffälligen (Verdacht des Versicherungsmißbrauchs) Schadensfällen insbesondere in der Reisegepäckversicherung. Zweck: Schadensaufklärung und -verhütung.

5. *Datenverarbeitung in der Versicherungsgruppe*

Zum Schutz der Versicherten werden einzelne Branchen (z. B. Lebens-, Kranken-, Sachversicherung) durch juristisch selbständige Gesellschaften betrieben. Um dem Kunden einen umfassenden Versicherungsschutz anbieten zu können, arbeiten die Gesellschaften häufig in Versicherungsgruppen zusammen. Zur Kostenersparnis werden dabei einzelne Bereiche zentralisiert, wie das Inkasso oder die Datenverarbeitung. So wird z. B. Ihre Adresse nur einmal gespeichert, auch wenn Sie Versicherungsverträge mit verschiedenen Gesellschaften der Gruppe abschließen; und auch Ihre Versicherungsnummer, die Art der Verträge, ggf. Ihr Geburtsdatum, Kontonummer und Postleitzahl, d. h. Ihre allgemeinen Vertrags-, Abrechnungs- und Leistungsdaten werden in einer zentralen Datensammlung geführt. Obwohl alle diese Daten nur zur Beratung und Betreuung des jeweiligen Kunden durch die einzelnen Gesellschaften verwendet werden, spricht das Gesetz auch hier von „Datenübermittlung", bei der die Vorschriften des Bundesdatenschutzgesetzes zu beachten sind. Branchenspezifische Daten — wie z. B. Gesundheitsdaten — bleiben dagegen unter ausschließlicher Verfügung der jeweiligen Gesellschaft.

Unserer Versicherungsgruppe gehören zur Zeit folgende Gesellschaften an: . . .

6. *Betreuung durch Versicherungsvertreter*

In Ihrem Versicherungsangelegenheiten werden sie durch unsere Vertreter betreut. Um diese Aufgabe ordnungsgemäß erfüllen zu können, erhalten die Vertreter von uns die notwendigen versicherungstechnischen Angaben, wie insbesondere Versicherungsnummer, Beiträge, Art des Versicherungsschutzes und des Risikos oder Zahl der Versicherungsfälle und Höhe von Versicherungsleistungen. Zum Zwecke von Vertragsanpassungen in der Personenversicherung werden an die Versicherungsvertreter auch Gesundheitsdaten übermittelt.

7. *Weitere Auskünfte und Erläuterungen*

Sie haben als Betroffener nach dem Bundesdatenschutzgesetz ein Recht auf Auskunft, sowie unter bestimmten Voraussetzungen ein Recht auf Berichtigung, Sperrung oder Löschung Ihrer in der Datei gespeicherten Daten.

Wegen eventueller weiterer Auskünfte und Erläuterungen wenden Sie sich bitte an den betrieblichen Datenschutzbeauftragten Ihres Versicherers. Richten Sie auch ein etwaiges Verlangen auf Auskunft, Berichtigung, Sperrung oder Löschung wegen der beim Rückversicherer gespeicherten Daten stets an Ihren Versicherer.

Sachregister

Abkürzungsverzeichnis

2. BMeldDÜV	Zweite Bundesmeldedaten-Übermittlungsverordnung
AA	Auswärtiges Amt
AIDS	Acquired Immune Deficiency Syndrome
AO	Abgabenordnung
APC	Arbeitsplatzcomputer
APIS	Arbeitsdatei PIOS innere Sicherheit
ARB	Allgemeine Rechtsschutzversicherungsbedingungen
AZR	Ausländerzentralregister
BAföG	Bundesausbildungsförderungsgesetz
BAG	Bundesarbeitsgericht
BASt	Bundesanstalt für Straßenwesen
BAW	Bundesanstalt für Wirtschaft
BAZ	Bundesamt für den Zivildienst
BDSG	Bundesdatenschutz
BfA	Bundesversicherungsanstalt für Angestellte
BfD	Bundesbeauftragter für den Datenschutz
BfV	Bundesamt für Verfassungsschutz
BG	Berufsgenossenschaft
BGA	Bundesgesundheitsamt
BGB	Bürgerliches Gesetzbuch
BGBl	Bundesgesetzblatt
BGS	Bundesgrenzschutz
BKA	Bundeskriminalamt
BKAG	Bundeskriminalamt-Gesetz
BKGG	Bundeskindergeldgesetz
BMA	Bundesminister für Arbeit und Sozialordnung
BMF	Bundesminister der Finanzen
BMI	Bundesminister des Innern
BMJ	Bundesminister der Justiz
BMJFFG	Bundesminister für Jugend, Familie, Frauen und Gesundheit
BMP	Bundesminister für das Post- und Fernmeldewesen
BMV	Bundesminister für Verkehr
BMVg	Bundesminister der Verteidigung
BMWi	Bundesminister für Wirtschaft
BND	Bundesnachrichtendienst
BT-Drs.	Bundestags-Drucksache
Btx	Bildschirmtext
BVerfG	Bundesverfassungsgericht
BVerfGE	Bundesverfassungsgerichtsentscheidung
BVerwG	Bundesverwaltungsgericht
BZR	Bundeszentralregister
BZRG	Bundeszentralregistergesetz
coArb	computerunterstützte Arbeitsverwaltung
coLei	computerunterstützte Leistungsgewährung
COMPAS	computerunterstütztes Ausbildungsvermittlungssystem
DAV	Dienstanschlußvorschriften
DB	Deutsche Bundesbahn
DBP	Deutsche Bundespost
DPA	Deutsches Patentamt
DV/dv	Datenverarbeitung
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
EPOS	Einsatz der Datenverarbeitung am Postschalter
EVP	Eignungs- und Verwendungsprüfung

FRV	Fahrzeugregisterverordnung
FTZ	Fernmeldetechnisches Zentralamt
FUS	Flugunfalluntersuchungsstelle
FuVE	Funkvermittlungseinrichtung
G 10	Gesetz zur Beschränkung der Brief-, Post- und Fernmeldegeheimnisse
GAN	Grenzaktennachweis
GG	Grundgesetz
GMBl	Gemeinsames Ministerialblatt
GRG	Gesundheits-Reformgesetz
HGB	Handelsgesetzbuch
HIV	Human Immundeficiency Virus
ICAO	Internationale Zivil-Luftfahrt-Organisation
INPOL	Informationssystem der Polizei
ISDN	Integrates Services Digital Network
JGG	Jugendgerichtsgesetz
JUSTIS	Justizstatistikinformationssystem
KBA	Kraftfahrt-Bundesamt
KPMD-S	Kriminalpolizeilicher Meldedienst in Staatsschutzsachen
KpS	Kriminalpolizeiliche personenbezogene Sammlungen
KSVG	Künstlersozialversicherungsgesetz
LAK	Landwirtschaftliche Alterskasse
LBA	Luftfahrt-Bundesamt
MAD	Militärischer Abschirmdienst
NADIS	Nachrichtendienstliches Informationssystem
NADIS-PZD	NADIS-Personenzentraldatei
NJW	Neue Juristische Wochenzeitschrift
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
PC	Personalcomputer
PIOS	Auskunftssystem über Personen, Institutionen, Objekte und Sachen
RDV	Recht der Datenverarbeitung (Fachzeitschrift)
RzBw	Rechenzentrum der Bundeswehr
SCHUFA	Schutzgemeinschaft für allgemeine Kreditsicherung GmbH
SGB I	Sozialgesetzbuch Erstes Buch
SGB X	Sozialgesetzbuch Zehntes Buch
SOWI	Sozialwissenschaftliches Institut der Bundeswehr
SPUDOK	Spurendokumentationssystem
START	Studiengesellschaft zur Automatisierung von Reise und Touristik
StDAV	Steuerdaten-Abruf-Verordnung
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
StVG	Straßenverkehrsgesetz
StVZO	Straßenverkehrs-Zulassungs-Ordnung

TB	Tätigkeitsbericht*)
THW	Technisches Hilfswerk
TKO	Telekommunikationsordnung
VDR	Verband der Rentenversicherungsträger
VZR	Verkehrszentralregister
WEWIS	Wehrersatzwesen-Informationssystem
WPflG	Wehrpflichtgesetz
ZEVIS	Zentrales Verkehrsinformationssystem
ZPO	Zivilprozeßordnung

*) Erster Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 8/2460
Zweiter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 8/3570
Dritter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 9/93
Vierter Tätigkeitsbericht ist erscheinen als Bundestags-Drucksache Nr. 9/1243
Fünfter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache 9/2386
Sechster Tätigkeitsbericht ist erschienen als Bundestags-Drucksache 10/877
Siebenter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache 10/2777
Achter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache 10/4690
Neunter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache 10/6816
Zehnter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache 11/1693