Deutscher Bundestag
8. Wahlperiode

Drucksache 8/3570

18. 01. 80

Sachgebiet 204

Unterrichtung

durch den Bundesbeauftragten für den Datenschutz

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

Gliederung

Druck: Bonner Universitäts-Buchdruckerei, 5300 Bonn
Alleinvertrieb: Verlag Dr. Hans Heger, Postfach 20 08 21, Herderstraße 56,
5300 Bonn 2, Telefon (0 22 21) 36 35 51

Gemäß § 19 Abs. 2 Satz 2 des Bundesdatenschutzgesetzes zugeleitet mit Schreiben des Bundesbeauftragten für den Datenschutz — I 192 111/2 — vom 18. Januar 1980

1 Überblick

1.1 Schwerpunkte der Tätigkeit im Berichtsjahr

Schwerpunkte meiner Tätigkeit im Jahr 1979 waren:

— die *Kontrolle* der Einhaltung des Datenschutzrechts bei der Arbeitsverwaltung, bei Trägern der Sozialversicherung sowie ihren Verbänden, beim Kraftfahrt-Bundesamt und beim Statistischen Bundesamt, aufgrund von Einzeleingaben auch bei Behörden des Sicherheitsbereichs und der Deutschen Bundespost,

— Die *Beratung* der zuständigen Bundesminister und einzelner Ausschüsse des Deutschen Bundestages zu verschiedenen Gesetzgebungsvorhaben (Melderechtsrahmengesetz, Personalausweisgesetz, Neuregelung des Sozialgeheimnisses, Bundeswahlordnung, Verkehrszentralregistergesetz, Statistik-Novellen), zur Vorbereitung anderer Vorschriften (Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen), Stellungnahmen insbesondere auch gegenüber dem Innenausschuß des Deutschen Bundestages zu den Datensammlungen des Bundeskriminalamts und Beteiligung an der Diskussion über die Amtshilfe von Polizeibehörden für Nachrichtendienste,

— *Öffentlichkeitsarbeit* zur Verbreitung von Kenntnissen über Informationswesen und Datenschutzrecht und zur Verstärkung des Problembewußtseins,

— Intensivierung der *Kooperation* mit den Landesbeauftragten für den Datenschutz und den Datenschutz-Aufsichtsbehörden

— sowie Vertiefung und Erweiterung der *internationalen Kontakte* mit dem Ziel praktischer Zusammenarbeit.

Obwohl die Kontrolltätigkeit gegenüber dem Vorjahr deutlich verstärkt werden konnte, mußten wichtige Institutionen, die Datenverarbeitung betreiben, noch unkontrolliert bleiben. Überdies konnten, soweit Prüfungen bereits stattfanden, meist nur Teilbereiche erfaßt werden. Mit dem weiteren Ausbau der Dienststelle wird gerade die Prüfungstätigkeit intensiviert werden müssen.

1.2 Fortschreitende Anwendung der Informationstechnik und Gefahren für die Individualrechte

Dei technische Entwicklung macht es möglich, immer mehr Informationen immer schneller zu verarbeiten und für die verschiedensten Zwecke auszuwerten. Die Kosten der Geräte sinken seit einiger Zeit beständig, während gleichzeitig Leistungsfähigkeit und Speicherkapazität sprunghaft zunehmen. Datenfernübertragung ist kein technisches Problem mehr.

Der technische Fortschritt ist faszinierend, wenn man an den möglichen gesellschaftlichen Nutzen denkt; er ist bedrückend, wenn man sich vergegenwärtigt, daß dieselben Möglichkeiten auf der anderen Seite zu gesteigerter Kontrolle und Entmündigung eingesetzt werden können. Sicher ist, daß die allgemeine Einführung neuer Kommunikationsformen wie Bildschirmtext, Kabelkommunikation, Satellitenfernsehen und damit verbundene Informations-, Unterhaltungs-, Fortbildungs- und sonstige „Dienste" erheblichen Einfluß auf die Formen des sozialen Zusammenlebens ausüben werden. Es ist ebenso sicher, daß dadurch neuartige oder zumindest wesentlich verstärkte Maßnahmen des Schutzes persönlicher Rechte gegenüber unangemessener Informationsverarbeitung erforderlich werden. Aber auch bereits realisierte oder in näherer Zukunft geplante Anwendungen der Datenverarbeitungs- und -übertragungstechnik werfen erhebliche Datenschutzprobleme auf.

Was über den gegenwärtigen Stand der Informationstechnologie und ihre Realisierung in Staat und Wirtschaft veröffentlicht wird, erreicht offenbar nur einen Teil der Bevölkerung. Dieser Umstand wirkt sich so aus, daß einerseits eine große Zahl von Menschen sich der Gefährdungen überhaupt nicht bewußt wird, andererseits viele Mitbürger der Zukunft mit übergroßer Sorge entgegensehen und dabei die Gegenmaßnahmen kaum noch wahrnehmen. Aufklärung über die aktuelle Situation wird nicht selten von pessimistischen Prognosen überlagert und verdrängt, und die jeweils unterschiedliche Einschätzung der allgemeinen politischen Entwicklung schlägt gerade bei Aussagen zur staatlichen Informationsverarbeitung voll durch.

Ich habe mehrfach erklärt, daß die bestehenden Informationssysteme es nicht rechtfertigen, die Bundesrepublik einen „Überwachungsstaat" zu nennen. Einige Erscheinungsformen der Informationserhebung und -verarbeitung geben jedoch Anlaß zur rechtlichen Kritik, und einige Vorhaben — in Staat und Wirtschaft — lassen bedenkliche Tendenzen erkennen, die Technik zur Sicherung bestimmter Interessen zu nutzen und dabei weitere Abhängigkeiten der betroffenen Menschen 'zu erzeugen. Dies geschieht oft im Namen durchaus anerkennenswerter gesellschaftlicher Ziele, aber eben ohne hinreichende Berücksichtigung nachteiliger Folgewirkungen für die Betroffenen.

Der Anwalt des Datenschutzes muß diese *beiden* Aspekte beachten: Er muß einerseits die Gefahren aufzeigen, andererseits darüber aufklären, wo sie nicht — oder in pessimistischer Sicht: noch nicht

— verwirklicht sind. Ein Journalist, der sich um die Aufklärung über die Informationsverarbeitung der öffentlichen Verwaltung besonders verdient gemacht hat, beschreibt diese Gratwanderung (die er auch als seinen eigenen Weg ansieht) wie folgt:

> „Verharmlosung betreibt, wer sich nur auf jene Veröffentlichungen stützt, die Polizei oder Dienste über ihre Computersysteme selber publiziert oder lanciert haben, und wer die vorhandenen Datensammlungen beschreibt, ohne Mißbrauchsmöglichkeiten aufzuzeigen . . .
>
> Übertreibung wiederum würde kaum andere Folgen zeitigen. Wer die Bundesrepublik des Jahres 1979 als perfekten Überwachungsstaat darstellt, redet ihn herbei. Er fördert jedenfalls die politische Resignation und die ängstliche Apathie, die sich selbst an Schulen und Hochschulen breitgemacht haben. Eine Generation aber, die sich (zu Unrecht) auf Schritt und Tritt beschattet wähnt, kann nicht jene Aktivitäten enfalten, die nottäten, einen Überwachungsstaat zu verhindern." (Jochen Bölsche, Der Weg in den Überwachungsstaat, Reinbek 1979, S. 9).

Vor diesem Hintergrund ist es zu sehen, wenn im folgenden einige bedeutsame Elemente des bestehenden Informationswesens, aber auch Entwicklungstendenzen charakterisiert werden.

Der Bereich öffentlicher Verwaltung, in dem die meisten personenbezogenen Daten anzutreffen sind, ist die Sozialverwaltung, hier insbesondere die Arbeitsverwaltung und die Sozialversicherung. Wollte man allein auf die Größe der Systeme abstellen, d. h. auf die Zahl der Personen, deren Daten gespeichert sind, so müßte an erster Stelle die in Würzburg befindliche Datenstelle des Verbandes Deutscher Rentenversicherungsträger e. V., Frankfurt/Main, mit bis zu 75 Millionen Personendatensätzen in einer Datei, ferner die Bundesanstalt für Arbeit mit ca. 30 Millionen Datensätzen genannt werden.

Für verschiedene Bereiche der Sozialverwaltung gibt es Ideen, aber auch schon Projekte, die auf eine zentrale Sammlung personenbezogener, insbesondere medizinischer Daten eines großen Personenkreises abzielen, um dadurch die Leistungsfähigkeit und Wirtschaftlichkeit des betreffenden Verwaltungszweiges zu erhöhen. Gegenüber solchen Bestrebungen — mögen sie in noch so guter Absicht unternommen werden — ist mit Nachdruck darauf hinzuweisen, daß eine Konzentration von Informationen über den einzelnen wesentliche Veränderungen in der Art und Weise der Gesundheitsvorsorge und -fürsorge mit sich bringen und vor allem das Verhältnis des Patienten/Versicherten zu Ärzten bzw. Krankenkassen beeinträchtigen würde. Durch die leichtere Möglichkeit der Mehrfachnutzung wird die Gefahr der Zweckentfremdung verstärkt. Außerdem wird man sich möglicherweise immer mehr auf vorhandene Bestände verlassen; damit aber erhöht sich die Gefahr der Nutzung veralteter und falscher Daten.

In der Abeitsverwaltung erreicht die Speicherung personenbezogener Daten insbesondere zu Zwekken der Arbeitsvermittlung inzwischen beträchtliche Ausmaße. So einig man sich über die Notwendigkeit effektiver Arbeitsvermittlung sein wird, so nötig ist es doch, über die Angemessenheit der anzuwendenden Mittel immer von neuem nachzudenken.

Ein besonderes Problemfeld ist auch die Sozialarbeit. Soweit ich mir auf diesem Gebiet wegen meiner begrenzten Zuständigkeit einen Einblick verschaffen konnte, ist die Sensibilität der hier anzutreffenden Daten besonders groß, der Schutz aber noch unzureichend realisiert.

Die Suche nach der stets aufgegebenen Antwort auf die Frage, wie weit zu Zwecken des Sozialstaates die Freiheitssphäre des Bürgers beschränkt werden sollte, ist nie beendet. Ein Erlahmen hier könnte dazu führen, daß die sozialstaatlichen Segnungen zu einem Instrumentarium sozialer Kontrolle, Gängelung und Bevormundung denaturiert würden, was sicher niemand will.

Als besonders „riskant", weil für die Betroffenen nicht durchschaubar, werden in der Bevölkerung nach wie vor die Informationssysteme im Sicherheitsbereich angesehen. Sie bedürfen deshalb laufender Überprüfung.

Mit besonders sensiblen Angaben arbeitet das Informationssystem PIOS (Personen, Institutionen, Objekte, Sachen) der Polizei, in dem Daten aus den Kriminalitätsbereichen Terrorismus und Rauschgift enthalten sind. Es liegt auf der Hand, daß ein solches System äußerst sorgfältig abgeschirmt werden muß; dies erscheint derzeit voll garantiert. Aber es bedarf auch strenger Regelungen über Umfang und Dauer der Datenspeicherung, und hier bestehen zum Teil noch erhebliche Lücken.

Dagegen enthält das nachrichtendienstliche Informationssystem NADIS nur Hinweise auf Aktenfundstellen, aber nicht auf Einzeldaten, die über die Personengrunddaten hinausgehen. Doch ist auch hier der Umfang der erforderlichen Registrierung infolge der Weite und Unbestimmtheit des gesetzlichen Auftrages an die Verfassungsschutzbehörden nur schwer abgrenzbar.

Im polizeilichen Fahndungssystem INPOL erweisen sich die Notierungen zur polizeilichen Beobachtung nach wie vor als besonders problematisch. Für sie fehlt die eindeutige Rechtsgrundlage sowohl im Bereich der Gefahrenabwehr als auch der Strafverfolgung. Die Zahl der beobachteten Personen ist allerdings im vergangenen Jahr erheblich reduziert worden.

Bei der geplanten Neukonzeption von INPOL wird darauf zu achten sein, daß der Grundsatz der Erforderlichkeit streng gewahrt bleibt.

Die Erforderlichkeit elektronischer Fahndungshilfen und die Rechtmäßigkeit der besonders wichtigen Bestandteile von INPOL, nämlich des Personen- und Sachfahndungsregisters, können nicht bestritten werden. Es wäre deshalb falsch zu sagen, daß „die" Dateien und/oder Karteien des Bundeskriminalamtes oder „das" System INPOL rechtswidrig wären. Auch ich habe dies nie behauptet.

Die der Datenverarbeitungstechnik immanenten Gefahren machen aber Einschränkungen und Sicherungen gegenüber bestimmten Elementen des vorhandenen kriminalpolizeilichen Instrumentariums erforderlich, und eine Anzahl solcher Restriktionen ist mit den beteiligten Stellen der Polizei vereinbart worden. Ich hoffe, daß sie nun bald in die Tat umgesetzt werden.

Das Institut der Amtshilfe muß aus datenschutzrechtlicher Sicht neu durchdacht werden. Immer wieder wird das allgemeine Amtshilfegebot (Artikel 35 GG) als Rechtfertigung für die Übermittlung personenbezogener Daten zwischen Behörden angeführt. Diese Auffassung verstößt jedoch gegen den aus der gesetzlichen Aufgaben- und Befugniszuweisung abzuleitenden Grundsatz der Zweckbindung von Daten. Ausnahmen können nur vom Gesetzgeber selbst festgelegt werden, wobei für jede Materie gesondert die gegensätzlichen Interessen abzuwägen und zu gewichten sind.

Zur Klärung der Rechtsfragen der Amtshilfe zwischen Polizei und Nachrichtendiensten (hierzu s. u. 2.8.1) hat der Bundesminister des Innern zunächst eine Arbeitsgruppe eingesetzt und später bei sechs Professoren des öffentlichen Rechts Stellungnahmen in Auftrag gegeben. Im November 1979 fand im Bundesministerium des Innern ein ganztägiges Gespräch mit diesen Gutachtern statt, an dem ich mich beteiligt habe. Das Ministerium wird die Stellungnahmen demnächst veröffentlichen und stellt Überlegungen an, welche Konsequenzen zu ziehen sind. Die Problematik der Amtshilfe geht aber über den Sicherheitsbereich weit hinaus. Dieses Rechtsinstitut darf nicht als Instrument dazu benutzt werden, die Zulässigkeitsbestimmungen des Datenschutzrechts „aus den Angeln zu heben".

Zu den größten zentralen Datenbeständen in der Bundesrepublik gehören das Verkehrszentralregister („Verkehrssünderkartei") und die Datei der Kraftfahrzeughalter, die beim Kraftfahrt-Bundesamt geführt werden. Beim Verkehrszentralregister ist im Zusammenhang mit der anstehenden gesetzlichen Regelung, an deren Vorbereitung ich beratend mitgewirkt habe, eine erhebliche Verbesserung des Datenschutzes zu erwarten. Umfang und Dauer der Speicherung sollen reduziert werden; Behörden und Gerichte sollen nur noch diejenigen Informationen erhalten, die sie jeweils für den konkreten Zweck benötigen. Bei den Daten der Fahrzeughalter kommt es mir darauf an, die Auswertung auf verkehrsbezogene Zwecke beschränkt zu halten und Bestrebungen zurückzuweisen, den Datenbestand als Ersatz-Adreßregister zu nutzen.

Ich habe deutlich gemacht, daß die Grundsätze der Erforderlichkeit und der Zweckbindung auch für das im Aufbau begriffene automatisierte Zentrale Verkehrs-Informationssystem (ZEVIS) verbindlich sind. An diesen Grundsätzen sind auch die im Konzept für ZEVIS vorgesehenen Möglichkeiten der Direktabfrage durch externe Stellen sowie der kombinierten Anfrage an beide Datenbestände zu messen.

Der Vollständigkeit halber sei angemerkt, daß es auch im privaten Bereich Informationssysteme gibt, die eine ähnliche Wirkung sozialer Kontolle haben können wie die staatlichen Informationssysteme. Für ihre Datenschutzkontrolle sind die Aufsichtsbehörden der Länder zuständig. Doch scheint es mir wichtig, die Aufmerksamkeit der Öffentlichkeit auch auf diese Datensammlungen von Versicherungsgesellschaften, Arbeitgebern oder Kreditschutzorganisationen zu lenken, die ständig Gegenstand einer großen Zahl von Beschwerden und Anfragen besorgter Bürger sind.

1.3 Stand des Datenschutzes im allgemeinen

Sieht man von den grundsätzlichen Bedenken gegen die erwähnten großen Informationssysteme ab und wendet sich der Art und Weise zu, in der Informationen innerhalb dieser und anderer Systeme verarbeitet werden, so gab es zu Beanstandungen bisher relativ wenig Anlaß. Schwere Verstöße gegen die Speicherungs- und Übermittlungsvorschriften des BDSG oder anderer Vorschriften über den Datenschutz sind — ebenso wie im ersten Berichtsjahr — selten gewesen; wirklicher Mißbrauch personenbezogener Daten, insbesondere ihre Verwendung zum persönlichen Nutzen von Amtswaltern ist nicht bekanntgeworden.

Wohl aber war in einer Reihe von Fällen zu bemängeln, daß Daten verarbeitet wurden, die für Zwecke der betreffenden Behörde nicht erforderlich waren oder deren Erhebung rechtlich bedenklich erschien. Auch haben meine Mitarbeiter bei örtlichen Kontrollen feststellen müssen, daß die zur Verwirklichung des Datenschutzes notwendigen technischen und organisatorischen Maßnahmen vielfach noch lückenhaft sind.

Mein Gesamteindruck aus der Kontrolltätigkeit des Berichtsjahres läßt sich so zusammenfassen: Die Behörden der Bundesverwaltung sind um mehr Datenschutz bemüht und haben vielfach bereits aus eigener Initiative Anstrengungen unternommen, um den Vorschriften des BDSG gerecht zu werden. Trotzdem hat sich gezeigt, daß man sich mit dem erreichten Zustand noch nicht begnügen darf; bei keiner der von mir kontrollierten Behörden war die Datenverarbeitung gänzlich ohne Mängel. Ich habe zugleich mit meiner Kritik, die nicht immer bis zu förmlichen Beanstandungen gehen mußte, Vorschläge zur Verbesserung des Datenschutzes gemacht und auch im Detail Maßnahmen zur wirksameren Datensicherung aufgezeigt. Nach meinen Feststellungen sind die betreffenden Behörden für solche Vorschläge aufgeschlossen und überwiegend auch bereit, ihnen zu folgen.

1.4 Eingaben und wichtige Beschwerdepunkte

Im Berichtsjahr haben mich etwa 2 500 Eingaben von Bürgern erreicht, die sich in ihren Rechten verletzt fühlten, Auskunft zu Rechtsfragen wünschten oder allgemeine Informationen erbaten. Etwa 15 % der Zuschriften habe ich zuständigkeitshalber an die Landesdatenschutzbeauftragten oder die Aufsichtsbehörden der Länder abgegeben.

Ein Schwerpunkt der täglichen Bürgereingaben lag in Anfragen, wo denn eigene Daten gespeichert seien. Soweit diese Schreiben keine konkreten Anhaltspunkte zu bestimmten Verwaltungsbeziehungen des Einsenders enthielten, konnten sie von mir auch nur mit allgemeinen Hinweisen beantwortet werden. In groben Umrissen wurde dabei mitgeteilt, welche Spreicherungsmöglichkeiten personenbezogener Daten in welchen Zusammenhängen bestehen könnten und daß eine konkrete Auskunft nur von der jeweils speichernden Stelle zu bekommen sei. In Zukunft soll der Bürger bei diesen allgemeinen Anfragen durch die „Transparenzbroschüre" (vgl. 1. TB*, 2.1 und unten 1.8) ausführlicher darüber informiert werden, wo er im allgemeinen Daten über sich vermuten und seine Rechte nach den Datenschutzgesetzen, insbesondere seine Rechte auf Auskunft, geltend machen kann.

Von Interesse ist auch, daß die in den Briefen angesprochene Problematik fast die gleiche wie im Vorjahr war. Die folgenden Fragen und Beschwerdepunkte traten am häufigsten auf:

— Nach wie vor beklagt sich eine große Anzahl von Bürgern darüber, daß für eine Auskunft über eingene Daten eine Gebühr bzw. ein Entgelt verlangt wird.

— Auch daß Angaben, die vom Kraftfahrt-Bundesamt bei An- und Ummeldungen von Kraftfahrzeugen erhoben werden, an Adressenverlage für Werbezwecke weitergegeben werden, wird bemängelt.

— Mißtrauen wird weiterhin den Sicherheitsbehörden entgegengebracht. Die Angst, daß die Teilnahme an einer Demonstration „automatisch" zu einer Speicherung beim BfV führt, scheint bei einem Teil der Bürger besonders ausgeprägt zu sein. Aber auch bei Grenzkontrollen vermuten manche Menschen, daß diese Überprüfungen Speicherungen bei einer Sicherheitsbehörde nach sich ziehen.

— Zahlreiche Bürger haben sich darüber beschwert, daß bei der Beantragung eines Fernsprechanschlusses von der Bundespost mehr erfragt wird, als zur Einrichtung des Fernsprechanschlusses notwendig ist.

— In vielen Eingaben wird auch die Angst vor dem Mißbrauch ärztlicher und psychiatrischer Gutachten im Rahmen der Arbeitsverwaltung deutlich. Außerdem wird befürchtet, daß neue gesetzliche Regelungen eine Durchbrechung des Arztgeheimnisses herbeiführen könnten.

1.5 Informationsbesuche und Kontrollen bei Bundesbehörden

Die schon im Jahre 1978 zur Vorbereitung systematischer Überprüfungen gem. § 19 Abs. 1 Satz 1 BDSG aufgenommenen Kontakte zu Bundesdienststellen habe ich durch weitere Informationsbesuche intensiviert. Sie verschaffen mir Einblick in die Aufgaben, die jeweilige Organisationsstruktur, den Stand der dort betriebenen Datenverarbeitung und die bisher eingeleiteten Datenschutzmaßnahmen. Dabei habe ich insbesondere den Bereichen der Bundesverwaltung Vorrang eingeräumt, die mir aus aktuellem politischen Anlaß, wegen eines festzustellenden besonderen Interesses der Öffentlichkeit, wegen sich auffällig häufender Bürgerbeschwerden oder wegen eines besonders großen Bestandes an gespeicherten personenbezogenen Daten interessant zu sein schienen. Unter diesen Gesichtspunkten wurden u. a. das Bundesamt für Finanzen, das Bundesverwaltungsamt, das Statistische Bundesamt, das Bundesarchiv, der Bundesnachrichtendienst, das Bundeskriminalamt sowie die Grenzschutzdirektion und ein Grenzschutzamt besucht. Gelegentlich waren diese Besuche auch mit Kontrollen gem. § 19 Abs. 1 Satz 1 BDSG in Teilbereichen verbunden oder dienten zugleich der schnellen Aufklärung mir vorliegender Bürgerbeschwerden.

Daneben habe ich mit einigen meiner Mitarbeiter zur Vertiefung unserer Kenntnisse über Datenverarbeitungs- und Datensicherungssyteme und ihre künftig zu erwartende Entwicklung zwei großen Herstellerfirmen von Datenverarbeitungsanlagen Informationsbesuche abgestattet. Die dort gewonnenen Erkenntnisse werden insbesondere meinen Mitarbeitern bei der Datenschutzkontrolle „vor Ort" hilfreich sein. Aber auch für die mir nach § 19 Abs. 1 Satz 2 BDSG obliegende Beratung der Bundesbehörden zu Datenschutzfragen waren die Besuche bei den vorgenannten Firmen nützlich.

Mir ist daran gelegen, daß sowohl bei meinen Kontaktbesuchen wie auch bei den eigentlichen Kontrollen der datenverarbeitenden Stellen eine sachliche Atmosphäre herrscht. Nur so kann Verständnis für die Aufgabe der jeweils anderen Seite entstehen und der für eine wirksame Kontrolle unerläßliche Informationsaustausch über die Probleme der betreffenden Datenverarbeitungsaufgabe und -organisation sichergestellt werden. Die Bereitschaft der datenverarbeitenden Stellen, mir Auskunft zu meinen Fragen und Einsicht in Unterlagen und Akten zu gewähren (§ 19 Abs. 3 Nr. 1 BDSG), wird um so größer sein, je mehr es mir und meinen Mitarbeitern gelingt, bei den kontrollierten Stellen Verständnis für meine Arbeit zu wecken. Umgekehrt werden sich meine Ratschläge und Forderungen leichter durchsetzen lassen, wenn sie an den Interessen der speichernden Stelle nicht vorbeigehen und deren Bedürfnisse berücksichtigen. Dies bedeutet nicht, daß durch „Zusammenarbeit" von Kontrollinstanz und kontrollierter Stelle jeweils die glatteste Lösung gefunden wird, um den gesetzlichen Vorschriften formal gerecht zu werden. Oberstes Ziel der Kontrolltätigkeit müssen vielmehr die schutzwürdigen Belange der Betroffenen bleiben. Wenn in Ausnahmefällen meine Forderungen nicht im gegenseitigen Einvernehmen durchsetzbar sind, werde ich — wie bisher — auch Auseinandersetzungen nicht scheuen, um den Interessen des Datenschutzes Geltung zu verschaffen.

* 1. TB = Erster Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz, vorgelegt zum 1. Januar 1979

Nach den bisherigen Erfahrungen war dies nur selten notwendig. Nur in wenigen Einzelfällen stieß ich zunächst auf deutliche Abwehrhaltung, die teils noch auf unzureichendes Verständnis für die Belange des Datenschutzes, teils darauf zurückzuführen sein mag, daß Kontrolle durch eine Institution, die außerhalb der Behördenhierarchie, aber innerhalb der Bundesregierung angesiedelt ist, manchen Behörden immer noch sehr ungewöhnlich erscheint.

Im allgemeinen verlaufen die Kontrollbesuche in sachlicher und aufgeschlossener Atmosphäre. Die internen Datenschutzbeauftragten der kontrollierten Stellen, die mir meist schon bei der Vorbereitung der Kontrollen behilflich sind, verstehen sich dabei als meine Gesprächspartner, die sich für die Sicherstellung des Datenschutzes bei der jeweils datenverarbeitenden Stelle primär verantwortlich fühlen. Ich habe keinen Anlaß, etwa mangelnde Auskunftsbereitschaft zu rügen, und kann generell feststellen, daß meinen Vorschlägen zur Verbesserung des Datenschutzes in der Regel gefolgt wird. Gleichwohl habe ich gelegentlich von meinem Beanstandungsrecht Gebrauch machen müssen, wenn sich bei Kontrollen gravierende Mängel der Datenverarbeitung gezeigt haben.

1.6 Verantwortlichkeit der Behörden für die Durchführung des Datenschutzes

Vereinzelt mußte ich oberste Bundesbehörden darauf hinweisen, daß ihre Verantwortlichkeit für den Datenschutz sich nicht auf die eigene Behörde und den etwaigen Erlaß von allgemeinen Verwaltungsvorschriften beschränkt, sondern sich auch auf die nachgeordneten Behörden und konkrete Kontrollen erstreckt. Ferner war in Einzelfällen festzustellen, daß der interne Datenschutzbeauftragte entweder zu zahlreiche andere Aufgaben oder zu wenig Mitarbeiter hatte, um seinen Verpflichtungen als Datenschutzbeauftragter angemessen nachzukommen. Nach meinen Beobachtungen lassen es die internen Datenschutzbeauftragten bisweilen an dem gebotenen Nachdruck fehlen, um ihren Forderungen, gegebenenfalls auch durch Fristsetzungen, Geltung zu verschaffen.

Im ersten Tätigkeitsbericht habe ich ausgeführt, es sei nicht meines Amtes, das gelegentlich geforderte „Gütezeichen" für datenschutzgerechte Systeme zu vergeben (1. TB, 6.2). Es ist auch nicht meine Aufgabe, „Obergutachter" zu sein. Wenn Anwender sich ein wissenschaftliches Gutachten erstatten lassen, so enthebt sie dies nicht ihrer datenschutzrechtlichen Verantwortung. Versuche, aus meinem Schweigen im Einzelfall ein Einverständnis mit den Ergebnissen eines Gutachtens zu konstruieren, muß ich zurückweisen.

Ich bin aber bereit, meinen Rat überall dort zu erteilen, wo er gesucht wird, und das Wissen und die Erfahrung meiner Dienststelle zur Verfügung zu stellen. Die Verwaltungen sollen durch meine Anregungen veranlaßt werden, die aufgeworfenen Probleme zu prüfen und zu lösen; dies muß aber in eigener Verantwortung geschehen. Meine gesetzliche Prüfungsaufgabe bleibt davon unberührt.

1.7 Kooperation mit anderen Datenschutzinstanzen

Die seit 1978 bestehende Konferenz der Landesbeauftragten und des Bundesbeauftragten für den Datenschutz ist im Berichtszeitraum zweimal zusammengetreten. Der Vorsitz der Konferenz wechselt künftig jährlich in alphabetischer Reihenfolge. Zur Vorbereitung der Sitzungen und Vertiefung des Gedankenaustausches sind inzwischen folgende Ad-hoc-Arbeitsgruppen gebildet worden:

— „Sicherheitsbereich" (unter meiner Federführung)

— „Steuerverwaltung"

— „Wissenschaft und Statistik".

Die Konferenz einschließlich der Arbeitsgruppen gibt die Möglichkeit, im Sinne des § 19 Abs. 5 BDSG auf eine enge Zusammenarbeit der für den öffentlichen Bereich zuständigen Datenschutzkontrollinstitutionen hinzuwirken und so im Interesse der betroffenen Bürger eine von der jeweils örtlichen Zuständigkeit unabhängige, möglichst einheitliche Handhabung des Datenschutzrechts für diesen Bereich zu erzielen. In den Sitzungen im Mai und November 1979 wurden u. a. folgende Themen abgehandelt:

— Sicherheitsbehörden und Datenschutz (Notwendigkeit bereichsspezifischer gesetzlicher Regelung der Befugnisse der Sicherheitsbehörden)

— Datenschutz in der Steuerverwaltung (Kontrollmöglichkeiten und Anwendung der Vorschriften des Datenschutzes über die Veröffentlichungs- und Auskunftspflicht im Bereich der Finanzverwaltung)

— Datenverarbeitung in der Statistik und für Zwecke der Wissenschaft und Forschung (Vorschläge zur datenschutzgerechten Gestaltung der Statistikgesetze unter Berücksichtigung der Bedürfnisse wissenschaftlicher Forschung nach Zugang zu personenbezogenen Daten)

— Schuldnerverzeichnis nach § 915 ZPO (Neuregelung des Zugangs zu Schuldnerverzeichnissen)

— Personalausweisgesetz (Verwendungsbeschränkung des fälschungsicheren und maschinenlesbaren Personalausweises)

— Entwurf eines Melderechtsrahmengesetzes

— Erhebung von Kosten für die Geltendmachung von Rechten nach den Datenschutzgesetzen.

Neben den Kontakten zu den Landesbeauftragten für den Datenschutz hat sich der unter meiner Federführung ebenfalls seit 1978 stattfindende Erfahrungsaustausch mit den innerbehördlichen Datenschutzbeauftragten der obersten Bundesbehörden im Sinne von § 15 BDSG bewährt.

Im Berichtsjahr wurde u. a. folgendes erörtert:

— Stand der Datensicherungsmaßnahmen in den obersten Bundesbehörden

— Allgemeine Verwaltungsvorschriften nach § 16 BDSG

— Verpflichtung der Mitglieder von Personalvertretungen auf das Datengeheimnis

— Abgrenzung von Unternehmensdaten zu personenbezogenen Daten.

Die bisher in den vorgenannten Kooperationsgremien gesammelten Erfahrungen zeigen die Notwendigkeit der gegenseitigen Abstimmung zur Wahrung einer einheitlichen Datenschutzpraxis in Bund und Ländern; sie beweisen aber auch, daß es weitgehend möglich ist, im Interesse des Bürgers eine einheitliche Anwendung der Datenschutzgesetze zu erreichen. Die Zusammenarbeit mit anderen Datenschutzinstanzen in den hierfür jetzt vorhandenen Gremien werde ich deshalb fortsetzen. Dies gilt auch für meine Beteiligung an den regelmäßigen Beratungen der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, dem sog. „Düsseldorfer Kreis". An einigen der dort gefundenen Verhandlungsergebnissen, die auch meinen Zuständigkeitsbereich berührten, habe ich besonders intensiv mitgewirkt (vgl. 2.9).

1.8 Öffentlichkeitsarbeit

Im Rahmen meiner Öffentlichkeitsarbeit habe ich im Berichtszeitraum an Interessenten zunächst weiterhin die schon als Einführung in die Rechte des Bürgers bewährte Broschüre „Was bringt das Datenschutzgesetz?" abgegeben. Vor allem Schüler, Studenten und Verbände zeigten reges Interesse daran. Um die in meinem ersten Tätigkeitsbericht angekündigte neue Schrift finanzieren zu können, mußte ich darauf verzichten, die bisherige Broschüre in dem an sich erforderlichen Umfang nachdrucken zu lassen. So konnte ich vielen Wünschen, insbesondere dem Verlangen nach Überlassen einer jeweils größeren Anzahl von Exemplaren zur Weiterverteilung an Dritte, nicht gerecht werden; ich habe im Einzelfall jedoch darauf hingewiesen, daß gegen eine Vervielfältigung durch den Empfänger keine Bedenken bestehen. Immerhin hat die Schrift eine Auflage von rd. 57 000 Exemplaren erreicht.

Auch den besonders zu Jahresanfang häufig an mich herangetragenen Wunsch auf Übersendung meines ersten Tätigkeitsberichts konnte ich zu meinem Bedauern nur vereinzelt erfüllen. Zwar habe ich an besonders Interessierte insgesamt 500 Exemplare eines Sonderdrucks des Berichts verteilt; der Druck weiterer Exemplare zur kostenlosen Abgabe war jedoch mangels Haushaltsmitteln nicht möglich. Ich mußte die Interessenten zunächst auf die Möglichkeit des Kaufs der Bundestagdrucksache verweisen. Inzwischen hat das Presse- und Informationszentrum des Deutschen Bundestages erfreulicherweise in seiner Schriftenreihe „Zur Sache" eine Broschüre veröffentlicht, die unter anderem meinen ersten Tätigkeitsbericht sowie eine kurze Einführung in die Rechte des Bürgers nach dem Bundesdatenschutzgesetz enthält. Ich hatte die Möglichkeit, an der Erstellung der Schrift mitzuwirken, so daß sie meinen Erwartungen voll entspricht; sie ist eine nützliche Information für den Bürger und andere interessierte Stellen.

Gleichwohl hielt ich es nach Auswertung der bisher eingegangenen Anfragen für geboten, dem Bürger eine neue Broschüre anzubieten, die ihm anhand der wichtigsten Beispiele Hinweise darauf geben soll, an welchen Stellen seine persönlichen Daten gespeichert sein könnten. Die Broschüre „Der Bürger und seine Daten" habe ich in Gemeinschaftsarbeit mit den Landesbeauftragten für Datenschutz, der Datenschutzkommission in Rheinland-Pfalz sowie den Datenschutzaufsichtsbehörden der Länder erstellt. Sie ist inzwischen erschienen und bei mir sowie den Landesbeauftragten kostenlos erhältlich.

Die wünschenswerte und weiterhin notwendige Intensivierung des Datenschutzbewußtseins in der Öffentlichkeit kann jedoch nicht allein durch die Abgabe von Informationsmaterialien an Interessenten erreicht werden. Wichtig ist nach wie vor auch das Interesse der Medien an meiner Arbeit. Die vielfältigen und häufig spontanen Zuschriften, die jeweils kurz nach Veröffentlichung von einschlägigen Artikeln in der Presse oder nach Rundfunk- oder Fernsehbeiträgen zum Thema Datenschutz bei mir eingehen, zeigen, daß auf diese Weise viele Bürger erreicht und in ihrem politischen Bewußtsein angesprochen werden. Es ist für mich demnach nur folgerichtig, die Medien weiterhin in angemessenem Umfang über meine Tätigkeit zu unterrichten. Dies ist in einer Reihe von Hintergrundgesprächen sowie durch eine Anzahl von Presseverlautbarungen geschehen.

1.9 Dateienregister

Im Berichtsjahr war eine große Zahl von Nachmeldungen zum Register der von öffentlichen Stellen des Bundes automatisch betriebenen Dateien zu verzeichnen. Dadurch ist das Register mittlerweile auf etwa 800 Dateibeschreibungen angewachsen. Trotz gewisser struktureller Schwächen und noch immer bei einzelnen Meldungen bestehender inhaltlicher Mängel hat sich das Register als eine Arbeitsunterlage für meine Kontrolltätigkeit bewährt. Daneben wird es gelegentlich zur Information von Betroffenen herangezogen, um darzulegen, welche Art der Datenspeicherung bei einzelnen Behörden erfolgt.

Von der Möglichkeit, das Register an Ort und Stelle einzusehen, hat jedoch noch kein Bürger Gebrauch gemacht. Auch deshalb ist eine Führung des Registers im automatisierten Verfahren zur Zeit nicht beabsichtigt.

1.10 Ausbau der Dienststelle — Personal und Sachhaushalt

Mit Verabschiedung des Bundeshaushaltsplans für 1979 standen der Dienststelle des Bundesbeauftragten insgesamt 26 Stellen zur Verfügung. Sie setzen sich wie folgt zusammen:

höherer Dienst 11, gehobener Dienst 4, mittlerer Dienst 2, Tarifangestellte 7, Lohnempfänger 2.

Damit war das in der ursprünglichen Personalplanung vorgegebene Ausbauziel noch nicht erreicht. Im Bundeshaushalt 1980 werden der Dienststelle noch 3 weitere Stellen (1 höherer Dienst, 2 gehobener Dienst) zugewiesen. Nach wie vor ist also noch ein Personalfehlbedarf zu verzeichnen. Ich gehe davon aus, daß er durch den Bundeshaushalt 1981 ausgeglichen werden kann.

Die der Dienststelle schon zur Verfügung stehenden Stellen konnten in Kooperation mit dem Bundesminister des Innern inzwischen (weitgehend) besetzt werden, obwohl die Personalauswahl — wie schon im ersten Tätigkeitsbericht dargelegt — sich wegen der vielseitigen Anforderungen, denen die Bewerber gewachsen sein sollten, als schwierig erwies.

Der Sachhaushalt der Dienststelle des Bundesbeauftragten mit einem Volumen für 1979 von etwas über 530 000 DM entspricht im wesentlichen den Erfordernissen des Dienstbetriebes. Da in der Öffentlichkeit weiterhin ein großes, noch ständig steigendes Informationsbedürfnis zu Fragen des Datenschutzes besteht, war mir daran gelegen, daß die Titel für die Erstellung und kostenlose Abgabe von Informationsmaterial verstärkt werden. Der Bedarf dürfte im Haushalt 1980 mit einem vorgesehenen Betrag von 75 000 DM in etwa gedeckt sein.

2 Stand des Datenschutzes in ausgewählten Bereichen

2.1 Allgemeine innere Verwaltung

In der allgemeinen inneren Verwaltung des Bundes dominieren noch die hergebrachten Verfahren der Informationsverarbeitung in Akten und Aktensammlungen. Daneben gibt es auch hier zahlreiche manuelle Karteien, die meiner Kontrolle unterliegen. Die automatisierte Datenverarbeitung wird nur in wenigen Bereichen eingesetzt, wo große Datenmengen zu bewältigen sind. Jedoch sind in zahlreichen obersten Bundesbehörden automatisierte Personalinformationssysteme entstanden.

Der Schwerpunkt meiner Tätigkeit lag in der Beratung. Meine Vorschläge zur Berücksichtigung des Datenschutzes bei Gesetzgebungsvorhaben zielten im wesentlichen darauf ab, die Zwecke bestimmter Datenverarbeitungsarten präzise zu definieren, um damit Grenzen für jede anderweitige Verarbeitung zu setzen. Ich halte dies für eine zentrale Aufgabe der bereichsspezifischen Datenschutzgesetzgebung.

2.1.1 Wahlen

In meinem ersten Tätigkeitsbericht (3.2.1) habe ich auf Überlegungen und erste Ansätze hingewiesen, die darauf gerichtet waren, in dem auszulegenden Wählerverzeichnis den Tag der Geburt zu streichen. Die Denkanstöße, die damit gegeben worden waren und die ich dem Bundesminister des Innern gegenüber später noch präzisiert habe, haben fortgewirkt. In die Neufassung der Bundeswahlordnung (BWO) vom 9. November 1979 (BGBl. I, S. 1805) ist eine Regelung aufgenommen worden, die derjenigen der Europawahlordnung entspricht. Danach kann der Betroffene die Streichung seines Geburtsdatums im auszulegenden Wählerverzeichnis beantragen (§ 21 Abs. 3 BWO). In der öffentlichen Bekanntmachung über die Eintragung in das Wählerverzeichnis sollen die Wahlberechtigten ausdrücklich auf die Möglichkeit, die Streichung ihres Geburtstages zu beantragen, hingewiesen werden. Ferner ist vorgesehen, daß Wahlberechtigte oder Träger von Wahlvorschlägen bei der Fertigung von Abschriften oder Auszügen die Geburtstage nicht mit notieren dürfen. Entsprechendes gilt, wenn die Gemeindebehörde selbst Abschriften oder Auszüge fertigt. Es ist ihr lediglich gestattet, Abschriften über Angehörige bestimmter Altersgruppen (z. B. Jung- oder Erstwähler oder über 60jährige Wahlberechtigte) zu fertigen und sie den Trägern von Wahlvorschlägen gegen Erstattung der Auslagen zugänglich zu machen. Eine Herausgabe von maschinell lesbaren Datenträgern oder von Daten mittels Datenübertragung ist nicht zulässig (§ 21 Abs. 4 BWO).

Damit bleibt allerdings das Problem, daß Wahlberechtigte, die lediglich das Wählerverzeichnis einsehen, auch die Geburtsdaten ihrer Mitbürger zur Kenntnis nehmen können. Dies ist datenschutzrechtlich unerwünscht, aber nicht zu verhindern, solange das Wählerverzeichnis zur Einsicht durch jedermann auszulegen ist. Es muß daher die Frage gestellt werden, ob an der Auslegung des Wählerverzeichnisses in der bisherigen Form festgehalten werden sollte. Die Auslegung soll es dem Wahlberechtigten ermöglichen festzustellen, ob er im Wählerverzeichnis eingetragen ist. Ferner soll er feststellen können, ob andere Personen möglicherweise zu Unrecht in das Register eingetragen sind. Diese Gründe vermögen die Auslegung des Wählerverzeichnisses heute jedoch nicht mehr zu rechtfertigen. Gegenwärtig erhält jeder im Wählerverzeichnis Eingetragene eine schriftliche Wahlbenachrichtigung. Dadurch kann er kontrollieren, ob er im Wählerverzeichnis eingetragen ist. Der Auslegung bedarf es nicht mehr. Die Auslegung zum Zwecke der Prüfung, ob andere Personen zu Unrecht eingetragen oder nicht eingetragen sind, mag ihre Berechtigung gehabt haben, als die Bürger eines Gemeinwesens einander noch kannten. Das ist heute kaum noch der Fall. Tatsächlich wird von dem Einsichtsrecht nur noch vereinzelt Gebrauch gemacht, wobei nicht geprüft werden

kann, ob dies zu den vom Gesetz vorgesehenen Kontrollzwecken oder aus anderen Gründen erfolgt. In Anbetracht dessen wäre es an der Zeit, aus datenschutzrechtlichen Gründen die Abschaffung der Auslegung zu fordern.

Gleichzeitig könnten Regelungen eingeführt werden, die es den an den Wahlen teilnehmenden Trägern von Wahlvorschlägen ermöglichen, gezielt zu werben, ohne daß Grundsätze des Datenschutzes verletzt werden. Die Wählerverzeichnisse werden heute in der Regel automatisiert geführt. Es ist daher ohne übermäßigen Aufwand möglich, Anschriftenaufkleber auszudrucken, die nur einmal verwendet werden können. Die Empfänger könnten verpflichtet werden, die Anschriften auch nur zu diesem einen Zweck der Wahlwerbung zu nutzen und keine Abschriften zu fertigen. Mir ist an einzelnen Beispielsfällen bekannt geworden, daß dieses Verfahren bereits praktiziert wird und funktioniert. Selbstverständlich darf bei solchen Anschriften das Geburtsdatum nicht mit ausgedruckt werden. Vielmehr lassen sich die Anschriften nach Altersgruppen sortiert (z. B. 18- bis 21jährige) ausdrucken. Diese Anschriften könnten sodann auch so zeitig vor den Wahlen ausgegeben werden, daß sie für die gezielte Werbung tatsächlich genutzt werden können. Jedem Wahlberechtigten sollte überdies die Möglichkeit gegeben werden zu verlangen, daß über ihn keine Angaben aus dem Wählerverzeichnis an Dritte übermittelt werden. Durch eine solche Sperre könnte er verhindern, daß er Wahlwerbesendungen erhält.

Eine weitere Anregung in meinem ersten Tätigkeitsbericht (2.3.4) bezog sich auf die zuweilen geübte Praxis der Parteien, durch Beobachter im Wahllokal anhand der Wählerverzeichnisse feststellen zu lassen, wer nicht zur Wahl geht. Meinen Vorschlag, die darin liegende Gefährdung des Wahlgeheimnisses durch eine Regelung im Wahlrecht auszuschließen, habe ich dem Bundesminister des Innern gegenüber später konkretisiert. Dieser hat meine Anregung aufgegriffen und in der Neufassung der Bundeswahlordnung vorgesehen, daß die Mitglieder des Wahlvorstandes nicht befugt sind, Angaben zur Person des Wählers so zu verlautbaren, daß sie von sonstigen im Wahlraum Anwesenden zur Kenntnis genommen werden können, es sei denn, daß die Feststellung der Wahlberechtigung es erfordert (§ 56 Abs. 4 Satz 4 BWO).

Ergänzend zu diesen Vorschlägen regte ich an zu prüfen, ob nicht die Mitglieder der Wahlvorstände und der Wahlausschüsse zur Verschwiegenheit über die ihnen amtlich bekannt gewordenen Angelegenheiten besonders verpflichtet werden sollten. In diesen Gremien könnten sich auch Mitglieder der Träger von Wahlvorschlägen befinden, und es sei nicht auszuschließen, daß sie ihren Gruppierungen aufgrund der ihnen zugänglichen Kenntnisse Angaben zuleiteten, die dem Wahlgeheimnis unterlägen (z. B. wer von den Mitgliedern der Wahl ferngeblieben sei). Der Bundesminister des Innern hat in § 5 Abs. 5 der Bundeswahlordnung eine entsprechende Regelung aufgenommen.

2.1.2 Sammelübersicht über Anträge und Petitionen

Die Sammelübersichten über Anträge und Petitionen, die der Petitionsausschuß dem Plenum des Deutschen Bundestages als Drucksachen vorlegt, enthielten bisher den vollen Namen, den Wohnort des Petenten und Angaben zum Inhalt der Eingabe. Interessierten (z. B. Auskunfteien) wurden dadurch unter Umständen wertvolle Informationen zugänglich. Zwar fallen die Übersichten nicht unter das BDSG; im Rahmen meiner Beratungsaufgabe habe ich aber darauf hingewiesen, daß durch diese Verfahrensweise schutzwürdige Belange der Betroffenen beeinträchtigt werden können. Überdies sei nicht auszuschließen, daß das Vertrauensverhältnis zwischen dem Betroffenen und dem Petitionsausschuß beeinträchtigt werde, wenn der Petent wisse, daß die Tatsache seiner Eingabe und ihr wesentlicher Inhalt praktisch veröffentlicht würde. Dem schloß sich der Petitionsausschuß an.

Die Sammelübersichten über Anträge zu Petitionen enthalten seit Anfang 1979 neben dem Aktenzeichen und dem Inhalt der Eingabe nur noch den Wohnsitz des Einsenders. Der Name wird nicht mehr in die Veröffentlichung aufgenommen. Durch diese Maßnahme wird dem Petenten hinlänglich Sicherheit gewährt und eine ausreichende Anonymisierung erreicht. Die Reidentifizierung durch die Zentralstelle des Petitionsausschusses ist jederzeit über das Aktenzeichen möglich, so daß die Sacharbeit der Abgeordneten nicht beeinträchtigt wird.

2.1.3 Novelle zum Bundespersonalausweisgesetz

Die Bundesregierung hat im August 1979 den Entwurf eines Gesetzes zur Änderung des Gesetzes über Personalausweise vorgelegt. In der ersten Beratung des Entwurfs am 20. September 1979 bestand unter den Vertretern aller Fraktionen Einigkeit darüber, daß ein neuer fälschungssicherer Personalausweis eingeführt werden müsse.

Selbstverständlich sind Maßnahmen der Kontrolle zu Zwecken der Gefahrenabwehr und Strafverfolgung im Rahmen des Polizei- und Strafprozeßrechts zulässig. Die Intensivierung dieser Art von Kontrolle ist, solange das Verhältnismäßigkeitsprinzip gewahrt ist, rechtlich nicht zu beanstanden.

Die Einführung eines maschinenlesbaren Personalausweises hat indes erhebliche Konsequenzen für den Datenschutz der Ausweisinhaber. Die vorgesehene Ausweiskarte ist mehr als ein fälschungssicheres Surrogat des bisherigen Ausweisbuches. Sie kann auch zum Instrument für eine weitaus effektivere Kontrolle über den Bürger werden. In der Öffentlichkeit ist die Frage diskutiert worden, ob mit diesem Ausweis nicht ein Ersatz-Personenkennzeichen geschaffen werde.

Das neue Ausweispapier soll zwar keine als Personenkennzeichen ausdrücklich bezeichnete Ziffernfolge enthalten. Die in der Lesezone des Ausweises einzutragenden Informationen erfüllen jedoch den Zweck, der seinerzeit mit der Einführung eines Personenkennzeichens angestrebt worden ist. Ein solches Kennzeichen muß nicht aus Ziffern bestehen. Die heute verfügbare Speicherkapazität und

Verarbeitungsgeschwindigkeit ermöglicht es, Worte und Zahlen wie ein Personenkennzeichen zu verarbeiten. Es gehört auch nicht zu den Charakteristika eines Personenkennzeichens, daß es unmittelbar aus den Personalien des Inhabers ableitbare Informationen wie etwa das Geburtsdatum enthält. Entscheidend ist vielmehr, daß für eine Vielzahl von Personen eine nach derselben Systematik zusammengesetzte, computergerechte Datenfolge zum eindeutigen Identifizierungsmittel gemacht wird. Dies ist bei dem geplanten Ausweis offenbar der Fall. Die Ausweisnummer wird nur einmal vergeben. Mit ihrer Hilfe können also auch alle die Personen eindeutig identifiziert werden, die denselben Namen tragen und am selben Tage geboren sind. Selbst ohne die Ausweisnummer könnte dies wahrscheinlich bis auf eine ganz geringe Zahl von Fällen erreicht werden. Die seinerzeit vom Rechtsausschuß des Deutschen Bundestages gegen das Personenkennzeichen geltend gemachten Einwendungen bestehen nach wie vor.

Die Gefahr eines solchen Personenkennzeichens besteht bekanntlich darin, daß bei seiner Verwendung in verschiedenen, zu unterschiedlichen Zwekken angelegten Datensammlungen diese maschinell miteinander verknüpft werden können und sich dadurch mit geringem Aufwand Kombinationen von Daten derselben Person vornehmen lassen, die vorher nicht oder nur auf umständlichere Weise möglich waren. Daß die neue Ausweiskarte mit ihrer perfekten Identifizierungsleistung für zahllose Verwendungszwecke „attraktiv" sein wird, liegt auf der Hand. Das neue System wird — anders als die bereits existierenden Kennzeichensysteme für Teilbereiche wie die Rentenversicherung — die gesamte über 16 Jahre alte Bevölkerung erfassen, soweit sie der Meldepflicht unterliegt. Die Daten des Personalausweises entsprechen zwar überwiegend den herkömmlichen Grunddaten des Inhabers, die nicht erst durch die Einführung des Personalausweises existent werden. Die eindeutige Identifizierbarkeit insbesondere innerhalb großer Datenbestände wird jedoch erst durch die Einbeziehung der Ausweisnummer (oder der erwähnten anderen Daten) in die maschinellen Verfahren erreicht.

Ich verkenne nicht, daß die eindeutige Identifizierbarkeit des einzelnen in vielen Zusammenhängen positiv zu bewerten ist. Es kann gerade dem Rechtsschutz des Bürgers dienen, daß durch Verwendung von Identifikationsdaten eine Verwechslung ausgeschlossen wird, z. B. bei der polizeilichen Fahndung. Doch ist es keineswegs für alle denkbaren Verwaltungs- oder wirtschaftlichen Zwecke geboten, daß die eindeutige Identifizierung bereits maschinell erfolgt. Auch im Computerzeitalter ist es den Verwaltungen und Unternehmen zumutbar und in der Regel der Sache eher förderlich, daß bei Zweifelsfällen Zusatzinformationen herangezogen und die Entscheidung, wer gemeint ist, individuell durch den jeweiligen Sachbearbeiter und eben nicht durch die Maschine getroffen wird. Für die datenschutzrechtliche Betrachtung muß entscheidend sein, daß die maschinellen Verknüpfungsmöglichkeiten mit Hilfe der eindeutig identifizierenden Ausweisnummer auch dann extensiv genutzt werden können, wenn sie nicht von vornherein beabsichtigt waren. Ich habe die Sorge, daß Datenbestände aufgebaut werden, in denen die Ausweisnummer enthalten ist, oder daß sie in bestehende Datensammlungen übernommen wird und so neue automatische Datenverbindungen geschaffen werden. Dieser Gefahr kann nur dadurch begegnet werden, daß die Verwendungszwecke des Ausweises und die Erfassung der Ausweisnummer eingeschränkt werden. In diese Richtung zielende Vorschläge, — die teilweise auch vom Hessischen Datenschutzbeauftragten ausgingen, — sind in den Gesetzentwurf aufgenommen worden:

— Im Gesetzentwurf ist nunmehr abschließend festgelegt, welche Daten in den Ausweis aufgenommen werden dürfen. Jeder spätere Zusatz bedarf einer Änderung des Gesetzes.

— Zusätzlich zum Verbot der Aufnahme des Fingerabdrucks ist nunmehr untersagt, andere verschlüsselte Angaben über die Person des Ausweisinhabers aufzunehmen.

— Die Seriennummer darf keine Daten über die Person des Ausweisinhabers oder Hinweise auf solche Daten enthalten.

— Eine zentrale Datei aller Ausweisinhaber wird es nicht geben. Die Bundesdruckerei, die die Ausweise herstellt, muß lediglich feststellen können, an welche Behörde sie bestimmte Seriennummern vergeben hat. Angaben zur Person des Ausweisinhabers dürfen nicht bei der Bundesdruckerei, sondern nur bei den örtlich zuständigen Personalausweisbehörden gespeichert werden. Diese dürfen auch die maschinelle Lesbarkeit des Ausweises nutzen, um auf die entsprechenden Dateien zuzugreifen.

— Auf andere Dateien darf mittels der Maschinenlesbarkeit des Ausweises grundsätzlich nicht zugegriffen werden. Ausgenommen davon sind lediglich Dateien, die für Zwecke der Grenzkontrolle und der Fahndung aus Gründen der Strafverfolgung oder der Gefahrenabwehr durch die hierfür zuständigen Behörden betrieben werden.

— Im nicht-öffentlichen Bereich darf der Ausweis zwar als Ausweis und Legitimationspapier verwendet werden; die maschinelle Lesbarkeit darf aber nicht genutzt werden, um automatisierte Dateien zu erschließen.

Mit diesen Einschränkungen ist sowohl den Belangen des Datenschutzes als auch dem Sicherheitsinteresse Rechnung getragen. Die Datenschutzbeauftragten des Bundes und der Länder haben ergänzend dazu anläßlich einer Konferenz am 8. November 1979 betont, daß mit dieser Regelung keinerlei Vorentscheidung über den zulässigen Umfang von Datenspeicherungen und -übermittlungen im Sicherheitsbereich gefallen sei. Nach wie vor sei die baldige Verabschiedung eines datenschutzfreundlichen Melderechts und die zügige Erarbeitung spezieller Datenschutzvorschriften für die Sicherheitsbehörden zu fordern.

Der Innenausschuß des Deutschen Bundestages hat bei der abschließenden Beratung des Gesetzentwurfs am 29. November 1979 diese Forderungen unterstützt und dem Bundestag folgenden Entschließungsantrag vorgelegt: „Der Deutsche Bundestag ist der Auffassung, daß angesichts der raschen Fortentwicklung der automatischen Datenverarbeitung und deren Einsatz in der öffentlichen Verwaltung über die Verabschiedung des Gesetzes zur Änderung des Gesetzes über Personalausweise hinaus weitere Maßnahmen erforderlich sind, um einen ausreichenden Schutz der Persönlichkeitsrechte der Bürger gegen mißbräuchliche Verwendung ihrer persönlichen Daten zu gewährleisten. Die Bundesregierung wird deshalb ersucht,

1. den Entwurf eines datenschutzgerechten Melderechtsrahmengesetzes einzubringen und
2. die Arbeiten zur Entwicklung bereichsspezifischer Datenschutzregelungen für die Sicherheitsbehörden nachdrücklich fortzusetzen."

In meiner Auffassung, daß die Verwendung der Seriennummer des geplanten, maschinell lesbaren Personalausweises gesetzlich geregelt werden muß, hat mich auch die Eingabe eines betroffenen Bürgers bestärkt, der mich auf eine unnötige Speicherung der Nummer des gegenwärtigen Personalausweises im Bereich der Universitätsbibliotheken hingewiesen hat. Die nicht in meine Zuständigkeit fallende Beschwerde richtete sich dagegen, daß in verschiedenen Hochschulbibliotheken des Landes Nordrhein-Westfalen bei der Beantragung eines Leseausweises für nicht der Hochschule angehörende Personen u. a. auch die Personalausweisnummer festgehalten wird, um in Zweifelsfällen eine sichere Identifizierung des Benutzers zu ermöglichen.

Eine Überprüfung dieser Praxis durch den Minister für Wissenschaft und Forschung des Landes Nordrhein-Westfalen ergab dann auch, daß auf die Speicherung der Personalausweisnummer zur Identifizierung des Bibliotheksbenutzers verzichtet werden kann. Der Minister hat inzwischen eine entsprechende Anordnung an die Hochschulen und sonstigen Einrichtungen seines Geschäftsbereiches erlassen.

2.1.4 Meldewesen

Die Bundesregierung hat auf der Grundlage der Ergebnisse der Sachverständigenanhörung am 20./21. November 1978 und meiner gutachtlichen Stellungnahme vom 15. Oktober 1978 (1. TB, 3.2.2) den Entwurf eines Melderechtsrahmengesetzes beschlossen. Die Summe der im wesentlichen gleich strukturierten kommunalen Melderegister ist die größte Sammlung personenbezogener Daten in der deutschen öffentlichen Verwaltung. Deshalb begrüße ich es sehr, daß sich die Auffassung durchgesetzt hat, daß die im wesentlichen aus den 60iger Jahren stammenden Landesmeldegesetze durch eine moderne, den Erfordernissen der inzwischen fast überall in diesem Verwaltungszweig eingesetzten automatischen Datenverarbeitung angepaßte Gesetzgebung abzulösen ist, die auch dem Datenschutz im notwendigen Umfang bereichsspezifisch Geltung verschafft. Ich habe diese Forderung in meiner gutachtlichen Stellungnahme nachdrücklich erhoben und Vorschläge für einen Gesetzentwurf unterbreitet.

Meine Vorschläge sind in den nunmehr vorliegenden Gesetzentwurf im wesentlichen übernommen worden. Die Abweichungen lassen sich zum Teil aus der von mir ausdrücklich vorbehaltenen Beschränkung der Regelungsbefugnis des Bundes auf Rahmenvorschriften erklären. Sie beruhen zum anderen Teil auf der Erwägung, daß Datenverarbeitung weithin als Teilbereich der Verwaltungsorganisation anzusehen ist, in der die Länder Handlungsfreiheit haben und in die der Bund grundsätzlich nicht eingreifen kann. Der Gesetzentwurf ist aus diesen Gründen in enger Zusammenarbeit mit den zuständigen Stellen der Länder entstanden. Ich habe mich an diesen Verhandlungen beteiligt und dabei für meine Vorschläge weitgehend Verständnis gefunden. Darüber hinaus habe ich im Rahmen meiner Beratungsaufgabe den Bundesminister des Innern bei der Ausgestaltung der den Datenschutz betreffenden Vorschriften des Entwurfs unterstützt.

Im einzelnen wurden folgende meiner wichtigsten Forderungen im Entwurf realisiert:

— Die Aufgaben der Meldebehörden werden auf die Feststellung und den Nachweis der Identität und der Wohnungen der Einwohner beschränkt. Die Übertragung weiterer Aufgaben bedarf einer Rechtsvorschrift.

— Der Datenkatalog der Anlage zu früheren Entwürfen wurde wesentlich reduziert und transparenter gestaltet. Der maximale Umfang der Datenspeicherung ist jetzt gesetzlich festgelegt.

— Die Verwendung der über die Grunddaten der Einwohner hinausgehenden Angaben, die von den Meldebehörden gespeichert werden, ist streng zweckgebunden. Die Verwendungszwekke sind gesetzlich festgelegt.

— Die Verpflichtung, schutzwürdige Belange des Betroffenen bei der Auswertung und Verarbeitung seiner Daten zu beachten, ist als bereichsspezifische Konkretisierung des Verhältnismäßigkeitsprinzip ausformuliert.

— Die Rechte des Betroffenen auf gebührenfreie Auskunft, auf Berichtigung und Löschung seiner Daten, auf Unterrichtung über erteilte Auskünfte an Dritte sowie auf Übermittlungs- und Auskunftssperren sind im Gesetzentwurf verankert.

— Die vorgesehenen Regelungen über Datenübermittlungen an andere Behörden, an öffentlich-rechtliche Religionsgesellschaften sowie über die Auskünfte an Private weichen zum Teil von meinen ursprünglichen Vorschlägen ab, genügen aber insgesamt in ihrem Datenschutzgehalt meinen Forderungen.

Auf meine Veranlassung hin ist im Gesetzentwurf klargestellt worden, daß Angaben, die von Hotelgästen, Krankenhauspatienten, Heimbewohnern usw. gegenüber den Inhabern und Leitern dieser Einrichtungen gemacht werden und die für die

zuständigen Behörden bereitzuhalten oder an sie zu übermitteln sind, nur für Zwecke der Gefahrenabwehr oder der Strafverfolgung ausgewertet und verarbeitet werden dürfen. Diese Zweckbindung mag schon der bisherigen Praxis entsprechen. Um denkbare Mißbräuche auszuschließen und den Betroffenen Klarheit über die Verwendung ihrer bei solchen Gelegenheiten angegebenen Daten zu verschaffen, habe ich eine entsprechende Aussage im Gesetzentwurf für notwendig gehalten; ich begrüße es, daß dem Anliegen entsprochen wurde.

Als wichtigen Fortschritt erkenne ich an, daß in der Vorschrift über die Erteilung erweiterter (also über Namen und Anschriften hinausgehender) Auskünfte vorgesehen ist, daß der Empfänger die Daten nur für den Zweck verwenden darf, zu dessen Erfüllung sie ihm übermittelt wurden. Die Beschränkung solcher Auskünfte auf Fälle, in denen ein rechtliches Interesse im Sinne der Verfolgung von Rechtsansprüchen glaubhaft gemacht wird, in Verbindung mit der Verpflichtung der Meldebehörde, den Betroffenen über die Auskunftserteilung zu unterrichten, sichert die schutzwürdigen Belange der Betroffenen ausreichend ab, auch wenn den Betroffenen für diese wenigen ausdrücklich genannten Daten — abweichend von meinem Vorschlag — kein Recht auf Sperrung der Auskunft eingeräumt wird. Andererseits berücksichtigt die Vorschrift in m. E. hinreichendem Maße die Interessen von Auskunftssuchenden, die ohne die Daten zu einer Rechtsverfolgung nicht in der Lage wären.

Zwei Problempunkte spielten in den Erörterungen, die ich mit dem Bundesminister des Innern geführt habe, eine herausragende Rolle. Sie betreffen die Datenübermittlungen an andere Behörden. Hier ging mein Vorschlag dahin, Namen, akademische Grade, Anschriften, Geburtstag und Geburtsort der Einwohner für andere Bedarfsträger aus dem öffentlichen Bereich frei verfügbar zu halten. Ich habe diesen Vorschlag in meiner gutachtlichen Stellungnahme eingehend begründet, u. a. auch damit, daß die freie Übermittlung der Daten sich im Rahmen der allgemeinen Aufgabenstellung des Meldewesens hält, Behörden insoweit nicht schlechter gestellt sein sollten als Private und sich keinerlei Zusatzinformationen aus dem Kontext ergeben. Schließlich ließe sich so der wesentliche Bedarf anderer Behörden an personenbezogenen Daten der Einwohner auf einfache Weise befriedigen, während sonst auch bei der Übermittlung dieser „harmlosen" Daten schwierige Erforderlichkeitsprüfungen vorzunehmen wären. Der Kabinettsentwurf ist diesem Vorschlag nicht gefolgt, sondern hat diesem „harmlosen" Datenkatalog noch Staatsangehörigkeit und Familienstand hinzugefügt. Angesichts dieser Erweiterung habe ich mich nicht in der Lage gesehen, der völligen Freigabe dieser Daten — wenn auch nur im öffentlichen Bereich — zuzustimmen. Der schließlich gefundene Kompromiß, daß die Daten zur rechtmäßigen Erfüllung der in der Zuständigkeit der Meldebehörde oder der Zuständigkeit des Empfängers liegenden Aufgaben erforderlich sein müssen, übernimmt die Generalklausel des § 10 Abs. 1 Satz 1 BDSG und entfernt sich damit von der wünschenswerten und im bereichsspezifischen Recht m. E. auch erreichbaren Konkretisierung des Datenschutzes. Wenn man von diesem Mangel aber absieht, erscheint die Vorschrift in ihrer einschränkenden Fassung akzeptabel.

Das andere sehr schwierige Problem bestand darin, die Belange der Sicherheitsbehörden bei ihren Datenanforderungen gegenüber den Meldebehörden in einer Weise zu berücksichtigen, die den Betroffenen nicht übermäßig belastet. Eine solche Belastung hätte es aber bedeutet, wenn die Sicherheitsbehörden im Interesse ihrer Ermittlungstätigkeit von der Pflicht, ihren Datenbedarf gegenüber der Meldebehörde im Einzelfall zu begründen, völlig ausgenommen würden, ohne daß gleichzeitig als Äquivalent andere Schutzvorkehrungen zugunsten des Betroffenen vorgeschrieben würden. Die im Entwurf gefundene Lösung, daß die Sicherheitsbehörde, die Daten von der Meldebehörde begehrt, darüber selbst eine Niederschrift erstellt, in der die betroffenen Personen und der Grund der Datenübermittlung festzuhalten sind, erscheint unter den gegebenen Umständen und bei Abwägung der beiderseitigen Interessen vertretbar. Die besonders zu sichernde Niederschrift ist spätestens nach Ablauf von zwei Jahren zu vernichten. In diesem Zeitraum haben die Datenschutzbeauftragten Gelegenheit, die Rechtmäßigkeit der Datenübermittlung zu kontrollieren und damit den Datenschutz durchzusetzen, den weder die Meldebehörde noch der Betroffene (dieser mangels eines Auskunftsrechts) sicherstellen kann.

Im ganzen halte ich den Entwurf in der vorgelegten Fassung für eine aus datenschutzrechtlicher Sicht geglückte Konzeption, der eine baldige Realisierung zu wünschen wäre. Wie in der noch immer neuen Materie des Datenschutzrechts überhaupt, wird man in seiner bereichsspezifischen Ausformung zu manchen neuen Vorschriften erst Erfahrungen sammeln müssen, um zu endgültigen und praktikablen Lösungen zu gelangen.

2.1.5 Bundesarchiv

Das Bundesarchiv in Koblenz gehört zu den Stellen des Bundes mit besonders umfangreichen Sammlungen personenbezogener Angaben. Der gesamte Bestand, der zum großen Teil noch aus der Zeit vor der Gründung der Bundesrepublik stammt, hat einen Umfang von etwa 70 000 laufenden Regal-Metern. Er enthält eine Fülle von personenbezogenen Angaben, darunter viele von hoher Empfindlichkeit.

Der Datenschutz im öffentlichen Bereich beruht wesentlich darauf, daß das Wissen über den einzelnen Bürger auf eine Vielzahl öffentlicher Stellen verteilt ist. Sobald Akten- und Datenbestände von den zuständigen Behörden nicht mehr benötigt werden, werden diese jedoch — wenn auch nur in einer (an der Archivwürdigkeit orientierten) Auswahl — bei einigen wenigen Archiven zusammengefaßt.

Die Aufgaben der Archive erschöpfen sich nicht darin, die Bestände sicher zu verwahren. In erster Linie sollen sie vielmehr die archivierten Materialien der Allgemeinheit für wissenschaftliche und publizistische Zwecke zugänglich machen. Datenschutzrechtlich stellt sich damit der Konflikt zwischen den Interessen der Betroffenen, die ihre von der Verwaltung gespeicherten Angaben vertraulich behandelt wissen wollen, und dem Interesse der Öffentlichkeit an der Transparenz zeitgeschichtlicher Bestände im Bereich von Regierung und Verwaltung, die Voraussetzung für wissenschaftliche Aufklärung und realitätsbezogene politische Auseinandersetzung ist. Durch die Freigabe von Unterlagen werden außerdem die Interessen der aktenführenden Behörden tangiert. Bei der Verwirklichung des Datenschutzes im Bundesarchiv ist weiterhin zu berücksichtigen, daß dieses auch einzelfallbezogene administrative Aufgaben wahrnimmt, indem es für Zwecke der Rentenfestsetzung Nachweise über Beschäftigungs- und Ausfallzeiten erstellt.

Ich bin deshalb dem Wunsch des Bundesarchivs, mit mir über die archivspezifischen Datenschutzfragen zu beraten, gern nachgekommen. Bei den Gesprächen haben sich sehr schnell einige neuralgische Punkte gezeigt.

Die Aufgaben des Bundesarchivs sind gesetzlich nicht geregelt. Seine Errichtung beruht auf einem Beschluß der Bundesregierung. Die Übergabe von Unterlagen der Behörden an das Bundesarchiv und die Benutzung von Archivalien im Bundesarchiv durch Außenstehende sind durch Verwaltungsvorschriften geregelt (§ 80 Gemeinsame Geschäftsordnung der Bundesministerien, Allgemeiner Teil — GGO I). Bereichsspezifische Vorschriften, die nach § 45 BDSG vorgehen, sind danach nicht vorhanden, die Vorschriften des BDSG mithin grundsätzlich anwendbar. Nur bei einem relativ geringen Teil der Archivalien handelt es sich allerdings um Dateien i. S. des § 2 Abs. 3 Nr. 3 BDSG. Die Verwaltungsvorschriften über die Abgabe von Beständen an das Bundesarchiv sowie die Benutzungsordnung unterscheiden nicht danach, ob eine Datei vorliegt; sie müßten sich deshalb insgesamt den Anforderungen des BDSG anpassen. Ob dies freilich geschehen kann, ohne daß archiv-fachliche Gesichtspunkte zu kurz kommen, erscheint zweifelhaft.

Nach dem Bundesdatenschutzgesetz hat eine Behörde Daten, die sie für die Erfüllung ihrer Aufgaben nicht mehr benötigt, zu sperren und auf Wunsch des Betroffenen zu löschen (§ 14). Das BDSG bekennt sich also zu einer an der jeweiligen Verwaltungsaufgabe orientierten zeitlich begrenzten Speicherung. Anders die erwähnten Verwaltungsvorschriften: Nach ihnen sollen die Datenbestände, wenn auch nur teilweise, an das Bundesarchiv übermittelt, von diesem auf unbegrenzte Zeit gespeichert und für die Benutzung durch Behörden sowie durch Außenstehende bereitgehalten werden. Auch wenn dies nur unter näher bestimmten Bedingungen erfolgt, wobei auch die schutzwürdigen Belange Betroffener eine Rolle spielen, ist der Widerspruch zum Regelungsgrundsatz des BDSG unübersehbar.

Ich habe dem Bundesminister des Innern, der sich seit einiger Zeit mit der Vorbereitung eines Bundesarchivgesetzes befaßt, mitgeteilt, daß ich aus der Sicht des Datenschutzes besondere Regelungen dringend für erforderlich halte, und habe meine Beratung dabei angeboten.

2.2 Rechtswesen/Justizverwaltung

Die hier vorgefundenen tatsächlichen Verhältnisse entsprechen weitgehend denen in der allgemeinen inneren Verwaltung; nur vereinzelt wird die automatisierte Datenverarbeitung als Arbeitsmittel eingesetzt. Das Bundeszentralregistergesetz ist eine vorbildliche Regelung bereichsspezifischen Datenschutzes, wenngleich auch dort noch Verbesserungen möglich sind. Das Gesetz bezieht sich aber nur auf die im Zentralregister gespeicherten Informationen. Wenn es vorschreibt, daß Eintragungen z. B. über Verurteilungen nach bestimmten Fristen zu löschen sind und der Betroffene sich danach als unbestraft bezeichnen kann, so bedeutet dies keineswegs, daß damit die Tatsache seiner Verurteilung auch anderswo in Vergessenheit geriete. Nach wie vor bleiben solche Angaben und Unterlagen in Akten erhalten, ohne einer Löschungspflicht zu unterliegen. Nach wie vor bestehen zwischen der Justizverwaltung und anderen Verwaltungsbereichen weitreichende Informationspflichten (z. B. nach der Anordnung über Mitteilungen in Strafsachen, s. u. 2.2.2), für die es keinerlei Löschungsregelungen gibt. Erste Anstöße mit dem Ziel einer Überprüfung dieser Verfahren haben mir gezeigt, daß hier noch weitgehend die Meinung vorherrscht, grundsätzlich seien alle Informationen notwendig, um sodann entscheiden zu können, welche tatsächlich gebraucht werden. Aus datenschutzrechtlicher Sicht ist jedoch umgekehrt zu fordern, daß regelmäßig nur ein Minimum an unbedingt erforderlichen Daten verfügbar gemacht wird und lediglich in Ausnahmefällen weitere Daten erhoben und verarbeitet werden dürfen. Bis diese Denkweise sich in der Verwaltungspraxis durchsetzt, wird indes noch geraume Zeit vergehen.

2.2.1 Datenschutz im Bundeszentralregister

Das Bundeszentralregistergesetz (BZRG) ist ein Musterbeispiel eines gelungenen bereichsspezifischen Datenschutzgesetzes. Es regelt im einzelnen, welche Daten in das Register aufgenommen und wie sie verarbeitet werden dürfen. Damit ist jedoch nicht gesagt, daß das Gesetz und sein Vollzug keinerlei Wünsche offen ließen. Dafür einige Beispiele:

Mehrfach haben sich Bürger bei mir beschwert, daß im Bundeszentralregister Strafen noch eingetragen waren, die nach den gesetzlich vorgesehenen Tilgungsfristen längst hätten gelöscht sein müssen. Meine Nachforschungen haben ergeben,

daß diesen Fällen in der Regel folgender Sachverhalt zugrunde lag: Der Betroffene war verurteilt worden, die Strafe aber zur Bewährung ausgesetzt. Nach Ablauf der Bewährungsfrist hat das Gericht die Strafe zwar erlassen, das Bundeszentralregister über die Vollstreckungserledigung aber nicht unterrichtet. Dies bewirkte beim Bundeszentralregister eine Ablaufhemmung hinsichtlich der Tilgungsfrist (§ 35 Abs. 2 BZRG) mit der Folge, daß die Verurteilung über die Fristen hinaus eingetragen blieb. Das Bundeszentralregister ist jetzt dazu übergegangen, automatisch zu berechnen, von wann ab mit einer nachträglichen Mitteilung über die Erledigung der Strafvollstreckung gerechnet werden kann. Nach Ablauf dieser Frist werden die entscheidenden Justizbehörden erinnert. Vielfach wurde nicht geantwortet oder es wurde mitgeteilt, die Akten seien nicht mehr auffindbar. In diesen letzteren Fällen hat das Bundeszentralregister unterstellt, daß die Strafe erlassen wurde, und die sofortige Entfernung der Entscheidung aus der Datenbank veranlaßt.

In einem anderen Einzelfall erbat ein Betroffener meine Hilfe, weil er befürchtete, in Dateien von Bundesbehörden als geisteskrank geführt zu werden. Er legte ärztliche Zeugnisse vor, aus denen sich zweifelsfrei ergab, daß er voll prozeß- und geschäftsfähig war. Ich habe dazu beigetragen, daß ihm dies von den betreffenden Behörden ausdrücklich bestätigt wurde. Besondere Erwähnung verdient in diesem Zusammenhang die Eintragung im Strafregister. Dort befinden sich zwei Eintragungen über Verfahren, die wegen Schuldunfähigkeit eingestellt worden waren. Auf mein Anraten hin hat der Betroffene nach § 23 Abs. 1 BZRG die Entfernung der Eintragung beantragt.

Dieser Einzelfall gibt jedoch Anlaß zu Überlegungen, wie Betroffenen, deren Schuldunfähigkeit nachträglich entfallen ist, geholfen werden kann. Geholfen werden muß hier, denn die Eintragungen unterliegen nicht den Tilgungsfristen. Sie werden erst entfernt, wenn der Betroffene 90 Jahre alt geworden ist. Zwar werden sie nicht in ein Führungszeugnis, wohl aber in eine unbeschränkte Auskunft (Behördenauskunft) aufgenommen. Der Betroffene erfährt von der Eintragung oft nichts, weil davon im Einstellungsbescheid nichts steht. Er bleibt damit praktisch bis an sein Lebensende als geisteskrank abgestempelt und registriert. Dem könnte dadurch begegnet werden, daß im Einstellungsbescheid auf die Eintragung und auf die Möglichkeit der nachträglichen Entfernung hingewiesen wird.

2.2.2 Anordnung über Mitteilungen in Strafsachen

Die Anordnung über Mitteilungen in Strafsachen (MiStra) ist eine interne Verwaltungsvorschrift, die vom Bundesminister der Justiz im Einvernehmen mit den Landesministern der Justiz erlassen worden ist. Sie regelt im einzelnen, unter welchen Voraussetzungen und in welchem Umfang Justizbehörden andere öffentliche Stellen über den Stand und die Ergebnisse von Strafsachen zu unterrichten haben. Zwar ist das BDSG auf Datenübermittlungen dieser Art vielfach nicht unmittelbar anwendbar, da es sich in der Regel um Mitteilungen aus Akten handelt, die vom BDSG nicht erfaßt sind. Es soll auch nicht verschwiegen werden, daß die MiStra selbst eine Datenschutzklausel enthält: Danach ist von einer Mitteilung abzusehen, wenn Anhaltspunkte dafür vorliegen, daß durch die Mitteilungen Interessen Betroffener oder Dritter beeinträchtigt werden können. Ungeachtet dessen handelt es sich aber bei den Mitteilungen um datenschutzrelevante Vorgänge. Daher sollte auch für sie der im BDSG zum Ausdruck gelangte allgemeine Rechtsgrundsatz gelten, daß personenbezogene Daten nur in dem Umfang übermittelt werden sollten, wie sie zur Aufgabenerfüllung unbedingt erforderlich sind. Bei einigen Übermittlungsanordnungen der MiStra ist zu bezweifeln, ob sie diesen Anforderungen voll entsprechen:

— So ist z. B. in Nummer 5 a. a. O. vorgesehen, daß bestimmte Mitteilungen, die dem Bundeszentralregister gemacht werden müssen (z. B. Verurteilungen, Aussetzungen der Strafe zur Bewährung, Sperre für Fahrerlaubnis, Schuldunfähigkeit nach § 12 Bundeszentralregistergesetz), auch der örtlich zuständigen Polizeibehörde übermittelt werden. Praktisch kann dies dazu führen, daß neben den Eintragungen im Bundeszentralregister auch am Wohnsitz des Betroffenen ein polizeiliches Dossier entsteht. Es ist aber zu fragen, ob die Polizei des Wohnsitzes (Nummer 12 MiStra) wirklich in allen Fällen wissen muß, daß ein Bürger z. B. an seinem Urlaubsort in eine Schlägerei verwickelt war und deswegen ein Strafverfahren durchgeführt worden ist. Dies ist m. E. erst dann von Bedeutung, wenn sie selbst gegen den Betroffenen ermittelt. Dann aber kann sie die erforderlichen Informationen sehr rasch vom Bundeszentralregister abrufen. Ich habe daher angeregt, die Übermittlungspflichten mit dem Ziel der Einschränkung zu überprüfen.

— Nach Nummer 12 a MiStra ist der zuständigen Verwaltungsbehörde (Wahlamt) die Urteilsformel mitzuteilen, wenn sich aus dem Urteil Konsequenzen für die Wahlberechtigung des Betroffenen ergeben. Die Verwaltungsbehörde benötigt jedoch nicht die gesamte Urteilsformel, sondern lediglich die Information, daß dem Betroffenen z. B. durch Richterspruch für eine bestimmte Zeit das Recht aberkannt worden ist, in öffentlichen Angelegenheiten zu wählen. Die Behörde braucht nicht zu wissen, wegen welcher Tat die Verurteilung erfolgte.

— In Strafsachen gegen Studierende und Inhaber akademischer Grade sind die Entscheidungen der jeweiligen Ausbildungsstätte mitzuteilen. Hier wäre m. E. zu überprüfen, ob die Mitteilungen in diesem Umfange erforderlich sind. Das Disziplinarrecht der Universitäten bietet nur in wenigen Fällen eine rechtliche Handhabe, gegen einen Studierenden, der straffällig geworden ist, Sanktionen zu verhängen. Auch die Mitteilungspflichten sollten dementsprechend eingeschränkt werden. Ich bezweifle auch, ob es erforderlich ist, für Studierende und Hörer

(Gasthörer) dieselben Mitteilungspflichten vorzusehen.

Dies sind nur einige Beispiele aus den Anregungen, die ich dem Bundesminister der Justiz zugeleitet habe. Die damit ausgelöste Diskussion wird sicher nicht kurzfristig zu Ergebnissen führen können, da außer den Justizverwaltungen zahlreiche Fachverwaltungen im Bund und in den Ländern als Empfänger von Mitteilungen beteiligt sind.

Der Bundesminister der Justiz hat in einer ersten Stellungnahme erklärt, dem Grundanliegen des Schutzes des Bürgers vor nicht erforderlichen Mitteilungen werde sowohl durch die Strafvorschrift des § 203 StBG als auch durch die Datenschutzbestimmungen Rechnung getragen. Dieser Schutz lasse sich allerdings noch verbessern. So könne erwogen werden, die MiStra dahin gehend zu ändern, daß künftig nicht mehr die gesamten Urteile (einschließlich der Urteilsgründe), sondern nur die Urteilsformel mitgeteilt werde, die Urteilsgründe hingegen nur im Einzelfall auf Grund einer Entscheidung des Staatsanwalts.

Dieser grundsätzlich positiven Äußerung des Bundesministers der Justiz stehen andere gegenüber, in denen die eingangs apostrophierte Haltung, der Staat müsse zunächst einmal alles wissen, um sodann entscheiden zu können, was er tatsächlich benötige, zum Ausdruck kommt.

So wurde mir entgegengehalten, die durch das Strafrecht und das Strafverfahrensrecht garantierte dauerhafte Friedensordnung könne nur bestehen, wenn „das Strafrecht und die an die Begehung von Straftaten geknüpften Rechtsfolgen in anderen Bereichen der öffentlichen Verwaltung in einem effektiven Verfahren durchgesetzt werden". Diese Zielsetzung werde gefährdet, wenn die Rechte des Betroffenen über das in der MiStra geregelte Maß hinaus bereits im Zeitpunkt des Strafverfahrens so stark in den Vordergrund gerückt würden, daß das notwendige Zusammenwirken der verschiedenen Träger öffentlicher Aufgaben Schaden leide. Das Ansehen des Staates bei der Bevölkerung werde dadurch beeinträchtigt.

Dazu bemerke ich: Inwieweit das Zusammenwirken der verschiedenen Träger staatlicher Aufgaben notwendig ist, hat der Gesetzgeber zu entscheiden. Das Strafrecht darf keineswegs ohne weiteres „in anderen Bereichen der öffentlichen Verwaltung durchgesetzt werden"; eine solche „Verlängerung" seiner Wirkung bedarf vielmehr jeweils besonderer Begründung (wie sie z. B. in den Vorschriften über die Nebenfolgen der Straftaten, §§ 45 ff. StGB, enthalten ist). Daß die Auswertung strafgerichtlicher Verurteilungen durch Verwaltungsbehörden nicht selbstverständlich ist, zeigt auch § 50 Bundeszentralregistergesetz. Wie weit etwa die Befugnis der Polizeibehörden geht, aus Strafverfahren Schlüsse für ihre Aufgabe der Gefahrenabwehr zu ziehen, ist noch nicht abschließend diskutiert. Ich will der öffentlichen Verwaltung keine Information vorenthalten, die sie benötigt, wohl aber diejenigen Informationen, die sie zur Erfüllung ihrer Aufgaben nicht unbedingt braucht. Daß sie nach den Bestimmungen der MiStra noch vielfältige verzichtbare Informationen erhält, ergibt sich aus den Überlegungen des Bundesministers der Justiz. Wenn im Regelfall auf die Mitteilung der Urteilsgründe verzichtet werden kann, dann haben die Fachverwaltungen bisher eine Fülle von personenbezogenen Daten über den jeweils Betroffenen erhalten, die für die Bearbeiter zwar interessant, aber keineswegs in jedem Fall für eine Entscheidungsbildung unerläßlich waren.

Soweit aus den Fachressorts des Bundes bereits Einwendungen geltend gemacht worden sind, werden sie sorgfältig gegen die Belange des Datenschutzes abzuwägen sein. Der Schwerpunkt der weiteren Diskussion wird in den Bundesländern liegen müssen. Dabei werden die Landesbeauftragten für den Datenschutz sowie die Datenschutzkommission in Rheinland-Pfalz ein gewichtiges Wort mitzureden haben.

2.2.3 Richtlinien für das Strafverfahren und das Bußgeldverfahren

Die Richtlinien für das Strafverfahren und das Bußgeldverfahren vom 1. Januar 1977 sind ergänzende Verfahrensregelungen, die sich in erster Linie an den Staatsanwalt wenden. Sie enthalten darüber hinaus Grundsätze, die auch für den Richter bedeutsam sein können. Ich habe sie auf ihre Vereinbarkeit mit den Grundsätzen des Datenschutzes überprüft und dem Bundesminister der Justiz einige Vorschläge unterbreitet:

In Nummer 236 der Richtlinien ist bestimmt, daß einigen namentlich genannten Stellen, die sich die Bekämpfung der Wirtschaftskriminalität zur Aufgabe gemacht haben, Abschriften von Strafurteilen oder Aktenauskünfte gegeben werden können, soweit nicht schutzwürdige Interessen dritter Personen oder sonstige Bedenken entgegenstehen.

Ich habe gegen die Übersendung vollständiger Urteilsabschriften aus datenschutzrechtlicher Sicht erhebliche Bedenken. Diese Praxis widerspricht meines Erachtens sowohl dem Resozialisierungsgedanken des Strafgesetzbuches als auch der Zielsetzung des Bundeszentralregistergesetzes. Durch die Übermittlung des gesamten Urteils werden schutzwürdige Belange des Betroffenen beeinträchtigt; denn die Urteile enthalten Angaben über den Betroffenen, die zwar für das Verständnis der Entscheidung, keineswegs aber für die empfangenden Einrichtungen erforderlich sind. Die Resozialisierung des Verurteilten hängt weitgehend davon ab, daß er sich nach Ablauf der im Bundeszentralregistergesetz vorgesehenen Fristen als unbestraft bezeichnen kann. Dieser Erfolg wird aber nahezu unmöglich gemacht, wenn die Verurteilung unter Angabe von Einzelheiten nicht nur publiziert, sondern auch so aufbereitet wird, daß sie in Dateiform gespeichert werden kann. Die empfangenden Einrichtungen können ihre Funktion zur Abwehr der Wirtschaftskriminalität auch dadurch erfüllen, daß sie lediglich auf die Arbeitsweise von Straftätern hinweisen. Dazu bedarf es aber nicht der Übermittlung personenbezogener Daten. Ich habe deswegen angeregt, die Urteilsabschriften nur noch in ausreichend anonymisierter Form zu übermitteln.

2.2.4 Datenschutz bei der Übermittlung von Angaben aus dem Schuldnerverzeichnis nach § 915 ZPO

Die nach den „Allgemeinen Vorschriften über die Erteilung und die Entnahme von Abschriften oder Auszügen aus den Schuldnerverzeichnissen" vom 1. August 1955 geübte Praxis der organisationsinternen Veröffentlichung von Listen aus dem Schuldnerverzeichnis entspricht in mancherlei Hinsicht nicht den Grundsätzen des Datenschutzes, wie sie im Bundesdatenschutzgesetz und den Landesdatenschutzgesetzen ihren Niederschlag gefunden haben.

Nach den allgemeinen Vorschriften erhalten Rechtsanwaltskammern, Industrie- und Handelskammern und gleichartige Berufsvertretungen sowie andere vertrauenswürdige Körperschaften, Personen und Unternehmen (z. B. Auskunfteien) vollständige Abschriften aus den Schuldnerverzeichnissen. Sie sind verpflichtet, die Angaben nach Ablauf bestimmter Fristen zu löschen bzw. die Listen zu vernichten. Die in § 1 Abs. 1 der Allgemeinen Vorschriften genannten Berufsvertretungen können die Listen ihren Mitgliedern zugänglich machen. Auch diese haben sich der Berufsvertretung gegenüber zu verpflichten, die Daten fristgerecht zu löschen bzw. die Listen zu vernichten. Nach § 6 können die Listen auch außenstehenden Dritten verfügbar gemacht werden, sofern sie sich der Berufsvertretung gegenüber verpflichten, den Löschungsdienst durchzuführen.

Der Kreis derjenigen, die auf diese Weise vollständige Listen der Schuldnerverzeichnisse empfangen, wird dadurch sehr groß. Dabei ist keineswegs gewährleistet, daß die vorgesehenen Auflagen auch erfüllt werden. Die angeschlossenen Unternehmen und Personen haben oftmals ein Interesse daran, die Informationen auch über die Fristen hinaus zu besitzen. Es kann daher nicht ausgeschlossen werden, daß die Löschungsauflagen von einem großen Teil der Empfänger nicht erfüllt werden. Eine Kontrolle findet praktisch nicht statt. Sie wäre nach dem BDSG auch bei der großen Anzahl der unter den dritten Abschnitt fallenden Unternehmen nicht möglich, da diese nur der Anlaßaufsicht unterliegen.

Ich habe daher dem Bundesminister der Justiz einen von den Datenschutzbeauftragten der Länder und mir gemeinsam erarbeiteten Änderungsvorschlag unterbreitet, der sicherstellen soll, daß sowohl das Befürfnis der Wirtschaft, sich rasch über die Bonität eines Vertragspartners zu informieren, als auch der Datenschutz in einem ausgewogenen Verhältnis zueinander stehen. Er sieht vor, daß die Übermittlung von Abschriften aus dem Schuldnerverzeichnis auf diejenigen Stellen beschränkt wird, die ihrerseits einer vollständigen Datenschutzkontrolle unterliegen. Dies sind die öffentlich-rechtlich organisierten Berufsvertretungen (Rechtsanwaltskammern, Industrie- und Handelskammern, Landwirtschaftskammern u. a.) und die unter den vierten Abschnitt des BDSG fallenden Stellen, namentlich also Auskunfteien. Diese Stellen — wie auch das Amtsgericht selbst — sollen die Listen nicht an andere Dritte weitergeben dürfen, sondern nur Einzelauskünfte erteilen. Ich gehe dabei davon aus, daß die Daten zu diesem Zwecke in Dateien gespeichert sind. Sollte dies nicht der Fall sein, müßte auf andere Weise sichergestellt werden, daß der Landesbeauftragte für den Datenschutz bzw. die Aufsichtsbehörden (§ 40 BDSG) von Amts wegen prüfen können, ob die Löschungsvorschriften beachtet werden. Das Ziel, die Weitergabe der Listen einzuschränken, wäre verhältnismäßig einfach zu erreichen; es bedürfte lediglich einer Änderung der Allgemeinen Vorschriften. § 915 ZPO brauchte nicht geändert zu werden.

Der Bundesminister der Justiz hat sich zu meinen Anregungen grundsätzlich positiv geäußert und sich bereit erklärt, die Probleme mit den beteiligten Ressorts in Bund und Ländern gründlich zu erörtern. Es scheint notwendig, auch die Bundesrechtsanwaltskammer, den Deutschen Industrie- und Handelstag, den Deutschen Anwaltverein und andere Organisationen zu beteiligen.

2.2.5 Datenschutz im Grundbuchwesen

Das Grundbuchrecht enthält sehr präzise Vorschriften über Art und Inhalt von Eintragungen in das Grundbuch und über die Zulässigkeit von Übermittlungen aus dem Grundbuch. Insoweit kann die Grundbuchordnung als ein bereichsspezifisches Datenschutzgesetz angesehen werden. Dies schließt jedoch nicht aus, daß auch hier die Datenschutzdiskussion Anstöße gibt, bisherige Verfahren zu überdenken und den Inhalt von Rechtsbegriffen zu überprüfen.

Ein Beispiel: Ein Bürger hat mich darauf hingewiesen, er habe als Miteigentümer eines Grundstückes einen Grundbuchauszug erhalten, in dem die Daten (u. a. Name, Beruf, Geburtsdatum, Eigentumsanteil) aller übrigen Miteigentümer aufgeführt gewesen seien. Diese Daten seien zwar für ihn sehr interessant, er frage sich aber, wie sich dieses Verfahren mit dem Datenschutz vertrage. Auf meine Anfrage hat mir der Bundesminister der Justiz mitgeteilt: Nach § 12 Abs. 2 i. V. m. § 12 Abs. 1 der Grundbuchordnung sei jedem, der ein berechtigtes Interesse darlege, Einsicht in das Grundbuch zu gestatten oder ihm eine Abschrift zuzuleiten. Das berechtigte Interesse sei aber nicht nur das Kriterium dafür, wer eine Abschrift aus dem Grundbuch verlangen könne, sondern auch dafür, in welchem Umfang sie zu erteilen sei. Diese letztere Entscheidung lasse sich jedoch nicht generell, sondern immer nur unter Berücksichtigung der konkreten Umstände des Einzelfalles treffen.

Nach § 55 Satz 1 Grundbuchordnung soll jede Eintragung dem Antragsteller oder dem eingetragenen Eigentümer sowie allen aus dem Grundbuch ersichtlichen Personen, zu deren Gunsten die Eintragung erfolgt sei oder deren Rechte betroffen seien, bekanntgegeben werden. Die Benachrichtigung habe die Eintragung wörtlich wiederzugeben (§ 42 Abs. 1 der Allgemeinen Verfügung über die Einrichtung und Führung des Grundbuches). Sie erfolge durch Übersendung einer Abschrift der Eintragung. Unter Eintragung sei dabei nicht etwa der gesamte Inhalt eines oder mehrerer Grundbuchblätter zu verstehen, son-

dern vielmehr der konkrete Inhalt einer bestimmten Eintragung.

Die Vorschriften der Grundbuchordnung über Art und Umfang der Eintragung und die Übermittlung von Daten aus dem Grundbuch haben gegenüber den Bestimmungen des Bundesdatenschutzgesetzes Vorrang. Sie ermöglichen es aber, bei der Erteilung von Auszügen auch Datenschutzgesichtspunkte zu berücksichtigen und die mitzuteilenden Angaben auf diejenigen zu beschränken, die zur Wahrung des berechtigten Interesses des Betroffenen unabdingbar erforderlich sind.

Gegenwärtig wird überwiegend noch so verfahren, daß der gesamte Inhalt eines oder mehrerer Grundbuchblätter übermittelt wird. Die Äußerung des Bundesministers der Justiz läßt aber erkennen, daß der Datenschutz Anlaß zu neuen Überlegungen gibt. Ich werde gemeinsam mit den Landesbeauftragten für den Datenschutz das Problem im Auge behalten.

2.2.6 Datenschutz im Bereich des Personenstandswesens — Aufgebot nach § 12 EheG —

Nach § 12 Ehegesetz in Verbindung mit § 3 Personenstandsgesetz erläßt der Standesbeamte vor der Eheschließung das Aufgebot. Es ist eine Woche lang öffentlich auszuhängen. Nach allgemeiner Auffassung, die auch in mehreren Eingaben betroffener Bürger zum Ausdruck gebracht worden ist, erfüllt das öffentliche Aufgebot heute seinen ursprünglichen Zweck, Dritte zur Anzeige von Ehehindernissen zu veranlassen, nicht mehr; es ist nur noch für die werbende Wirtschaft und für Auskunfteien von Interesse. Wer seine bevorstehende Eheschließung bekanntgeben möchte, hat dazu andere Möglichkeiten. Wem daran nicht gelegen ist, der sollte dazu nicht durch den Aushang des Aufgebots gezwungen werden.

Der Verzicht auf das Aufgebot ist bereits 1972 von der vom Bundesminister der Justiz gebildeten Eherechtskommission angeregt worden und entspricht der Empfehlung der Internationalen Kommission für das Zivilstandswesen zum Eheschließungsrecht aus dem Jahr 1976. Die Vorschläge gewinnen heute durch die sich immer stärker entwickelnde Sensibilisierung für Fragen des Datenschutzes ein stärkeres Gewicht.

Der Bundesminister der Justiz teilt diese Auffassung. Er hat vorgesehen, in dem Entwurf eines Zweiten Eherechtsreformänderungsgesetzes die Abschaffung des Aufgebots vorzuschlagen. An seiner Stelle soll eine Anmeldung der beabsichtigten Eheschließung mit einer Anmeldefrist von 4 Wochen treten.

2.3 Steuerverwaltung

Anläßlich eines Informationsbesuches im Bundesamt für Finanzen am 3. April 1979 habe ich mir einen ersten Überblick über die dort geführten Dateien und die Art der gespeicherten Daten verschafft. Schon bei dieser ersten Begegnung ergab sich, daß über den Umfang meiner Kontrollbefugnis im Bereich der Finanzverwaltung kein Einvernehmen zu erreichen war. Mir wurde entgegengehalten, das in § 30 der Abgabenordnung verankerte Steuergeheimnis setze meinem Recht, personenbezogene Einzelvorgänge einzusehen, Grenzen. Nur wenn ein Steuerpflichtiger sich beschwerdeführend an mich wende, könne ich die Unterlagen einsehen, denn dann habe er der Offenbarung zugestimmt (§ 30 Abs. 4 Nr. 3 AO). Ich könne ferner anonymisierte Dateiauszüge einsehen und mich generell über den Aufbau, Inhalt und den Schutz von Dateien unterrichten. Einer Offenlegung von Einzelvorgängen ohne Zustimmung des Betroffenen stehe jedoch § 30 Abs. 4 Nr. 2 AO entgegen. Die Vorschrift besagt, daß eine Offenlegung nur erlaubt ist, wenn „sie durch Gesetz ausdrücklich zugelassen ist". Dies sei im BDSG nicht der Fall.

Dazu bemerke ich:

Das BDSG gilt nach §§ 1 und 7 für Behörden und sonstige öffentliche Stellen des Bundes. Dazu gehören auch die Finanzbehörden des Bundes. Ausdrücklich erwähnt sind sie in § 12 Abs. 2 Nr. 1, wo bestimmt ist, daß die generell geltende Veröffentlichungspflicht „für Bundes- und Landesfinanzbehörden, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung in Dateien speichern", nicht gilt. In diesen Fällen besteht nach § 13 Abs. 2 auch keine Auskunftspflicht.

Meiner Kontrollbefugnis unterliegen nach § 19 Abs. 1 BDSG alle in § 7 Abs. 1 aufgeführten Behörden und sonstigen öffentlichen Stellen des Bundes. Daß auch die Finanzbehörden dazu zu zählen sind, ergibt sich aus § 19 Abs. 3 Satz 3: Aus der Verweisung auf § 12 Abs. 2 Nr. 1 folgt, daß die dort erwähnten Finanzbehörden, die Dateien zu Kontroll- und Prüfzwecken führen, diese nur mir selbst oder einem von mir Beauftragten zu öffnen haben. Eine Ausnahme gilt nur in den Fällen, in denen die zuständige oberste Bundesbehörde (hier der Bundesminister der Finanzen) im Einzelfall feststellt, daß die Einsicht in Unterlagen und Akten die Sicherheit des Bundes oder eines Landes gefährdet. In einer gemeinsamen Stellungnahme haben meine Kollegen in den Bundesländern und ich unsere Überzeugung zum Ausdruck gebracht, daß der Gesetzgeber auch die Finanzbehörden des Bundes und der Länder der Datenschutzkontrolle unterstellt hat. Würde sich die Rechtsauffassung der Finanzverwaltung durchsetzen, hätte dies eine empfindliche Schwächung der Datenschutzkontrolle zur Folge.

Die Wahrnehmung meiner gesetzlichen Kontrollaufgabe ist mir unmöglich, wenn ich nicht in der Lage bin, bei Überprüfungen vor Ort auch Stichproben vorzunehmen. Durch solche Kontrollaufgaben, die im Interesse des Steuerpflichtigen liegen, wird das Steuergeheimnis nicht tangiert. Daß die Vertraulichkeit der Daten durch mich gewahrt wird, versteht sich von selbst. Andere Behörden, für deren Daten besondere Amtsgeheimnisse gelten, wie z. B. das Statistische Bundesamt, haben

dies verstanden. Ich hoffe, auch mit der Finanzverwaltung ein Einvernehmen zu erzielen, ohne daß der Gesetzgeber eingreifen muß.

2.4 Volkszählung und Statistik

2.4.1 Gesetzgebung

Auf dem Gebiet der Statistik hat der Bundestag im abgelaufenen Jahr seine Beratungen zu verschiedenen Gesetzentwürfen abgeschlossen, die für den Datenschutz von weitreichender Bedeutung sind. Meine Vorstellungen zur Ausgestaltung des Datenschutzes, die ich bereits während der Vorbereitung der Vorhaben gegenüber der Bundesregierung zum Ausdruck gebracht und in meinem ersten Tätigkeitsbericht näher erläutert habe (vgl. 1. TB, 3.3, insbesondere 3.3.4 bis 3.3.6), habe ich auf Wunsch des Innenausschusses des Deutschen Bundestages in den Beratungen der Berichterstatter näher erläutert. Über die bereits von der Bundesregierung aufgenommenen Anregungen hinaus sind dabei weitere meiner Vorschläge berücksichtigt worden. Beispiele hierfür sind:

- die Aufnahme einer Regelung über die getrennte und besonders gesicherte Aufbewahrung von Namen, Anschriften und sonstigen Identifizierungsdaten sowie über deren Löschung im Zeitpunkt der Aufgabenerledigung (§ 11 Bundesstatistik-Gesetz),
- eine präzisere Regelung der Voraussetzungen, unter denen statt des Betroffenen ein „Ersatzauskunftspflichtiger" befragt werden darf (§ 5 Volkszählungsgesetz),
- die nur noch freiwillige Erhebung von Angaben zur Gesundheit im Rahmen des Mikrozensus (Artikel 1 a Statistikbereinigungsgesetz).

Mit diesen Gesetzen wird der Datenschutz auf einem Gebiet wesentlich verbessert, das für fast jeden Bürger unmittelbare praktische Bedeutung hat. Durch verschiedene Präzisierungen wurden auch die Bedingungen für die Datenschutzkontrolle bei den Statistischen Ämtern verbessert. Der Gesetzgeber hat beim Volkszählungsgesetz eine Möglichkeit vorgesehen, Einzelangaben den Kommunen für eigene statistische Aufbereitungen zu überlassen, wobei durch Satzung sichergestellt sein muß, daß die Daten ausschließlich statistisch genutzt werden. Den Landesbeauftragten für den Datenschutz erwachsen daraus bedeutende neue Kontrollaufgaben.

2.4.2 Erhebung von Namen bei statistischen Erhebungen

Im Frühjahr 1979 wurde auf der Grundlage einer EG-Verordnung (Verordnung Nr. 495/78 vom 6. März 1978, Amtsblatt der EG Nr. L 78/3) die Gehalts- und Lohnstrukturerhebung 1978 als Repräsentativstatistik durchgeführt. Nach der Verordnung sind die in die Erhebung einbezogenen Unternehmen verpflichtet, für jeden ihrer Arbeitnehmer verschiedene Angaben insbesondere zum Arbeitsentgelt, zur Qualifikation und zur Beschäftigung zu machen. Die Erhebungsliste sieht für jeden Beschäftigten eine Zeile mit rd. 20 Angaben vor. Eine fortlaufende Zählnummer pro Arbeitnehmer ist vorgedruckt. Zusätzlich ist vom Unternehmen laut Überschrift in Spalte 2 anzugeben: „Name oder Nummer des Arbeitnehmers (wichtig bei Rückfragen)".

Gegen die namentliche Bezeichnung wurden aus dem Kreis der Landesbeauftragten für den Datenschutz Bedenken erhoben. Mit Recht wurde darauf hingewiesen, daß durch die offene Namensangabe ein erheblich größeres Mißbrauchsrisiko entsteht als bei Eintragung der Personalnummer oder eines anderen Ordnungszeichens. Das Statistische Bundesamt hat demgegenüber Bedenken geäußert, von dem von der EG-Kommission verbindlich festgelegten Fragebogen abzuweichen. Darüber hinaus liege es nicht im Sinne der Statistik, die Schaffung von Personalnummern in den Betrieben anzuregen, da hierdurch ein datenschutzrechtlicher Gefährdungstatbestand geschaffen werden könne.

Eine Erörterung mit dem Statistischen Bundesamt hat zu folgendem Ergebnis geführt:

Den statistischen Ämtern kommt es allein auf die Identifizierungsmöglichkeit, nicht auf die Kenntnis der Namen an. Die Bezeichnung der Betroffenen mit einer Nummer ist das schonendere Mittel, da sie die Bestimmung der Betroffenen erschwert. Daher soll künftig bei ähnlich gelagerten Erhebungen darauf hingewirkt werden, daß die auskunftspflichtigen Betriebe möglichst ausschließlich mit Nummern arbeiten. Soweit Personal- oder Gehaltsnummern in einen Betrieb nicht existieren, soll dieser angeregt werden, eine Liste mit Nummern und Namen zu erstellen, die zu vernichten ist, sobald die Plausibilitätskontrollen abgeschlossen sind. Soweit bei der Durchführung geltender statistischer Vorschriften zweifelhaft sein kann, ob eine Verpflichtung des Betriebs zur Erstellung einer solchen Liste aus den gesetzlichen Vorschriften ableitbar ist, soll in den begleitenden Erläuterungen darauf hingewiesen werden, daß die Betriebe unter datenschutzrechtlichen sowie unter arbeits- und dienstrechtlichen Gesichtspunkten gehalten sind, von mehreren Identifizierungsmöglichkeiten diejenige zu wählen, die die schutzwürdigen Belange ihrer Beschäftigten am wirksamsten vor Beeinträchtigungen sichert. Bei der statistischen Gesetzgebung soll künftig die Angabe von Namen durch Nummern ersetzt werden.

2.4.3 Überprüfung des Statistischen Bundesamtes

Die Überprüfung der Datenverarbeitung im Statistischen Bundesamt hat zwar einige Schwachstellen und Mängel aufgedeckt, sie hat aber auch gezeigt, daß dem Datenschutz in diesem Amt — beeinflußt durch das bereits vor Inkrafttreten des BDSG geltende Statistik-Geheimnis — ein hoher Stellenwert beigemessen wird. Generell kann ich dem Amt eine sorgfältige Planung für den Umgang mit personenbezogenen Daten bescheinigen. Die kritischen Punkte liegen in erster Linie in der EDV und in ihrem Umfeld. Die angetroffenen Mängel

lassen nicht den Schluß zu, daß Rechte der Betroffenen verletzt sind, doch kann dies auch nicht mit der notwendigen Sicherheit ausgeschlossen werden.

Im einzelnen habe ich folgende Erkenntnisse gewonnen:

— Die interne Übersicht über die gespeicherten Daten — wie sie nach § 15 Nr. 1 BDSG gefordert wird — ist in der Aufbereitung unzweckmäßig. Sie läßt die Informationsflüsse und -zusammenhänge, die Standorte der Datenbestände und die Verantwortlichkeiten für die einzelnen Daten nicht erkennen und muß auch um einzelne Übermittlungswege vervollständigt werden.

  Die für die Neugestaltung der Übersicht erforderlichen Angaben sind weitgehend in verschiedenen anderen Unterlagen vorhanden und dokumentiert. Die vorhandenen Aufzeichnungen müssen ausgewertet werden, damit die Übersicht für den ihr zugedachten Zweck, zentraler Nachweis und zentrales Arbeitsmittel für den internen Datenschutzbeauftragten zu sein, genutzt werden kann.

— Das Amt hat ein Konzept für die Dokumentation von DV-Anwendungen entwickelt, das in seiner Sorgfalt und Detaillierung als besonders geeignet für den Nachweis der ordnungsgemäßen Anwendung der DV-Programme (§ 15 Nr. 2 BDSG) angesehen werden kann. Die Umsetzung der Hausverfügung bereitet jedoch erhebliche Schwierigkeiten. Mir konnte keine Organisationsakte vorgelegt werden, die nach dem 1978 beschlossenen Muster vollständig angelegt war.

— Schwierigkeiten habe ich auch bei der Aufbewahrung von Belegen und EDV-Zusammenstellungen festgestellt, die sich noch im Geschäftsgang befinden. Die Probleme sind nicht unerheblich, da z. B. bei einer großen Statistik täglich bis zu 100 000 Einzelbelege eintreffen und bearbeitet werden müssen.

— Das Rechenzentrum wird zwar als closed-shop-Betrieb geführt, jedoch ist der Kreis der Zugangsberechtigten sehr groß. Die Maßnahmen zur Kontrolle des Zu- und Abgangs von Personen sowie des Umlaufs der Datenträger waren unzureichend. Die Organisation dieses Bereiches habe ich beanstandet.

— Außerhalb des gesicherten Bereichs liegt der Lochsaal mit etwa 80 Arbeitsplätzen. Auch hier halte ich die Abgangskontrolle nach Nr. 2 der Anlage zu § 6 BDSG für nicht gewährleistet.

— Ebenfalls beanstandet habe ich die Lagerung von zur Vernichtung bereitgestellten Lochkarten, die in beschrifteten Kartons in einem allgemein zugänglichen Gang standen.

— Die Archivierung von Erhebungsbelegen, Erfassungsbelegen und Ausdrucken ist zum Teil verbesserungsbedürftig. Ich habe vorgeschlagen, Art und Dauer der Archivierung in der Übersicht nach § 15 Nr. 1 BDSG festzuhalten.

— Die Verpflichtung, in den Erhebungsformularen auf die Rechtsvorschrift hinzuweisen, die die Erhebung anordnet (§ 7 BStatG a. F., der dem § 9 Abs. 2 BDSG entspricht), wird mit ganz geringen Ausnahmen sorgfältig durchgeführt. Die Hinweise gehen in vielen Fällen über die Nennung der Rechtsgrundlage hinaus und verfolgen damit ein Anliegen, das auch ich propagiere: der Betroffene soll darüber aufgeklärt werden, für welche Zwecke seine Angaben benötigt werden, was mit seinen Daten geschieht und gegebenenfalls was mit seinen Daten nicht geschieht, letzteres, um beim Betroffenen mögliche Befürchtungen und Vorbehalte abzubauen. Diese weitergehende Aufklärungsarbeit begrüße ich sehr.

Das Statistische Bundesamt arbeitet an der Entwicklung eines umfassenden Sicherheitskonzeptes. Da die personellen Voraussetzungen dafür geschaffen sind, ist zu erwarten, daß die bestehenden Schwachstellen, insbesondere bei der systematischen Erfassung und Analyse der sicherheitsrelevanten Vorgänge, beseitigt werden.

Auch wenn für das Rechenzentrum ein Neubau geplant ist, sind während der Übergangszeit zusätzliche Anstrengungen unerläßlich. Die extrem hohe Zahl von verfügbaren Datenträgern läßt es nicht zu, auf eine wirksame Abgangskontrolle zu verzichten.

2.5 Personalwesen

2.5.1 Personalinformationssysteme

Der Bundesminister des Innern benutzt ein Personal- und Stelleninformationssystem (IPSIS) zur Unterstützung der Personal- und Stellenplanung. Das System wird auf der EDV-Anlage des Bundesverwaltungsamtes geführt. Um einen Eindruck von den dort bestehenden Schutzmaßnahmen zu gewinnen, haben meine Mitarbeiter das Rechenzentrum des Bundesverwaltungsamtes in Bonn besucht. Es zeigte sich, daß noch Schwachstellen bestehen, die aber zum Teil durch die baulichen Verhältnisse bedingt sind. Es wurde angeregt, bei dem bevorstehenden Neubau des Rechenzentrums Datenschutz- und Datensicherheitsaspekte angemessen zu berücksichtigen; ich habe meine Beratung hierfür angeboten.

2.5.2 Speicherung von Beurteilungsnoten

Die Aufnahme von Beurteilungsnoten in eine Personaldatenbank, die Gegenstand einer Eingabe war, wird unterschiedlich gehandhabt. Während eine oberste Bundesbehörde lediglich das Datum der letzten Beurteilung speichert, legen andere oberste Bundesbehörden Wert darauf, auch die Beurteilungsnote zu speichern, allerdings nur die Gesamtnote, nicht die sie bildenden Einzelnoten und ebensowenig etwaige abweichende Beurteilungen der einzelnen Vorgesetzten oder Gegenvorstellungen und Widersprüche des Beurteilten. Das Gesamturteil (vgl. § 41 Abs. 2 Bundeslaufbahnver-

ordnung) ist also immer nur ein Teil dessen, was in den Personalakten zur Beurteilung des Bediensteten enthalten ist.

Für die Beschränkung der Speicherung auf das Datum der Beurteilung spricht, daß dadurch ein Zwang zur Einsichtnahme in die vollständigen Beurteilungsunterlagen geschaffen wird, wenn eine Beurteilung zur Grundlage einer Personalentscheidung gemacht werden soll.

Gegen die Beschränkung der Speicherung auf das Beurteilungsdatum wird vorgebracht, die Beurteilungsnote (oder gar: die letzten — z. B. vier — Beurteilungsnoten) werde für eine Reihe von Auswertungen benötigt. So werde durch die maschinelle Aufstellung der Vorbereitungslisten für eine Beurteilung zu einem Beurteilungsstichtag (für eine oder mehrere Besoldungsgruppen) erhebliche Verwaltungsarbeit eingespart; gleichartige Listen hätten früher manuell geschrieben werden müssen. Das Gesamturteil sei neben anderen Daten (z. B. Beförderungseignung, allgemeines Dienstalter) maßgebend für die Beförderung eines Beamten. Für die gesamte Bundesfinanzverwaltung etwa werde je Besoldungsgruppe und je Sparte eine Beförderungsreihenfolge maschinell festgelegt; hierbei werde aus dem Gesamturteil und dem Dienstalter ein „Beförderungsdienstalter" errechnet, eine wiederholte gute Beurteilung werde mit einem „Bonus" (Verbesserung des Beförderungsdienstalters) berücksichtigt. Daher müßten auch die Vorbeurteilungen gespeichert werden.

Hiergegen ist einzuwenden: Wird lediglich das Gesamturteil gespeichert, so erhält dieses Datum einen Stellenwert, der ihm angesichts der allseits eingeräumten Schwächen des Beurteilungswesens nicht zukommt. Dieses Datum wird dann zur Grundlage von späteren Entscheidungen gemacht, obwohl es durch den Inhalt der Personalakte — Beiheft „Beurteilungen" — u. U. in seiner Aussage stark relativiert werden kann. Denn bekanntlich werden Gesamturteile nach ganz verschiedenen Maßstäben gegeben; es sei lediglich daran erinnert, daß die Person der Beurteilenden, die Person des Beurteilten, der Aufgabenkreis im Beurteilungszeitraum usw. die Gesamtnote stark beeinflussen können. Diese Faktoren sind aus der Personalakte ersichtlich, nicht dagegen aus der gespeicherten Gesamtnote. Datenschutzrechtlich stellt sich hier also das Problem der Unrichtigkeit gespeicherter Daten durch Unvollständigkeit:

Wenn ein Teiltatbestand aus dem umfassenden Datenbestand „Personalakte" in ein Personalinformationssystem eingegeben wird, so muß vorher geprüft werden, ob der so entstehende Auszug aus der Personnalakte durch das Herauslösen aus dem Zusammenhang wegen der dann entstehenden Unvollständigkeit unrichtig wird oder zur Grundlage von Entscheidungen gemacht werden darf, die die vollständige Kenntnis der Personalakte voraussetzen. Es leuchtet ohne weiteres ein, daß das gespeicherte Datum der letzten Beurteilung allenfalls die Funktion einer Wiedervorlageverfügung hat, aber kaum zur Grundlage von Entscheidungen gemacht werden kann. Bei dem gespeicherten Gesamturteil ist das nicht anders: auf der Grundlage dieser Teildatenmenge dürfen keine Entscheidungen getroffen werden, deren Grundlage die Personalakte sein sollte.

Es wird nicht verkannt, daß die Verwendung von Teildatenmengen — wie hier — für die Verwaltung bequemer sein kann. Aber zwingend ist dies nicht, wie sich schon daraus ergibt, daß ein so großes Ressort wie das Bundesinneministerium sich für die Zwecke seines Personalinformationssystems damit begnügt, nur das Datum der letzten Beurteilung zu speichern. Was im Bundesinneministerium aus gutem Grunde, nämlich dem, die vollständige Personalakte vor einer Entscheidung beizuziehen, praktiziert wird, kann nicht in anderen Ressorts zu unüberwindlichen Schwierigkeiten führen. Ich werde daher weiter darauf hinwirken, daß in Personalinformationssystemen nur solche Teildatenmengen gespeichert werden, welche das Personalführungsinstrument „Personalakte" nicht zu umgehen suchen. Die obersten Bundesbehörden, die der Speicherung von Teildatenmengen — wie der Gesamtnote — das Wort reden, leugnen im Grunde, daß Personalentscheidungen nur auf der Grundlage der vollständigen Personalakten getroffen werden dürfen. An die Stelle der Personalakten setzen sie die unvollständigen Datenbestände des Personalinformationssystems. Die Verwendung der Gesamtnote aus der Personaldatenbank für Beförderungsentscheidungen sollte daher in Zukunft unterbleiben.

2.5.3 Registrierung von Grundbesitz

Ein Angehöriger der Bundesfinanzverwaltung hat sich bei mir darüber beschwert, daß seinem Antrag, in seiner Personalkarteikarte die Eintragung PE (= Privateigentum: Eigenheim, Eigentumswohnung) zu löschen, nicht entsprochen worden sei. Die Speicherung der Tatsache, daß er Eigentümer einer Wohnung sei, sei für dienstliche Zwecke nicht erforderlich.

Der Bundesminister der Finanzen hat die Erforderlichkeit der Speicherung dieses Datums zunächst damit begründet, daß vorhandener, von Beamten bewohnter Grundbesitz ein wichtiges Indiz für die Mobilität des Bediensteten sei. Wer ein Eigenheim oder eine Eigentumswohnung besitze, sei stärker an den gegenwärtigen Dienstort gebunden als der Inhaber einer Mietwohnung. Ich habe dagegen eingewandt, die genannte Information sei ungeeignet, um auf die Versetzungsbereitschaft zu schließen; auch bei vorhandenem Grundbesitz könne Versetzungsbereitschaft gegeben sein. Ferner lägen nicht alle Daten, die der Dienstherr für nützlich halte, auch im Rahmen der Zweckbestimmung des Dienstverhältnisses. Sie seien auch nicht sämtlich zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich.

Der Bundesminister der Finanzen hat daraufhin eingeräumt, daß die Kennzeichnung „Eigentumswohnung/Eigenheim" zu der Zeit, als die Personaldatenbank der Bundesfinanzverwaltung eingerichtet wurde, als Hilfe für eine erste, grobe Auswahl der für eine Versetzung in Betracht kommenden

Beamten wichtig gewesen sei. Die Bedeutung dieses Merkmals sei jedoch inzwischen erheblich geringer geworden, so daß darauf verzichtet werden könne.

Darüber hinaus hat der Bundesminister der Finanzen erklärt, daß zukünftig darauf geachtet werde, Datenarten, die durch Zeitablauf oder Änderung der Verhältnisse ihre Bedeutung verloren hätten und deren Speicherung deshalb zur Wahrung berechtigter Interessen der speichernden Stelle nicht mehr erforderlich sei, generell nicht mehr in der Datenbank fortzuführen.

2.5.4 Datenschutz im Bereich von Dienst- und Arbeitsverhältnissen

In zahlreichen Fällen werden beim Eingehen oder im Rahmen eines Beschäftigungsverhältnisses ärztliche Untersuchungen erforderlich. Dabei wird dem Arzt eine Fülle von personenbezogenen Daten offenbart. Insbesondere anläßlich der Einstellung von Bewerbern für den öffentlichen Dienst, der Übernahme in das Beamtenverhältnis, der Prüfung der Verwendungsfähigkeit für einen bestimmten Arbeitsplatz, der Prüfung der vorzeitigen Versetzung in den Ruhestand, aber auch sonst bei Inanspruchnahme eines Personalarztes werden personenbezogene Daten erhoben. Im Zusammenwirken mit dem Leitenden Arzt des Ärztlichen und Sozialen Dienstes der obersten Bundesbehörden im Bundesministerium des Innern wurde zum Schutz dieser Daten eine die Interessen der Dienstherren/Arbeitgeber wie der Bediensteten berücksichtigende Lösung gefunden, die nach den konkreten Zwecken der ärztlichen Untersuchung differenziert.

Es wurde Übereinstimmung erzielt, daß in der Regel nur das Ergebnis der ärztlichen Untersuchung an die personalbearbeitende Stelle übermittelt wird, während die für die Beurteilung im einzelnen erhobenen Daten beim Personalarzt verbleiben. Dort können sie vom untersuchten Bediensteten jederzeit eingesehen werden, nicht dagegen vom Dienstherrn/Arbeitgeber.

Die Mitteilung an die personalbearbeitende Stelle beschränkt sich also auf die Beantwortung der dem Personalarzt gestellten Frage und besagt z. B. lediglich, daß ein Bewerber für eine Übernahme in das Beamtenverhältnis oder für eine Verwendung auf einem bestimmten Dienstposten uneingeschränkt oder nur eingeschränkt geeignet ist und ggf., welche Einschränkungen vorliegen. Bei Entscheidungen des Dienstherrn/Arbeitgebers, die aufgrund eines diesem eingeräumten Ermessens getroffen werden, kann in Einzelfällen, z. B. bei der vorzeitigen Versetzung eines Beamten in den Ruhestand, eine noch ausführlichere Auskunft geboten sein. Der Umfang der Auskunft läßt sich nicht generell bestimmen.

Grundsätzlich gilt aber, daß in keinem Fall alle Unterlagen, die beim Personalarzt entstehen, für die Entscheidung der personalbearbeitenden Stelle geeignet und/oder erforderlich sind. Der Verhältnismäßigkeitsgrundsatz gebietet, zu den Personalakten nur solche Unterlagen aus dem Bereich des ärztlichen und sozialen Dienstes zu nehmen, die für Zwecke der Personalverwaltung erforderlich sind.

Das Recht des Bediensteten auf Einsicht in die vollständigen Personalakten wird nicht dadurch beeinträchtigt, daß ein Teil der auf den Bediensteten bezogenen ärztlichen Unterlagen zu seinem Schutze nicht zu den Personalakten im formellen Sinne kommt. Soweit sie beim ärztlichen und sozialen Dienst verbleiben, kann der Untersuchte sie dort einsehen. Auf dieses Einsichtsrecht wird der Bedienstete bei der Untersuchung ausdrücklich hingewiesen.

Ferner konnte Einvernehmen darüber erzielt werden, daß die Übersendung von ärztlichen Unterlagen über einen Bediensteten von einer Dienststelle an eine andere Dienststelle nicht ohne weiteres zulässig ist, sondern regelmäßig der Zustimmung des Betroffenen (vgl. § 3 BDSG) bedarf. In Fällen, in denen der Bedienstete zur Zustimmung verpflichtet ist und die Zustimmung pflichtwidrig nicht erteilt, ist es Sache des Dienstherrn/Arbeitgebers, nicht aber des Arztes, daraus Konsequenzen zu ziehen.

Wieweit schließlich die Übersendung ärztlicher Unterlagen von einer ärztlichen Dienststelle an eine andere ärztliche Dienststelle zulässig ist, läßt sich ebenfalls nicht allgemein beantworten. Grundsätzlich gilt die ärztliche Schweigepflicht auch gegenüber einem anderen Arzt. Das ist nur dann nicht der Fall, wenn eine Befugnis des Arztes zur Offenbarung entweder aus einer Rechtsnorm oder aus der Zustimmung des betroffenen Bediensteten hergeleitet werden kann.

2.5.5 Bundespersonalausschuß — Personalakten

In den Verfahrensordnungen über die Feststellung des erfolgreichen Abschlusses der Einführung von Beamten in die Aufgaben der Laufbahnen des mittleren, gehobenen und höheren Dienstes zum Zwecke des Aufstiegs — GMBl. 1979, 79, 80 — hat der Bundespersonalausschuß bestimmt, daß ihm zur Feststellung des erfolgreichen Abschlusses der Einführungszeit „die Personalakten" vorzulegen seien. Gegen diese Regelungen und die auf ihrer Grundlage beruhende Vorlagepraxis der von den Verfahrensordnungen angesprochenen Bundesbehörden habe ich datenschutzrechtliche Bedenken erhoben, weil der in der Datenübermittlung (Übersendung der Personalakten) liegende Eingriff in die persönliche Rechtsstellung des Beamten in diesem Umfange nicht gerechtfertigt erscheint. Im einzelnen habe ich meine Bedenken wie folgt begründet:

Zu den „anderen Vorschriften über den Datenschutz" im Sinne des § 19 BDSG, deren Einhaltung ich zu kontrollieren habe, gehören die Rechtssätze über die Geheimhaltung der Personalakten. Nach der ständigen Rechtsprechung des Bundesverwaltungsgerichts (BVerwGE 19, 179, 185 mit weiteren Nachweisen; 35, 225, 227) gehören Personalakten grundsätzlich zu den Vorgängen, die „ihrem Wesen nach geheimgehalten werden müssen". Sie dürfen daher ohne Einwilligung des Beamten

grundsätzlich nur von einem eng begrenzten Personenkreis mit besonderer dienstlicher Verantwortung (Personalreferent, Behördenleiter) eingesehen werden; sie genießen sowohl im dienstlichen Interesse als auch im schutzwürdigen persönlich-privaten Interesse des Beamten einen besonderen Vertrauensschutz (im Sinne eines besonderen Amtsgeheimnisses gem. §§ 10, 24, 45 Satz 2 Nr. 1 BDSG), der sich auch auf den Verkehr der Behörden untereinander erstreckt (BVerwG a. a. O.).

Der Bundespersonalausschuß übt seine Tätigkeit zwar unabhängig und in eigener Verantwortung, aber innerhalb der gesetzlichen Schranken aus (§ 95 Bundesbeamtengesetz). Zu den gesetzlichen Schranken gehört das gesamte Datenschutzrecht. Nach dem Bundesdatenschutzgesetz steht jede Datenübermittlung als ein Fall der Datenverarbeitung (§§ 1 Abs. 1, 2 Abs. 2 Nr. 2 BDSG) unter dem Vorbehalt der Erlaubnis durch Rechtsnorm oder der Einwilligung des Betroffenen (§ 3 BDSG). Nach dem Datenschutzrecht außerhalb des BDSG, das hier anzuwenden ist, gilt gemäß der Rechtsprechung des Bundesverfassungsgerichts zum Persönlichkeitsschutz — Artikel 2 Abs. 1 i. V. m. Artikel 1 Abs. 1 GG — grundsätzlich dasselbe: eine Datenübermittlung ist als ein Eingriff in die persönliche Rechtsstellung anzusehen, der nur unter strenger Beachtung des Verhältnismäßigkeitsgrundsatzes zulässig ist.

§ 102 Abs. 2 Bundesbeamtengesetz bestimmt, daß alle Dienststellen dem Bundespersonalausschuß Amtshilfe zu leisten, ihm auf Verlangen Auskünfte zu erteilen und Akten vorzulegen haben, soweit dies zur Durchführung seiner Aufgaben erforderlich ist. Indem diese Regelung auf die Erforderlichkeit abstellt, ist sie Ausdruck des verfassungsrechtlichen Verhältnismäßigkeitsgrundsatzes und daher in seinem Sinne zu interpretieren. Für das begrenzte Anliegen, das die genannten Verfahrensordnungen verfolgen, nämlich die Feststellung des erfolgreichen Abschlusses der Einführung für den Aufstieg in die nächsthöhere Laufbahn, ist aber die Vorlage „der (vollständigen) Personalakten", einschließlich z. B. medizinischer Gutachten, Disziplinarakten usw., mit Sicherheit nicht erforderlich. Es genügt der Teil der Personalunterlagen, der für die zu treffende Feststellung unmittelbar von Bedeutung ist.

Der Meinungsaustausch über das aufgeworfene Problem zwischen dem Bundesminister des Innern, dem Bundespersonalausschuß und mir ist noch nicht abgeschlossen.

2.5.6 Personalvertretungsrecht (Betriebsverfassungsrecht) und Datenschutz

Mit unterschiedlicher Intensität haben sich seit Inkrafttreten des BDSG im Personalvertretungsrecht und im Betriebsverfassungsrecht Konfliktsituationen ergeben, die darauf zurückzuführen sein dürften, daß das BDSG und ihm folgend die Landesdatenschutzgesetze die Interessengegensätze zwischen Personal/Belegschaft einerseits und Behörden- bzw. Unternehmensleitung andererseits nicht — oder nicht hinreichend — berücksichtigt haben.

Insbesondere folgende Fragen haben sich gestellt:

- Ist der Personalrat/Betriebsrat sonstige „öffentliche Stelle" (§§ 1 Abs. 2 Nr. 1, 7 Abs. 1 BDSG) bzw. „Personenvereinigung des privaten Rechts" (§§ 1 Abs. 2 Nr. 2 und 3, 22 Abs. 1 BDSG) und damit selbständige speichernde Stelle?
- Ist der Personalrat/Betriebsrat im Verhältnis zur Dienststelle/zum Betrieb Dritter im Sinne von § 2 Abs. 3 Nr. 2 BDSG?
- Sind die Mitglieder des Personalrats/Betriebsrats gem. § 5 BDSG auf das Datengeheimnis zu verpflichten? Wenn ja: durch wen? (Dienststellen-/Betriebsleitung?; nur der Vorsitzende, der seinerseits die übrigen Mitglieder des Personalrats/Betriebsrats verpflicht?)
- Können die Mitglieder des Personalrats/Betriebsrats sich weigern, sich gem. § 5 BDSG verpflichten zu lassen, und welche Rechtsfolgen hätte das?
- Hat der interne Datenschutzbeauftragte Kontrollbefugnisse gegenüber dem Personalrat/Betriebsrat? Wenn ja: welche?
- Welche Mitwirkungs-/Mitbestimmungsrechte hat der Personalrat/Betriebsrat bei der Einführung und Veränderung von Personalinformationssystemen? Welche hat er bei Kontrollen durch technische Einrichtungen?

Ich habe Zweifel, daß sich diese Probleme allein im Wege der Auslegung der bestehenden Gesetze zufriedenstellend lösen lassen. Deshalb sollte bald geprüft werden, ob nicht im Bereich des Personalvertretungs-/Betriebsverfassungsrechts bereichsspezifische Regelungen notwendig sind. Ziel dieser Prüfung sollte sein, die Informationsbeziehungen zwischen beiden Seiten so zu gestalten, daß die automatische Datenverarbeitung oder das Datenschutzrecht nicht zu Verschiebungen des Kräfteverhältnisses führen.

2.6 Sozialverwaltung, Gesundheitswesen

2.6.1 Problemüberblick

Jeder Bundesbürger (u. U. auch Ausländer) bekommt vom Staat Hilfe, wenn er sie braucht. Wichtigste Errungenschaft des Hilfe gewährenden Sozialstaates sind der Schutz der Gesundheit, die Vorsorge für das Alter, die Arbeitsvermittlung und die Wiedereingliederung in das Arbeitsleben (Rehabilitation).

Das im Laufe der Jahre entstandene „System sozialer Sicherung" läßt sich durch einige wesentliche Eigenschaften beschreiben:

- die Vielfalt der zu erledigenden Aufgaben.
- Massenhaftigkeit der Fälle.

So hatte beispielsweise die Berufsgenossenschaft für den Einzelhandel in Bonn 1978 nahezu 140 000 Unfälle zu bearbeiten.

— die vielfältige Gliederung einzelner Träger der sozialen Sicherung.

So hat die Arbeitsverwaltung 146 Arbeitsämter unterschiedlicher Größe mit 501 Nebenstellen. Eine einzige Ersatzkasse hat allein über 1 000 Zweigstellen in der Bundesrepublik.

— vielfältige, zumeist gesetzlich festgelegte Verflechtungen.

Ein Beispiel hierfür ist das Meldeverfahren für die gesetzliche Sozialversicherung (sog. DEVO/DÜVO-Datenfluß). Wer als Arbeitnehmer ein Beschäftigungsverhältnis eingeht, wird automatisch in ein Meldeverfahren einbezogen, an dem — jedenfalls in der Regel — der Arbeitgeber, die Krankenkasse, die Bundesversicherungsanstalt für Angestellte oder die Datenstelle der Deutschen Rentenversicherung (DSRV) und die Bundesanstalt für Arbeit beteiligt sind.

Es liegt auf der Hand, daß diese Gegebenheiten den Einsatz technischer Hilfsmittel wie der EDV erforderlich machen. Dabei ist die Automatisierung im Bereich der sozialen Sicherung zur Zeit noch beschränkt auf eine vergleichsweise geringe Zahl von Anwendungen. Als wichtigste automatische Anwendungen sind das Leistungs- und Beitragswesen sowie die Lohn- und Gehaltsabrechnung für interne Zwecke der Träger zu nennen. Diese Anwendungen sind charakterisiert durch die große Zahl der verarbeiteten Daten und die dadurch entstehenden großen Dateien. Gegenwärtig überwiegt noch die zentrale Verarbeitung der Daten mit Großrechnern.

Die Aufwendungen für sämtliche Sozialleistungen (Sozialbudget) werden im Jahre 1979 schätzungsweise [1]) 452 Mrd. DM betragen. Die Bundesrepublik liegt damit unter den Ländern der Europäischen Gemeinschaft — gemessen am Bruttoinlandsprodukt — in der Spitzengruppe mit den höchsten Sozialleistungen. Der Anstieg der Aufwendungen für Sozialleistungen ist bei nahezu stagnierender Beschäftigtenzahl politisch zu einem Problem höchster Priorität geworden. Die für meine Aufgabe wesentlichen. Schlußfolgerungen lassen sich in zwei Trends zusammenfassen:

— dem Bemühen, kostenverursachende Faktoren durch geeignete Maßnahmen der Vorausschau möglichst auszuschalten.

Das erfordert eine Veränderung des Aufgabenspektrums in Richtung auf Prävention und eine Wandlung der Institutionen sozialer Vorsorge in Richtung auf moderne Dienstleistungsunternehmen.

— einem verstärkten Zwang, die Rationalisierungsvorteile der EDV zu nutzen.

Die Ausprägungen dieses Trends sind gegenläufig: Dem Bemühen, die Vorteile dezentral am Arbeitsplatz eingesetzter Hardware zu nutzen, steht das Bestreben gegenüber, für Teilfunktionen gemeinsame zentrale Einrichtungen aufzubauen. Beispiele für arbeitsplatzorientierte Systeme sind die im Aufbau befindlichen Informationssysteme der Innungs- und Betriebskrankenkassen. Wichtige Beispiele für zentrale, im Aufbau befindliche Einrichtungen sind die „Clearingstelle" der Arbeitsmedizinischen Dienste der Bauberufsgenossenschaften in München und das von der Arbeitsgemeinschaft für Gemeinschaftsaufgaben der Krankenvesicherung in Essen diskutierte System für die sozialärztlichen Dienste DVDIS (s. u. 2.6.8).

Diese Entwicklungen mögen aus sozialpolitischer Sicht geboten sein. Wie ich oben ausgeführt habe (s. o. 1.2), bestehen aber datenschutzrechtliche Bedenken gegen den Aufbau zentraler Datenbestände, welche die Gefahren der Zweckentfremdung verstärken.

Ich befürchte, daß der vom System der sozialen Sicherung verwaltete Bürger zunehmend entmündigt und passiviert wird, die unterschiedlichen Träger sozialer Vorsorge zu einem einheitlichen „Informationsblock" zusammenwachsen und der schon jetzt auch für Fachleute schwer zu überblikkende Bereich der sozialen Sicherung vollends undurchschaubar wird. Es ist das Hauptanliegen des Datenschutzes, derartigen — denkbaren — Fehlentwicklungen von vornherein entgegenzuwirken.

Während sich der Datenschutzgedanke in den Sicherheitsbehörden durchzusetzen beginnt, bereitet es im Bereich der sozialen Sicherung gelegentlich Schwierigkeiten, Verständnis für die Belange des Datenschutzes zu wecken. Im Unterschied zur Sicherheitsverwaltung gewährt der Staat hier Leistungen, tut also im Prinzip Gutes. Es ist gegenwärtig noch schwer zu vermitteln, daß zur Erreichung eines an sich guten Zwecks nicht jedes Mittel gerechtfertigt ist. Um der Sache willen muß ich mich auch dann äußern, wenn die Durchsetzung des Datenschutzes in manchen politischen Bereichen ein Umdenken erforderlich macht. Dabei geht es nicht darum, die Gesundheits- oder Sozialpolitik dem Datenschutz unterzuordnen. Der Datenschutz muß vielmehr in die Zielsetzung der Gesundheits- und Sozialpolitik von vornherein einbezogen werden.

2.6.2 Umfrage bei den Spitzenverbänden der Sozialversicherungsträger zum Sozialgeheimnis

Um festzustellen, welche auf Sozialdaten bezogene Anfragen in der Praxis tatsächlich erfolgen und wo der Schwerpunkt der Datenanforderungen liegt, habe ich während des Berichtsjahres eine Umfrage bei den Spitzenverbänden der Sozialversicherungsträger durchgeführt, da entsprechendes Material bei den in erster Linie dafür zuständigen Ressorts (Bundesminister für Arbeit und Sozialordnung, Bundesminister der Justiz) nicht vorhanden war. Die Umfrage hatte folgende Ergebnisse:

— Die meisten Anfragen kamen von den Leistungsträgern der Sozialversicherung. Die

[1]) Schewe/Nordhorn/Schenke/Meurer/Hermser, Übersicht über die Soziale Sicherung, 9. Aufl., Bonn 1977, S. 26.

zweitgrößte Gruppe bildeten die Justizbehörden (Gerichte, vor allem Sozialgerichte, Staatsanwaltschaften). Auch die Polizeibehörden gehörten zu den häufig anfragenden Stellen.

— Als ein erfreuliches Zeichen ist es zu werten, daß in zahlreichen Fällen die Anfragenden auf das Erfordernis der Einwilligung des Betroffenen hingewiesen wurden.

— Anfragen des Verfassungsschutzes und des Bundesnachrichtendienstes spielen nach dem übersandten Material keine nennenswerte Rolle.

Nicht erfaßt werden konnten allerdings Anfragen, die auf dem sog. „kleinen Dienstweg" gestellt, also im Rahmen guter „persönlicher Beziehungen" abgewickelt wurden. Hier liegt nach den bisherigen Erkenntnissen eine in ihrer Größenordnung nicht überschaubare Grauzone, die aber im Zuge wachsenden Datenschutzbewußtseins wahrscheinlich schon kleiner geworden ist und wohl weiter kleiner werden wird.

Der Erhebungszeitraum liegt nicht in allen Fällen genau fest, bezieht sich aber in der Regel auf die drei Jahre nach Inkrafttreten des § 35 SGB I (1. Januar 1976—31. Dezember 1978).

Im übrigen enthalten die Zusammenstellungen nur Angaben darüber, von wem welche Fragen gestellt worden sind. Ob und wie der angesprochene Sozialversicherungsträger die an ihn gerichtete(n) Frage(n) beantwortet hat, läßt sich dem vorliegenden Material nicht entnehmen. Das ist darauf zurückzuführen, daß die Anfragen häufig (fern)mündlich beantwortet werden.

2.63 Novellierung des § 35 SGB I

Bei zahlreichen Besprechungen habe ich die Gesichtspunkte vorgetragen, die aus meiner Sicht bei einer Novellierung des § 35 SGB I berücksichtigt werden sollten. Es sind dies vor allem:

— Wie bisher sollte der Schutz der Sozialdaten umfassend durch eine generalklauselartige Formulierung gewährleistet werden. Ausnahmen, also Fälle befugter Offenbarung von Sozialdaten, sind als solche eng, d. h. nicht generalklauselartig, zu umschreiben und in einem abschließenden Katalog zusammenzufassen, um die in der Praxis bestehenden Unsicherheiten zu beseitigen. Ein allgemeiner Hinweis auf gesetzliche Mitteilungspflichten — vgl. § 35 Abs. 1 Satz 2 SGB I — reicht nicht aus, weil dabei offenbleibt, welche Vorschriften derartige Pflichten vorsehen.

— Abschließend ist auch zu regeln, welche Behörden und Stellen die Sozialdaten zu schützen haben.

— § 35 Abs. 1 SGB I geht von dem Begriff des (Sozial)Geheimnisses aus. Die Verwendung des Geheimnisbegriffs führt aber in der Praxis zu Schwierigkeiten, weil unsicher ist, wann im Einzelfall ein Geheimnis vorliegt. Diese Schwierigkeiten würden vermieden werden, wenn entsprechend der Begrifflichkeit des BDSG von „personenbezogenen Daten" die Rede wäre, wie es auch in § 203 Abs. 2 Satz 2 StBG der Fall ist, wo „Einzelangaben über persönliche oder sachliche Verhältnisse eines anderen" (vgl. § 2 Abs. 1 BDSG) einem Geheimnis im Sinne des § 203 Abs. 1 StGB gleichgestellt werden.

  Wegen des unterschiedlichen Anwendungsbereichs des BDSG und des SGB wären allerdings neben den personenbezogenen Daten — wie bisher — auch die „Betriebs- und Geschäftsgeheimnisse" zu nennen.

— Vorstellungen eines in sich geschlossenen Systems der sozialen Sicherung mit der Folge einer generellen Privilegierung der Datenübermittlung innerhalb der Sozialverwaltung (bei gleichzeitiger „Abschottung" derselben nach außen) sind weder tatsächlich noch datenschutzrechtlich noch rechtspolitisch haltbar.

  Tatsächlich finden Datenübermittlungen sowohl innerhalb der Sozialverwaltung wie nach außen in zahlreichen Fällen statt, in denen dies zur Aufgabenerfüllung der jeweiligen speichernden Stellen erforderlich ist; vgl. § 10 Abs. 1 Satz 1 BDSG, § 35 Abs. 2 SGB I. Datenschutzrechtliches Kriterium für die Zulässigkeit einer Datenübermittlung ist also die Erforderlichkeit derselben für die Erfüllung einer konkreten Aufgabe eines konkreten Trägers der Sozialverwaltung oder eines anderen Verwaltungsträgers. Die Erforderlichkeit wird also durch ein materielles Kriterium, nicht aber durch die formelle Zugehörigkeit zu einem Verwaltungsbereich bestimmt.

  So wenig es im Hinblick auf die Erforderlichkeit einer Datenübermittlung für die Aufgabenerfüllung eine „Einheit der Sozialverwaltung" gibt, so wenig gibt es eine solche „Einheit" für Teilbereiche der Sozialverwaltung, z. B. für die Sozialversicherung oder für die Arbeitsverwaltung. Die Aufgabenerfüllung derartiger Teilbereiche der Sozialverwaltung richtet sich nach teils übereinstimmenden, teils aber auch gesonderten Zielvorgaben. Folglich kann auch für einen solchen Teilbereich nicht von einem einheitlichen Begriffsinhalt der Erforderlichkeit (der Datenübermittlung für die Aufgabenerfüllung) ausgegangen werden. Nur eine Prüfung im konkreten Einzelfall kann ergeben, ob eine und welche Datenübermittlung von einer speichernden Stelle an eine andere zur Aufgabenerfüllung erforderlich ist.

  Schließlich ist gegenüber Einheits-Vorstellungen noch darauf hinzuweisen, daß die Übermittlung von Daten selbst dann den Regeln für die Datenübermittlung unterfallen kann, wenn zwei Teile derselben Behörde oder sonstigen öffentlichen Stelle (§ 1 Abs. 2 Nr. 1 BDSG) beteiligt sind. Auch die Datenübermittlung innerhalb einer Behörde kann eine Übermittlung an Dritte sein, und zwar insbesondere dann, wenn die Teile verschiedene Aufgaben haben oder für einen anderen räumlichen Bereich zuständig sind (vgl. §§ 1 Abs. 2 Satz 2, 2 Abs. 3 Nr. 2 BDSG; Artikel 17 Abs. 3 BayDSG; § 14 Abs. 3 Saarl. DSG; § 8 Satz 1 DSG NW).

Rechtspolitisch — darauf habe ich wiederholt hingewiesen — ist davon auszugehen, daß die Technologie entscheidungsneutral ist und Einheits-Vorstellungen nicht stützt: Datenverarbeitung ist heute zentral wie dezentral möglich. Die Entscheidungsfreiheit, die vor zehn Jahren durch den damaligen Technologiestand noch eingeengt war, ist zurückgewonnen worden. Vorstellungen von einer „Einheit" der Verwaltung oder von Verwaltungsteilbereichen, die einen inzwischen überholten technologischen Entwicklungsstand widerspiegeln, der die Zentralisierung begünstigte, weil er dezentrale Lösungen noch nicht wie heute ermöglichte, können keine brauchbare Entscheidungshilfe mehr sein.

— Eine generelle Regelung der mutmaßlichen Einwilligung — als Rechtfertigung zur Offenbarung von Sozialdaten — im Sozialgesetzbuch ist problematisch, weil § 3 Satz 2 BSDG — von besonderen Umständen abgesehen — für die Einwilligung des Betroffenen die Schriftform verlangt.

  Bereichsspezifische Regelungen wie § 35 SGB I sollten grundsätzlich nicht hinter den Anforderungen des allgemeinen Datenschutzrechts zurückbleiben. Ob es Einzelfälle gibt, aus denen die Notwendigkeit einer Ausnahmeregelung hergeleitet werden könnte, bedarf sorgfältiger Prüfung.

— Die Vielgliedrigkeit des Systems der sozialen Sicherung bringt es mit sich, daß Sozialdaten, die bei der Inanspruchnahme eines Arztes, sei es eines frei praktizierenden, sei es eines Krankenhausarztes, erhoben werden, durch die für die Funktionsfähigkeit der sozialen Sicherung erforderlichen vielfältigen Übermittlungen im Ergebnis weniger geschützt sind als beim Arzt: während etwa der Arzt, seine berufsmäßig tätigen Gehilfen und die bei ihm zur Vorbereitung auf den Beruf Tätigen ein Zeugnisverweigerungsrecht haben (vgl. §§ 53 Abs. 1 Nr. 3 StPO, 383 Abs. 1 Nr. 6 ZPO), während Aufzeichnungen und andere Gegenstände einschließlich der ärztlichen Untersuchungsbefunde nicht der Beschlagnahme unterliegen (vgl. § 97 Abs. 1 Nr. 2 und 3, Abs. 2 Satz 2 StPO), ändert sich die Rechtslage, sobald die bis dahin besonders geschützten Daten die Arztpraxis oder das Krankenhaus verlassen: dieselben Daten, die beim Arzt oder im Krankenhaus besonders geschützt werden, verlieren diesen Schutz, sobald sie in einen anderen Kontext gelangen. Dabei kann nicht bestritten werden, daß die Schutzwürdigkeit und Schutzbedürftigkeit dieser Daten nicht unterschiedlich ist, je nachdem, ob sie sich noch beim Arzt (oder im Krankenhaus) oder schon woanders befinden. Es ist daher zu fordern, daß Daten, die unter ein Zeugnisverweigerungsrecht und ein Beschlagnahmeverbot fallen, dieses Schutzes nicht verlustig gehen, weil sie aus der Sphäre erhöhten Schutzes in eine Sphäre gelangen, die de lege lata nicht in gleichem Umfang geschützt ist. Ihre Qualität ändert sich hierdurch nämlich nicht. Das Zeugnisverweigerungsrecht und das Beschlagnahmeverbot sind daher entsprechend zu erweitern. Ausgangspunkt einer entsprechenden Regelung muß also die Qualität der Daten, nicht aber ihr — zufälliger — Aufbewahrungsort sein.

§ 35 Abs. 1 SGB I zählt unter den zum Schutze der Sozialdaten Verpflichteten auch die Aufsichtsbehörden auf. Daß diese bei der Ausübung ihrer Aufsichtsbefugnisse auch Kenntnis von Sozialdaten erlangen müssen, liegt auf der Hand. Es gibt aber keine Rechtsvorschrift, die den in § 35 SGB I genannten Aufsichtsbehörden ausdrücklich gebietet, ihre Kenntnisse nur für Aufsichtszwecke (im Rahmen ihrer Aufsichtsbefugnisse) zu verwerten.

Die Gefahren, die sich hier für den Schutz der Sozialdaten auftun, sind groß. Sie werden noch steigen, wenn — wie z. Z. erwogen — die Aufsichtsbehörden nach einer Änderung des § 35 Abs. 2 SGB I zu den Leistungsträgern in den Kreis der privilegierten Amtshilfeberechtigten hinzutreten. Was das tatsächlich bedeutet, wird durch einen Blick auf die von § 35 SGB I erfaßten Sozialverwaltungsbereiche anschaulich: Hierher gehören die Ausbildungsförderung, die Arbeitsförderung, die Sozialversicherung, das soziale Entschädigungsrecht (also Kriegsopfer, Wehr- und Zivildienstgeschädigte, Impfgeschädigte, Opfer von Gewaltverbrechen), das Wohngeld, das Kindergeld, die Jugendhilfe und die Sozialhilfe. Zu den Aufsichtsbehörden für diese Aufgaben zählen die für Arbeit und Soziales, für Jugend, Familie und Gesundheit, für Kultus, Wissenschaft und Forschung sowie für Inneres zuständigen Ressorts. Es läßt sich leicht vorstellen, daß hier ein Anreiz bestehen könnte, Daten weiterzugeben.

Bei einer Novellierung des § 35 SGB I muß eindeutig klargestellt werden, daß das Geheimhaltungsgebot auch innerhalb der Leistungsträger und in gleicher Weise innerhalb der Aufsichtsbehörden, nämlich im Verhältnis der mit unterschiedlichen Aufgaben befaßten Organisationseinheiten oder Bediensteten zueinander, streng einzuhalten ist. Dies gilt erst recht für Aufsichtsbehörden, die neben Aufgaben der sozialen Sicherung auch andere Aufgaben wahrzunehmen haben. Es muß verhindert werden, daß z. B. eine Aufsichtsbehörde, die Teil der Behörde ist, die zugleich für den Verfassungsschutz zuständig ist, dem Verfassungsschutz Sozialdaten offenbart.

2.6.4 Infratest-Sozialforschung

Anläßlich der Kontrolle der Bundesanstalt für Arbeit stießen meine Mitarbeiter im Juni/Juli 1979 auf einen Vorgang, der sofort ihre Aufmerksamkeit weckte:

Das Bundeskabinett hatte in seiner Sitzung am 25. Mai 1977 beschlossen, eine empirische Untersuchung über die Effizienz der Arbeitsvermittlung zu vergeben. Der Bundesminister für Arbeit und Sozialordnung beauftragte daraufhin die Firma Infratest-Sozialforschung GmbH & Co. KG, diese Untersuchung in 25 ausgesuchten Arbeitsamtsbezirken durchzuführen. Die Bundesanstalt für Arbeit wurde

gebeten, den Mitarbeitern der Firma Infratest zur Durchführung des Forschungsauftrags bestimmte Daten (Name und Anschrift von 7 000 Arbeitslosen und früheren Arbeitslosen) zugänglich zu machen. In internen Vermerken lehnten die zuständige Fachabteilung und der Datenschutzbeauftragte der Bundesanstalt die Herausgabe der Daten ab, weil sie gegen § 35 SGB I verstoße; die Verantwortlichen bei der Bundesanstalt würden sich im Fall einer Weiterleitung der Daten strafbar machen: es könne nicht angehen, daß eine Einrichtung, mit der die Bundesanstalt nichts zu tun habe, geschützte Daten bekomme.

Der Präsident der Bundesanstalt richtete deswegen am 20. Oktober 1977 eine Rückfrage an den Bundesminister für Arbeit und Sozialordnung. Dieser teilte daraufhin mit, die Bundesregierung messe der geplanten Untersuchung außerordentlich großes Gewicht bei. Einer weiteren Verbesserung des Vermittlungssystems und der Vermittlungsmöglichkeiten komme entscheidende Bedeutung zu. Von dem Forschungsauftrag würden hierzu wichtige Hinweise ebenso erwartet wie auch die Gewinnung von Grundlagen für die weitere Gesetzgebungsarbeit. In diesem Sinne habe auch der Deutsche Bundestag im Zusammenhang mit der Verabschiedung des 4. Änderungsgesetzes zum Arbeitsförderungsgesetz die Bundesregierung in einer Entschließung aufgefordert zu prüfen, ob sich auf Grund der Ergebnisse der geplanten Untersuchung Änderungen des Arbeitsförderungsgesetzes empfählen (BT-Drucksache 8/1053). Eine entsprechende Auswertung der Untersuchung setze voraus, daß die Ergebnisse möglichst repräsentativ seien. Die einzige diesen Anforderungen gerecht werdende Möglichkeit hierfür biete die unmittelbare Übergabe der Adressen von Arbeitslosen und früheren Arbeitslosen an das von der Bundesregierung beauftragte Forschungsinstitut. Bei der gebotenen Güterabwägung zwischen der notwendigen Geheimhaltung und wichtigen öffentlichen Interessen sei im vorliegenden Fall das zwingende öffentliche Interesse für die Durchführung des vom Sozialforschungsinstitut vorgeschlagenen Verfahrens zur Beschaffung der Adressen der zu befragenden Personen zu bejahen. Allerdings sei eine vorherige Verpflichtung der an der Untersuchung beteiligten Mitarbeiter des Instituts sowie der Interviewer gem. § 1 des Verpflichtungsgesetzes (s. Artikel 42 des Einführungsgesetzes zum Strafgesetzbuch vom 2. März 1974 — Bundesgesetzblatt I S. 469 ff) erforderlich. Die Verpflichtung solle durch die Bundesanstalt für Arbeit vorgenommen werden.

Daraufhin wurden der INFRATEST-Sozialforschung von der Bundesanstalt für Arbeit Namen und Anschriften von

— 3 529 Arbeitslosen in 25 von der Bundesanstalt als repräsentativ ausgewählten Arbeitsamtsbezirken und

— 3 394 Abgängern aus Arbeitslosigkeit (Wiederbeschäftigten) in denselben Arbeitsamtsbezirken

zugänglich gemacht.

Ich halte dies für unzulässig. § 35 Abs. 1 SGB I, der hier auch für die Zeit nach Inkrafttreten des BDSG anzuwenden ist, schützt Geheimnisse, insbesondere die zum persönlichen Lebensbereich gehörenden Geheimnisse sowie die Betriebs- und Geschäftsgeheimnisse. Die unbefugte Offenbarung dieser Geheimnisse ist nach § 203 StBG strafbar. Daraus wird erkennbar, welchen Rang der Gesetzgeber dem Schutz des „Sozialgeheimnisses" eingeräumt hat.

Nun sind Name und Anschrift allein zwar in der Regel keine Geheimnisse im Sinne des § 35 SGB I. Es ist aber unstreitig, daß die Tatsache, arbeitslos zu sein oder gewesen zu sein, ein solches Geheimnis ist.

Nach § 35 Abs. 1 Satz 2 SGB I ist eine Offenbarung der zum persönlichen Lebensbereich gehörenden Geheimnisse dann nicht unbefugt, wenn

— der Betroffene zustimmt oder

— eine gesetzliche Mitteilungspflicht besteht.

Eine Zustimmung der Betroffenen ist nicht eingeholt worden. Der Bundesminister für Arbeit und Sozialordnung hat mir auch keine Vorschrift benennen können, aus der sich eine gesetzliche Mitteilungspflicht im Sinne des § 35 Abs. 1 Satz 2 SGB I ergibt, wonach die Offenbarung des Namens und der Anschrift in Verbindung mit dem Datum Arbeitslosigkeit befugt wäre.

Der Bundesminister für Arbeit und Sozialordnung macht geltend, angesichts des Ziels der Untersuchung habe an der Übermittlung von Namen und Anschriften der Arbeitslosen ein zwingendes öffentliches Interesse bestanden. Die Untersuchung sei zwingend geboten gewesen, um der Bundesregierung Kenntnisse zu vermitteln, die sie zur Bekämpfung der Arbeitslosigkeit unbedingt benötigt habe. Hierzu sei sie durch das Sozialstaatsgebot des Grundgesetzes rechtlich verpflichtet.

Ein zwingendes öffentliches Interesse ist indessen kein selbständiger Erlaubnistatbestand. Als Grund für eine Ausnahme von dem Geheimhaltungsgebot ist es vom Gesetzgeber zwar in den in § 7 Abs. 4 Satz 3 Arbeitsförderungsgesetz genannten Fällen zugelassen worden. Dort geht es jedoch um einen völlig anderen Sachverhalt, nämlich um Datenübermittlungen an Finanzbehörden zwecks Verfolgung bestimmter Steuerstraftaten, wenn daran ein zwingendes öffentliches Interesse besteht. Eine Übertragung dieses als Ausnahmeregelung formulierten Tatbestandes auf andere Sachverhalte ist wegen des Eingriffscharakters von Datenübermittlungen und der sich daraus ergebenden hochrangigen Bewertung der durch § 35 SGB geschützten Geheimnisse nicht möglich.

Ich kann auch nicht akzeptieren, daß eine Notlage bestanden hätte, die — etwa unter Übernahme des den §§ 34, 35 StGB zugrunde liegenden Rechtsgedankens — als Rechtfertigung für gesetzwidriges Handeln herangezogen werden könnte. Ungeachtet dessen, ob eine solche Argumentation außerhalb des Strafrechts überhaupt zulässig ist, war die schwierige Arbeitsmarktlage wohl kaum mit einer Gefahr für hochrangige Rechtsgüter vergleichbar, wie sie etwa das Strafrecht als Rechtfertigungs-

oder Entschuldigungsgrund für tatbestandsmäßige Gesetzesverletzungen anerkennt.

Der Bundesminister für Arbeit und Sozialordnung hat für sein Vorgehen ferner geltend gemacht, die Untersuchung habe repräsentativ sein müssen. Viele Personen seien zwar zu einem sofortigen Interview bereit, wenn der Befrager selbst sie darum bitte, gäben aber nicht im voraus einer dritten Person ihre Zustimmung zu einem Interview, das erst Tage oder Wochen später stattfinden würde. Die Repräsentativität sei also bei gesondert vorausgehender Zustimmung angesichts der zu erwartenden hohen Weigerungsquote nicht erreichbar gewesen. Es habe sogar die Gefahr bestanden, daß wichtige Problemgruppen aus Verweigerungsgründen, die mit ihrem Problem zusammenhingen, nicht erkannt worden wären. Es komme noch hinzu, daß die Bereitschaft zur Zustimmung gegenüber Vertretern einer wissenschaftlich arbeitenden Institution größer sei als gegenüber Beamten des Arbeitsamtes.

Diese Erwägungen können nach der dargestellten Rechtslage als Rechtfertigungsgrund nicht durchgreifen. Davon abgesehen ist es auch nicht überzeugend, wenn behauptet wird, daß die Zustimmung schwierig zu erlangen gewesen wäre. Denn wie der Bundesminister für Arbeit und Sozialordnung selbst betont, ist die anschließende Erhebung der Daten durch das Sozialforschungsinstitut nach ausdrücklicher vorheriger Belehrung über die Freiwilligkeit erfolgt. Die Ausfallqoute nach dieser Belehrung war so gering, daß sie die Repräsentativität der Untersuchung nicht beeinträchtigt hat. Ein solches Verhalten der Befragten liegt schon deshalb nahe, weil es ihrer Interessenlage entsprach, nach Kräften dazu beizutragen, durch ihre Unterstützung der Untersuchung den Zustand der Arbeitslosigkeit für sich und andere möglichst zu beseitigen oder zu verkürzen.

Angesichts dieser Umstände ist die Vermutung nicht verständlich, daß dieselben Personen — nach entsprechender Belehrung über den Sinn der Untersuchung — der Bundesanstalt für Arbeit ihre Zustimmung verweigert hätten, Name, Anschrift und die Tatsache der (früheren) Arbeitslosigkeit dem Sozialforschungsinstitut mitzuteilen, damit auf dieser Grundlage die Befragungsaktion erfolgen konnte.

Der Verstoß gegen § 35 SGB I wird zwar hinsichtlich seiner Auswirkungen dadurch gemildert, daß die Bundesanstalt für Arbeit gemäß dem Erlaß des Bundesministers für Arbeit und Sozialordnung vom 7. November 1977 die Verantwortlichen der Infratest-Sozialforschung nach § 1 Verpflichtungsgesetz vom 2. März 1974 (Artikel 42 EGStGB — BGBl. I S. 469, 547 f.) verpflichtet hat. Diese Verpflichtung ersetzt allerdings nicht die fehlende Zulässigkeitsvoraussetzung für die Datenübermittlung.

Für den Bundesminister für Arbeit und Sozialordnung waren die arbeitsmarktpolitischen Gründe ausschlaggebend. Für die Zukunft strebt er an, § 35 SGB I so zu ergänzen, daß eine Offenbarung — wie im vorliegenden Fall — ausdrücklich für zulässig erklärt wird. Es bleibt abzuwarten, ob und in welchem Umfang diese Absicht verwirklicht wird; die Beurteilung nach geltendem Recht bleibt hiervon unberührt. Auch nach einer Novellierung des § 35 SGB I soll der Schutz der Sozialdaten einen sehr hohen Stellenwert behalten; hierin weiß ich mich mit dem Bundesminister für Arbeit und Sozialordnung einig.

2.6.5 Arbeitsverwaltung

Einer der Schwerpunkte meiner Tätigkeit im Jahre 1979 betraf Datenschutzprobleme in der Arbeitsverwaltung. Maßgebend dafür waren die hohe Zahl von Bürgereingaben und die — jedenfalls in der Vergangenheit — oft unbefriedigende und langwierige Beantwortung der Eingaben durch die Bundesanstalt für Arbeit. Um mir einen ersten Überblick über diese komplexe und vielfach gegliederte Verwaltung mit über 50 000 Mitarbeitern zu verschaffen, habe ich ihre Arbeitweise zunächst vor Ort in einem Arbeitsamt untersuchen lassen. Darauf aufbauend habe ich eine erste Teilüberprüfung der Hauptstelle der Bundesanstalt vornehmen lassen. Im einzelnen wurden folgende Stellen der Arbeitsverwaltung besucht:

- Arbeitsamt Bad Kreuznach (3 Tage, 2 Mitarbeiter)
- Hauptstelle der Bundesanstalt für Arbeit in Nürnberg und Landesarbeitsamt Nordbayern (2 Wochen, 2 Mitarbeiter)
- Zentralarchiv für ärztliche Gutachten der BA in Holzkirchen bei München (1 Tag, 2 Mitarbeiter)
- Arbeitsamt Essen (1 Tag, 1 Mitarbeiter)
  (unangemeldete Überprüfung der Vermittlungskartei anhand einer Einzelangabe)
- Arbeitsamt Marburg (1 Tag, 2 Mitarbeiter)
  (Diskussion der Pilotanwendung der halboffenen Arbeitsvermittlung)
- Arbeitsamt Bonn
  (Überprüfung eines Fortbildungskurses im Rahmen des AFG).

Ich habe bei dieser Vielzahl von Kontakten mit der Arbeitsverwaltung, bei unterschiedlichen Auffassungen in Sachfragen, durchweg gute Erfahrungen gemacht. Leitung und Mitarbeiter der Bundesanstalt waren kooperations- und auskunftsbereit; die Bundesanstalt hat in ihrer Reaktion auf meine Prüfberichte viel Entgegenkommen gezeigt. Ich bin zuversichtlich, daß die gegenwärtig gute Atmophäre erhalten bleibt und auch in Zukunft eine konstruktive Zusammenarbeit ermöglicht.

Die Überprüfungen haben folgende Ergebnisse gebracht.

a) Arbeitsamt Bad Kreuznach

Bei diesem Arbeitsamt handelt es sich um eine Dienststelle mittlerer Größe mit etwa 215 Mitarbeitern. Im Bezirk des Amtes leben etwa 285 000

Einwohner, davon rd. 92 000 abbhängig Beschäftigte. Die Arbeitslosenquote betrug 6,1 %.

Die wichtigsten Aufgaben der örtlichen Arbeitsverwaltungen, die Arbeitsvermittlung und die Berufsberatung werden bis jetzt noch in manuellen Verfahren abgewickelt. Die wichtigsten automatisierten Anwendungen sind die Zahlbarmachung von Leistungen, Statistiken, die computergestützte Arbeitsvermittlung für qualifizierte Berufe (gegenwärtig noch bei den Landesarbeitsämtern) und die Auswertung von Standardtests des psychologischen Dienstes.

Die erforderliche Rechenkapazität stellt das Zentralamt bei der Hauptstelle der Bundesanstalt zur Verfügung. Herr des Verfahrens ist die Hauptstelle, d. h. bei ihr liegen die Entwicklung und Durchführung der EDV-Verfahren. Entsprechend diesem vergleichsweise geringen Automatisierungsgrad liegt das Schwergewicht der Datenschutzprobleme in der Handhabung der manuellen Verfahren.

Vermittlungskartei

Jeder Arbeitslose wird bei seinem ersten Kontakt mit dem Amt in diese Kartei aufgenommen. Die umfangreichen Angaben der Arbeitslosen werden ergänzt durch Vermerke des Sachbearbeiters. In die als Tasche ausgestaltete Karteikarte können verschiedene zusätzliche Papiere eingelegt werden, z. B. ärztliche und psychologische Gutachten. Je nachdem, wie häufig ein Arbeitsloser Kontakt mit dem Arbeitsamt hat, können so umfangreiche Dossiers mit sehr eingehenden Details entstehen. Bedenken ergeben sich zusätzlich aus der langen Lebensdauer der Vermittlungskarten. Wenn etwa ein Arbeitnehmer im Abstand von mehreren Jahren erneut arbeitslos wird, lebt die alte Karte, z. B. auch mit alten Gutachten, wieder auf. Bei dem besuchten Arbeitsamt war die Kartei in nicht verschließbaren Schränken untergebracht — die Schlüssel waren im Laufe der Jahre abhanden gekommen.

Die Arbeitsverwaltung hat es in der Vergangenheit abgelehnt, betroffenen Arbeitslosen Auskunft aus der Kartei gem. § 13 BDSG zu geben, weil es sich nur um „verwaltungsinterne Arbeitsmittel" handle. Die Bundesanstalt für Arbeit hat diese Position inzwischen aufgegeben. Damit ist erfreulicherweise die volle Anwendbarkeit des BDSG auf die wichtigsten manuellen Dateien der Arbeitsämter nicht mehr bestritten.

Es bleiben aber im Zusammenhang mit dieser Kartei eine Reihe von Problemen, die dringend klärungsbedürftig sind. Die Aufbewahrungsfristen für die Vermittlungskarten sind zu lang, es fehlen präzise Löschungsfristen. Bei der gegenwärtigen Praxis sind so Fälle denkbar, wo einem Arbeitslosen aufgrund des über ihn angelegten umfangreichen Dossiers jede faire Chance für eine weitere Vermittlung genommen ist. Die Bundesanstalt ist zur Zeit dabei, neue Lösungen zu erarbeiten.

Entbindung von der ärztlichen Schweigepflicht

Der ärztliche Dienst des Arbeitsamtes Bad Kreuznach benutzte ein Formular, in dem folgende Erklärung verlangt wurde:

„Ich befreie hiermit alle Ärzte, die mich behandelt haben oder begutachtet haben, von ihrer ärztlichen Schweigepflicht und bin damit einverstanden, daß sie die Befunde (etc.), die sie über mich besitzen, zur Sachaufklärung, Vermeidung von Doppeluntersuchungen und Einsparung von Unkosten miteinander austauschen."

Diese pauschale Entbindung von der ärztlichen Schweigepflicht ist zu weitgehend und widersprach im übrigen einem einschlägigen Erlaß der Bundesanstalt. Die Bundesanstalt hat die ihr unterstellten Behörden angewiesen, derartige Formulare nicht weiter zu benutzen.

Gutachten und Tests beim psychologischen Dienst

Anforderungen von psychologischen Gutachten oder Eignungsuntersuchungen gehen ein von der Berufsberatung, der Arbeitsvermittlung, der Verwaltung (bei Einstellung eigenen Personals) und der Leistungsabteilung. Einige Standard-Eignungstests werden beim Zentralamt in Nürnberg maschinell ausgewertet. Die Ergebnisse dieser Tests gehen danach an die örtlichen Berufsberatungen zurück.

Im untersuchten Arbeitsamt waren die Gutachten und Testunterlagen des Psychologischen Dienstes nur mangelhaft gesichert. Dies ist um so gravierender, als die Unterlagen des Psychologischen Dienstes gegenwärtig noch 15 Jahre aufbewahrt werden, das Material somit Generationen von z. B. Schulabgängern und Umschülern nachweist.

Die Bundesanstalt hat zugesagt, diese Mängel bis Ende des Jahres 1979 zu beheben.

b) Hauptstelle der Bundesanstalt für Arbeit in Nürnberg

Zwar kann eine zweiwöchige Überprüfung durch zwei meiner Mitarbeiter nur einen ersten Eindruck vermitteln. Dabei ergaben sich allerdings teilweise gravierende Mängel in der Konzeption des Datenschutzes.

Interne Übersicht nach § 15 Nr. 1 BDSG

Die Bundesanstalt für Arbeit konnte keine den Anforderungen des § 15 Nr. 1 BDSG genügende Übersicht vorlegen. Insbesondere fehlte in den vorgelegten, als solchen durchaus brauchbaren Unterlagen eine Bestandsaufnahme der manuellen Dateien — ein Umstand, der angesichts des gegenwärtig noch eher geringen Automatisierungsgrads besonders ins Gewicht fällt. Die Bundesanstalt hat zugesagt, die Mängel umgehend zu beseitigen. Es war so nicht möglich, auf gesicherter Grundlage darüber zu befinden, ob die ordnungsgemäße Anwendung der DV-Programme (§ 15 Nr. 2 BDSG) kontrollierbar ist und die Datensicherungsanforderungen der Anlage zu § 6 BDSG erfüllt sind.

Interner Datenschutzbeauftragter

Die unmittelbar dem Präsidenten der Bundesanstalt unterstellte Organisationseinheit des Datenschutzbeauftragten war personell unterbesetzt, die Qualifikationen wegen unzureichender EDV-Kenntnisse

nicht optimal. Da der Datenschutzbeauftragte an den Besprechungen der Abteilungsleiter nicht teilnahm, erfuhr er häufig zu spät von Neuerungen und hatte Schwierigkeiten, sich mit den Belangen des Datenschutzes gegenüber den Abteilungen durchzusetzen. Die Bundesanstalt hat meine Anregung, die Stelle des Datenschutzbeauftragten personell und qualifikationsmäßig besser auszustatten, aufgegriffen. Aus mir nicht bekannten Gründen sind die Bemühungen der Bundesanstalt jedoch teilweise bereits in den Haushaltsberatungen der Selbstverwaltungsorgane gescheitert.

Auch die Selbstverwaltungsorgane sollten sich der Einsicht nicht verschließen, daß es praktisch unmöglich ist, Datenschutz mit nur vier Mitarbeitern in einer so umfangreichen, vielfältig gegliederten Verwaltung verwirklichen zu wollen.

Psychologischer Dienst

Meine Mitarbeiter haben nur einen Teil der dortigen Aufgaben näher betrachten können. Folgende Einzelprobleme möchte ich besonders hervorheben:

— Einverständniserklärung der Betroffenen

Die Bundesanstalt hat in der Vergangenheit psychologische Tests auch ohne ausdrückliche schriftliche Einwilligung der Betroffenen veranstaltet und eine lediglich konkludente Einwilligung genügen lassen. Die entsprechenden Formulare enthielten darüber hinaus noch nicht die gem. § 9 Abs. 2 BDSG erforderliche Rechtsaufklärung. Die Tests und Gutachten und die Speicherung der daraus gewonnenen Daten sollen nunmehr nur noch mit schriftlicher Einwilligung stattfinden. Die Bundesanstalt hat eine Neuregelung des Verfahrens für Ende des Jahres 1979 angekündigt.

— Aufbewahrungsfristen für psychologische Testunterlagen und Gutachten.

Die Unterlagen werden gegenwärtig weit über zehn Jahre aufbewahrt — eine Frist, die angesichts der besonderen Sensibilität und der zeitlich begrenzten Aussagefähigkeit des gespeicherten Materials zu lang ist. Bei der Überprüfung hat sich überdies herausgestellt, daß Bänder mit Daten eines bestimmten Tests unendlich gesperrt waren, d. h. eine Löschung war nicht vorgesehen. Ich habe die Bundesanstalt aufgefordert, umgehend und differenziert nach den jeweiligen Verwendungszwecken dieser Daten eine datenschutzgerechte Regelung der Löschungsfristen zu realisieren.

— Verhältnis psychologischer Fachdienst — EDV-Abteilung

Der psychologische Fachdienst konnte keine schriftlichen Unterlagen vorlegen, in denen die Informationsbeziehungen zum zuständigen EDV-Referat präzis festgehalten werden. Der Fachdienst, der sich nicht als „Herr der Daten" fühlte, war nicht in der Lage, die genaue Anzahl der Dateien, die genaue Satzzahl, den Satzaufbau und die Datensicherungsmaßnahmen anzugeben. Es war auch möglich, daß die EDV-Abteilung eine große Anzahl von ad-hoc-Aufträgen für Programmentwicklungen oder Auswertungen ohne ausreichend detaillierte Vorgaben der Fachabteilung in Angriff nehmen konnte. Die Initiative ging dabei eher von der EDV-Abteilung als von der eigentlich verantwortlichen Fachabteilung aus. Bei diesem Sachverhalt war eine den Anforderungen von Nr. 10 der Anlage zu § 6 Abs. 1 Satz 1 BDSG entsprechende Organisationskontrolle nicht möglich. Die unbestritten bestehenden generellen Erlasse und Dienstanweisungen können diese tatsächlichen Kommunikationsmängel nicht ausgleichen.

Computergestützte Arbeitsvermittlung

Für bestimmte, besonders qualifizierte Berufe betreiben die Landesarbeitsämter eine „Computergestützte Arbeitsvermittlung". Über dieses Verfahren haben sich meine Mitarbeiter beim Landesarbeitsamt Nordbayern informiert. Bei dem eingesetzen Terminalsystem, das in absehbarer Zeit durch ein anderes, bei den einzelnen Arbeitsämtern installiertes System abgelöst wird, bestand keine ausreichende Zugriffs-, Eingabe-, Zugangs- und Abgabekontrolle. Wegen der bevorstehenden Umstellung habe ich darauf verzichtet, diese Mängel förmlich zu beanstanden.

Datenabgleich beim Arbeitserlaubnisverfahren für Ausländer

Der Datenschutzbeauftragte eines Düsseldorfer Unternehmens hatte sich mit der Bitte an mich gewandt, die Rechtmäßigkeit des Vorgehens der Arbeitsämter im Arbeitserlaubnisverfahren für ausländische Arbeitnehmer zu überprüfen.

Das Arbeitsamt Düsseldorf hat an Unternehmen Vordrucke versandt, die folgenden Satz enthielten: „Da ab 1. April 1978 die Überwachung des Arbeitserlaubnisverfahrens mit Hilfe der EDV erfolgt, benötige ich die Versicherungsnummer der ausländischen Arbeitnehmer." Mit diesen Vordrucken wollte das Arbeitsamt Daten für ein automatisches Verfahren erheben, ohne daß dafür eine Anweisung der Hauptstelle bestand. Das Versenden der Vordrucke wurde auf meine Initiative eingestellt. Dies war deshalb problemlos, weil die Arbeitsverwaltung die Versicherungsnummern inzwischen auf anderem Wege erhält.

Bei der Überprüfung dieses Verfahrens in der Hauptstelle ergab sich darüber hinaus folgender, datenschutzrechtlich problematischer Sachverhalt:

In der Bundesanstalt findet ein maschineller Abgleich „Ausländer" statt. Es werden dabei Daten über die Beschäftigungsverhältnisse, die gem. §§ 10, 178 AFG in Verbindung mit der DEVO/DÜVO erhoben werden, mit solchen Angaben verglichen, welche die Bundesanstalt im Rahmen des Arbeitserlaubnisverfahrens gem. § 19 AFG erhält. Auf diese Weise sollen ausländische Arbeitnehmer, die ohne Arbeitserlaubnis beschäftigt werden, herausgefunden werden. Es stellt sich so das grundlegende Problem, ob die Bundesanstalt Daten, die sie für einen bestimmten Zweck rechtmäßig erlangt hat, auch ohne ausdrückliche Rechtsgrundlage für einen anderen Zweck benutzen darf. Diese Frage ist im Grundsatz zu verneinen. Die Bundesanstalt

kann sich für ihre Rechtsauslegung auf einen Erlaß des Bundesministers für Arbeit und Sozialordnung vom 3. November 1977 berufen, wonach der Abgleich zulässig sei, weil er zur rechtmäßigen Erfüllung der Aufgaben erforderlich sei.

Ich bestreite nicht die Notwendigkeit als solche, derartige Aufgaben zu erledigen. Dies muß aber in rechtlich einwandfreier Form geschehen. Ich halte das Verfahren schon deshalb für bedenklich, weil hier eine Aufgabe der eingreifenden Verwaltung mit den Mitteln der Leistungsverwaltung erfüllt wird, ohne daß dieses den Betroffenen bekannt ist. Zudem sind die entsprechenden Veröffentlichungen nach § 12 Abs. 1 BDSG unrichtig, weil dieser Zweck nicht angegeben ist.

Dieser Fall belegt, wie problematisch sog. Datenabgleiche schon innerhalb einer einzigen Organisation sein können. In einem ähnlich gelagerten Fall hat die Bundesanstalt auf meine Beanstandung hin ein entsprechendes Verfahren eingestellt. Hier ging es um den Datenabgleich der Versichertendatei mit der Leistungsempfängerdatei, um festzustellen, wer Leistungen von der Bundesanstalt bezieht, ohne anspruchsberechtigt zu sein.

c) Zentralarchiv für ärztliche Gutachten in Holzkirchen bei München

Die Bundesanstalt hat 1972 beim Arbeitsamt Holzkirchen auf Beschluß des Vorstandsausschusses für Rechts- und Verwaltungsfragen ein zentrales Archiv für ärztliche Gutachten errichtet. In dieses Archiv werden die bei den ärztlichen Diensten der einzelnen Arbeitsämter ausgesonderten Arztakten aufgenommen, die dort mikroverfilmt und archiviert werden. Der Bestand umfaßt derzeit etwa 4 Mio. Arztakten aus den Jahren 1965 bis 1974.

Die vorhandenen Sicherungsmaßnahmen sind angesichts der gelagerten hochsensiblen Daten unzureichend. Ich habe die Bundesanstalt aufgefordert, auch zu überprüfen, ob die Aufrechterhaltung des Archivs unter Kostengesichtspunkten — einschließlich der Kosten angemessener Sicherungsmaßnahmen — weiter vertretbar ist.

d) Arbeitsamt Essen

Eine Bürgerin hatte in einer Eingabe behauptet, das Arbeitsamt Essen verstoße in ihrem Fall gegen Bestimmungen des Datenschutzgesetzes. Ich habe die entsprechenden Dateien und Akten des Arbeitsamtes daraufhin — unangemeldet — überprüfen lassen. Die Ergebnisse waren teilweise besorgniserregend. In der als Tasche ausgestalteten Vermittlungskarte der betreffenden Bürgerin waren z. B. folgende Daten enthalten:

— mehrere ärztliche Gutachten, das erste datiert von 1970

— die erste Vermittlungskarte aus dem Jahre 1969

— ein Notizzettel, ohne Bearbeiter- oder sonstigen Vermerk, auf dem stand: „wird ausfallend", „wird beleidigend"

— ein unterschriebener Sachbearbeitervermerk mit irrelevanten Zitaten, wie „Sie müssen nicht schlauer sein als alle Professoren"

— ein Ausschnitt aus einer großen deutschen Zeitung mit einem Artikel über die psychischen Probleme der arbeitslosen Bürgerin; Überschrift: „Gerdas Kampf gegen die Isolation".

Wie Besuche bei anderen Arbeitsämtern gezeigt haben, sind dort die Vermittlungskarten frei von unsachlichen Eintragungen, z. B. beim Arbeitsamt Bonn. Auch bei der Aufbewahrung von Gutachten in der Vermittlungskarte gibt es offenbar eine unterschiedliche Praxis.

Die Arbeitsverwaltung ist aufgefordert, bei der geplanten Neukonzeption der Arbeitsvermittlung die Belange des Datenschutzes auch insofern zu berücksichtigen. Andernfalls besteht die Gefahr, daß in einer nicht bekannten Anzahl von Fällen Bürgern eine faire Chance für eine erfolgreiche Arbeitsvermittlung genommen ist.

e) Arbeitsamt Bonn

Im Rahmen von Arbeitsförderungsmaßnahmen hat das Arbeitsamt Bonn die Gesellschaft für wirtschaftsberufliche Bildung GmbH (GWB) in Bonn/Alfter beauftragt, für sog. schwer vermittelbare Arbeitslose einen besonderen Lehrgang zu entwikkeln. Rechtsgrundlage dieses Kurses ist die neu in das AFG eingeführte Vorschrift des § 41 a. Der Lehrgang, ein sog. Eignungs- und Motivierungskurs, verfolgt neben fachlichen auch psychologisch-therapeutische Ziele. Insbesondere werden im Verlaufe des Kurses verschiedene psychologische Tests veranstaltet. Am Ende des Lehrgangs soll dem zuständigen Arbeitsberater des Arbeitsamtes in einem Zeugnis über den Erfolg der Maßnahmen berichtet werden. Noch zwei Wochen vor Beginn des Kurses gab es keinerlei Regeln über die Verwendung, Übermittlung und Löschung der psychologischen Daten.

Auf meine Anregung hin haben die Beteiligten umgehend Maßnahmen eingeleitet, um wenigstens das Verfahren datenschutzgerecht zu gestalten:

— Die vertragliche Vereinbarung zwischen dem Arbeitsamt und der GWB wurde um eine Datenschutzklausel ergänzt. Darin verpflichtet sich die GWB, spätestens ein Jahr nach Lehrgangsende alle personenbezogenen Daten zu löschen; die Bundesanstalt ist berechtigt, die Einhaltung des Datenschutzes bei der GWB zu überprüfen.

— Die GWB veranstaltet psychologische Tests nur mit ausdrücklicher schriftlicher Einwilligung der Lehrgangsteilnehmer.

— Die Testdaten sind nur einigen, namentlich genannten Personen in der GWB zugänglich.

— Die Abschlußzeugnisse dürfen nur dem zuständigen Arbeitsberater zugänglich gemacht werden.

Dieser Einzelfall verweist auf Probleme von grundsätzlicher Bedeutung. Zunächst ist der Stellenwert

von psychologischen Tests und Gutachten im Rahmen von Arbeitsförderungsmaßnahmen noch ungeklärt. Problematisch ist es auch, wenn staatliche Aufgaben wie hier von einem privaten Träger erledigt werden, ohne daß ausreichender Einfluß auf die entstehenden Datensammlungen genommen wird — man denke etwa an die Probleme, die bei einem Konkurs eines privaten Trägers auftreten können. Ich werde darauf hinwirken, daß die Hauptstelle der Bundesanstalt die bei Lehrgängen der Arbeitsämter auftretenden datenschutzrechtlichen Probleme generell regelt.

f) Arbeitsamt Marburg

Zur Vertiefung der bei der Hauptstelle der Bundesanstalt und dem Landesarbeitsamt Nordbayern gewonnenen Eindrücke über das geplante Verfahren „Halboffene Arbeitsvermittlung" wurde ein Informationsbesuch beim Arbeitsamt Marburg durchgeführt, das für ein Pilotverfahren ausgewählt wurde. Das bei der Arbeitsverwaltung bestehende System der Datenerfassung mit maschinenlesbaren Belegen soll durch ein Terminalsystem abgelöst werden. Dieses Terminalsystem soll zusätzlich für eine Automatisierung der Arbeitsvermittlung genutzt werden. Der manuelle Vergleich von Stellengesuchen und Stellenangeboten wird durch den Dialog über Terminals ersetzt werden.

Bei dem Besuch wurde im Rahmen einer ausführlichen Information über den gegenwärtigen Stand des Projekts auch das Konzept für die Datensicherung vorgestellt. Die Bundesanstalt für Arbeit hat dem Hersteller Auflagen für die Entwicklung des Betriebssystems gemacht, die nach meinem ersten Eindruck geeignet sind, die Sicherheit des Verfahrens zu gewährleisten.

Eine weitere projektbegleitende Beratung durch meine Dienststelle ist vereinbart.

2.6.6 Verband Deutscher Rentenversicherungsträger (VDR)

Die wichtigsten beim Verband Deutscher Rentenversicherungsträger (VDR) mit Hilfe der elektronischen Datenverarbeitung durchgeführten Aufgaben sind:

- Sammeln der DEVO/DÜVO-Datenströme und Verteilen auf die Empfänger im Bereich der Sozialen Sicherung (z. B. Rentenversicherungsträger).
- Aufdecken und Verhindern von Doppel- und Mehrfachvergaben von Versicherungsnummern.
- Herstellen von Querverbindungen zwischen den Trägern der Rentenversicherung.
- Ermitteln der Versichertenbestände.
- Datenaustausch innerhalb der Europäischen Gemeinschaften.

Zur Erfüllung dieser Aufgaben werden zwei große Datenbestände geführt:

- die Stammsatzdatei mit etwas 45 Millionen personenbezogenen Datensätzen und
- die DEVO/DÜVO-Sicherungsdatei mit insgesamt bis zu 75 Millionen personenbezogenen Datensätzen.

Die Stammsatzdatei enthält die Versicherungsnummer, ein sog. Namenselement und Angaben über den zuständigen Versicherungsträger, Kontenstillegung, Verweisungen, die Betriebsnummer der Krankenkassen sowie ggf. Informationen für den Datenaustausch innerhalb der Europäischen Gemeinschaften. Im „Namenselement" war bis zum 1. Oktober 1979 neben dem Namen, Vornamen und Geburtsort auch die Anschrift enthalten. Zu diesem Zeitpunkt wurde sie auf meine Initiative hin durch eine Anschriftenvergleichszahl ersetzt. Eine ausführliche Diskussion unter den Versicherungsträgern sowie Testläufe hatten nämlich ergeben, daß sich meine Forderung, auf die Anschrift zu verzichten, realisieren ließ. Die Anschrift wird in eine Vergleichzahl umgesetzt, die bei der Verarbeitung zu gleichwertigen Ergebnissen führt, einen Rückschluß auf die Anschrift jedoch nicht zuläßt. Diese von der Rentenversicherung durchgeführte Maßnahme zeigt beispielhaft, wie durch den Verzicht auf Speicherung von lesbaren Informationen die Sensibilität von Datensammlungen verringert werden kann, ohne die Arbeitsergebnisse zu beeinträchtigen.

In der DEVO/DÜVO-Sicherungsdatei werden die Daten, die dem VDR von den Krankenkassen und den Arbeitgebern zugehen und an die zuständigen Versicherungsanstalten verteilt werden, gespeichert. Dies sind im Laufe eines Jahres bis zu 25 Millionen Sätze. Da zusätzlich zu den Sätzen des laufenden Jahres auch die der beiden davorliegenden Jahre aufbewahrt werden, ergibt sich ein Gesamtbestand von bis zu 75 Millionen Sätzen.

Nach Auffassung des VDR ist der Bestand aus folgenden Gründen erforderlich, die ich aber nicht akzeptieren kann:

- Eingabekontrolle.

  Nur aus der Sicherungsdatei lasse sich die Weiterleitungsstelle feststellen, welche die Daten von Krankenkassen gesammelt weitergibt. Tatsächlich läßt sich aber bereits aus der im Datensatz enthaltenen Betriebsnummer der absendenden Krankenkasse auf die zuständige Weiterleitungsstelle schließen.

- Aufklärung von Fehlern bei der Datenübermittlung.

  Mit der Sicherungsdatei könne eine schnelle und vollständige Berichtigung aller betroffenen Versicherungskonten durchgeführt werden, wenn bei der Datenübermittlung auf dem Wege von der Krankenkasse über den Verband zu den Versicherungsträgern Fehler entstehen.

  Derartige Fehler können aber m. E. nie vollständig ausgeschlossen werden. Wollte jede datennehmende Stelle deshalb die übermittelten Datensätze duplizieren und jahrelang aufbewahren, so würde dieses Verfahren zu einer unzu-

lässigen und aufwendigen zusätzlichen Datenspeicherung führen.

— Weiterleitung eingehender Meldungen mit stillgelegter Versicherungsnummer unter der aktuellen Versicherungsnummer.

Bei Eingang von Meldungen mit stillgelegter Versicherungsnummer werden diese mit aktueller Nummer weitergeleitet. Um bei Rückfragen nachvollziehen zu können, wer der Absender der Meldung ist, hält der VDR eine Protokollierung für erforderlich. Beim Versicherungsträger verweist jedoch die stillgelegte Versicherungsnummer stets auf die aktuelle Nummer. So kann festgestellt werden, wer die Veränderung der Daten veranlaßt hat.

— Durchführung der jeweils geltenden Bemessungsverordnung.

Nur mit den Sätzen der Sicherungsdatei sei es möglich, die Anzahl der Pflichtversicherten zur Durchführung der Bemessungsverordnung festzustellen.

Dazu ist aber nicht erforderlich, die Adressen in den Satz aufzunehmen.

Ich habe bei der Hauptabteilung IV des VDR in Würzburg eine einwöchige Überprüfung durchgeführt, um festzustellen, ob die bestehenden Dateien ausreichend gesichert und ob die für die Beibehaltung der DEVO/DÜVO-Sicherungsdatei angeführten Gründe stichhaltig sind.

Ohne verkennen zu wollen, daß der VDR bei seinen Bemühungen für mehr Datensicherheit beachtliche Erfolge zu verzeichnen hat, bin ich zu dem Ergebnis gekommen, daß die größte mir bekannte Sammlung personenbezogener Daten in der Bundesrepublik nicht ausreichend geschützt ist. Diese Beurteilung ist zu sehen vor einem besonderen Bewertungshintergrund: Datensammlungen dieses Umfanges bedürfen eines besonders zuverlässigen Schutz- und Sicherheitssystems. Ich habe den Verband aufgefordert,

— auf der Basis einer verbesserten Übersicht nach § 15 Nr. 1 BDSG eine Risiko- und Schwachstellenanalyse durchzuführen, die das Entwickeln eines Gesamtsystems ermöglicht,

— die organisatorische Transparenz der fünf Abteilungen des Verbandes zu verbessern,

— sicherzustellen, daß beim VDR nur solche Datenverarbeitungsaufgaben durchgeführt werden, die sich auf die gesetzlich festgelegten Aufgaben, insbesondere die Funktion als Clearingstelle, beschränken,

— Umfang und Inhalt der vorhandenen Datensammlungen auf ihre Erforderlichkeit zu überprüfen.

Diese Aufforderung gründet sich auf folgende Erwägungen:

— Projekt Raucherentwöhnungs-Therapie

Der Verband hat zusammen mit der Bundesversicherungsanstalt für Angestellte ein EDV-Verfahren entwickelt, das Aufschluß über die Wirksamkeit verschiedener Therapien geben soll. Es ist fraglich, ob der VDR überhaupt ein derartiges Projekt durchführen darf. Darüber hinaus wurden eine Reihe von Verstößen gegen Gebote der Datensicherung festgestellt. Ich habe den VDR aufgefordert, eine Einstellung des Projekts zu erwägen, zumal das Bundesversicherungsamt das entsprechende Projekt bei der Bundesversicherungsanstalt für Angestellte wegen fehlender Rechtsgrundlage beanstandet hat.

— DEVO/DÜVO-Sicherungsdatei

Ich habe den VDR aufgefordert, umgehend in seinen Gremien Wege zu suchen, die einen zentralen Sicherungsbestand dieser Größenordnung entbehrlich machen. Die vorgetragenen Argumente zur Beibehaltung der Datei haben mich nicht überzeugt. Die weitere Diskussion wird zeigen, ob auf den Bestand verzichtet, ob der Informationsgehalt reduziert oder ob die Aufbewahrungsdauer verkürzt und damit das Datenvolumen verringert werden muß. Die Speicherung der Anschriften halte ich für keinesfalls erforderlich; ich habe sie deshalb beanstandet.

— Schwächen in der Organisation des Datenschutzes

Die interne Übersicht nach § 15 Nr. 1 BDSG enthält reichhaltiges Material und gute Ideen, ihr Informationsgehalt reicht aber angesichts der Größe der vorhandenen Datensammlungen noch nicht aus. Da nicht für alle Anwendungen schriftliche Arbeitsaufträge erteilt werden, ist eine Kontrolle der ordnungsmäßigen Programmanwendung im Sinne von § 15 Nr. 2 BDSG nicht möglich. Auch eine wirkungsvolle Zugangskontrolle fehlt, u. a. weil der Kreis der Zutrittsberechtigten nicht genau definiert ist. Die Funktionstrennung innerhalb der Arbeitsvorbereitung ist nicht streng durchgeführt. Ich habe diese Mängel beanstandet.

2.6.7 Nachüberprüfung der Barmer Ersatzkasse

Die Barmer Ersatzkasse (BEK) in Wuppertal, eine der großen deutschen Ersatzkassen mit weit über 3 Millionen Mitgliedern habe ich bereits im Jahre 1978 überprüft. Über die Ergebnisse habe ich in meinem ersten Tätigkeitsbericht (siehe dort 3.5.3.2) berichtet. Wegen Meinungsverschiedenheiten in einigen, für mich zentralen Fragen und um festzustellen, welche konkreten Verbesserungen die Kasse schon realisiert hat, habe ich im Jahre 1979 eine eintägige Nachprüfung durchgeführt. Dieser Besuch hat eine einvernehmliche Klärung der in der Vergangenheit strittigen Fragen gebracht. Ich möchte folgende Punkte besonders erwähnen:

— Die Kasse hat eine vorbildliche Übersicht nach § 15 Nr. 1 BDSG erstellt.

— In meinem ersten Tätigkeitsbericht hatte ich die mangelhafte Datensicherung der Leistungskarten in den Geschäftsstellen der Kasse beanstandet. Die BEK hat daraufhin als Sofortmaßnahme den Kauf von mit Sicherheitsschlössern versehenen Büromöbeln veranlaßt. Sie wird darüber

hinaus in einer Umstellungsaktion, die ca. ein Jahr dauern wird, zukünftig die Leistungskarten in abschließbaren Behältnissen aufbewahren.

— In meinem ersten Tätigkeitsbericht hatte ich die unzureichende Sicherung von Rechenzentrum und Datenträgerarchiv beanstandet. Die BEK wird in den nächsten Monaten ein Einbruchsmeldesystem mit Polizeinotruf nach den Vorschriften des Verbandes der Sachversicherer installieren.

— Die BEK war in der Vergangenheit der Auffassung, bei den Leistungskarteien handele es sich nicht um Dateien im Sinne des Gesetzes.

Inzwischen besteht Einigkeit über die Anwendbarkeit des § 13 BDSG auch auf die manuell betriebene Leistungskartei. Die BEK praktiziert seit einiger Zeit ein — gebührenfreies — Auskunftsverfahren, bei dem grundsätzlich auch Diagnosedaten offenbart werden. In begründeten Ausnahmefällen ist eine Unterrichtung durch einen Arzt nach Wahl des Betroffenen vorgesehen.

2.6.8 DVDIS

Die Arbeitsgemeinschaft für Gemeinschaftsaufgaben der Krankenversicherung (AGK) in Essen hat im Berichtsjahr ihr Konzept für das System „Datenerfassung, Verarbeitung, Dokumentation und Informationsverbund in den sozialärztlichen Diensten mit Hilfe der elektronischen Datenverarbeitung" — DVDIS — (vgl. 1. TB, 3.5.1 a) weiter entwickelt. Das Forschungsvorhaben DVDIS will feststellen, wie die Arbeit des vertrauensärztlichen Dienstes durch die automatische Datenverarbeitung unterstützt werden kann. Zu diesem Zweck sollen einem Pilotprojekt maximal drei vertrauensärztliche Dienststellen angeschlossen werden.

Das Forschungsvorhaben DVDIS wird vom Bundesminister für Forschung und Technologie gefördert. An dem Bewilligungsverfahren der Mittel für die Zeit vom 1. Juli 1979 bis 30. Juni 1982 war meine Dienststelle beteiligt. Ich habe darauf hingewirkt, daß in den Bewilligungsbescheid folgende Bestimmungen aufgenommen wurden:

„Es ist sicherzustellen, daß

— die bisherigen Verantwortlichkeiten für die Daten in den vertrauensärztlichen Dienststellen nicht verändert werden,

— eine Zugriffsmöglichkeit über eine Leitung von außerhalb der Dienststelle, in der die Versicherten untersucht werden, nicht gegeben ist,

— eine Datenübermittlung von einer der in der Pilotphase hinzugezogenen vertrauensärztlichen Dienststellen nur in der Verantwortung der jeweils zuständigen Vertrauensärzte erfolgen darf.

Die Daten dürfen für keine anderen Zwecke als die des Forschungsvorhabens verwendet werden. Nach Abschluß von DVDIS sind die speziell hierfür gespeicherten Daten wieder zu löschen. Es ist zu prüfen, in welchem Umfang die Einwilligung des Betroffenen (§ 3 Satz 1 Nr. 2 BDSG) zur Grundlage der mit DVDIS bezweckten Untersuchung gemacht werden kann. Nach Möglichkeit ist von diesem Verfahren Gebrauch zu machen."

Ferner habe ich gegenüber den Beteiligten festgestellt, daß meine Stellungnahme im Rahmen der Förderung des Forschungsprojekts in keiner Weise als Präjudiz für eine spätere Entscheidung darüber verstanden werden darf, was aufgrund der mit dem Pilotprojekt gewonnenen Erkenntnisse zu veranlassen sein werde. In keinem Fall dürfe DVDIS als Wegbereiter einer Bürgerdatenbank (medizinisches Informationssystem) in zentraler oder dezentraler Organisationsstruktur angesehen werden, da derartige Unternehmungen datenschutzrechtlich auf immer größere Bedenken stießen. Hinzu kommt, daß die Aussagen über die mit DVDIS verfolgten Ziele bisher keine für eine abschließende Beurteilung ausreichende Konkretisierung erfahren haben.

2.6.9 Berufsgenossenschaft für den Einzelhandel

Das Datenschutzkonzept der Berufsgenossenschaft wies z. T. erhebliche Mängel auf. Es war nicht möglich, die „ordnungsgemäße Anwendung der Datenverarbeitungsprogramme" i. S. des § 15 Nr. 2 BDSG zu überwachen; wesentliche, in der Anlage zu § 6 Abs. 1 Satz 1 BDSG angeführte Anforderungen waren nicht erfüllt.

Im einzelnen waren folgende Mängel festzustellen:

— Die nach § 15 Nr. 1 BDSG geforderte Übersicht war unzulänglich und zum Teil falsch angelegt, weil der Begriff des personenbezogenen Datums verkannt wurde. Als Herr der Daten war fälschlicherweise die „EDV" und nicht die zuständige Fachabteilung angegeben.

— Die Programmdokumentation war unzureichend. Es fehlten Unterlagen über Systemkonzepte und deren Genehmigung durch die Fachabteilung, daraus abgeleitete Programmvorgaben und Datenflußpläne.

— Die Arbeitsablaufbeschreibungen waren ebenfalls unzureichend; es fehlten nachprüfbare Aufträge der Fachabteilungen, und es war nicht möglich, die Nutzung und Belegung der Datenträger nachzuprüfen und zu verfolgen.

— Wesentliche in der Anlage zu § 6 Abs. 1 Satz 1 BDSG genannte Anforderungen waren nicht erfüllt. Dies gilt insbesondere für die Regelung der Zutritts-, Abgangs- und Organisationskontrolle. Weder das Vier-Augen-Prinzip noch die Funktionstrennung noch der closed-shop-Betrieb waren gewährleistet.

Die Mängel waren insgesamt so gravierend, daß die Berufsgenossenschaft ein völlig neues Datenschutz- und Datensicherungskonzept entwickeln muß.

An diese Überprüfung hat sich eine inzwischen gute, konstruktive Zusammenarbeit angeschlossen. Meine Mitarbeiter haben gemeinsam mit dem Datenschutzbeauftragten der Berufsgenossenschaft

eine neue interne Übersicht entwickelt und ihn bei der Neukonzeption beraten, während die Mitarbeiter der Berufsgenossenschaft meiner Dienststelle bei der Klärung von Fachproblemen behilflich sind.

An diesem Beispiel zeigt sich, daß Überprüfungen sich nicht in bloßer Kritik erschöpfen sollten. Sie können bei Wahrung unterschiedlicher Standpunkte in ein fruchtbares gegenseitiges Beratungsgespräch übergehen.

2.6.10 Überprüfung des Bundeswehrzentralkrankenhauses Koblenz

Meine Kompetenzen im Bereich des Gesundheitswesens sind auf wenige Institutionen im Bereich des Bundes beschränkt. Um mir einen ersten Überblick über die Datenverarbeitung in einem Krankenhaus zu verschaffen, habe ich eine eintägige Überprüfung des Bundeswehrzentralkrankenhauses Koblenz durchgeführt. Da in diesem Krankenhaus auch Zivilpersonen behandelt werden, dürften die Eindrücke, die meine Mitarbeiter gewonnen haben, zu einem Teil auch auf andere Krankenhäuser übertragbar sein.

Die wichtigsten Informationsflüsse lassen sich wie folgt beschreiben:

Der Soldat als Patient hat eine Überweisung vom Truppenarzt, die er bei der Aufnahme vorlegt. Er füllt dort einen Anmeldevordruck aus. Die Daten werden in ein Laborsystem (SILAB) eingegeben. Die Überweisung und eine Adrema-Folie begleiten den Patienten in die Fachabteilungen. Dort werden alle Unterlagen mit der Folie beschriftet. Nach Entlassung geht ein Entlassungsbericht an den Truppenarzt. Die übrigen Unterlagen (Befunde etc.) gehen nach einer Übergangszeit in das Amt für Medizinalstatistik in Remagen. Dort werden nach Angabe des Krankenhauses z. Z. etwa 180 Millionen Urkunden (Krankenblätter, Befunde usw.) aufbewahrt. Die Aufbewahrungsfrist beträgt gegenwärtig 50 Jahre. Eine Mikroverfilmung dieser Unterlagen in naher Zukunft ist vorgesehen.

Der zivile Patient bringt bei seiner Einweisung eine Kostenübernahmeerklärung der Krankenkasse und eine Einweisung der Krankenkasse mit. Ansonsten gibt es im krankenhausinternen Informationsfluß keine Unterschiede zu den Soldaten.

Nach der Entlassung des Patienten werden personenbezogene Daten zu Abrechnungszwecken an die Krankenkasse weitergeleitet. Auch die Unterlagen der Zivilpatienten werden dem Amt für Medizinalstatistik in Remagen zugeleitet. Sie werden dort ca. 30 Jahre aufbewahrt.

Zum Zeitpunkt der Überprüfung wurde im Bundeswehrzentralkrankenhaus ein Laborsystem (SILAB) eingesetzt, das die Funktionen Patientenaufnahme und Laborauswertung miteinander verbindet. Das System SILAB soll Anfang 1980 durch ein neues System abgelöst werden, dessen Soll-Konzept zu einem Teilmodul „Patientenaufnahme" mir vorgelegt wurde. Nach meinen Feststellungen waren die Zugriffsregelung und die Übersicht nach § 15 Nr. 1 BDSG für das System SILAB nicht ausreichend. Auch fehlten Regelungen, welche die aus meiner Sicht zu langen Aufbewahrungsfristen für ärztliche Unterlagen deutlich verkürzen. Ich habe meine Bedenken zur Sprache gebracht und mit den Verantwortlichen einen weiteren Erfahrungsaustausch beim Aufbau des neuen Systems vereinbart.

2.6.11 Einzelfälle

Frage nach dem Einkommen

Zur Beurteilung der Berufs- bzw. Erwerbsunfähigkeit läßt die Bundesversicherungsanstalt für Angestellte ärztliche Gutachten erstellen. Dabei hat in einem Fall der Gutachter nach dem Einkommen des Ehegatten gefragt. Der Rentenantragsteller hat die Beantwortung dieser Frage verweigert und sich an mich gewandt mit der Bitte, bei der Bundesversicherungsanstalt für Angestellte zu klären, ob Angaben über die Höhe des Gehalts notwendig seien. Meine Rückfrage hat ergeben, daß diese Frage vom begutachtenden Arzt gestellt wurde, ohne daß dies von der Bundesversicherungsanstalt für Angestellte vorgesehen ist. Dies ist ein Beispiel dafür, daß die kritische Aufmerksamkeit des Betroffenen wesentlich dazu beitragen kann, das Datenschutzbewußtsein bei Stellen, die Daten erheben, zu stärken.

Anschriftenübermittlung zu Werbezwecken

Eine Ersatzkasse wandte sich seit Jahren an Betriebe, um Adressen von Auszubildenden für die Mitgliederwerbung zu erhalten. Die Weitergabe der Adressen vom Arbeitgeber an die Kasse einschließlich der zusätzlichen Information „Auszubildender" und „Arbeitgeber" erfolgte ohne Einverständniserklärung des Betroffenen. Ich habe der Krankenkasse mitgeteilt, daß ein solches Verfahren bedenklich sei. Die Kasse weist seitdem in ihrem Schreiben an die Ausbildungsbetriebe darauf hin, das Einverständnis der Betroffenen sei einzuholen.

Eine andere Ersatzkasse, die auf die gleiche Weise um Mitglieder geworben hat, konnte sich meiner Auffassung nicht anschließen, sie hat aber den Versand der Formschreiben bis aus weiteres eingestellt.

Ich werde zusammen mit den Landesbeauftragten auf ein einheitliches, datenschutzgerechtes Vorgehen hinwirken.

Offenbarung des Geburtsdatums, offener Versand von Mitteilungen

Ein Bürger hat sich bei mir darüber beschwert, daß auf Drucksachen einer Krankenkasse die Mitgliedsnummer, die u. a. das Geburtsdatum enthält, aufgedruckt ist.

Ich habe die Offenbarung des geschützten personenbezogenen Datums „Geburtsdatum" beanstandet und die Kasse zur Stellungnahme aufgefordert. Vorübergehende verwaltungstechnische Schwierigkeiten bei der Verfahrensumstellung, die ich nicht verkennen will, vermögen an dieser rechtlichen Beurteilung nichts zu ändern.

Die Bundesversicherungsanstalt für Angestellte hat sich meinen Bedenken gegen die offene Versendung von Versicherungsnummern inzwischen angeschlossen. Sie wird in Zukunft im Schriftwechsel mit natürlichen Personen keine offenen Postkarten mehr, sondern nur noch die Briefform benutzen.

Auch eine Berufsgenossenschaft hat sich inzwischen entschieden, auf die Versendung personenbezogener Daten mit Postkarte grundsätzlich zu verzichten. Für alle Einzelversendungen und die Versendung sensiblerer Daten werden von der Berufsgenossenschaft normale Briefe benutzt. Lediglich Massenvorgänge, die weniger sensible Daten enthalten, werden in Briefen verschickt, die mit Scheinverschlüssen oder Punktverschlüssen versehen sind. Dies kann akzeptiert werden, da das unbefugte Öffnen derartiger Umschläge unter Verletzung des Briefgeheimnisses erfolgt.

Vorlage des Mutterpasses

Seit einiger Zeit erhalten schwangere Frauen einen Pauschalbetrag von 100 DM, wenn sie während der Schwangerschaft und nach der Geburt die vorgeschriebenen Vorsorgeuntersuchungen vornehmen lassen. Einige Krankenkassen zahlen diesen Betrag nur aus, wenn der sog. Mutterpaß vorgelegt wird, ein Dokument, das zahlreiche personenbezogene Daten z. B. auch über Schwangerschaftsabbrüche, Geschlechtskrankheiten usw. enthalten kann. Gegen ein entsprechendes Verfahren einer Krankenkasse hat sich ein praktischer Arzt gewandt. Die Kasse hat meine datenschutzrechtlichen Bedenken akzeptiert und verlangt jetzt nur noch eine einfache schriftliche Erklärung der Wöchnerin, daß sie die vorgesehenen Untersuchungen hat vornehmen lassen bzw. vornehmen wird.

2.7 Verkehrswesen

Im Bereich des Verkehrswesens stand im Berichtszeitraum die Datenverarbeitung beim Kraftfahrt-Bundesamt im Vordergrund. Dort wurde eine Prüfung vorgenommen, die bereits wichtige Veränderungen ausgelöst hat. Besondere Aktualität erhält dieser Bereich durch das geplante Verkehrszentralregister-Gesetz und durch die weiteren Automationspläne des Kraftfahrt-Bundesamtes.

2.7.1 Kraftfahrt-Bundesamt

Die Überprüfung der Datenverarbeitung beim Kraftfahrt-Bundesamt (KBA) in Flensburg konzentrierte sich auf die beiden großen Datensammlungen personenbezogener Daten — die Datei der Kraftfahrzeuge mit amtlichem Kennzeichen und das Verkehrszentralregister (VZR, sogenannte Verkehrssünderkartei) — sowie auf die Organisation des Rechenzentrums.

Die Besonderheiten beim KBA liegen darin, daß es sich bei den Dateien um an zentraler Stelle geführte Datensammlungen handelt und daß aus diesen Datenbeständen in vielfältiger Weise Auskünfte an die unterschiedlichsten Stellen erteilt werden. Die Angaben zu dem Halterbestand erhält das KBA von den Zulassungsstellen. Die Meldungen zum VZR kommen von Gerichten, Bußgeld- und Führerscheinstellen. Alle diese Meldungen erfolgen aufgrund von Rechtsvorschriften und werden beim KBA zu Auskunftszwecken bereitgehalten sowie statistisch ausgewertet.

Die Datenübermittlung aus diesen zentralen Beständen bedarf einer besonders sorgfältigen und kritischen Beobachtung, weil die bereichsspezifische Vorschrift für die Auskunfterteilung aus dem VZR-Bestand lediglich die auskunftberechtigten Stellen beschreibt, aber nichts über den jeweiligen Umfang der Auskunft sagt, und weil eine bereichsspezifische Regelung für die Auskunftserteilung aus dem Halterbestand gänzlich fehlt. Auskünfte werden daher nach den allgemeinen Grundsätzen der Amtshilfe und nach Maßgabe der allgemeinen Übermittlungsregelungen des BDSG erteilt. Die Praxis der Handhabung der Auskunfterteilung erweist sich jedoch in verschiedener Hinsicht als problematisch.

Neben der Beantwortung von Anfragen an die Datenbestände veräußert das BKA auch Anschriften von Kfz-Haltern an Adreßverlage, jedoch nur dann, wenn der Betroffene bei der An- oder Ummeldung seines Fahrzeugs dazu ausdrücklich sein Einverständnis erteilt hat. Die Quote der Halter, die ihre Daten für Werbungs- und Meinungsforschungszwecke freigeben, hat in den letzten beiden Jahren ständig abgenommen und liegt jetzt bei 15 %. Das KBA wird damit als Datenlieferant für die Adreßverlage zunehmend unergiebiger. Die Frage, ob es überhaupt hingenommen werden soll, daß eine Behörde Daten, die sie für Verwaltungszwecke erhalten hat, an die Privatwirtschaft veräußert, hat an Dringlichkeit verloren.

Übersicht über die Art der gespeicherten Daten

Die Übersicht nach § 15 Nr. 1 BDSG war zu beanstanden. Nahezu alle Dateibeschreibungen müssen überarbeitet werden. Die Überprüfung ergab, daß zum Teil Angaben fehlten (z. B. über regelmäßige Datenempfänger) und zum Teil die Eintragungen unrichtig und unklar waren (z. B. wurden anstelle der Aufzählung der Datenarten globale Angaben oder Hinweise auf die Rechtsgrundlage gemacht; in anderen Fällen enthielt die Dateibeschreibung widersprüchliche Angaben). Außerdem habe ich festgestellt, daß nicht alle Dateien in der Übersicht aufgeführt waren; z. B. fehlte die Personaldatei.
An der Sorgfalt und an der Genauigkeit, mit der die Übersicht geführt wird, ist erkennbar, welche Bedeutung eine Behörde diesem zentralen Arbeitsmittel für die Realisierung des Datenschutzes beimißt. Ein umfassender Überblick über die ankommenden, in der Behörde umlaufenden und die abgehenden Informationsströme läßt sich kaum anders verschaffen. Ohne genaues Wissen, welche Wege die Informationen nehmen, ist eine systematische Risiko- und Schwachstellenanalyse nicht möglich. Diese wiederum ist Voraussetzung für Entscheidungen darüber, welche technischen und organisatorischen Maßnahmen zum Schutze der Daten erforderlich sind.

Nachweis der ordnungsgemäßen Anwendung der DV-Programme

Die nach § 15 Nr. 2 BDSG zu gewährleistende ordnungsgemäße Anwendung der Datenverarbeitungsprogramme konnte von mir nicht überprüft werden, da Dokumentations-Richtlinien, ein Rechenzentrum-Betriebshandbuch und Verfahrensregelungen zum Programmauftrag noch in der Entwicklung sind und erst 1980 angewendet werden sollen. Auf die Notwendigkeit, die erforderlichen Regelungen so schnell wie möglich zu schaffen und danach zu verfahren, habe ich mit Nachdruck hingewiesen.

Dagegen habe ich positiv zur Kenntnis genommen, daß die Mitarbeiter der Fachbereiche in Fort- und Weiterbildungsmaßnahmen das notwendige Verständnis für die Arbeitsweise der EDV erhalten, damit sie die Umsetzung der Anforderungen an die Datensicherheit in dem technischen Teil der Verfahrensabläufe verstehen und künftig verantwortlich bei der Freigabe von DV-Verfahren mitwirken können.

Kfz-Halterdatei

Für die detaillierte Untersuchung eines Verfahrensablaufs habe ich die Bestandsführung der Kfz-Halterdatei ausgewählt. Die Überprüfung dieses Verfahrens war deshalb angezeigt, weil in der Vergangenheit das KBA mehrfach dem Vorwurf ausgesetzt war, unzulässigerweise Anschriften an Adreßverlage veräußert und damit gegen Strafvorschriften des BDSG verstoßen zu haben. Dieser pauschale Vorwurf ist nach meinen Erkenntnissen unbegründet.

Bei der Überprüfung der Halterdatei habe ich festgestellt, daß die organisatorische Abwicklung von der Ankunft der auf Formularen und Magnetbändern gelieferten Daten bis zur Eingabe der Daten in die Speicher des KBA aus der Sicht des Datenschutzes klar und straff gegliedert ist. Der Umfang der Verarbeitung — allein etwa 50 000 Belege pro Tag — verlangt eine bis ins einzelne gehende Festlegung jedes Arbeitsschrittes. Insbesondere wird große Sorgfalt auf die korrekte Erfassung der Daten verwandt. Jeder Beleg wird nach der Übernahme auf magnetische Datenträger in einem zweiten Arbeitsgang durch nochmalige Eingabe und maschineninternen Datenvergleich auf fehlerfreie Erfassung geprüft.

Diese Prüfverfahren stellt in Verbindung mit den automatisierten Plausibilitätsprüfungen eine nahezu 100%ige Richtigkeit der eingegebenen Daten sicher. Angesichts der Menge der zu verarbeitenden Daten halte ich diesen Aufwand auch für erforderlich.

Das beschriebene Prüfverfahren bei der Datenerfassung wird in Ausnahmefällen aus Gründen der Arbeitsüberlastung insoweit eingeschränkt, als auf die Doppelerfassung von Name und Anschrift verzichtet und die Richtigkeit dieser beiden Angaben stichprobenweise durch manuellen Vergleich mit dem automatisch erstellten Kontrollausdruck überprüft wird. Unter den genannten Umständen und bei der Beschränkung auf die beiden Datenarten halte ich diese Regelung für vertretbar. Das verbleibende „statistische Restrisiko" für eine fehlerhafte Datenerfassung muß hingenommen werden. Mir sind während der vergangenen beiden Jahre nur verschwindend wenige Fälle bekanntgeworden, bei denen das KBA für eine falsche Datenerfassung verantwortlich war bzw. bei denen sich der Sachverhalt nicht mehr exakt rekonstruieren ließ und damit die Möglichkeit offenließ, daß die fehlerhafte Speicherung des Freigabevermerks durch das KBA verursacht worden war.

In Beschwerden über das KBA wurde häufig davon ausgegangen, daß die generelle Ursache für gezielte Werbeschreiben die Informationsweitergabe durch das Amt sei. Dabei wird jedoch außer acht gelassen, daß die Tatsache der Kfz-Halterschaft auch anderen Stellen bekannt ist; z. B. Händlern, Herstellern, Versicherungen, Automobilclubs, Werkstätten, Tankstellen usw.

In einigen von mir überprüften Fällen lag der Fehler bei den meldenden örtlichen Zulassungsstellen. Die Angabe zur Sperrung der Daten für die gewerbliche Adressenauswertung war aus dem An- bzw. Ummeldeformular falsch übertragen worden. Es kam auch vor, daß die Einwilligungserklärung von einem Beauftragten, jedoch nicht im Sinne des Betroffenen abgegeben wurde.

Unabhängig davon, ob ein Fehlverhalten vorliegt oder der Betroffene einfach seine einmal erteilte Einwilligung zurücknehmen möchte, kommt das Amt dem Verlangen des Betroffenen in jedem Fall nach, sperrt die Daten sofort für die weitere Veräußerung und fordert bei bereits übermittelten Anschriften den Adreßverlag auf, die Angaben in seinem Bestand zu löschen.

Für verbesserungsbedürftig wurden die Sicherungsmaßnahmen in den Erfassungsräumen befunden. Hier sind weitere organisatorische und technische Vorkehrungen erforderlich, um die Gefahr eines Mißbrauchs zu verhindern.

Auskunft aus den Halterbeständen

Da das KBA einen zentralen Datenbestand aller registrierten Fahrzeuge hat, erhält es zahlreiche Anfragen öffentlicher und privater Stellen zu Halterangaben über bestimmte Kraftfahrzeuge.

Um die Halter verkehrswidrig abgestellter, nicht mehr zugelassener, schrottreifer oder seit längerer Zeit unerlaubt parkender Fahrzeuge ermitteln zu können, haben z. B. Stadt- und Kreisverwaltungen, Universitäten, Parkhausbetriebe, Unternehmen, Flughafengesellschaften, Standortverwaltungen und in einem Fall auch ein ausländisches Landesforstinspektorat das KBA um Auskunft gebeten.

Aber auch Auskunftsbegehren, die sich nicht auf Verkehrsverstöße beziehen und nicht mit der Teilnahme am Straßenverkehr zusammenhängen, erhält und beantwortet das KBA. In diesen Fällen wird der Halterbestand als zentrales und vergleichsweise aktuelles Adreßregister benutzt; z. B. erfragt das Bundeskriminalamt (BKA) Anschriften von Personen, die mit Haftbefehl gesucht werden; erwartet das Bundesverwaltungsamt (BVA) Angaben über

den Wohnsitz von BAföG-Empfängern, die ihren Rückzahlungsverpflichtungen nicht nachkommen; will das BKA die Wohnanschriften von Personen erfahren, die sich im Ausland eine Waffe gekauft haben, um zu überprüfen, ob diese Personen im Inland gegen das Waffengesetz verstoßen oder als Waffenlieferanten für Straftäter in Frage kommen.

Für die Beantwortung der Anfragen durch das KBA gibt es keine spezielle Regelung. Auf § 26 Abs. 5 StVZO können Übermittlungen aus dem Halterbestand nicht gestützt werden, da dort als Auskunftsstellen nur die örtlichen Zulassungsstellen genannt sind. Daher ist bei der Prüfung der Zulässigkeit von Übermittlungen von den §§ 10 und 11 BDSG auszugehen. Bei ihrer Anwendung kann aber nicht außer Betracht bleiben, daß es sich bei der Halterdatei des KBA um einen zentralen Datenbestand handelt, der — als Ausnahme von dem Prinzip der dezentralen Ausführung von Verwaltungsaufgaben — für ganz spezielle Zwecke geschaffen wurde. Die Aufteilung der Verwaltungsaufgaben auf viele Behörden ist auch ein grundlegendes Datenschutzprinzip, weil damit zugleich die Verteilung der personenbezogenen Daten gesichert ist. Wird dieser Grundsatz aus besonderen Gründen einmal durchbrochen und werden die Daten zentral zusammengefaßt, so muß ihre Nutzung auf den zugrundeliegenden Zweck begrenzt bleiben, wenn es nicht zu Konsequenzen kommen soll, die nicht intendiert waren und deren datenschutzrechtliche Tragweite kaum zu übersehen wäre. Zusätzlich zu den in §§ 10 und 11 BDSG genannten Voraussetzungen muß deshalb eine Übermittlung aus zentralen Datenbeständen streng auf den ihrer Errichtung zugrunde liegenden Zweck begrenzt werden, soweit nicht vorrangige Rechtsvorschriften eingreifen.

Daher bestehen gegen die Beantwortung von Anfragen an den Halterbestand dann keine datenschutzrechtlichen Bedenken, wenn sie sich auf Verkehrsverstöße oder auf zivilrechtliche Ansprüche beziehen, die mit der Teilnahme am Straßenverkehr zusammenhängen. Soweit es an diesem Zusammenhang fehlt, habe ich Bedenken, weil es nicht Zweck dieses zentralen Bestandes ist, wie ein allgemeines zentrales Meldesystem zu wirken.

Ich habe mit dem KBA vereinbart, daß Anfragen, die auf der Basis dieser Regeln nicht beantwortet werden können, mit mir abgestimmt werden und daß eine Sammlung der schwierigeren Fälle angelegt wird, um eine generelle und tragfähige Lösung für die Auskunftserteilung in Abstimmung mit den beteiligten Behörden zu finden.

Da der Zweckbindungsgrundsatz noch keineswegs allgemein akzeptiert wird, halte ich eine bereichsspezifische Regelung für erforderlich. Für ihre Erarbeitung ist Eile geboten, weil zentrale Bestände allein auf Grund ihres Vorhandenseins eine stetig wachsende Nachfrage nach Anschriften auslösen; außerdem auch deshalb, weil die verschiedenen Datenbestände des KBA in einem Datenbanksystem zusammengefaßt werden sollen. Das neue Zentrale Verkehrsinformationssystem (ZEVIS) mit der Möglichkeit des Direktzugriffs durch andere Behörden ist projektiert und läuft bereits in einer Pilotanwendung. Die Datenverarbeitung beim KBA bekommt damit eine qualitativ andere Dimension, die vom Datenschutz her gesehen erhebliche Probleme mit sich bringt (vgl. dazu u. 2.7.2).

Verkehrszentralregister

Zum Verkehrszentralregister (VZR) werden von Verwaltungsbehörden und Gerichten Entscheidungen in Ordnungswidrigkeitenverfahren, über Beschränkungen der Fahrerlaubnis sowie über Verurteilungen im Zusammenhang mit der Teilnahme am Straßenverkehr gemeldet. Die eingehenden Meldungen werden in eine manuell geführte Hängeregistratur eingestellt, die nach Aktenzeichen geordnet ist. Daneben wird eine automatische Datei geführt mit Angaben zur Identifizierung der Person, dem Aktenzeichen und dem gültigen Tilgungsdatum. Die Benutzung dieser Index-Datei geht der Bearbeitung an der manuellen Registratur voraus und schafft die Voraussetzung, gezielt auf den Registerbestand zuzugreifen.

Die Überprüfung der Bestandsführung hat ergeben, daß das Verfahren aus der Sicht des Datenschutzes gut organisiert ist. Durch das Mitführen des Tilgungsdatums im automatisierten Teil des VZR wird im vierzehntägigen Rhythmus die Tilgungsreife von Eintragungen überprüft, und die betreffenden Vorgänge werden im Reißwolf vernichtet.

Zu beanstanden war allerdings — wie auch beim Halterbestand — die Art der Aufbewahrung der Meldungen. Es fehlte an geeigneten Maßnahmen gegen den unberechtigten Zugang zu den Bearbeitungsräumen sowie geeigneten Maßnahmen gegen den Verlust und die unbefugte Kenntnisnahme und Entwendung der Belege. Das Amt hat hierzu die notwendigen Änderungen bereits in Angriff genommen.

Folgende Vorschläge zur Verbesserung des Datenschutzes wurden vom KBA aufgegriffen:

— Bei unberechtigten Anfragen wird künftig das Auskunftsersuchen nicht mehr zusammen mit dem Ablehnungsbescheid im Original zurückgesandt. Für Kontrollzwecke werden solche Anfragen befristet aufbewahrt und damit ein Risiko für den Anfrager geschaffen.

— Bei der Auskunft an den Betroffenen selbst wird ihm künftig das vorgesehene Tilgungsdatum für die Eintragung im VZR-Bestand mitgeteilt. Die Mitteilung darüber war bisher unterblieben, weil das Tilgungsdatum als Bearbeitungvermerk und nicht als personenbezogenes Datum klassifiziert war.

— Bei Sammelsendungen mit Auskünften aus dem VZR-Bestand soll wegen der hohen Zahl von Informationen und dem daraus sich ergebenden größeren Schutzbedürfnis das Wertpaket als Versendungsart in Betracht kommen.

  Eine gleiche Regelung muß auch für die Sammelsendungen an das KBA angestrebt werden.

  Eine Änderung der Versendungsart für Einzelmitteilungen wurde von der zuständigen obersten Bundesbehörde abgelehnt, da dies z. B. für

Einschreibsendungen zu einer Erhöhung der Portokosten um ca. 338 000 DM und zu einem Personalmehrbedarf von 4 Kräften führen würde.

Darüber hinaus hat die Überprüfung der VZR-Bestandsführung dazu geführt, daß sich folgende Verfahren aus der Sicht des Datenschutzes als verbesserungsbedürftig erweisen. Änderungen der nachstehend beschriebenen Vorgänge sind jedoch zuvor mit den meldenden und auskunftsberechtigten Stellen, insbesondere den Ländern, abzustimmen.

— Meldungen an das VZR enthalten manchmal nicht registerfähige Angaben. Dies ist z. B. der Fall, wenn bei einer Verurteilung wegen Raubüberfalls auch eine Verurteilung wegen Fahrens ohne Führerschein erfolgt (Tatmehrheit). Im VZR darf nur die Strafe für „Fahren ohne Führerschein", eingetragen werden. In der Regel machen die mitteilenden Behörden alle nicht registerfähigen Angaben unkenntlich; wo dies nicht geschehen ist, werden diese Angaben beim KBA „geschwärzt".

  Datenschutzrechtlich handelt es sich bei der Meldung weitergehender Angaben um eine unzulässige Übermittlung an das KBA; der Fehler wird zwar nachträglich beim KBA „geheilt", so daß weitere unzulässige Übermittlungen dieser Daten unterbleiben; Aufgabe des Datenschutzes ist es jedoch, jeder Mißbrauchsmöglichkeit z. B. infolge einer unbefugten Bekanntgabe von Daten (vgl. § 5) entgegenzuwirken.

  Außerdem richten sich meine Bedenken gegen die Wirksamkeit der Datenschwärzung. Unter Umständen können die mit Filzschreiber durchgestrichenen Angaben noch zur Kenntnis genommen werden.

  Die meldenden Stellen müssen deshalb veranlaßt werden, nur registerpflichtige Teile von Entscheidungen mitzuteilen. Im geplanten Verkehrszentralregistergesetz (E-VZRG) sollte dies ausdrücklich klargestellt werden.

— Wenn wegen Tateinheit von registerpflichtigen und nicht registerpflichtigen Verstößen nur eine einheitliche Strafe ausgesprochen wird, läßt die Höhe des Strafmaßes auf nicht registerpflichtige Straftaten/Verstöße schließen, sofern der schwererwiegende Teil, der das Strafmaß bestimmt, ein nicht registerpflichtiger Tatbestand ist.

  Diese Rückschlüsse können nicht nur das KBA, sondern auch alle auskunftsberechtigten Stellen ziehen, so daß bei jeder Übermittlung schutzwürdiger Belange der Betroffenen verletzt werden. Außerdem muß der Betroffene in diesen Fällen ungerechtfertigte Nachteile in Kauf nehmen, weil nach der Höhe des Strafmaßes die Tilgungsfrist für seine Eintragungen bestimmt wird.

  Der Referentenentwurf des VZR-Gesetzes sieht auf meine Anregung hin vor, daß in diesen Fällen die Eintragung des Strafmaßes unterbleibt (§ 8 Abs. 1 und 2 E-VZRG). Ich bin der Auffassung, nach diesem Grundsatz sollte sich die Praxis der Datenspeicherung beim KBA schon jetzt richten.

— Auskünfte aus dem VZR an Gerichte und Behörden werden in Form von Ablichtungen aller Eintragungen erteilt. Der Inhalt der Auskunft ist daher unabhängig vom jeweiligen Anlaß und damit auch vom konkreten Informationsbedürfnis.

  Die Auskunftsregelung in § 30 Straßenverkehrsgesetz (StVG) sagt lediglich, daß Auskunft zu erteilen ist. Die Vorschrift bestimmt jedoch den Inhalt der Auskunft nur insoweit, als verlangt wird, die Auskunft „so zu erteilen, daß die anfragende Stelle die Akten über die den Eintragungen zugrunde liegenden Entscheidungen beiziehen kann". Während diese Regelung noch einen Ansatz für den Umfang der Datenübermittlung durch das KBA erkennen läßt, wird in § 13 E-VZRG bestimmt, daß der Inhalt der Eintragungen zu übermitteln ist. Beide Regelungen sind unbefriedigend. Solange über den Umfang der Übermittlungen nichts ausgesagt wird, ist — wenn § 10 BDSG nicht direkt angewendet wird — zumindest von den gleichen Grundsätzen wie im § 10 BDSG auszugehen; d. h. entscheidend ist danach die Erforderlichkeit der jeweiligen Aufgabe für den Einzelfall.

  Wie in der Praxis der Umfang der Auskünfte über das erforderliche Maß hinausgeht, zeigt sich z. B., wenn eine Führerscheinstelle auf Grund eines Antrages auf Ausstellung eines Ersatzführerscheins anfragt. In diesem Fall genügt die Information, ob Angaben gespeichert sind, die der Ausstellung eines Ersatzdokumentes im Wege stehen, z. B. ein Fahrverbot oder die Entziehung der Fahrerlaubnis. Tatsächlich wird der gesamte Registerinhalt übermittelt. In einem anderen Fall beschwerte sich ein Bürger darüber, daß die Tatsache, daß er vor über neun Jahren die Fahrlehrerprüfung nicht bestanden hat, allen anfragenden Gerichten und Behörden mitgeteilt wurde, obwohl keinerlei Sachzusammenhang bestand.

  Das BKA begründet die generelle Erteilung von Totalauskünften damit, daß der Anfragezweck (Ausstellung von Ersatzführerscheinen) nicht immer erkennbar sei. Doch gerade dieser Umstand, daß der Anfragezweck nicht erkennbar ist, müßte unter Datenschutzgesichtspunkten beim Amt Bedenken gegen die Vollauskunft hervorrufen.

  Die Beantwortung der Anfragen von Führerscheinstellen könnte in vielen Fällen mit Formschreiben nur unter Angabe des Aktenzeichens, aber ohne Namen und Anschrift, also in einer für die Übermittlung anonymisierten Form geschehen, womit im übrigen auch eine kostengünstigere Lösung geschaffen wäre.

  Ich halte es für dringend geboten, daß der Umfang der Auskünfte aus dem VZR auf den jeweiligen Anfragezweck abgestellt wird.

Rechenzentrum und Archiv

Die automatisierte Verarbeitung von Daten gewinnt beim KBA zunehmend an Bedeutung. Die Aufgabe, aktuelle Register für Auskunftszwecke

bereitzuhalten, verlangt die zeitnahe Erfassung der eingehenden Meldungen sowie kurzfristige Zugriffsmöglichkeiten auf die Datenbestände.

Dies hat Auswirkungen auf die Organisation des Arbeitsablaufs und ist verbunden mit Konsequenzen zur Gewährleistung des Datenschutzes.

Schon jetzt kann aus dem Kfz-Halterbestand rund um die Uhr Auskunft erteilt werden. Nach der Einrichtung des geplanten Zentralen Verkehrsinformationssystems ZEVIS wird auch der VZR-Bestand in der Gesamtdatenbank verfügbar sein und kann zum Abruf durch externe Stellen über Direktanschluß bereitgehalten werden (vgl. dazu u. 2.7.2.).

Die jederzeitige Auskunftsbereitschaft bedeutet für den Arbeitsablauf im Rechenzentrum den Drei-Schichten-Betrieb, mit den in solchen Fällen häufig festzustellenden organisatorischen Problemen, daß insbesondere während der personell schwach besetzten Nachtschicht z. B. die Funktionstrennung wie auch das Vier-Augen-Prinzip nicht eingehalten werden.

Die Situation der Datenverarbeitung beim KBA ist auch dadurch gekennzeichnet, daß das Gebäude für den DV-Bereich umgebaut und den gestiegenen Sicherheitserfordernissen angepaßt werden soll und deshalb die augenblicklichen und dringend verbesserungsbedürftigen Verhältnisse nur als Provisorium angesehen werden können. Trotz der absehbaren Neuorganisation des DV-Bereichs kann ich das bewußte Inkaufnehmen von Risiken und Schwachstellen bei der Datensicherung nicht billigen. Zu beanstanden war u. a. folgendes:

— Es ist gegenwärtig nicht gewährleistet, daß Personen sich jeweils nur in den Räumen aufhalten, die ihrer Funktion zugeordnet sind.

— Die Bestandsführung im Archiv ist lückenhaft. Mein Vorschlag, einen Durchschlag der Arbeitsaufträge zu Zwecken der Bestandskontrolle im Archiv zu belassen, wurde vom KBA aufgegriffen. Diese Sicherungsmaßnahme bleibt jedoch unwirksam und wird überflüssig, wenn — wie das Amt mir mitteilt — „weitere Kontrollmaßnahmen mit dieser Unterlage, wie z. B. Kontrolle des Rückflusses der Datenträger, ... nicht durchgeführt werden".

  Kontrollaufzeichnungen haben nur Sinn und Zweck, wenn sie tatsächlich der Kontrolle und nicht lediglich der Legitimation dienen.

— Datenträger mit nicht mehr benötigtem Inhalt wurden bisher nur vor dem Versand an Externe gelöscht. Das Amt hat mir jetzt bestätigt, daß darüber hinaus auch Magnetbänder mit sensiblen Daten (z. B. VZR-Daten) sowie Bänder, die außerhalb des Archivs lagern, nicht mehr nur zum Überschreiben freigegeben, sondern zuvor durch Beseitigung der Aufzeichnungen gelöscht werden.

— Das Datenträgerarchiv ist vom Materiallager zu trennen. Wenn diese Trennung nicht durchgeführt wird, bleibt auch die geplante Alarmanlage im Archiv wirkungslos, denn es ist vorgesehen, „daß zur Vermeidung von Fehlalarm die Anlage bei der Tür zur Materialanlieferung abschaltbar sein muß". Diesen Umstand kann sich auch ein Unbefugter zunutze machen.

Ich habe gefordert, daß auch für die Übergangszeit bis zum Bezug des umgebauten DV-Bereichs kurzfristig realisierbare Änderungen zur besseren Gewährleistung der Zugangs- und Abgangskontrolle ergriffen werden, um zumindest die Sicherheitsschwelle erkennbar anzuheben.

2.7.2 ZEVIS

Kurz vor meinem Kontrollbesuch beim KBA im August 1979 übersandte mir der Bundesminister für Verkehr eine 16-seitige Beschreibung des Zentralen Verkehrsinformationssystems ZEVIS. Unter diesen Umständen konnten nur einige der mit dem Aufbau von ZEVIS zusammenhängenden datenschutzrechtlichen Fragen an Ort und Stelle besprochen werden.

Aus mir in anderem Zusammenhang bekanntgewordenen Unterlagen habe ich entnommen, daß das Konzept für ein Informationssystem schon vor Jahren entwickelt wurde und daß bereits 1978 Fertigstellungstermine für den Auf- und Ausbau von ZEVIS festgelegt wurden. Da die datenschutzrechtliche Problematik des geplanten Datenbanksystems offensichtlich war, hätte ich eine frühere Unterrichtung für sinnvoll erachtet.

Das Zentrale Verkehrsinformationssystem ZEVIS soll aus der Zusammenfassung der beim KBA vorhandenen zentralen Dateien zu einem Datenbanksystem bestehen. Mit diesem Konzept wird die bisherige Trennung der einzelnen Datenbestände aufgegeben; jede Anfrage richtet sich dann an den gesamten Datenbankbestand. Dazu werden in das System neben Angaben aus den Halterbeständen (amtliches Kennzeichen, Versicherungskennzeichen, Hersteller, Fahrgestell-Nr., Halter) und Angaben aus dem automatisierten Teil des VZR (Angaben zur Person, Tilgungsdatum, Aktenzeichen) Erkenntnisse über die Entziehung der Fahrerlaubnis aufgenommen.

Wenn also beispielsweise die Anfrage an die Datenbank dahin lautet, was über eine bestimmte Person gespeichert sei, so können in einem Arbeitsgang Informationen aus allen Datenbeständen herausgesucht werden, z. B. „X ist Halter folgender Fahrzeuge ..., er ist im Verkehrszentralregister verzeichnet und hat Fahrerlaubnissperre".

Dieses aus verarbeitungstechnischen Gründen wirtschaftliche Zugriffsverfahren wirft erhebliche Probleme auf. Aus den ehemals getrennten Dateien durften bisher nur unter jeweils bestimmten Voraussetzungen Auskünfte erteilt werden. Wenn jetzt mit einer Anfrage der gesamte Datenbestand abgefragt wird, was vorher nur über mehrere Auskunftsersuchen erreicht werden konnte und mit der jeweiligen Überprüfung zur Auskunftsberechtigung verbunden war, so kann darin eine Gefahr für die Einhaltung der Zweckbestimmung der einzelnen Daten liegen. Durch ZEVIS wird nämlich nicht nur der amtsinterne Arbeitsablauf rationalisiert, son-

dern es werden auch Nutzungsmöglichkeiten eröffnet, die bei der bisherigen Form der Verarbeitung nicht bestehen. Im ersten Fall muß insbesondere sichergestellt sein, daß bei der Arbeit an der Datenbank das Datengeheimnis gewährleistet bleibt; im zweiten Falle ist insbesondere zu berücksichtigen, daß nach § 2 Abs. 2 Nr. 2 das Bereithalten zum Abruf der Übermittlung aller abrufbaren Daten gleichsteht.

In der Endausbaustufe sollen alle oben genannten Angaben im Direktzugriff auch mittels Datenfernverarbeitung verfügbar sein.

Gegenwärtig befindet sich ZEVIS in der Anfangsphase. In einer pilotartigen Anwendung wurde die Direktabfrage an den automatisierten Teil des VZR mit einer Führerscheinstelle und einer Bußgeldbehörde getestet; Vorbereitungen für kombinierte Anfragen an den Halter- wie an den VZR-Bestand laufen. Die Direktabfrage durch das polizeiliche Informationssystem INPOL ist vorgesehen; sie soll sich nach Auskunft des Bundeskriminalamtes ausschließlich auf Namen und Anschrift von Haltern und auf die Richtigkeit der technischen Daten (Motornummer etc.) erstrecken (vgl. auch 2.8.2, Neukonzeption des INPOL-Systems).

Meine Bedenken gegenüber der bestehenden Übermittlungspraxis aus den Halterbeständen und aus dem VZR habe ich oben dargelegt. Um so größere Bedenken habe ich, wenn die ohnehin bestehenden Schwierigkeiten bei der Handhabung der Zweckbindung der Daten und des Erforderlichkeitsprinzips bei der Auskunftserteilung durch das neue Datenbankkonzept und der Direktanschlußmöglichkeit vergrößert werden. Selbst so harmlos erscheinende Daten wie Fahrzeug- und Halterangaben lassen mit Hilfe der Datenbank-Software Auswertungen zu, die Aufschlüsse über Tatbestände und Verhaltensweisen des einzelnen geben, die mit dem Verkehrswesen nichts mehr zu tun haben, wie z. B. über vermögensrelevante Tatbestände (hohe Geldausgaben für teure Wagen, Liquidität durch Fahrzeugverkauf), über das Konsumverhalten (Kauf bestimmter Fahrzeugtypen, Farbgeschmack, Repräsentationsbedürfnis), über den Aufenthalt (Zulassungsantrag gestellt am ... in ...) und über Wohnungen (Wo wohnt A, wo sind gehäuft Personen mit der Staatsangehörigkeit B zugezogen, welche Fahrzeughalter wohnen im Wohnviertel C?

Deshalb wird es die vordringliche Aufgabe sein, zu prüfen und festzulegen,

- welche Stellen welche Daten erhalten dürfen,
- wie die Berechtigungsprüfung der Benutzer vorgenommen wird,
- wie unbefugte Benutzer festgestellt und an der Benutzung gehindert werden,
- wie sichergestellt werden kann, daß die Datenbank nur für konkrete Sachverhalte und im erforderlichen Umfang abgefragt wird.

Diese und weitere Fragen zur Verfahrenssicherheit müssen vor der Inbetriebnahme von ZEVIS zweifelsfrei geklärt sein. Ohne bereichsspezifische rechtliche Regelungen darf ein Direktzugriff auf die zentralen Datenbestände beim KBA nicht ermöglicht werden.

Solange das technisch Machbare und die Wünsche der Benutzer mit den Anforderungen des Datenschutzes und der Datensicherheit nicht zur Dekkung gebracht sind, kann ich das Konzept ZEVIS nicht gutheißen.

2.7.3 Verkehrsunternehmen mit Bundesbeteiligung

In meinem ersten Tätigkeitsbericht (vgl. 1. TB, 3.6.2.2.) habe ich am Beispiel des Bestellscheins für eine Kundenkarte beim Frankfurter Verkehrs- und Tarifverbund (FVV) darauf hingewiesen, daß die Bürger bei einer Datenerhebung nach § 9 Abs. 2 BDSG auch dann über die Rechtsgrundlage bzw. die Freiwilligkeit ihrer Angaben aufzuklären sind, wenn die Erhebung durch einen privatrechtlich organisierten Verbund erfolgt, in dem öffentliche Stellen (hier: Deutsche Bundesbahn und der Eigenbetrieb Stadtwerke Frankfurt a. M.) zusammenwirken. Das gemeinsame Vorgehen der Datenschutzinstanzen (beteiligt waren auch der Hessische Datenschutzbeauftragte und der Regierungspräsident in Darmstadt) hat den Verkehrs-Verbund veranlaßt, sein automatisiertes Bestellverfahren grundlegend umzustellen. Erreicht wurde nicht nur eine klare Trennung zwischen für die Bearbeitung notwendigen und freiwilligen Fragen, sondern auch eine deutliche Reduzierung des Umfangs. Neben fünf obligatorischen Angaben wird um zwölf freiwillige Angaben zur Auswertung für die Verkehrsplanung und um eine ausdrückliche Einwilligung zur Speicherung und Verarbeitung dieser Daten gebeten. Seit der Einführung des neuen Verfahrens im April 1979 sind neue Beschwerden nicht bekanntgeworden.

2.8 Öffentliche Sicherheit

2.8.1 Allgemeine Bemerkungen und übergreifende Probleme

Allgemein ist ein wachsendes Datenschutzbewußtsein im Sicherheitsbereich festzustellen. Dies läßt sich durch konkrete Maßnahmen belegen, an denen ich größtenteils mitgewirkt habe (vgl. im einzelnen nachstehend). Bei allen wichtigen Sicherheitsbehörden des Bundes sind bereits neue Bestimmungen über den Datenschutz in Kraft gesetzt (BKA, BfV, z. T. BGS) oder befinden sich in Bearbeitung (BGS, MAD, BND). Es besteht auch eine grundsätzliche Bereitschaft, datenschutzrechtliche Bedenken bei geplanten oder bestehenden Maßnahmen zu berücksichtigen. Von dem oft befürchteten Zusammenschluß aller Datensysteme der Sicherheitsbehörden kann keine Rede sein. Die Notwendigkeit, auch innerhalb der Ämter selbst den Zugang zu Dateien nur zuzulassen, soweit dies jeweils erforderlich ist, hat man erkannt, und es wird (z. B. im BKA und BfV) danach verfahren. Wenn behauptet wird, die Sicherheitsbehörden würden allmählich die Bundesrepublik mit einem alles übergreifenden Netz

überziehen, so trifft dies nach meinen Erfahrungen nicht zu. Mehr und mehr wird bei den Computern der Sicherheitsbehörden auch dazu übergegangen, das Vergessen vorzuprogrammieren.

Allerdings bedeutet all dies nicht, daß die zuständigen Stellen nicht weiterhin wachsam bleiben müssen. Jedes neue Vorhaben muß sorgfältig von Anfang an daraufhin überprüft werden, ob es nicht einen datenschutzrechtlichen Rückschritt mit sich bringt oder bringen könnte. Das gilt z. B. für die Neukonzeption von INPOL. Dabei sollten die jeweiligen Behörden die Datenschutzbeauftragten des Bundes und der Länder noch mehr als bisher von Anfang an beteiligen, damit Vorschläge aus der Sicht des Betroffenen berücksichtigt werden können, bevor Fakten geschaffen sind. Auch sind die erreichten datenschutzrechtlichen Verbesserungen nur als ein erster — wenn auch wichtiger — Schritt zu verstehen, der im übrigen noch nicht überall getan wurde. Das betrifft vor allem die noch zu lösenden Rechtsprobleme grundsätzlicher Art, wie allein die Problematik der Rechtsgrundlagen für die Tätigkeit von BND und MAD oder bestimmte Maßnahmen wie die polizeiliche Beobachtung („beobachtende Fahndung") zeigen.

Zur Kontrolltätigkeit im Sicherheitsbereich

Bei der Kontrolle und Mitarbeit an einer Verbesserung des Datenschutzes in diesem Bereich wurde wiederum deutlich, daß es ganz entscheidend auf die Detailarbeit ankommt. Entgegen manchen Äußerungen Dritter ist es gerade im Sicherheitsbereich mein Bestreben, die Probleme primär im Gespräch mit den betroffenen Behörden zu regeln. Die öffentliche Rechenschaft ist dann der Tätigkeitsbericht. Daneben aber kommt der öffentlichen Diskussion unterstützender Charakter zu, sie ist für die Schärfung des Datenschutzbewußtseins unerläßlich.

Transparenz

Es läge sowohl im Interesse des Bürgers als auch der Sicherheitsbehörden selbst, wenn über Art und Umfang bestimmter Maßnahmen mehr informiert würde, um unbegründete und damit unnötige Ängste zu vermeiden oder abzubauen. Die Öffentlichkeit wird auch eher mehr als weniger Verständnis für bestimmte Maßnahmen haben, wenn bekannt ist, welchem Zweck diese Maßnahmen dienen und auf welche Rechtsgrundlagen sie sich stützen.

Als ein Beispiel für viele sei die INPOL-Abfrage genannt, die der BGS und die Bayerische Grenzpolizei bei der Grenzkontrolle vornehmen. Es wurde und wird weithin befürchtet, daß hierbei eine Speicherung der personenbezogenen Daten erfolge oder aber eine Kopie oder Fotografie der Ausweisdokumente angefertigt werde, soweit die Abfrage durch Auflegen des Dokumentes auf ein Video-Gerät durchgeführt wird.

Dieses Video-Gerät hat aber keine andere Funktion, als die Daten auf einen Bildschirm in einem anderen Raum zu übertragen, in dem sich ein Datensichtgerät befindet. Dieses dient der Abfrage, ob die betreffende Person zur Fahndung oder Aufenthaltsermittlung ausgeschrieben ist. Die Ausweisdokumente werden hierbei weder fotokopiert noch fotografiert. Diese Routine-Abfrage ist insbesondere auch nicht in Verbindung mit dem Fotografieren von Ausweisdokumenten für den BND zu sehen. Letzteres ist ein Sonderproblem im Rahmen der Amtshilfetätigkeit zwischen BGS und BND (hierzu s. unten). Die Abfrage im Fahndungsbestand des BKA selbst führt zu keiner Speicherung. Bei vielen Zuschriften konnte ich durch diese Klarstellung Furcht und Mißtrauen beseitigen.

Oft, wenn nicht generell, wären solche Ängste vermeidbar gewesen, wenn die zuständigen Sicherheitsbehörden diese Art der Fahndungsüberprüfung an der Grenze von Anfang an bekanntgegeben hätten. Die Bekanntgabe einer solchen allgemeinen Fahndungsmethode führt auch nicht zu einem Sicherheitsdefizit, wie manchmal von den zuständigen Stellen behauptet oder befürchtet wird. An der Grenze muß ohnehin jedermann damit rechnen, entsprechend dem gesetzlichen Auftrag des BGS kontrolliert zu werden.

Tätigkeitsüberblick

In diesem Jahr konnten eine Reihe von Informationsbesuchen und zwei technische Einzelprüfungen durchgeführt werden. Mit 170 Einzeleingaben zur Tätigkeit der Sicherheitsbehörden war ein sprunghafter Anstieg der Beschwerdefälle gegenüber dem Vorjahr zu verzeichnen. In mehreren Fällen erfolgte die Prüfung durch Aktenstudium vor Ort. Ich gehe davon aus, daß diese Art von Prüfung im nächsten Jahr intensiviert werden kann.

Mehrere Einzeleingaben führten unabhängig vom konkreten Fall zu generellen Verbesserungsvorschlägen, die von den Sicherheitsbehörden aufgegriffen wurden. Bei keiner Prüfung oder Anfrage ist bisher vom Sicherheitsvorbehalt des § 19 Abs. 3 Satz 4 BDSG Gebrauch gemacht worden. Auch sind die Behörden (in unterschiedlichem Umfang) in vielen Fällen meiner Anregung gefolgt, auf das Auskunftsverweigerungsrecht gegenüber den Betroffenen nach § 13 Abs. 2 BDSG zu verzichten, weil jeweils keine Ausforschung zu befürchten war. Ich habe jedoch zur Vermeidung von Mißverständnissen gegenüber dem Einsender stets klargestellt, daß diese Auskünfte Ausnahmen sind und nicht als Präzedenzfälle mißverstanden werden dürfen. Es ist auch selbstverständlich, daß durch meine Vermittlung zwischen Bürger und Sicherheitsbehörden die Tätigkeit dieser Behörden nicht gefährdet werden darf.

Bei fünf Eingaben dieses Jahres konnte eine vollständige Löschung, in einem Fall eine Teil-Löschung, in zwei Fällen eine andere (weniger belastende) Art der Speicherung und in einem Fall bei zwei Behörden eine Aktenbereinigung erreicht werden. Bei vielen Eingaben hat sich herausgestellt, daß die befürchtete Speicherung nicht vorlag, ohne daß dies in allen Fällen mitgeteilt werden konnte. In den übrigen Eingaben waren datenschutzrechtliche Verstöße zum Zeitpunkt der Prüfung nicht feststellbar.

Oft ergab sich aus den Eingaben, daß eine Verarbeitung personenbezogener Daten allein durch

Sicherheitsbehörden der Länder in Betracht kam. Die Einsender befürchteten dann, daß die entsprechenden Daten im INPOL-System gespeichert seien, und gingen davon aus, daß ich über die Rechtmäßigkeit der Erhebung und evtl. weiteren Speicherung befinden könne. Dies ist jedoch nur in Ausnahmefällen möglich.

BKA und BfV betreiben Informationssysteme, in die neben diesen beiden Behörden auch die Polizeibehörden der Länder bzw. die Landesämter für Verfassungsschutz Informationen einstellen, soweit sie für die Teilnehmer dieser Informationssysteme von Bedeutung sind. Verantwortlich für die Richtigkeit und Rechtmäßigkeit dieser Speicherung sind grundsätzlich die eingebenden Dienststellen, also die dem Informationssystem angeschlossenen und eingabeberechtigten Polizeidienststellen bzw. Landesämter für Verfassungsschutz. Nur die Dienststellen, die die jeweiligen Informationen eingestellt haben, dürfen diese auch verändern und löschen.

Die Rechtmäßigkeit der Speicherung ergibt sich jeweils aus dem landesrechtlichen Polizeirecht (für die Gefahrenabwehr) oder dem Strafverfahrensrecht (für die Strafverfolgung). § 9 BDSG bzw. die parallelen landesrechtlichen Vorschriften verweisen auf die rechtmäßige Aufgabenerfüllung der jeweilig speichernden Stelle. Soweit — wie im Polizeirecht — landesrechtliche Besonderheiten eine Rolle spielen können, ist also auch eine unterschiedliche Beurteilung von Land zu Land möglich.

Für die Kontrolle der Zulässigkeit der Verarbeitung personenbezogener Daten durch die Sicherheitsbehörden der Länder sind die jeweiligen Landesbeauftragten für den Datenschutz zuständig. Dies gilt grundsätzlich auch für die Kontrolle der von diesen Dienststellen in die Informationssysteme der Sicherheitsbehörden des Bundes eingegebenen personenbezogenen Daten.

Von den dargestellten Grundsätzen wird man jedoch eine Ausnahme machen müssen, wenn in einem bestimmten Bereich generell Daten eingegeben werden, deren Erhebung nicht von einer Rechtsgrundlage gedeckt ist. Die Zentralstelle — also das Bundeskriminalamt oder das Bundesamt für Verfassungsschutz — oder der Bundesminister des Innern als Fachaufsichtsbehörde wäre in diesem Fall verpflichtet, das Land darauf hinzuweisen und zur Löschung dieser Daten im gemeinsamen Informationssystem aufzufordern. Da die Verarbeitung von Daten durch Stellen des Bundes nur zur rechtmäßigen Aufgabenerfüllung dienen darf, wäre in einem solchen Fall auch ein Beanstandungsrecht des Bundesbeauftragten gegeben.

Ich habe die Petenten auf diese Problematik aufmerksam gemacht und die Eingaben auf Wunsch an die zuständigen Kontrollinstanzen weitergeleitet.

Beratung

Besondere Bedeutung messe ich der Beratung über wünschenswerte Verbesserungen des Datenschutzes, z. B. durch neue Richtlinien oder bei Veränderungen von Datenauskunftssystemen bei. Zur Koordinierung und Intensivierung dieser Arbeit, die die Datenschutzbeauftragten der Länder ebenso betrifft, wurde unter meiner Federführung ein „Arbeitskreis Sicherheit" der Datenschutzbeauftragten des Bundes und der Länder gebildet. Er hat bisher zweimal getagt und sich mit Dingen befaßt, die einer gemeinsamen Lösung bedürfen. Sie betrafen u. a. die Probleme der Rasterfahndung, der Neukonzeption für das polizeiliche Informationssystem sowie die Verbesserung der Richtlinien über kriminalpolizeiliche personenbezogene Sammlungen.

Amtshilfe zwischen Polizei und Nachrichtendiensten

In meinem ersten Tätigkeitsbericht habe ich anläßlich der Zusammenarbeit zwischen BGS und BfV sowie der (damals noch) bestehenden Teilanschlüsse des BfV mit INPOL und des BKA mit NADIS darauf hingewiesen, daß die Zusammenarbeit und Amtshilfe zwischen Polizei und Nachrichtendiensten der Klärung bedarf (vgl. 1. TB, 3.4.3.3 und 3.4.4.2). Folgende Gesichtspunkte sind hier zu beachten: der Grundsatz der Zweckbindung der jeweils für die Aufgabenerfüllung einer Behörde gesammelten Daten; die Versagung polizeilicher Befugnisse für die Nachrichtendienste und die grundsätzliche Trennung der Ämter, die durch die Pflicht zur Amtshilfe nicht umgangen werden darf; schließlich die Frage, ob und wenn ja unter welchen Voraussetzungen die allgemeine Amtshilfe überhaupt eine ausreichende Rechtsgrundlage für die Übermittlung personenbezogener Daten sein kann. Nach einem Informationsbesuch bei der Grenzschutzdirektion im Januar dieses Jahres habe ich dem Bundesminister des Innern in einem internen Schreiben Fragen zu den Rechtsgrundlagen der Zusammenarbeit von Polizei und Nachrichtendiensten gestellt. Nach Bekanntwerden des Fotografierens von Ausweisdokumenten durch den BGS für den BND sah ich mich zusätzlich veranlaßt, in einer Pressemitteilung vom 11. April 1979 meine Auffassung zu diesem generellen Problem nochmals öffentlich darzulegen. Der Bundesminister des Innern hat im Laufe des Jahres sechs Rechtswissenschaftler mit der Erstellung von Gutachten zu diesen Fragen beauftragt. Die Gutachten sind inzwischen abgegeben worden. Ich hoffe, daß nunmehr die erforderlichen Schritte zur Lösung der Problematik eingeleitet werden.

Sicherheitsüberprüfung

§ 9 Abs. 2 BDSG verlangt, daß der Betroffene bei der Erhebung von Daten auf die ihr zugrundeliegende Rechtsvorschrift oder auf die Freiwilligkeit seiner Angaben hingewiesen wird. Die bei der Sicherheitsüberprüfung von den Bundesbehörden verwendeten Fragebogen entsprechen dieser gesetzlichen Pflicht jedoch nicht, denn es fehlt ein entsprechender klarer Hinweis. Bisher wird lediglich auf die Notwendigkeit der Sicherheitsüberprüfung allgemein und im Zusammenhang mit den Pflichten der Bundesrepublik Deutschland aus dem Nordatlantikvertrag hingewiesen. Im Entwurf für ein neues Formular ist zwar zusätzlich ein Hinweis auf

beamten- und tarifvertragliche Bestimmungen vorgesehen. Doch ist diesen auch bei weiter Auslegung keine Pflicht des einzelnen zur Erteilung von Auskünften im Rahmen der Sicherheitsüberprüfung zu entnehmen. Ein § 9 Abs. 2 BDSG entsprechender Hinweis ist auch gar nicht möglich, solange die erforderliche gesetzliche Grundlage fehlt. Auf Freiwilligkeit kann man zumindest nicht generell abstellen. Eine eindeutige Rechtsgrundlage für die Pflicht des Betroffenen, Angaben zu machen, ist dagegen bisher nicht ersichtlich.

Damit besteht auch eine Diskrepanz zu der andererseits gesetzlich festgelegten Plicht des BfV, bei der Sicherheitsüberprüfung mitzuwirken. Die Rechtsgrundlage, die die Pflicht des Betroffenen zu einer Mitwirkung an der Sicherheitsüberprüfung statuiert, wird hierdurch aber nicht ersetzt. Zur Beseitigung sowohl dieser Diskrepanz als auch zur Erfüllung der gesetzlichen Pflicht nach § 9 Abs. 2 BDSG wäre es wünschenswert, wenn die Sicherheitsüberprüfung insgesamt gesetzlich eindeutig geregelt würde. Dieses Problem besteht übrigens auch für die Sicherheitsüberprüfung von Wehrpflichtigen (s. u. 2.8.6).

2.8.2 Bundeskriminalamt (BKA)

Allgemeines

Die Arbeitskontakte mit dem BKA waren auch in diesem Jahr besonders intensiv. Das liegt nicht nur daran, daß wiederum die meisten Eingaben diese Sicherheitsbehörde betrafen, sondern ist vor allem im Zusammenhang mit meinen Aktivitäten im Rahmen des Dateienberichts (hierzu unten) sowie mit der Beteiligung an der Neukonzeption von INPOL zu sehen. Außerdem fand eine erste technische Detailprüfung im BKA statt.

Trotz erheblicher Meinungsverschiedenheiten während der Diskussion über den ersten Dateienbericht des Bundesministers des Innern fanden die Gespräche in einer sachlichen Atmosphäre statt. Besonders erfreulich ist, daß das BKA — ähnlich wie der BGS — eine recht aufgeschlossene Haltung gegenüber meinen Anregungen zu möglichst großer Offenlegung der Tätigkeiten einnimmt. Das Amt hat vielfach auf das Auskunftsverweigerungsrecht gegenüber dem Bürger verzichtet, wenn auch — wegen der schwierigeren Aufgabenstellung — nicht immer so umfassend wie der BGS.

Neben den vorgenannten, teilweise realisierten Verbesserungen ist auf folgende Veränderungen oder Neuerungen hinzuweisen die alle eine Verstärkung des Datenschutzes bewirken:

— Die neuen Richtlinien über kriminalpolizeiliche personenbezogene Sammlungen (KpS):

  Mit der Verabschiedung dieser Richtlinien im März d. J. ist ein erster wichtiger Schritt in die richtige Richtung getan. Insbesondere wird grundsätzlich durch die nunmehr gültige Zehnjahresfrist für die Aufbewahrung von Akten ein erheblicher Fortschritt gegenüber dem bisherigen Zustand erreicht. Wichtig ist jetzt die Überprüfung anhand der praktischen Anwendung dahin gehend, inwieweit weiter differenzierende Löschungsfristen möglich sind. Ich habe dem Bundesminister des Innern noch vor der Verabschiedung der Richtlinien Anregungen für weitere Verbesserungen schriftlich erläutert. Der bei mir eingerichtete „Arbeitskreis Sicherheit" der Datenschutzbeauftragten des Bundes und der Länder beschäftigt sich ebenfalls mit diesen Fragen.

  Erwähnt sei, daß die KpS zum Teil mangels ausreichenden Personals, zum Teil wegen noch nicht geklärter Rechtsfragen im Zusammenhang mit der Daktyloskopie noch nicht in vollem Umfang angewandt werden. Statt dessen wird nach einer vorläufigen Dienstanweisung zur Durchführung der KpS verfahren (s. u. Technische Detailprüfung).

— Beendigung der teilweisen Zugriffsberechtigung des BfV auf INPOL:

  In meinem ersten Tätigkeitsbericht hatte ich gegen die Zugriffsberechtigung des BfV auf Teilsysteme von INPOL rechtliche Bedenken angemeldet (3.4.4.2.).

  Der Bundesminister des Innern ist diesen Bedenken gefolgt und hat vor kurzem die Zugriffsberechtigung des BfV auf den Fahndungsbestand in INPOL sowie auf den Bereich Terrorismus in PIOS eingestellt.

  Noch nicht endgültig geklärt sind Art und Umfang der Verbindung zwischen dem BfV und der Abteilung Staatsschutz des BKA, das seine Akten gegenwärtig in NADIS registriert. Zur Zeit können beide Behörden auf den jeweiligen Bestand zurückgreifen. Hier bedarf es noch eingehender Erörterungen aller zuständigen Stellen sowohl zu den grundsätzlichen Rechtsfragen als auch zu den gegenseitigen wirklich begründeten Informationsbedürfnissen. Diese Fragen sind nicht zuletzt auch deshalb so schwierig, weil sich die Aufgaben der verschiedenen Ämter im Bereich des Staatschutzes überschneiden. Ich bin an diesen Gesprächen beteiligt.

— Keine Ausschreibung zur polizeilichen Beobachtung durch das BKA in Fällen der Gefahrenabwehr:

  In meinem ersten Tätigkeitsbericht habe ich darauf hingewiesen, daß das BKA für die Ausschreibung zur beobachtenden Fahndung, bei der es sich überwiegend um eine Maßnahme der Gefahrenabwehr handelt, keine Zuständigkeit besitzt (1. TB, 3.4.4.4).

  Der Präsident des BKA hat mir nunmehr versichert, daß das BKA nur noch Ausschreibungen im Rahmen der eigenen Ermittlungszuständigkeit vornimmt.

  Es bleibt grundsätzlich die Frage, inwieweit das polizeiliche Mittel der beobachtenden Fahndung überhaupt rechtlich abgesichert ist.

— Übermittlung von Namen und Anschrift des inländischen Versenders von Schußwaffen oder Munition in das Ausland:

Nach § 27 Abs. 4 der Ersten Waffenverordnung i. d. F. v. 15. Februar 1979 (BGBl. I S. 184) sollte das BKA grundsätzlich Name und Anschrift des inländischen Versenders oder Verkäufers von Waffen und Munition an die Polizeidienststellen des Heimatortes des ausländischen Erwerbers übermitteln. Das BKA hat dies bisher auch regelmäßig getan. Ich habe Bedenken erhoben, weil zumindest die regelmäßige Übermittlung in jedem Fall außer Verhältnis zu dem erstrebten Zweck steht, dem anderen Staat bei der Verfolgung entsprechender Straftaten zu helfen. Der Bundesminister des Innern hat sich diesen Bedenken angeschlossen. Das BKA übermittelt jetzt nur noch in begründeten Ausnahmefällen Namen und Anschrift des inländischen Versenders an die ausländische Polizeibehörde. Außerdem soll die Vorschrift bei nächster Gelegenheit entsprechend geändert werden.

— Als Beispiel für eine unbegründete Kritik an Sicherheitsbehörden sei ein Ermittlungsfall im Spionagebereich erwähnt, der in Presse und Fernsehen Anlaß zu Vorwürfen gegen Ermittlungsbeamte des BKA, zum Teil auch gegen Beamte des BfV, war. Die betreffende Akte wurde sorgfältig vor Ort geprüft. Dabei habe ich festgestellt, daß die Ermittlungen sehr zügig durchgeführt worden waren, daß zu den Ermittlungen nach Aktenlage durchaus Anlaß bestand und daß die Akten in vorbildlicher Weise geführt wurden. Insbesondere hat das BKA alle beteiligten Behörden in diesem Zusammenhang von der schon bald nach Beginn der Ermittlungen erfolgten Einstellung des Verfahrens unterrichtet und darauf hingewiesen, daß bezüglich der betreffenden Person keinerlei Verdachtsmomente mehr verblieben seien. Die Ermittlungsakte ist wegen des noch nicht aufgeklärten Grundsachverhalts weiter erforderlich; auf meine Anregung hin ist sie aber nicht mehr in NADIS registriert. Das BfV hat seinerseits dem Betroffenen auf Wunsch eine schriftliche Bestätigung ausgestellt, wonach auch seitens dieser Behörde keinerlei Verdachtsmomente bestehen geblieben seien. All dies war in der öffentlichen Berichterstattung nicht enthalten.

— In einem anderen Fall hatte ich im 1. Tätigkeitsbericht darauf hingewiesen, daß eine Speicherung nur noch für vorübergehende Zeit zulässig sein könne. Hier ist inzwischen die Löschung erfolgt.

Ungeachtet der zum Teil noch nicht gelösten rechtsgrundsätzlichen Probleme wurden bei der Prüfung von Einzeleingaben in keinem Fall datenschutzrechtliche Verstöße durch das BKA festgestellt. Dabei ist daran zu erinnern, daß das BKA selbst grundsätzlich nur für die Rechtmäßigkeit derjenigen Daten verantwortlich ist, die es selbst in die von ihm betriebenen zentralen Dateien eingestellt hat (vgl. oben 2.8.1., Tätigkeitsüberblick).

Zum „Dateienbericht"
des Bundesministers des Innern

Gegenstand des Berichtes war eine kritische Bestandsaufnahem aller Dateien und Karteien im BKA. Er wurde am 25. April 1979 dem Innenausschuß des Deutschen Bundestages und kurz vor Beginn der Sitzung auch mir erstmals zugeleitet. Der Bericht fand starke Beachtung in der Öffentlichkeit. Der Innenausschuß, der sich in mehreren Sitzungen damit beschäftigt hat, forderte mich auf, kurzfristig eine Stellungnahme aus datenschutzrechtlicher Sicht abzugeben. Diese Stellungnahme konnte wegen des Zeitdruckes zunächst im wesentlichen nur auf der Grundlage des Berichts des Bundesministers des Innern erfolgen. Dabei war festzustellen, daß der Bericht eine Reihe von Problemen ansprach, auf die ich in meinem ersten Tätigkeitsbericht sowie anläßlich von Gesprächen mit den zuständigen Stellen und in meinem Schreiben an den Bundesminister des Innern im Anschluß an meinen Informationsbesuch bei der Grenzschutzdirektion im Januar 1979 (s. u. 2.8.3) hingewiesen hatte. Das betraf insbesondere die Zugriffsberechtigung des BfV auf Teilbereiche von INPOL, die nicht vollständige Sicherung der Grenzfahndungsbestände gegen den Zugriff Unberechtigter sowie noch unzureichende Regelungen bezüglich der Datei PIOS (Personen, Institutionen, Objekte, Sachen). Darüber hinaus machte ich zu manchen Dateien Bedenken rechtsgrundsätzlicher Art geltend. Sie bezogen sich vor allem auf die — durch die Polizeien der Länder, nicht durch das BKA erfolgte — sehr pauschale erkennungsdienstliche Behandlung und Aufbewahrung der Unterlagen über Flüchtlinge aus Ungarn und der DDR, sowie die Besucherkontrolle bei Häftlingen, die wegen terroristischer Gewalttaten verurteilt sind oder sich in Untersuchungshaft befinden. In mehreren ausführlichen Erörterungen mit dem BKA-Präsidenten konnte ich weitere, im Bericht der Prüfgruppe nicht enthaltene Einzelheiten aufklären. Gleichzeitig wurde Einigkeit darüber erzielt, daß mehrere Dateien nicht mehr fortgeführt werden sollten und in anderen Teilbereichen Verbesserungen des Datenschutzes erforderlich sind. So hat der Präsident des BKA u. a. zugesagt, die Datei Heroin Fernost, die schon zum damaligen Zeitpunkt nicht mehr im aktuellen Bestand geführt wurde, demnächst zu löschen und beim Personenkreis, der von der Besucherkontrolle bei der Häftlingsüberwachung betroffen ist, auf eine Einschränkung hinzuwirken. Hinsichtlich der Organisationsdatei der Staatsschutzabteilung des BKA wurde in einem weiteren Gespräch eine für beide Seiten vertretbare Regelung vereinbart, die eine erhebliche Reduktion der als verdächtig registrierten links- und rechtsextremistischen Organisationen bewirkte.

Viele meiner in der ersten Stellungnahme aufgezeigten Bedenken wurden dadurch gemildert. Die rechtsgrundsätzlichen Bedenken insbesondere bezüglich der Datei über die Grenzüberwachung im Auftrag der Nachrichtendienste, der fehlenden eindeutigen Rechtsgrundlage für die Besucherkontrolle usw. mußten jedoch aufrechterhalten bleiben. All dies habe ich in einer ergänzenden Stellungnahme zusammengefaßt.

Meine Ausführungen sind teilweise als eine Art persönlicher Schuldvorwurf gegenüber den Beam-

ten des BKA oder anderer Sicherheitsbehörden mißverstanden worden. Das war und ist selbstverständlich nicht der Fall, wie ich in meiner Stellungnahme gleich eingangs betont habe.

Ungeachtet der bei den Einzelerörterungen teilweise auftretenden Spannungen muß die Diskussion um den Dateienbericht insgesamt als fruchtbar bezeichnet werden, weil bei allen Beteiligten das Bewußtsein sowohl für Notwendigkeiten der inneren Sicherheit als auch des Datenschutzes geschärft wurde, abgesehen von den unmittelbar erreichten Verbesserungen. Leider konnten jedoch bisher nicht alle Zusagen erfüllt werden, da das BKA ja nicht allein entscheidungsbefugt ist. Es ist zu hoffen, daß die zuständigen Bund-Länder-Gremien diese Zusagen „einlösen" oder der vom Bundesminister des Innern angekündigte zweite Dateienbericht die Konsequenzen aus den bisherigen Erörterungen zieht.

Neukonzeption des INPOL-Systems

Das BKA bereitet gegenwärtig zusammen mit den Vertretern der Landeskriminalämter die auf Beschlüsse der Innenministerkonferenz zurückgehende Neukonzeption des INPOL-Systems vor. Die Zielvorstellungen der Neukonzeption lassen sich wie folgt umreißen:

— die grundsätzliche zentrale Speicherung aller Vorgänge in Bund und Ländern, zu denen eine kriminalpolizeiliche Akte angelegt wird sowie

— die Errichtung eines Teilverbundes mit den Auskunftssystemen des Bundeszentralregisters (BZR), des Ausländerzentralregisters (AZR) und des Kraftfahrt-Bundesamtes (KBA).

Im Herbst fanden hierzu erste eingehende Erörterungen im BKA über die damit verbundenen Probleme aus datenschutzrechtlicher Sicht statt. Dabei habe ich deutlich gemacht, daß diese Planungen nach meiner Auffassung nicht mit den rechtlichen Gegebenheiten in Einklang stehen. Diese Bedenken wiegen schwerer als die durch die Konzeption beabsichtigten nicht unerheblichen Verbesserungen des Datenschutzes insbesondere durch eine zentrale Überwachungsmöglichkeit der registrierten Daten.

Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich im November mit dieser Frage befaßt und ist zu dem gleichen Ergebnis gekommen. Eine zentrale Speicherung von Straftätern oder vermuteten Straftätern in polizeilichen Informationssystemen des BKA ist bereits nach dem Wortlaut des BKA-Gesetzes nur für überregionale Täter möglich. Das ergibt sich sowohl aus der Grundsatzvorschrift des § 1 Abs. 1 Satz 2 BKA-Gesetz, aus dem Begriff der Erforderlichkeit für die Übermittlung von Daten an das BKA durch die Landeskriminalämter i. S. § 3 BKA-Gesetz und aus dem Vergleich mit § 4 BKA-Gesetz, der allein für Freiheitsentziehungen (zur Vermeidung von Doppelausschreibungen) eine umfassende Meldepflicht vorsieht. Eine totale Erfassung polizeilich relevanter Vorgänge würde im übrigen gegen den Grundsatz der Verhältnismäßigkeit verstoßen, so daß auch deshalb der Begriff „alle Nachrichten" i. S. des § 2 Abs. 1 Nr. 1 BKA-Gesetz einschränkend ausgelegt werden muß. Die Entstehungsgeschichte von § 2 BKA-Gesetz, die eine andere einfachrechtliche Auslegung nahelegen könnte, ist daher kein ausreichendes Gegenargument. Es muß deshalb ein Weg gefunden werden, klare Kriterien zu entwickeln für Deliktsgruppen, die in jedem Fall in ein überregionales System eingestellt werden können (wie z. B. Terrorismus- und Rauschgiftkriminalität, Kraftfahrzeugdiebstahl und Verstöße gegen das Waffenrecht) und solchen, die lediglich in einer regionalen, möglicherweise sogar nur örtlichen Kartei erfaßt zu sein brauchen und auch nur dort erfaßt sein dürfen.

Für den beabsichtigten generellen (wenn auch nur auf bestimmte Daten beschränkten) Zugriff auf die vorerwähnten zentralen Register (BZR, AZR, KBA) fehlt es dagegen an jeglicher Rechtsgrundlage. Soweit Bestimmungen über Auskünfte an Polizeien vorliegen, wie nach § 39 Bundeszentralregistergesetz, erlauben diese jeweils nur die Auskunft in Einzelfällen.

Technische Detailprüfung

Im Juni fand zum ersten Mal eine technische Detailprüfung statt, die sich auf die Daktyloskopie und das Verfahren bei der Löschung von Sicherungsbändern bezog (vgl. 1. TB, 3.4.7.1).

Zum Bereich Daktyloskopie

Hier war zu überprüfen, ob bei der Verformelung von Fingerabdruckblättern zum Zwecke der Speicherung im Rechner des BKA die Fristen der neuen Richtlinien über kriminalpolizeiliche personenbezogene Sammlungen eingehalten werden. Es wurde festgestellt, daß dies nicht der Fall war, sondern auch Unterlagen verformelt wurden, die nach den KpS an sich auszusondern wären. Daraufhin wurde ein Übernahmeverfahren vereinbart, mit dem diese Mängel ohne zusätzlichen Personaleinsatz weitgehend behoben werden können. Dieses wurde inzwischen in der bereits erwähnten vorläufigen Dienstanweisung des BKA umgesetzt und gilt für die Aussonderung aller Unterlagen. Danach werden insbesondere zunächst alle beim BKA vorhandenen Unterlagen über Kinder, Vermißte und Personen über 70 Jahre sofort ausgesondert und vernichtet. Dasselbe gilt für Unterlagen, bei denen ohne weitere Nachprüfung erkennbar ist, daß sie unzulässigerweise erhoben wurden oder die kraft Urteils zu vernichten sind.

Von den daktyloskopischen Unterlagen werden allerdings zur Zeit nur diejenigen vernichtet, die nicht hätten erhoben werden dürfen oder deren Vernichtung von einem Richter angeordnet ist. Im übrigen wird vorerst bei den genannten Personengruppen nur die Verformelung der vorhandenen Fingerabdrücke zurückgestellt. BMI und BKA halten nämlich eine von den KpS abweichende Behandlung der daktyloskopischen Unterlagen für gerechtfertigt, wenn die Unterlagen nach der Verformelung nicht mehr unter den Namen der Betroffenen abfragbar sind und auf den Unterlagen nach Ablauf der KpS-Fristen alle Hinweise über Ort, Zeit und Anlaß der erkennungsdienstlichen (ed-) Behandlung entfernt werden. Ein zunächst unbe-

kannter Täter ist dadurch im Falle erneuter Straffälligkeit über die hinterlassenen Spuren mit Hilfe der im BKA über ihn vorhandenen daktyloskopischen Unterlagen identifizierbar. Ich habe mich in meiner Stellungnahme für den Innenausschuß des Deutschen Bundestages gegen diese abweichende Behandlung der Daktyloskopie gewandt. Denn es kann für die Anwendung der Löschungsfristen keinen Unterschied machen, ob es sich um Fingerabdrücke oder anderes polizeiliches Material handelt. Wenn die Polizei nicht annehmen darf, daß der Betroffene wieder straffällig wird (in diesem Fall wäre eine Aufbewahrung über die KpS-Fristen hinaus zulässig), dann muß die Löschungsfrist für alle polizeilichen Informationen über diese Person gelten.

Vor einer endgültigen Stellungnahme bedarf es noch eingehender Erörterungen mit den Datenschutzbeauftragten der Länder, da die Daktyloskopie ein gemeinsames Informationssystem der Polizeien des Bundes und der Länder werden soll.

Zum Verfahren der Löschung bei den Sicherungsbändern

Hier ging es darum, die Einhaltung der im ersten Tätigkeitsbericht geschilderten Löschungsverfahren im BKA bezüglich der Sicherungsbänder zu überprüfen. Dabei wurde festgestellt, daß durch den Einsatz eines neuen Reinigungs- und Prüfgerätes seit Anfang Mai 1979 alle Bänder bei der Freigabe zur Wiederverwendung gelöscht werden. Die Löschung erfolgt durch vollständige Überschreibung mit gleichen Zeichen im Zuge der Prüfung. Die Pflicht zur physikalischen Löschung i. S. § 14 Abs. 3 BDSG ist insoweit also vollständig erfüllt.

Es hat sich jedoch gezeigt, daß die vom BKA gewollte Vier-Wochenfrist für die Freigabe der Sicherungsbänder nach dem gegenwärtigen Stand der Technik bei den im BKA verwendeten Datenbanksystemen noch nicht eingehalten werden kann. Sie muß aus Sicherungsgründen vorläufig auf drei Monate festgesetzt werden. Da gewährleistet ist, daß aus den Sicherungsbeständen keine Auskunft oder sonstige Verwertung erfolgt, sie vielmehr allein der Rekonstruktion des Datenbestandes im Notfall dienen, bestehen hiergegen keine Bedenken angesichts des noch relativ kurzen Freiraumes bis zur Freigabe der Sicherungsbänder zwecks Löschung.

2.8.3 Bundesgrenzschutz

Allgemeines

Informationsbesuche bei der Grenzschutzdirektion Koblenz, dem Grenzübergang Aachen und am Flughafen Düsseldorf im Januar und April dieses Jahres gaben Gelegenheit, mir einen ersten Eindruck von der Aufgabenerfüllung des Grenzschutzeinzeldienstes (GSE) zu verschaffen. Dabei wurde eine Fülle von Fragen aus datenschutzrechtlicher Sicht aufgeworfen. Ein Teil von ihnen betrifft die Amtshilfe des BGS für die Nachrichtendienste, deren Problematik generell gelöst werden muß (s. o. 2.8.1). Ein anderer Teil betrifft die Verbindung zwischen Grenzschutzdirektion und INPOL. Meine Bedenken sind hier allerdings aufgrund der Erörterungen mit den zuständigen Stellen inzwischen weitgehend gemildert. Die GSD gab bis vor kurzem auch solche Daten in den allgemeinen Zentralen Personenindex des BKA ein, die überwiegend oder ausschließlich grenzpolizeilichen Bezug hatten mit der Folge, daß jeder daran angeschlossene Teilnehmer über die bei der Grenzschutzdirektion vorhandenen Unterlagen Auskunft erhielt. Die für die Aufgaben des Grenzschutzes erforderlichen Daten dürfen jedoch nicht mit den Auskunftssystemen des BKA und der allgemeinen Polizeien der Länder vermengt werden. Die Aufgaben von Grenzschutz und allgemeiner Polizei sind (abgesehen von der Fahndung einschließlich der polizeilichen Beobachtung für polizeiliche Zwecke) nur zu einem geringen Teil identisch. Polizei ist nicht gleich Polizei. Also ist ein Zugriff auf andere Daten als solche, die zu den vorgenannten Aufgaben jeweils erforderlich sind, zu verhindern. Anläßlich eines Besuches im Januar 1979 bei der GSD und in einem Schreiben an den Bundesminister des Innern vom März 1979 habe ich daher die Einrichtung eines abgeschotteten Zentralen Personenauskunftssystems des BGS vorgeschlagen statt der bisherigen Verquickung mit dem Zentralen Personenindex des BKA. Nunmehr gibt die GSD nur noch solche Daten in den allgemeinen Zentralen Personenindex ein, die in der Tat für alle angeschlossenen Polizeibehörden erforderlich sind, insbesondere Daten für die allgemeine aktuelle Fahndung.

Alle anderen Daten werden in einen geschützten Bestand von INPOL eingegeben, der nur Grenzpolizeibehörden zugänglich ist.

Allerdings erhält der an den allgemeinen Zentralen Personenindex angeschlossene Teilnehmerkreis immer noch die Information, daß weiterer (Daten-) Bestand über die betreffende Person vorhanden ist, auf den er allerdings nicht zugreifen kann. Doch muß auch dies noch unterbunden werden, da auch solche Informationen nicht erforderlich sind und zu unbegründeten Verdachtsmomenten Anlaß geben könnten.

Dies könnte behoben werden, wenn meinem Vorschlag nach einem vollständig selbständigen Zentralen Personenindex der GSD gefolgt wird.

Ein weiteres Problem ist unter anderem die teilweise mangelhafte technische Sicherung bei der Grenzschutzdirektion. Auch hier stehen Verbesserungsmaßnahmen noch aus, wie eine zusätzliche Überprüfung im November des Jahres ergab. Doch hat der Bundesminister des Innern eine umfassende Überprüfung der technischen Sicherheitsmaßnahmen angekündigt. Sie sollte vordringlich betrieben werden.

Erzielte oder beabsichtigte Verbesserungen

Hier sind folgende Maßnahmen erwähnenswert:

— Früher wurden von der Grenzschutzdirektion auch Personen registriert, über die von anderen Polizeidienststellen angefragt wurde, auch wenn bei der Grenzschutzdirektion selbst keine

Erkenntnisse über diese Personen vorlagen. Nunmehr erfolgt eine Eingabe von Personalien in den Zentralen Personenindex des BKA durch die Grenzschutzdirektion nur noch bei eindeutig grenzpolizeilichem Bezug.

— Eingaben in den offenen und/oder geschützten Bestand der INPOL-Fahndung dürfen nur noch nach vorheriger Prüfung durch einen Beamten des gehobenen oder höheren Dienstes und nach festgelegten, gegenüber früher erheblich eingeengten Kriterien, erfolgen. Dies bewirkt eine weitere Reduzierung der Ausschreibungen zur Fahndung oder Beobachtung.

— Die veralteten Richtlinien für die Grenzfahndung werden überarbeitet auf der Grundlage der Richtlinien für kriminalpolizeiliche personenbezogene Sammlungen.

— Entsprechend meiner Anregung wird geprüft, ob für den BGS ein eigener abgeschotteter Zentraler Personenindex aufgebaut werden soll.

— Bei den Grenzschutzämtern werden im Zusammenhang mit ihrer Zuständigkeit zum Erlaß von Bußgeldbescheiden Karteien geführt. Hierfür bestanden bisher teils gar keine Regelungen, teils sehr lange Aufbewahrungsfristen. Nunmehr wurden neue Fristen vereinbart, die sich an der Regelung über das Gewerbezentralregister orientieren. Nach deren Ablauf werden die Unterlagen vernichtet.

— Bei der Übernahme der bisher manuell geführten Datenbestände bei der Grenzschutzdirektion in den automatisierten Zentralen Personenindex wurden in erheblichem Umfang vorhandene Bestände **vernichtet.**

Prüfung von Einzeleingaben

Während im vergangenen Jahr keine Eingabe über datenschutzrechtlich relevante Tätigkeit des BGS einging, waren es in diesem Jahr über 30.

Sie standen i. d. R. im Zusammenhang mit der Grenzkontrolle.

Es ist hervorzuheben, daß in keinem Fall eine Speicherung vorlag und es bei jeder Einzelanfrage möglich war, Auskunft zu erteilen, weil keine Ausforschung befürchtet werden mußte. In manchen Fällen, in denen sich der Einsender zunächst an das zuständige Grenzschutzamt gewandt hatte, war dem Bürger von diesen Dienststellen schon eine volle Auskunft erteilt worden. Die Überprüfungen durch mich haben auch jeweils die Richtigkeit dieser Angaben bestätigt. Als Fazit ist daher festzustellen, daß im Bereich des BGS keine Einzeleingabe Anlaß zu Beanstandungen gegeben hat. Da unter den vorerwähnten Einzeleingaben auch solche waren, in denen Speicherungen in bezug auf Grenzübertritte zu Ostblockstaaten vermutet wurden, ist damit gleichzeitig dargetan, daß es beim BGS anders als offenbar bei der Bayerischen Grenzpolizei keine generelle Registrierung der Grenzübertritte zu und von Ostblockstaaten gab und gibt.

Die Hauptprobleme beim BGS liegen in den unter „Allgemeines" erwähnten Punkten, insbesondere in Art und Umfang der Amtshilfe für die Nachrichtendienste, für die eine einheitliche Lösung gefunden werden muß (s. o. 2.8.1).

Übermittlung von Daten über Wehrpflichtige aus den Melderegistern an den BGS zu Anwerbungszwecken

Die Meldebehörden übermitteln den Grenzschutzkommandos (GSK) regelmäßig personenbezogene Daten über Wehrpflichtige. Die Daten werden von den GSK dazu benutzt, für den Eintritt in den Grenzschutzdienst zu werben. Nach jeder Werbeaktion werden die Daten vernichtet.

Gegen dieses Verfahren bestehen keine Bedenken. Nach § 49 Abs. 1 Nr. 1 Bundesgrenzschutzgesetz können diejenigen Männer zum Polizeivollzugsdienst im Bundesgrenzschutz verpflichtet werden, die einem zum Wehrdienst aufgerufenen Geburtsjahr angehören und nach dem Musterungsergebnis für den Wehrdienst zur Verfügung stehen.

Wenn seitens des BGS diese Möglichkeit so gehandhabt wird, daß statt einer Verpflichtung die erforderlichen Polizeivollzugsbeamten im Wege der Werbung und damit der Freiwilligkeit gewonnen werden, so ist dies nicht zu beanstanden.

2.8.4 Bundesnachrichtendienst

Allgemeiner Überblick

Nach wie vor besteht hier wie beim Militärischen Abschirmdienst, (soweit es sich nicht um Maßnahmen im Rahmen des Gesetzes zu Artikel 10 Grundgesetz handelt) das Problem der Rechtsgrundlage. Dies erschwert meine Prüfungstätigkeit deshalb, weil dadurch in entsprechenden Einzelfällen die für meine Kontrolle entscheidende Frage nach der Rechtsgrundlage grundsätzlich ausgeklammert werden muß. Ich wiederhole deshalb meine Anregung aus dem ersten Tätigkeitsbericht (1. TB, 3.4.6), trotz aller nicht zu verkennenden Schwierigkeiten eine gesetzliche Grundlage zu schaffen.

Während es 1978 noch keine Einzeleingaben zu prüfen gab, belief sich die Zahl der ausschließlich oder auch die Tätigkeit des BND betreffenden Zuschriften in diesem Jahr auf mehr als 20. Dabei war jedoch der überwiegende Teil veranlaßt durch die im Zusammenhang mit der Amtshilfediskussion (s. o. 2.8.1) zu sehende Problematik des Fotografierens von Ausweisdokumenten durch den BGS für den BND.

Die Erörterungen mit den zuständigen Stellen im Bundeskanzleramt und im BND haben gezeigt, daß man den Erfordernissen des Datenschutzes aufgeschlossen gegenübersteht. Sieht man von der Rechtsgrundlagenproblematik ab, so ist festzustellen, daß in keinem Einzelfall Beanstandungen vorzunehmen waren.

Wiederholt in der Öffentlichkeit anzutreffende falsche Vorstellungen über einen angeblichen Daten-

verbund zwischen BND und den anderen Nachrichtendiensten oder gar dem BKA in Form eines gegenseitigen und automatischen Zugriffs auf die jeweiligen Informationssysteme veranlassen mich, erneut darauf hinzuweisen, daß es einen solchen Verbund nicht gibt. Wohl aber besteht eine Zusammenarbeit in Einzelfällen aufgrund der Richtlinien über die Zusammenarbeit in Staatsschutzangelegenheiten i. d. F. vom 23. Juli 1973. Das Hauptproblem liegt auch hier in der Notwendigkeit möglichst klarer gesetzlicher Regelung im Zusammenhang mit den Fragen der Amtshilfe allgemein (hierzu s. o. 2.8.1., Amtshilfe zwischen Polizei und Nachrichtendiensten).

Geplante Verbesserungen und Einzelfragen

Im BND werden gegenwärtig umfassende Überlegungen über eine weitere Verbesserung des Datenschutzes angestellt, die sowohl Fragen der Speicherung, der Übermittlung und der Löschung als insbesondere auch der Auskunftsmöglichkeit in Einzelfällen betreffen. Dabei wird u. a. die Möglichkeit der Bildung verschiedener Kategorien als Grundlage für eine differenzierte Lösung geprüft. Hierbei werden meine Vorstellungen und Vorschläge mit berücksichtigt.

Nach Bekanntwerden des Fotografierens von Ausweisdokumenten durch den BGS für den BND habe ich mich an Ort und Stelle über dieses Problem sowie über andere Grundsatzprobleme informiert. Aus diesen Gesprächen ist im Zusammenhang mit einer Vielzahl entsprechender Einzeleingaben folgendes festzustellen:

— Zur Art der Verwertung der Ausweisdokumente:

  Ich habe mich davon überzeugt, daß die Ausweisdokumente ausschließlich nach Sachgesichtspunkten klassifiziert und registriert werden. Insbesondere besteht hierfür keine automatisierte Datei. Deshalb ist es auch praktisch nicht möglich nachzuprüfen bzw. herauszufinden, ob eine bestimmte Person in diesen Dokumenten festgehalten ist.

  An der grundsätzlichen Problematik der Rechtsgrundlage und der Zulässigkeit der Übermittlung dieser Dokumente durch den BGS an den BND ändert dies allerdings nichts.

— Zur Frage der Postkontrolle nach § 3 Gesetz zu Artikel 10 GG (G 10):

  Im Rahmen der sogenannten strategischen Kontrolle des BND nach § 3 G 10 werden grundsätzlich keine personenbezogenen Erkenntnisse durch den BND verwertet. Die Weitergabe personenbezogener Angaben in Fällen, in denen dem zuständigen Sachbearbeiter besondere Gesichtspunkte auffallen, hält sich streng an den Rahmen des § 3 Abs. 2 G 10. So wurden z. B. im vergangenen Jahr nur in ganz wenigen Ausnahmefällen personenbezogene Erkenntnisse im Rahmen des § 3 Abs. 2 G 10 weitergegeben.

— Prüfung von Einzeleingaben und Verzicht auf das Auskunftsverweigerungsrecht:

  Bezüglich der Prüfung von Einzeleingaben ist zunächst darauf hinzuweisen, daß das Bundeskanzleramt bisher in keinem Fall von der Möglichkeit des § 19 Abs. 3 Satz 4 BDSG Gebrauch gemacht hat, mir Auskünfte zu verweigern.

  Den Petenten gegenüber hat der BND hingegen fast immer auf seinem Auskunftsverweigerungsrecht nach § 13 Abs. 2 BDSG bestanden. Lediglich in zwei Fällen, wovon der eine im Zusammenhang mit dem Fotografieren von Ausweisdokumenten, der andere im Zusammenhang mit der Werbung des BND für Mitarbeiter stand, ist der BND meiner Anregung zum Verzicht auf das Auskunftsverweigerungsrecht gefolgt. Im letzten Fall wurde insbesondere befürchtet, daß der BND eventuell ungehinderten Zugang zu Dateien der Universitäten oder anderer Institutionen habe, um Name und Anschrift der Personen herauszufinden, die über ihr Interesse an eine Tätigkeit im höheren Dienst des BND befragt werden sollen. Dies ist jedoch nach meinen Ermittlungen, in die ich auch die im konkreten Fall angesprochene Universität einbezogen habe, nicht der Fall. Der BND erhielt diese Angaben allein aus allgemein zugänglichen Quellen. Ich hoffe, daß der BND in Zukunft häufiger derartige Auskünfte ermöglicht, um gerade immer wieder anzutreffenden Fehlvorstellungen über Art und Umfang seiner Tätigkeit entgegenzutreten. Dabei erkenne ich das Sicherheitsinteresse des BND an, nicht ausgeforscht zu werden.

2.8.5 Bundesamt für Verfassungsschutz

Allgemeines und Überblick

— *Neue Löschungsrichtlinien*

  Als wichtigstes Ergebnis dieses Jahres für den Datenschutz im Bereich des BfV sind die neuen Löschungsrichtlinien zu bezeichnen. Während es bisher keine generellen Überprüfungsfristen gab, bringen die seit kurzem in Kraft gesetzten Richtlinien erhebliche Verbesserungen des Datenschutzes. So sind z. B. die Aufzeichnungen über extremistische Bestrebungen jedenfalls nach 15 Jahren von Amts wegen auf ihre Erforderlichkeit zu überprüfen. Daneben bleibt die Praxis der Zeitspeicherung bestehen. Hierbei handelt es sich um eine nur vorübergehende Speicherung bestimmter Fälle, bei denen dann eine Löschung erfolgt, wenn sich in diesem Zeitraum keine neuen Erkenntnisse ergeben. Dieses Verfahren soll nach Auskunft des BfV auch weiter ausgebaut werden, um in besonderen Fällen von Anfang an eine frühere Relevanzprüfung von Amts wegen (also unabhängig von einer Einzeleingabe oder Prüfung durch mich) zu gewährleisten. Hinsichtlich der Löschung in den Protokollbändern entsprechen die Richtlinien meiner im ersten Tätigkeitsbericht erläuterten Auffassung, wonach auch in den Protokollbändern grundsätzlich gelöscht werden muß, da sonst nicht von einer Löschung im physikalischen Sinne gesprochen werden

kann, wie sie § 14 Abs. 3 BDSG verlangt (vgl. 1. TB, 3.4.7.1). Selbstverständlich muß nach ersten Erfahrungen mit den neuen Fristen geprüft werden, inwiefern weitere Verbesserungen möglich sind.

Bereits vor Anwendung der neuen Richtlinien wurde eine erhebliche Anzahl von Datensätzen im nachrichtendienstlichen Informationssystem NADIS gelöscht; bei einer großen Anzahl von Datensätzen wird darüber hinaus gegenwärtig die Möglichkeit der Löschung geprüft. Mit weiteren erheblichen Reduzierungen des Datenbestandes ist aufgrund der fortlaufenden Anwendung der neuen Richtlinien zu rechnen.

— *Prüfungsergebnisse und Verzicht auf das Auskunftsverweigerungsrecht*

Nach dem BKA betrafen die meisten Einzeleingaben das BfV. Oft war die befürchtete Speicherung nicht festzustellen. In fünf Fällen konnte eine Löschung und in einem Fall, der als Überhang vom letzten Jahr noch zur Entscheidung anstand, eine Zeitspeicherung erreicht werden, ohne daß hierdurch Sicherheitsinteressen des BfV beeinträchtigt worden wären. Allerdings würde ich es in diesem Zusammenhang begrüßen, wenn das BfV sich mehr als bisher zu einer Auskunft gegenüber dem Einsender bereitfinden könnte. In weiteren Gesprächen mit dem Amt und dem Bundesminister des Innern sind Ansätze für eine Einigung erkennbar geworden. Insbesondere wird es darauf ankommen, bestimmte Fallgruppen zu bilden, im Rahmen derer dann eine Prüfung für eine Auskunftserteilung im Einzelfall mit grundsätzlich positiver Vorgabe durchgeführt werden kann.

Insgesamt waren unter Berücksichtigung der vorgenannten Hinweise bei den Überprüfungen der Einzeleingaben keine Beanstandungen veranlaßt.

Einzelprobleme

Aus der Vielzahl von Eingaben und den verschiedenen Erörterungen, die ich mit dem BfV sowie den zuständigen Stellen im Bundesministerium des Innern über Verbesserungen des Datenschutzes im Bereich des BfV führte, seien folgende Einzelfragen hervorgehoben:

— zur Begrenzung des Zugriffs des BfV auf Dateien im INPOL-System des BKA s. o. 2.8.2;

— zur Frage der Anlegung und Speicherung personenbezogener Akten im Zusammenhang mit der Beobachtung von Bestrebungen:

Es ist ein grundsätzliches Problem, in welchem Umfang im Rahmen der gesetzlich vorgesehenen Beobachtung von Bestrebungen neben der Einstellung von Erkenntnissen über Einzelpersonen in die Organisationsakte auch eine personenbezogene Speicherung und/oder Anlegung von Akten erfolgt. Bisher gibt es keine befriedigende Lösung. Zwar besteht bereits eine formelle Restriktion aufgrund innerdienstlicher Anweisungen (die allerdings in einem inzwischen bereinigten Fall, den ich zu prüfen hatte, nicht eingehalten wurde). Gleichwohl muß der Versuch unternommen werden, klare materielle Kriterien zu entwickeln, nach denen im Zusammenhang mit der Beobachtung von Bestrebungen auch personenbezogene Akten angelegt werden und/oder eine personenbezogene Speicherung erfolgen dürfen. Der Bundesminister des Innern hat zugesagt, hier Überlegungen für weitere Verbesserungen anzustellen.

— Weniger belastende Form der Speicherung

Bei der Prüfung eines Einzelfalles wurde festgestellt, daß der Einsender, wie von ihm vermutet, in der Abteilung Spionage des BfV personenbezogen registriert war. Dies war zunächst auch mit Recht geschehen, doch entfiel die Rechtfertigung weiterer unveränderter personenbezogener Speicherung, nachdem aus der Aktenlage erkennbar war, daß jeglicher Spionageverdacht ausgeräumt worden war. Ich habe daher diesen Fall zum Anlaß genommen, die Frage zu erörtern, wie die weitere Speicherung in solchen Fällen vorgenommen werden darf, wenn — wie im vorliegenden Fall — die Akte nur noch aus Verwaltungsgründen erforderlich ist, z. B. aufgrund fortlaufender Eingaben der betreffenden Person im Zusammenhang mit dem früheren Verfahren. Das BfV hat zugesagt, in solchen Fällen eine Umspeicherung der Akte auf ein neutrales Aktenzeichen vorzunehmen. Damit wird klargestellt, daß die Person nicht mehr aus Verfassungsschutzgründen gespeichert wird.

— Beobachtung von Betriebsratswahlen

Im Rahmen der gesetzlichen Aufgabe nach § 3 Abs. 1 Nr. 1 des Bundesverfassungsschutzgesetzes (Beobachtung verfassungsfeindlicher Bestrebungen) koordiniert das BfV Erhebungen über Betriebsratswahlen und wertet die Ergebnisse aus. Im Jahre 1978 wurden in Zusammenarbeit mit den Landesbehörden für Verfassungsschutz aus ca. 900 größeren Betrieben Angaben erhoben. Rund 4 600 Betriebsratsmitglieder oder ca. 2 % aller gewählten Betriebsratsmitglieder in der Bundesrepublik wurden dadurch in die Erhebungen einbezogen. Das BfV hat nach eigener Auskunft in keinem Fall Einzelangaben über bestimmte Betriebsratsmitglieder an Dritte weitergegeben. Außerdem erfolgte in keinem Fall eine neue personenbezogene Speicherung allein aufgrund der Tatsache der Wahl zum Betriebsrat, weil dies allein kein Grund für eine personenbezogene Speicherung durch das BfV sein kann und ist.

Als die Tatsache der Beobachtung von Betriebsratswahlen in der Öffentlichkeit bekannt wurde, war mangels schneller Aufklärung durch die zuständigen Behörden der Eindruck entstanden, als würde jedes Betriebsratsmitglied in der Bundesrepublik allein aufgrund dieser Eigenschaft personenbezogen beim BfV gespeichert und als finde eine rege Übermittlung personenbezogener Daten von Betriebsräten zwischen BfV und anderen Stellen statt. Diese Sorge kam auch in einer Eingabe des Betriebsrats einer

größeren Firma zum Ausdruck. Sie war, wie die vorstehenden Ausführungen zeigen, unbegründet.

— In einer anderen Eingabe und ebenso jüngst bei öffentlichen Veranstaltungen wurde die Sorge geäußert, daß Personen, die Mitglieder von Amnesty International oder für diese Organisation tätig sind, personenbezogen registriert würden. Meine Ermittlungen ergaben keinen Anhaltspunkt dafür, daß jemand nur deshalb vom BfV beobachtet oder gespeichert wird, weil er Mitglied dieser Vereinigung ist oder für sie Demonstrationen anmeldet oder in sonstiger Weise ihre Tätigkeit unterstützt.

— Angebliche Überprüfung von Teilnehmern an einer Demonstration in Frankreich:

Wie schnell sich unbegründetes Mißtrauen gegenüber dem BfV (und dies gilt wohl für alle Sicherheitsbehörden) breitmachen kann, zeigt folgender Fall. Deutsche Teilnehmer an einer Demonstration in Frankreich wurden an der Grenze von französischen Sicherheitsbeamten überprüft. Die Demonstranten vermuteten, daß es sich hierbei um deutsche Sicherheitsbeamte gehandelt habe und daß ihre Namen an das BfV weitergeleitet worden seien. Diese Befürchtung brachten sie einem Landtagskandidaten gegenüber zum Ausdruck, der sich an mich mit der Bitte um Überprüfung wandte. Ohne jedoch meine Antwort abzuwarten oder aber bei den für die Grenzkontrolle zuständigen Behörden nachzufragen, veröffentlichte der Einsender den von ihm vermuteten Sachverhalt als angebliche generelle Überprüfungsmaßnahme deutscher Sicherheitsbehörden, die er in scharfer Form kritisierte. Die deutschen Sicherheitsbehörden hatten jedoch mit den Aktivitäten der französischen Beamten nichts zu tun und haben mit ihnen nicht zusammengearbeitet.

— Angebliche Speicherungen beim BfV als Grund für die Ablehnung von Bewerbungen:

Wie leichtfertig und verantwortungslos die Furcht vor den Verfassungsschutzbehörden ausgenutzt werden kann, zeigt ein Fall, in dem ein Einsender um Überprüfung angeblicher Speicherung seiner personenbezogenen Daten beim BfV bat. Eine Firma hatte seine Einstellung mit der Begründung abgelehnt, daß beim Verfassungsschutz nachteilige Erkenntnisse über seine Person vorlägen. (Einen ähnlichen Fall hat es bereits im vorigen Jahr gegeben).

Die Überprüfung zeigte, daß die betreffende Firma die angebliche Speicherung als Vorwand verwendete, um die ihr unwillkommene Bewerbung des Einsenders abschlägig zu bescheiden. Dies ergab sich bereits daraus, daß im konkreten Fall für eine Sicherheitsüberprüfung, die allein Grundlage für die Übermittlung eventueller Erkenntnisse über den betreffenden Bewerber hätte sein können, nicht das BfV, sondern der MAD zuständig gewesen wäre. Bei beiden Behörden lagen tatsächlich keine entsprechenden Nachfragen oder Erkenntnisse vor. In diesem Fall haben beide betroffene Sicherheitsbehörden die Auskunft gestattet. Würde auch in solchen Fällen vom Auskunftsverweigerungsrecht der Sicherheitsbehörden Gebrauch gemacht und nicht wie im vorgenannten Beispiel darauf verzichtet, dann bliebe grundlos Mißtrauen oder Furcht bei den Betroffenen zurück.

— Erste technische Detailprüfung:

Im Herbst wurde eine erste technische Detailprüfung durchgeführt. Sie hatte den Zweck, die Sicherheitsmaßnahmen bei der Archivierung der Protokollbänder und -bestände allgemein, das Verfahren und den Zeitraum bei der Löschung der Sicherungsbestände sowie die Dateienübersicht und Programmdokumentation zu überprüfen.

Dabei wurde festgestellt, daß die Dateienübersicht und die Programmdokumentation aus datenschutzrechtlicher Sicht nicht zufriedenstellend angelegt waren. Dies war offenbar in erster Linie auf eine unzutreffende restriktive Auslegung der Pflicht nach § 15 BDSG durch die Fachaufsicht zurückzuführen. Das BfV versprach jedoch umgehende Verbesserungen auf der Grundlage meiner Vorschläge. Aus diesem Grunde konnte von einer förmlichen Beanstandung abgesehen werden. Ich werde diesen Punkt jedoch weiter im Auge behalten. Im übrigen wurden keine nennenswerten Mängel entdeckt. Die Prüfung verlief mit voller Unterstützung und Offenheit seitens des BfV.

2.8.6 Bundesministerium der Verteidigung und Amt für Sicherheit der Bundeswehr

Allgemeines und Überblick

Auch in diesem Bereich war sowohl auf dem Sektor der Wehrersatzverwaltung als auch bezüglich der Tätigkeit des Militärischen Abschirmdienstes (MAD) ein sprunghafter Anstieg der Eingaben zu verzeichnen. Die Arbeitsatmosphäre kann ich auch hier wieder als erfreulich bezeichnen. Das gilt nicht zuletzt auch für den Tätigkeitsbereich des MAD. In allen Fällen wurden meine Anregungen zu einer Verbesserung des Datenschutzes aufgegriffen, so daß auch hier in keinem Fall eine Beanstandung ausgesprochen werden mußte.

Wehrersatzverwaltung

Folgende Problembereiche, die jeweils Gegenstand mehrerer Eingaben waren, sind hervorzuheben:

— Speicherung von Personen, die endgültig aus der Wehrüberwachung ausscheiden:

Während früher auch die Daten von Personen, die endgültig aus der Wehrüberwachung ausscheiden (Wehrdienstunfähige, vom Wehrdienst Befreite und anerkannte Kriegsdienstverweigerer) bis zum davon unabhängig bestehenden Ablauf der Wehrpflicht weiterhin vollständig im Wehrinformationssystem (Wewis) gespeichert blieben, werden diese Daten nunmehr aufgrund meiner Empfehlung nach rechtskräftiger Feststellung des Ausscheidens aus der

Wehrüberwachung gelöscht. Es bleiben lediglich die zu statistischen Zwecken anonymisierten Angaben gespeichert. Außerdem wird in Aktenform der Nachweis über die Gründe für das Ausscheiden bei dem jeweiligen Kreiswehrersatzamt aufbewahrt. Personenbezogen in Dateien gespeichert werden also nur noch die Daten der Wehrpflichtigen, die weiterhin der Wehrüberwachung unterliegen.

— Übermittlung von Daten über Reservisten an den Verband der Reservisten der Deutschen Bundeswehr e. V. durch den Bundesminister der Verteidigung:

Dieser Sachverhalt wurde in mehreren Eingaben gerügt, weil hier unzulässige Datenübermittlungen in unbekanntem Ausmaß befürchtet wurden. Nach eingehender Prüfung des Sachverhalts kann jedoch folgendes festgestellt werden:

Die Übermittlung beschränkt sich allein auf Name, Vorname und Anschrift des entlassenen Soldaten. Sie geschieht zur Reservistenbetreuung durch den Verband der Reservisten der Deutschen Bundeswehr e. V. Die Mitarbeit der Reservisten ist freiwillig. Die Betreuung besteht in der Veranstaltung wehrpolitischer Seminare, militärischer Übungen etc. Dies ist als eine im öffentlichen Interesse liegende Aufgabenerfüllung in Wahrnehmung des Verteidigungsauftrages nach Art. 87 a GG zu sehen. Während sie bis 1971 vom Bundesministerium der Verteidigung selbst wahrgenommen wurde, erfolgte dann eine Übertragung auf den Verband der Reservisten, die einerseits einer Intensivierung der Arbeit dienen, andererseits den freiwilligen Charakter der Reservistenbetreuung unterstreichen sollte. Der Verband, der überwiegend aus Bundesmitteln finanziert wird, kann seine Aufgabe aber nur erfüllen, wenn ihm die Daten der entlassenen Soldaten im vorerwähnten Umfang mitgeteilt werden.

Bei dieser Überprüfung wurde allerdings auch festgestellt, daß verschiedene Ortsgruppen der Reservistenverbände noch alte Adressenaufkleber bei der Werbung um Mitarbeit verwendeten, die die Personenkennziffer des betroffenen Soldaten enthielten. Der Bundesminister der Verteidigung hat auf meinen Vorhalt den Reservistenverband angewiesen, die Verwendung alter Adressenaufkleber einzustellen und diese zu vernichten. Eine Übermittlung der Personenkennziffer an die Reservistenverbände erfolgt nicht mehr.

— Datenabgleich zwischen Industrieunternehmen und Kreiswehrersatzämtern:

In mehreren Zeitschriften war vermutet worden, daß ein solcher Datenabgleich stattgefunden habe oder stattfinde.

Meine Nachforschungen haben folgendes ergeben:

In den Jahren 1972 und 1975, also vor Inkrafttreten des BDSG, hat in der Tat ein größeres Unternehmen dem zuständigen Kreiswehrersatzamt je einen Ausdruck mit den Daten der wehrpflichtigen Arbeitnehmer zugeleitet, die bei dem Werk aus Gründen der Rezession entlassen werden sollten. Die Übergabe erfolgte zu dem Zweck, diesen Arbeitnehmern die Entlassung durch Einberufung zum Wehrdienst zu ersparen und den Wehrpflichtigen den Anspruch auf Weiterbeschäftigung nach dem Arbeitsplatzschutzgesetz nach Ableistung des Wehrdienstes zu erhalten. Hierdurch konnte ca. 50 Personen die Entlassung erspart werden.

Die Aktion geschah jeweils mit Zustimmung der zuständigen Wehrbereichsverwaltung, aber ohne Kenntnis des Bundesministers der Verteidigung. Seitdem hat ein solches Verfahren, das trotz des gut gemeinten Anliegens datenschutzrechtlich bedenklich ist, nicht mehr stattgefunden. Es würde auch gegen zwischenzeitlich erlassene Anweisungen des Bundesministers der Verteidigung verstoßen.

Militärischer Abschirmdienst (MAD)

Hier ist auf folgende Problempunkte hinzuweisen:

— Rechtsgrundlage der Tätigkeit des MAD:

Ebenso wie beim BND fehlt auch für den MAD eine klare gesetzliche Aufgaben- und Befugnisumschreibung, soweit es sich nicht um die Tätigkeit im Rahmen des G 10 handelt. Insoweit kann auf die Ausführungen zum BND verwiesen werden (s. o. 2.8.4).

— Rechtsgrundlage für Sicherheitsüberprüfungen im Rahmen der Erfüllung der Wehrpflicht:

Ähnlich wie andere Behörden (s. o. 2.8.1) verfügen auch die Wehrbereichsbehörden und der MAD über keine klare Rechtsgrundlage für die Durchführung der materiell an sich unbestreitbar notwendigen Sicherheitsüberprüfungen. Kann schon normalerweise die Lücke nicht mit dem Hinweis auf die Freiwilligkeit der Angaben geschlossen werden, so gilt dies im Bereich der Wehrpflicht um so mehr und vor allem dort, wo Reservisten sich einer erneuten Sicherheitsüberprüfung unterziehen müssen, weil sie im Rahmen der Planungen für den Verteidigungsfall entsprechend eingeplant werden müssen. Während man für die Berufssoldaten notfalls auf die §§ 7 ff. des Soldatengesetzes und wohl überwiegend auf die Freiwilligkeit zurückgreifen kann, fehlt es für die Wehrpflichtigen an ähnlichen Bestimmungen. § 24 des Wehrpflichtgesetzes, der die Pflichten einer der Wehrüberwachung unterliegenden Person abschließend regelt, enthält keinerlei Hinweis auf Auskunftspflichten, die auch nur annähernd die Sicherheitsüberprüfung betreffen könnten. Der Bundesminister der Verteidigung hat jedoch angekündigt, daß er bei der nächsten Änderung des Wehrpflichtgesetzes eine entsprechende Befugnis in dieses Gesetz aufnehmen will. Es wäre erfreulich, wenn der Bundesminister des Innern dies zum Anlaß nähme, auch seinerseits für eine entsprechende Klarstellung im übrigen Bereich zu sorgen.

— In einer Eingabe der gesamten Studentenschaft einer baden-württembergischen Universität war auf der Basis von Presseveröffentlichungen befürchtet worden, daß Daten von allen Angehörigen der Universität an den MAD zu weiteren Überprüfungen weitergeleitet worden seien. Meine Nachforschungen haben ergeben, daß eine Verbindung mit dem MAD in keinem Fall bestanden hat.

— Nach anderen Presseverlautbarungen sollen „Schnüffelaktionen gegen Wehrpflichtige" in der Form stattfinden, daß die Daten des gesamten Jahrgangs einzuberufender Wehrpflichtiger mit dem Bestand der Personaldaten im nachrichtendienstlichen Informationssystem NADIS abgeglichen und überprüft werden. Nach meinen Ermittlungen wurden nur in einem Fall vor meinem Amtsantritt die von Wehrersatzbehörden gespeicherten Daten der tauglich gemusterten Wehrpflichtigen eines Jahrganges mit NADIS abgeglichen, um herauszufinden, ob sich hierunter Personen befinden, die von der Bundeswehr fernzuhalten sind und deshalb gar nicht erst eingezogen werden sollten. Dieses Verfahren wird nicht mehr praktiziert.

2.8.7 Hausinspektion des Deutschen Bundestages

Anläßlich der im Zusammenhang mit der Sammlung von Besucherscheinen aufgetauchten datenschutzrechtlichen Probleme wurde der Hausinspektion des Deutschen Bundestages ein erster Informationsbesuch abgestattet.

Folgendes ist aus den dabei geführten Erörterungen festzuhalten:

— Die Besucherscheine, die in Dateiform abgelegt werden, werden nunmehr maximal ein Jahr aufbewahrt. Anschließend werden sie vernichtet.

— Die Hausinspektion besitzt eine umfassende sachliche polizeiliche Zuständigkeit. Sie ist lediglich in örtlicher Hinsicht beschränkt, nämlich auf die für die Erfüllung der Aufgaben des Bundestages notwendigen Gebäude.

  Das Hauptproblem ist die Frage der Rechtsgrundlage ihres Tätigwerdens. Die Hausinspektion ist eine Sonderpolizei des Bundes; der Präsident des Deutschen Bundestages übt mit ihrer Hilfe seine unmittelbar im Grundgesetz verankerte Polizeigewalt aus. Zwar wird in der Literatur vereinzelt behauptet, die Befugnisse seien aus der insoweit fortgeltenden Generalklausel des preußischen Polizeiverwaltungsgesetzes abzuleiten. Doch wird diese sehr zweifelhafte Auffassung, die nirgends ausdrücklich niedergelegt ist, offenbar von der Hausinspektion selbst nicht geteilt.

  Sie stützt ihre Befugnisse vielmehr unmittelbar auf Artikel 40 Abs. 2 GG. Das ist jedoch ebenfalls problematisch, denn die unmittelbare Anwendbarkeit einer Bestimmung des Grundgesetzes ist, wie Artikel 13 Abs. 3 GG zeigt, die absolute Ausnahme und dann beschränkt auf eine bestimmte Maßnahme. Eine Dienstanweisung aus dem Jahre 1976 enthält in Anlehnung an die allgemeinen Grundsätze des Polizeirechts der Länder einen „Befugniskatalog", der den Polizeivollzugsbeamten als Richtlinie für ihr polizeiliches Handeln dient. Diese Dienstanweisung wird zur Zeit überarbeitet. Der künftigen Dienstanweisung wird der Musterentwurf eines einheitlichen Polizeigesetzes des Bundes und der Länder zugrunde gelegt. Besser wäre es freilich, wenn die Hausinspektion sich auf ein Polizeigesetz stützen könnte. Es war auch bereits mehrfach der Entwurf eines Befugnisgesetzes für die Hausinspektion vorgesehen, doch wurden die Arbeiten stets mit dem Hinweis auf ein notwendiges einheitliches Bundespolizeigesetz zurückgestellt. Das Vorhaben für ein einheitliches Bundespolizeigesetz wird aber zur Zeit nicht mehr weiter verfolgt. Damit besteht insbesondere gegenwärtig keine Möglichkeit, die Grundlagen für die erforderlichen und vertretbaren Informationsbefugnisse aller Polizeien des Bundes zu vereinheitlichen und durch klare Beschreibung in rechtsstaatlicher Weise festzulegen.

2.8.8 Zusammenfassende Würdigung und Ausblick auf die Tätigkeit im Jahre 1980

Das Jahr 1979 brachte für den Datenschutz im Bereich der Sicherheitsbehörden Fortschritte. Bei der Wertung der hier geschilderten Verbesserungen, die zum Teil durch meine Tätigkeit erreicht, zum Teil aus Eigeninitiative der Behörden entwikkelt wurden, muß bedacht werden, daß die Probleme des Datenschutzes gerade im Sicherheitsbereich nicht von heute auf morgen lösbar sind. Daher ist weiterhin zu fordern, den bereichsspezifischen Datenschutz zu verbessern. Dies kann auch durch innerdienstliche Vorschriften geschehen. Auf längere Sicht ist jedoch eine Novellierung und Präzisierung der bestehenden gesetzlichen Teilvorschriften zusätzlich erforderlich. Das gilt insbesondere für Vorschriften wie die Sammlungs- und Übermittlungsvorschriften nach dem Bundeskriminalamtsgesetz und dem Bundesverfassungsschutzgesetz. In diesen Zusammenhang gehört aber auch die Forderung nach eindeutigen gesetzlichen Grundlagen für die Tätigkeit von BND und MAD. Da Datenschutz ganz wesentlich in möglichst weitgehender Offenheit besteht, sollten sich die Sicherheitsbehörden darüber hinaus stets bemühen, die Schwelle des „absoluten Geheimnisses" nicht zu früh anzusetzen. Hier wird — wie an manchen Beispielen gezeigt — nur unnötiges Mißtrauen und unbegründete Angst geschaffen. Deshalb sollte die Bestimmung des § 13 Abs. 2 BDSG, die den Sicherheitsbehörden die Möglichkeit gibt, grundsätzlich und ohne Angabe von Gründen die Auskunft zu verweigern, neu überdacht werden, auch wenn es einige Fälle in diesem Jahr gegeben hat, in denen kein Gebrauch von § 13 Abs. 2 BDSG gemacht wurde.

Bei einem Vergleich mit dem Datenschutz im Bereich der Sicherheitsbehörden des Auslandes dürfte die Bundesrepublik günstig abschneiden. So

besteht im westlichen Ausland in wichtigen Ländern wie Großbritannien noch überhaupt kein Datenschutzgesetz, geschweige denn eine unabhängige Institution zur datenschutzrechtlichen Kontrolle. Es ist auch bekannt, daß gerade in England die Sicherheitsbehörden bislang alles daran setzten, den Schleier ihrer Geheimnisse nicht „lüften" zu müssen. In anderen Ländern wie z. B. in Frankreich besteht zwar die Möglichkeit einer Kontrolle auch im Sicherheitsbereich, doch ist nach bisherigen Auskünften eine eingehende Kontrolle, und sei es nur in Details, nicht erfolgt.

Außerdem ist es nach dem französischen Datenschutzgesetz der Datenschutzkommission untersagt, mehr als eine förmliche Antwort an den Einsender zu erteilen (Artikel 39 des Gesetzes Nr. 78 - 17 vom 6. Januar 1978). Die in diesem Jahr bei mir abgehaltene internationale Konferenz von unabhängigen Datenschutzkontrollinstitutionen hat gezeigt, daß der Datenschutz im Sicherheitsbereich in der Bundesrepublik wohl am weitesten gediehen ist. Nach allen bisherigen Erfahrungen muß auch gesagt werden, daß dies die Arbeit der Sicherheitsbehörden nicht beeinträchtigt oder gar gefährdet.

Als einen Schwerpunkt meiner Tätigkeit im Jahre 1980 sehe ich die weitere Intensivierung meiner Kontrolltätigkeit bei den Sicherheitsbehörden des Bundes unabhängig von konkreten Eingaben der Bürger.

Außerdem plane ich, mir durch weitere Informationsbesuche einen ersten Einblick über den Umfang der Informationsverarbeitung bei nicht so sehr im Blickpunkt der Öffentlichkeit stehenden Dienststellen des Sicherheitsbereichs zu verschaffen (z. B. bei Zollfahndungsdienststellen und bei der Bahnpolizei).

Für sehr wichtig halte ich auch die ständige Diskussion mit den Landesbeauftragten für den Datenschutz über die uns gemeinsam betreffenden Probleme der Sicherheitsbehörden im Arbeitskreis Sicherheit.

2.9 Nicht-öffentlicher Bereich

2.9.1 Versicherungen

Im Jahr 1979 haben sich wiederum viele Bürger an mich gewandt, um sich über die von Versicherungsgesellschaften verwendete formularmäßige Erklärung zum Datenschutz (sog. Datenschutzklausel) zu beschweren (zu den Einzelheiten vgl. 1. TB, 3.7.2.). Die in dieser Sache geführten Verhandlungen der Datenschutz-Kontrollinstanzen und des Bundesaufsichtsamtes für das Versicherungswesen mit der Versicherungswirtschaft konnten inzwischen abgeschlossen werden. Das Ergebnis, dessen praktische Umsetzung das Bundesaufsichtsamt im Laufe des Jahres 1980 durchgesetzt haben wird, besteht aus folgenden Teilen:

a) Die Versicherungsunternehmen werden eine Klausel mit einem neuen Text verwenden, dessen Formulierung so verbessert wurde, daß der Betroffene erkennen kann, welche seiner personenbezogenen Angaben zu welchen Zwecken welchen anderen Stellen übermittelt werden können. Da aus Raumgründen jedoch eine erschöpfende Darstellung nicht möglich ist, wird dem Versicherungsnehmer im Text der Klausel angeboten, ihm auf Wunsch zusätzliche Informationen zur Datenübermittlung zuzusenden.

b) Für diese Information wurde ein Merkblatt erstellt, das brancheneinheitlich verwendet werden wird. Darin werden die verschiedenen Fälle der Datenübermittlung näher dargestellt.

c) Um verschiedene Zweifelsfragen bei der Anwendung der Klausel und im Zusammenhang mit der Verarbeitung der personenbezogenen Daten zu klären, hat das Bundesaufsichtsamt für das Versicherungswesen die Unternehmen, die die Klausel verwenden möchten, aufgefordert, gemäß § 13 Versicherungsaufsichtsgesetz einen Antrag auf Genehmigung einer hierfür vorgegebenen geschäftsplanmäßigen Erklärung zu stellen. Darin wird z. B. geregelt, wie zu verfahren ist, wenn ein Versicherungsnehmer die Ermächtigungsklausel oder Teile von ihr gestrichen hat. Ferner ist z. B. festgelegt, daß die Übermittlung von Gesundheitsdaten an Versicherungsvertreter zu unterbleiben hat, wenn der Antragsteller seine Angaben nicht im Antragsformular gemacht, sondern sie statt dessen unmittelbar (unter Umgehung des Vertreters) dem Versicherer mitgeteilt hat.

Man kann heute noch nicht sagen, daß mit diesen Maßnahmen alle Datenschutzprobleme in der Versicherungswirtschaft gelöst sein werden; gewiß handelt es sich aber um einen wichtigen Schritt in Richtung auf eine bürgerfreundliche Verwirklichung des Datenschutzes.

2.9.2 Kreditsicherung

Auch bezüglich der in der Kreditwirtschaft verwendeten sog. Schufa-Klausel haben die Datenschutz-Aufsichtsbehörden der Länder in Verhandlungen mit den betreffenden Spitzenverbänden eine wesentliche Verbesserung erreicht (zum Sachverhalt und zur datenschutzrechtlichen Problematik s. 1. TB, 3.7.3.). Der Umfang der zu übermittelnden Daten wird präziser umschrieben (z. B. „die Daten des Kreditnehmers ... über die Aufnahme (Kreditbetrag, Laufzeit, Ratenhöhe) und Abwicklung dieses Kredits"). Außerdem sollen sämtliche Schufa-Geschäftsstellen mit ihren Anschriften und ihrem Wirkungsbereich bezeichnet werden, so daß der Betroffene sich direkt an die zuständige Stelle wenden kann.

Auch bei Anerkennung dieser Fortschritte kann die gefundene Lösung noch nicht voll befriedigen. Die Kreditwirtschaft hat sich zwar bereit gefunden, die neugefaßten Klauseln zu verwenden, beharrt jedoch auf ihrer Auffassung, daß die Datenübermittlung auch ohne Einwilligung zulässig sei, weil die Interessen der beteiligten Wirtschaftsunternehmen den schutzwürdigen Belangen der Betroffenen

vorgingen, so daß sich die Zulässigkeit aus § 24 BDSG ergebe. Die Gefahr künftiger Konflikte liegt damit auf der Hand.

Zu bedauern ist außerdem, daß sich die Kreditwirtschaft nicht bereit gefunden hat, die Klausel so informativ zu gestalten, wie dies von seiten der Datenschutz-Aufsichtsbehörden für wünschenswert gehalten wird. In der Klausel ist lediglich davon die Rede, daß der „Schutzgemeinschaft für Allgemeine Kreditsicherung" bestimmte Daten „zur Speicherung" übermittelt werden können. Für den Betroffenen ist aber weniger interessant, daß seine Daten bei der Schufa gespeichert werden; entscheidend für seine Datenschutzposition ist vielmehr, daß seine Daten damit allen Vertragspartnern der Schufa im Rahmen der Anschlußverträge zur Verfügung stehen. Daß der Wunsch nach einer entsprechenden Klarstellung mit dem Hinweis abgelehnt wurde, der Raum auf den Formularen sei zu knapp, zeugt von einer bedauerlichen Geringschätzung des Anspruchs des Bürgers auf Information.

3 Allgemeine Erfahrungen aus Prüfungen

3.1 Datenschutz als Organisationsaufgabe

Die Durchsetzung des Datenschutzes ist ganz wesentlich eine Organisationsaufgabe. Dabei ist es erforderlich, den inneren Zusammenhang zwischen

— der Übersicht über die Art der Daten (§ 15 Nr. 1),

— der Überwachung der ordnungsgemäßen Programmanwendung (§ 15 Nr. 2) und

— den Sicherungsauflagen (§ 6 und Anlage dazu)

zu erkennen und damit ein umfassendes Konzept zu entwickeln, das den Datenschutz sicherstellt.

Entsprechende organisatorische Veränderungen zur Verwirklichung des Datenschutzes sind vielfach unverzichtbar. Zum „Trost" der Datenverarbeiter kann aber bemerkt werden, daß sie oft zugleich den Nebeneffekt besserer Leistungsfähigkeit der Datenverarbeitung selbst haben und eine Vorbedingung für die bessere Steuerung der Arbeitsabläufe im eigenen Interesse der Behörde bzw. des Unternehmens sind.

Bei meinen Überprüfungen wurden solche Gesamtkonzepte überwiegend vermißt, und es zeigte sich, daß auch gute Lösungen für einzelne Probleme ein umfassendes Konzept nicht ersetzen können.

Das Fehlen klarer organisatorischer Lösungen liegt zu einem erheblichen Teil daran, daß die jeweilige EDV-Abteilung — zu unrecht — als Herr der Daten und Verfahren angesehen wird und die Fachabteilungen in die Rolle von Zulieferern geraten. Eine weitere Ursache ist das verbreitete Unbehagen gegenüber Kontrollen und Einschränkungen, von denen die eigenen Mitarbeiter betroffen wären. Es ist aber möglich, gemeinsam mit den davon Betroffenen und ihren Interessenvertretungen geeignete Schutzmaßnahmen zu entwickeln und einzuführen. Diese Art des Vorgehens ist auch deshalb zweckmäßig, weil das Verständnis für Kontrollmaßnahmen Voraussetzung für die Akzeptanz ist.

Insbesondere bei großen Datenbeständen werden manche möglichen Maßnahmen zur Verbesserung des Datenschutzes aus Kostengründen unterlassen. Dabei wird übersehen, daß gerade dann die Verantwortung für den Schutz personenbezogener Daten zu wirkungsvollen organisatorischen Maßnahmen verpflichtet.

3.2 Übersicht über die gespeicherten Daten

Um die notwendigen stellenspezifischen Verfahrensregelungen entwickeln und durchführen zu können, ist es erforderlich, die Strukturen und Abläufe kritisch zu prüfen. Dazu muß die Leitung eine genaue Übersicht über alle Informationsflüsse im eigenen Hause sowie von und nach außen gewinnen. Diesen Anspruch soll die Übersicht gemäß § 15 Nr. 1 BDSG erfüllen.

Im einzelnen soll diese Übersicht den folgenden Aufgaben dienen:

— Zulässigkeitsnachweis

  Anhand der Darstellung der Datenarten und der zugehörigen Aufgaben ist nachzuweisen, daß die Zulässigkeitsvoraussetzungen für jede Phase der Verarbeitung vorliegen und insbesondere die Daten nur von denen zur Kenntnis genommen werden, für die diese Kenntnis erforderlich ist.

— Offenlegung von Verantwortlichkeiten

  Durch die Angabe des für die Datensammlung zuständigen Bearbeiters wird die Verantwortung sichtbar und damit überprüfbar gemacht.

— Auswahl von Sicherungsmaßnahmen

  Nur anhand des Nachweises über alle Standorte, Transportwege, Verarbeitungen und Zugriffsmöglichkeiten können eine an den Datenarten und Zugänglichkeiten orientierte Risiko- und Schwachstellenanalyse durchgeführt und die angemessenen Maßnahmen ausgewählt werden, um die Ausführung der Datenschutzvorschriften zu gewährleisten.

— Überwachung der Programmanwendung

  Zur Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme ist es er-

forderlich, die Funktionen der Programme daraufhin zu überprüfen, ob sie für die einzelnen Datenfelder genau die vorgesehenen Verarbeitungsschritte durchführen.

— Verpflichtung und Schulung

Der in der Übersicht nachgewiesene befugte Personenkreis ist auf das Datengeheimnis zu verpflichten und den Aufgaben entsprechend zu schulen. Der Nachweis der Standorte der Datenträger ermöglicht darüber hinaus die Feststellung der außerdem zu verpflichtenden Personen (z. B. Wartungstechniker, Reinigungsdienst).

— Wahrung der Rechte der Betroffenen

Die Übersicht erleichtert die Erteilung von Auskünften an die Betroffenen, die Durchführung von Berichtigungen und den Erlaß stellenspezifischer Regelungen zur Sperrung und Löschung.

Eine Dateien-Übersicht, die diese Anforderungen im wesentlichen erfüllt, habe ich nur bei einer der überprüften Stellen vorgefunden. Bei vielen anderen bestand die Übersicht praktisch nur aus den gesammelten Meldungen zu dem von mir geführten Register bzw. zu den Veröffentlichungen im Bundesanzeiger. So konnte es vorkommen, daß Programme eingesetzt wurden, deren Existenz der Behördenleitung bzw. dem internen Datenschutzbeauftragten nicht bekannt waren. In einem anderen Fall ging aus den Unterlagen des internen Datenschutzbeauftragten nicht hervor, welche Dateien und Anwendungen außerhalb des Hauses in Zweigstellen der Behörde betrieben werden. Dateien, die nicht in automatisierten Verfahren verarbeitet werden und nicht zur Übermittlung bestimmt sind, fehlten fast immer. Zwar gilt § 15 BDSG für diese Dateien nicht; Aufzeichnungen darüber sind gleichwohl notwendig, um eine Kontrolle darüber zu ermöglichen, ob die Voraussetzungen der Ausnahmevorschrift des § 1 Abs. 2 Satz 2 gegeben und die nach § 6 notwendigen Sicherungsmaßnahmen getroffen sind.

3.3 Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme

Die ordnungsgemäße Anwendung von Datenverarbeitungsprogrammen kann nur gewährleistet werden, wenn

— die Programme selbst kontrollierbar sind,

— die Verantwortung für jeden einzelnen Einsatz eines Programms nachgewiesen wird und

— innerhalb eines Programmablaufs die Zulässigkeit und Richtigkeit der einzelnen Anwendungsfälle kontrollierbar sind.

3.3.1 Programmkontrolle

Die Programmkontrolle ist erst in ganz bescheidenen Ansätzen möglich. Das liegt zum Teil daran, daß häufig schon die Dokumentation unzureichend ist und erst im Laufe der Zeit auf den erforderlichen Stand gebracht werden kann. Ein Teil der Programmkontrolle muß darin liegen, daß die Fachabteilung das Verfahren durch konkrete Vorgaben an die EDV-Abteilung bestimmt und das Einhalten der Vorgaben bei der Abnahme der Programme überprüft.

Bei den größeren der überprüften Behörden werden die Notwendigkeit eines solchen Vorgehens in zunehmendem Maße erkannt und entsprechende Verfahrensvorschriften entwickelt und angewendet. Insgesamt überwiegen aber noch die negativen Erfahrungen.

3.3.2 Einsatzkontrolle

Die Kontrolle des Programmeinsatzes ist in der Regel mit geringem Aufwand realisierbar. Die von den existierenden Betriebssystemen bereitgestellten Protokollierungen ermöglichen eine bis auf Sonderfälle vollständige Aufzeichnung der tatsächlichen Abläufe. Wird durch organisatorische Maßnahmen sichergestellt, daß für jeden Programmeinsatz ein nachprüfbarer Auftrag der zuständigen Abteilung vorliegt, so ist ein Soll-Ist-Vergleich leicht durchführbar.

Bei den Überprüfungen wurde festgestellt, daß bei einer Reihe von Anwendern derartige Kontrollen zumindest als Stichproben durchgeführt werden. Häufig wurden solche Kontrollen jedoch unterlassen. In einem Fall wurden sogar die vom Betriebssystem vorgesehenen Protokollierungen außer Kraft gesetzt

3.3.3 Einzelfallkontrolle

Verfahren, die gewährleisten, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben und daraus abgerufen worden sind, werden im allgemeinen nicht eingesetzt, insbesondere nicht im polizeilichen Informationssystem. Sie wurden nur in ganz wenigen Sonderfällen angetroffen.

Das Fehlen entsprechender Maßnahmen wird oft damit begründet, daß eine lückenlose Aufzeichnung aller Datenverarbeitungsvorgänge zu arbeitsaufwendig ist und zudem neue Dateien mit zusätzlichen Datenschutzproblemen schafft. Denn die Protokolldateien würden dann auch z. B. Löschungen und ergebnislose Anfragen enthalten und damit deutlich über die Angaben in den Bestandsdateien hinausgehen.

Die Möglichkeit zur Kontrolle verlangt aber nicht unbedingt eine exzessive Protokollierung. Einen ausreichenden Schutzeffekt können auch organisatorische Maßnahmen haben.

Solche organisatorische Maßnahmen können sein

— das Entwerten bzw. Abzeichnen der Eingabebelege

— das Dokumentieren der Personaleinsatzzeiten

— das Aufzeichnen des Eingabeplatzes und des Datums der Eingabe bzw. der letzten Änderung im Datensatz

— das Einschränken der Zugriffsmöglichkeit des Sachbearbeiters auf den Teil des Bestandes, für den er allein verantwortlich ist.

Dort, wo es nach der Art der Anwendung angemessen ist, können organisatorische Maßnahmen durch stichprobenartige Protokollierung in ihrer Wirkung verstärkt werden. Diese Protokolle sind möglichst bald zu Kontrollzwecken auszuwerten und dann zu vernichten.

Die technischen und organisatorischen Möglichkeiten, Einzelfallkontrollen auch ohne vollständige Protokollierung durchzuführen, sind bei weitem nicht ausgeschöpft. Die Anwender sollten sich verstärkt bemühen, hierfür stellenspezifische Lösungen zu entwickeln.

3.4 Sicherungsmaßnahmen

Die notwendigen Maßnahmen ergeben sich aus der Risiko- und Schwachstellenanalyse und sind deshalb von Fall zu Fall unterschiedlich. Sie können hier nicht erschöpfend erörtert werden. Die folgende Darstellung beschränkt sich auf die bei Überprüfungen am häufigsten angetroffenen Mängel.

3.4.1 Abgrenzung der Sicherheitsbereiche

Bei allen überprüften Stellen waren für den Rechenzentrumsbetrieb Sicherheitsbereiche vorgesehen. Die bauliche Sicherung dieser Bereiche einschließlich aller Türen und Türschlösser war jedoch nur bei wenigen Stellen geeignet, unberechtigtes Eindringen wirksam zu verhindern. Die Zugangsregelungen waren oft zu pauschal, so daß auch Personen zu Einrichtungen Zutritt hatten, für die dafür keine Notwendigkeit bestand. Dadurch wurde die Zahl der Zutrittsberechtigten unvertretbar groß. In einem Fall besaßen 90 Personen einen Sicherheitsschlüssel und konnten praktisch unkontrolliert an nahezu sämtliche Datenträger gelangen.

3.4.2 Führung des Datenträger-Bestands

Die Sorgfalt bei der Verwahrung und Verwaltung von Datenträgern entsprach häufig nicht den zu stellenden Anforderungen. So wurden z. B. für die Lagerung beschriebener Bänder Räume benutzt, die auch Personen betreten durften, die zur Nutzung dieser Daten aber nicht befugt waren. Diese Personen unterstanden keiner besonderen Aufsicht.

Häufig wurden keine Belege über den Verbleib der aus dem Archiv entnommenen Datenträger geführt; gelegentlich konnten die Maschinenbediener unkontrolliert Datenträger verwenden, und in einem Fall fehlten sogar Aufzeichnungen darüber, welche Dateien auf welchen Bändern geführt wurden.

Oft wurden die Gefährdungen unterschätzt, die bei der Lagerung nicht mehr benötigter Datenbestände entstehen können. In einigen Fällen wäre es leicht möglich gewesen, Magnetbänder mit überholten Daten (Stand vom Vortage) unbemerkt zu entnehmen und wieder zurückzubringen. In zwei Fällen standen größere Mengen nicht mehr benötigter Lochkarten in leicht zugänglichen Fluren unbeaufsichtigt zur Abholung bereit.

3.4.3 Transport von Datenträgern

Eine besondere Gefährdung liegt stets im Transport von Daten, vor allem soweit sie auf Papier lesbar wiedergegeben sind. Bei unverschlossenen Sendungen, wie sie weithin immer noch üblich sind, ist die Kenntnisnahme durch Dritte z. B. dann möglich, wenn die Sendung dem Betroffenen in den Hausbriefkasten geworfen wird. Die vom Briefgeheimnis geschützte Versendung im geschlossenen Umschlag setzt sich erst langsam durch. Das dafür oft angeführte Kostenproblem darf hier aber nicht den Ausschlag geben.

Während beim Versand von maschinenlesbaren Datenträgern mit personenbezogenen Daten die Versandform „Wertpaket" schon weit verbreitet ist, erfolgt der Rücktransport nicht gelöschter Magnetbänder gelegentlich noch im einfachen Paket. Dies zeigt, daß die Sorgfalt, die auf die Sicherung des Ablaufs verwendet wird, beim Schutz personenbezogener Daten noch nicht genügend geübt wird.

Eine sichere Methode, Daten auf dem Versandweg vor unbefugter Nutzung zu schützen, ist die kryptografische Verschlüsselung. Entsprechende Verfahren stehen zwar schon zur Verfügung, für den Einsatz durch unterschiedliche Teilnehmer fehlen jedoch noch Normen und zuverlässige Verfahren der Schlüsselverwaltung. An den Arbeiten zur Normung im Rahmen des DIN bin ich beteiligt.

4 Zum weiteren Ausbau des Datenschutzes

4.1 Bereichsspezifische Vorschriften

Das BDSG ist als umfassendes „Grundgesetz" des Datenschutzes angelegt und enthält deshalb notwendigerweise eine Vielzahl von Generalklauseln und unbestimmten Begriffen. Diese begründen für die Praxis Unsicherheiten und sind vielfach auch nicht hinreichend streng, um den wünschenswerten Schutz von Interessen der Bürger in allen Zusammenhängen zu gewährleisten. Den Verfassern des Gesetzes war bewußt, daß zu diesem Gesetz bereichsspezifische Datenschutznormen hinzutreten müßten, die den Schutz des Bürgers in wichtigen Bereichen von Verwaltung und Wirtschaft verstärken müssen. In einigen Bereichen mag es auch angehen, hinter den allgemeinen Regeln zurückzubleiben, wenn der Gefähr-

dungstatbestand genau bekannt ist und einen geringeren Schutz, als im allgemeinen Gesetz vorgesehen, erfordert. Es kann nicht entschieden genug betont werden, daß bereichsspezifische konkrete Datenschutznormen, wie sie bereits in den vorangehenden Abschnitten gefordert worden sind, vordringlich benötigt werden. Einige solcher Bestimmungen sind inzwischen geschaffen worden, so die Novellen zur Statistikgesetzgebung (vgl. oben 2.4.1), oder doch in Vorbereitung, so zum Teil das neue Personalausweisgesetz (oben 2.1.3), das Melderechtsrahmengesetz (oben 2.1.4) und das Verkehrszentralregistergesetz. Die an die Neufassung von § 35 SGB I anknüpfende Gesetzgebung zum Sozialdatenschutz (oben 2.6.3) ist bedauerlicherweise noch nicht vollendet worden, obwohl auch hier nach wie vor ein erheblicher Regelungsbedarf besteht. Die Informationsverarbeitung durch Sicherheitsbehörden muß ebenfalls gesetzlich geregelt werden (oben 2.8.8).

Darüber hinaus hat sich erwiesen, daß das geltende Datenschutzrecht den besonderen Problemen nicht hinreichend gerecht wird, die durch den Datenbedarf für Zwecke der wissenschaftlichen Forschung entstehen. Hier können sich Konflikte mit verschiedenen Geheimhaltungsvorschriften ergeben, so mit dem Sozialgeheimnis (§ 35 SGB I), mit dem Arztgeheimnis und anderen Berufsgeheimnissen, mit dem Statistikgeheimnis und neuerdings auch mit besonderen Bestimmungen in Statistikgesetzen. Spezialbestimmungen finden sich in den Landesdatenschutzgesetzen und anderen Landesgesetzen. Über die Angemessenheit der geltenden Normen und über ihre korrekte Anwendung besteht Streit; insbesondere halten die Vertreter der Wissenschaft eine den Datenschutz bevorzugende Abwägung zwischen dem Geheimhaltungsinteresse der Betroffenen und dem Bedürfnis nach wissenschaftlicher Verwertung personenbezogener Daten für zu einseitig. Zwar werden solche Bedenken nicht durch eine für alle Felder der wissenschaftlichen Forschung geltende Regelung zu überwinden sein; viel spricht dafür, daß der vom Bundesgesetzgeber bei den Statistikgesetzen gewählte Weg zweckmäßiger ist, die Zulässigkeit der Datenverarbeitung für wissenschaftliche Zwecke je nach Materie differenziert zu regeln. Zu fordern ist jedoch, daß zumindest einige Grundsätze der Verwendung personenbezogener Daten für Forschungszwecke in relativ allgemeiner Form niedergelegt werden — nicht zuletzt damit sich für den Gesamtbereich der Forschung ein gemeinsamer Verhaltenscodex entwickeln kann.

Besonderer Regelungsbedarf besteht auch für das Archivwesen (oben 2.1.5). Verschiedene Anfragen von zeitgeschichtlich Interessierten und öffentliche Diskussionen über die Problematik der Publikation von Archivmaterialien haben gezeigt, daß es hier an allgemeingültigen Vorstellungen fehlt. Aus der Sicht mancher sind die Archive eine offene Flanke des Persönlichkeitsschutzes, während andere darauf abstellen, daß die Aufarbeitung der Zeitgeschichte auch den Zugriff auf Archivmaterial in möglichst weitem Umfang notwendig mache. Diese Frage spielt auch eine Rolle im Zusammenhang mit der geplanten Übernahme des Berliner Document-Center durch die Bundesregierung.

Im privaten Bereich der Informationsverarbeitung habe ich bei meiner Zusammenarbeit mit den zuständigen Aufsichtsbehörden der Länder verschiedene Problemfelder erkannt, für die besondere Datenschutzregeln gesetzlich fixiert werden sollten. Während die Verwendung von Anschriften zu Werbezwecken bereits im BDSG geregelt ist und eine Verbesserung dieser Regelungen dort ihren Platz finden könnte (vgl. 1. TB, 4.4), ist bei den Auskunfteien eine Mehrzahl von Einzelproblemen regelungsbedürftig, so daß ein besonderes Gesetz nach schwedischem oder amerikanischem Vorbild erwägenswert wäre. Insbesondere sollte verhindert werden, daß Kreditauskunfteien auch zu Zwecken tätig werden, die mit der Gewährung von Krediten nur wenig gemeinsam haben, wie etwa zur Sicherung von Vermieter- oder Arbeitgeberinteressen. Entscheidend ist freilich letztlich nicht die gesetzestechnische Einordnung solcher Regeln, ihre etwaige Verselbständigung oder ihre Einfügung in andere Gesetze, sondern die Schaffung sachnaher und den neueren Erkenntnissen des Datenschutzes entsprechender Gesetze überhaupt.

Spezialgesetzliche Vorschriften erscheinen auch wünschenswert für die Verarbeitung von Personaldaten durch Arbeitgeber/Dienstherren. Hier besteht die Gefahr, daß Personaldaten in Personalinformationssysteme in einem Ausmaß gespeichert und verarbeitet werden, das durch das konkrete Arbeitsverhältnis nicht mehr gefordert wird, sondern anderen Interessen des Arbeitgebers/Dienstherrn oder sogar Dritter dient. Der Gesetzgeber sollte daher Einschränkungen festlegen, die sich ausschließlich an den spezifischen Erfordernissen des Arbeits- bzw. Dienstrechtsverhältnisses orientieren.

Schließlich fehlt es an hinreichend wirksamen Schutzbestimmungen gegenüber Presse, Rundfunk und Film. Bereits parallel zum Gesetzgebungsverfahren über das BDSG waren Bestimmungen für einen spezifischen Datenschutz geplant. Sie müßten weiterverfolgt werden; denn hier ist eine Schwachstelle des Datenschutzes geblieben, die durch die Rechtsprechung zum allgemeinen Persönlichkeitsrecht nicht vollständig ausgefüllt wird.

Spezielle Datenschutzbestimmungen sind auch für die „Neuen Medien" erforderlich, deren versuchsweise Einführung inzwischen in verschiedenen Bundesländern betrieben wird. Ich kooperiere auf diesem Gebiet mit den Landesbeauftragten.

4.2 Zur Aufgabe des Datenschutzes

§ 1 BDSG bestimmt als Aufgabe des Datenschutzes, der Beeinträchtigung schutzwürdiger Belange der Betroffenen „durch den Schutz personenbezogener Daten vor Mißbrauch bei der Speicherung, Übermittlung, Veränderung und Löschung" entgegenzuwirken. Der Begriff „Mißbrauch" ist auch in der Überschrift des Gesetzes enthalten.

Tatsächlich geht es keineswegs nur um Schutz vor „Mißbrauch", sondern viel allgemeiner um die richtige Verteilung und Verwendung von Informationen und um die Verhinderung unnötiger oder einseitig

belastender Maßnahmen der Informationsverarbeitung. Die schutzwürdigen Belange, deren Beeinträchtigung entgegengewirkt werden soll, erschöpfen sich entgegen einer weit verbreiteten Vorstellung nicht in der Geheimhaltung „privater" oder „intimer" Daten oder in der Abwehr von „Schnüffelei" und Kenntnisnahme durch Unbefugte. Die verfassungsrechtliche Wurzel des Datenschutzes liegt nicht nur in Art. 1 Abs. 1 GG (Schutz der Menschenwürde) und Art. 2 Abs. 1 GG (freie Entfaltung der Persönlichkeit), sondern in einer Mehrzahl von Grundrechten, zu denen auch die Gewissensfreiheit, die Meinungs-, Versammlungs- und Vereinigungsfreiheit, das Post- und Fernmeldegeheimnis und die Berufsfreiheit gehören. Schutzwürdig ist auch das Interesse daran, nicht durch zweckfremde Weitergabe von Informationen z. B. in der eigenen beruflichen oder wirtschaftlichen Entwicklung behindert zu werden — zumindest dann, wenn die Verwendung unangemessen ist, weil sie so abseits von der ursprünglichen Zweckbestimmung liegt, daß der Betroffene damit im Normalfall nicht zu rechnen braucht.

Datenschutz ist ein Instrument unter anderen, die durch organisatorische und technische Überlegenheit begründete Schwäche des einzelnen oder kleiner Gruppen zu vermindern, tendenziell also mehr Waffengleichheit zu schaffen. Die Methode, mit der dies angestrebt wird, ist die Aufteilung der Informationen auf verschiedene Stellen und ihre Beschränkung auf die jeweils unverzichtbare Menge, in gewisser Weise also ihre „Rationierung" — mit der gewollten Folge, daß die Handlungsmöglichkeiten der einzelnen Stellen bis zu einem bestimmten Grade eingeschränkt werden. Die Rechtsprinzipien, durch die dies bewerkstelligt wird, sind die Zweckbindung der Information und das Erforderlichkeitsprinzip. Zusätzlich tritt das Prinzip der Transparenz der Informationsverarbeitung hinzu, das die Verwirklichung der anderen beiden Prinzipien kontrollierbar macht.

Aus diesen allgemeinen Überlegungen folgt, daß das BDSG in Richtung eines „Grundgesetzes der Informationsverarbeitung" weiterentwickelt werden muß, in dem die genannten tragenden Rechtsprinzipien für alle Phasen der Informationsverarbeitung noch stärker betont und in allen Verwaltungszweigen zur Geltung gebracht werden. Das ist bereits verfassungsrechtlich geboten: die Belastung des Bürgers, die mit der Erhebung und der Verarbeitung ihn betreffender Daten verbunden ist, darf nach dem Verhältnismäßigkeitsprinzip nur so weit gehen, wie der jeweilige Zweck der Datenverarbeitung es rechtfertigt. Daraus folgt auch in den Fällen eine Zweckbindung, wo das BDSG dies noch nicht explizit bestimmt. Es wird sich nicht vermeiden lassen, Ausnahmen von diesem strengen Prinzip zuzulassen, doch bedürfen sie besonderer Regelung und können nicht allein aus dem Gebot der Amtshilfe begründet werden.

4.3 Fortentwicklung des BDSG

Über die Novellierung des BDSG wird seit seinem Inkrafttreten gesprochen. Vorschläge dazu kamen aus Kreisen der Politik, der Wissenschaft, der Anwender in Verwaltung und Wirtschaft, schließlich auch von Betroffenen, also von denjenigen, zu deren Schutz das Gesetz erlassen wurde und die damit offenbar unzufrieden sind. Vor einiger Zeit hat die FDP-Fraktion des Deutschen Bundestages einen ausformulierten Gesetzentwurf zur Änderung des BDSG vorgelegt. Neuerdings existiert auch ein Entwurf der CDU/CSU.

Ich sehe hier davon ab, zu diesen Gesetzentwürfen im einzelnen Stellung zu nehmen. Sie enthalten eine Reihe von Vorschlägen, die ich nachdrücklich unterstütze, zum Teil selbst an anderer Stelle vorgebracht habe und hier nicht alle zu wiederholen brauche, weil durch ihre Aufnahme in Gesetzesinitiativen bereits hinreichende Aussicht auf ihre Verwirklichung besteht. Ich beschränke mich im folgenden daher auf einige grundsätzliche Überlegungen, die — jedenfalls zu einem Teil — über die bereits bekannten Forderungen hinausgehen und Anstöße zu weitergehenden Überlegungen geben sollen.

4.3.1 Anwendungsbereich des Gesetzes (Dateibegriff)

Während der Datenschutz im bereichsspezifischen Recht nicht an formale technisch-organisatorische Voraussetzungen der Informationsverarbeitung anknüpft, greift das BDSG nur ein, wenn personenbezogene Daten in der Form einer Datei verarbeitet werden (§ 1 Abs. 2, § 2 Abs. 3 Nr. 3). Verarbeitungsformen, die diesem Kriterium nicht genügen, sind vom Schutz ausgeschlossen.

Die Frage, ob eine Datensammlung als Datei anzusehen ist, führt kaum noch zu erheblichen Kontroversen. In der Praxis ist unbestritten, daß jede Datensammlung, die in automatisierten Verfahren verarbeitet wird, als Datei anzusehen ist. Auch für viele andere Formen organisierter Datenverarbeitung, z. B. Datensammlungen auf Karteikarten, ist anerkannt, daß es sich dabei um Dateien im Sinne des BDSG handelt.

Wenn trotzdem in der öffentlichen Diskussion der Dateibegriff kritisiert wird, so liegt dies nur zum Teil daran, daß dabei Auslegungsprobleme auftreten können. Mitbestimmend dürfte sein, daß die damit getroffene Abgrenzung nicht als zweckmäßig angesehen wird.

So gibt es z. B. Formen der Datenverarbeitung, die zwar keine Dateien im Sinne des BDSG benutzen und deshalb von den entsprechenden Regelungen nicht erfaßt werden, die aber so organisiert sind, daß eine vergleichbare Verfügbarkeit erreicht wird. Dazu gehören insbesondere entsprechend zweckmäßig aufgebaute Listen und z. B. durch Nachweisverfahren inhaltlich erschlossene Aktensammlungen. Die technischen Möglichkeiten der Mikroverfilmung erlauben es dabei, sehr viele Informationen auf engem Raum verfügbar zu halten.

Wenn für solche Sammlungen ein Fundstellennachweis verwendet wird, der sich auf Dateien stützt, so sind zwar die in den Nachweis-Dateien enthaltenen personenbezogenen Daten durch das BDSG geschützt, die oft wesentlich präziseren Angaben aus den nachgewiesenen Fundstellen aber nicht.

Es besteht daher die Gefahr, daß die Entscheidung, ob die Betroffenen ihre Datenschutzrechte wahrnehmen können, von technischen und organisatorischen Zufälligkeiten, die noch dazu von der speichernden Stelle beeinflußt — um nicht zu sagen: manipuliert — werden können, abhängt. Zudem ist zu berücksichtigen, daß bestimmte Formen der Informationsverarbeitung, deren Bedeutung künftig noch wachsen wird, wie insbesondere im Bereich der Zeichen- und Bildübertragung sowie der automatischen Textverarbeitung, vom Dateibegriff nicht voll erfaßt werden.

Deshalb sollten über die bisher vom BDSG erfaßte Datenverarbeitung hinaus auch andere Formen des Umgangs mit personenbezogenen Daten entsprechend geregelt werden. Viele Vorschriften des BDSG wie z. B. die zum Datengeheimnis (§ 5), die über technische und organisatorische Maßnahmen (§ 6) sowie die Übermittlungsregelungen sind ohne weiteres auch auf Daten in Listen, Akten u. ä. anwendbar. Einige andere Vorschriften müßten zur Anwendung auf Daten, die sich nicht in Dateien befinden, neu angepaßt werden. Ich nenne einige Beispiele:

— Sinnvolle Veröffentlichungen über gespeicherte Daten setzen voraus, daß der Kreis der Betroffenen, die Art der Daten und die Aufgaben, bei denen diese Daten verwendet werden, in knapper und verständlicher Form beschrieben werden können. Dies ist im allgemeinen nur bei strukturierten Datensammlungen (z. B. bei Listen) möglich, bei Akten dagegen häufig nicht. Die Pflicht zur Veröffentlichung sollte also nicht immer bestehen, könnte aber entsprechend erweitert werden.

— Für die bereits vorhandenen Datenbestände im privaten Bereich wäre eine Benachrichtigungspflicht nur dann realisierbar, wenn die Anschriften der Betroffenen an leicht auffindbaren Stellen angegeben sind, was aber nicht immer der Fall sein dürfte. Auch soweit eine Stelle personenbezogene Angaben nur beiläufig (unangefordert) erhält und diese Kenntnis nicht verwertet, wäre eine Benachrichtigung kaum zuzumuten. Die Pflicht zur Benachrichtigung wäre also nur mit Einschränkungen auszudehnen.

— Um einem Betroffenen Auskunft auch über solche Dateien erteilen zu können, die nicht nach Personen geordnet sind oder so geordnet werden können, wird es in der Regel notwendig sein, daß der Betroffene die Art der Daten oder andere Umstände der Speicherung genau bezeichnet, damit die speichernde Stelle die Daten auch finden kann. Die Auskunftspflicht müßte in diesen Fällen deshalb von der Mitwirkung des Betroffenen abhängig gemacht werden.

— Wenn das Interesse an der Vollständigkeit einer Dokumentation überwiegt, könnten Berichtigungen und Löschungen als richtigstellende Ergänzungen angefügt werden; die nachträglich als falsch oder unzulässig erkannte Darstellung wäre dann entsprechend zu kennzeichnen und eventuell zu sperren. Deshalb müßte hier zumindest die Löschungsvorschrift gelockert werden.

Die Schwierigkeiten, die mit der Formulierung eines Abgrenzungskriteriums verbunden sind, das den Dateibegriff ersetzen könnte, sollten nicht unterschätzt werden. Auch der völlige Verzicht auf den Dateibegriff, wie er verschiedentlich vorgeschlagen worden ist, dürfte nicht zu einer praktikablen Regelung führen, da der Anwendungsbereich des Datenschutzgesetzes dann nicht mehr überschaubar wäre. Ein korrekter Gesetzesvollzug und eine wirksame Datenschutzkontrolle mit vertretbarem Aufwand könnten nicht mehr gewährleistet werden. Es ist auch fraglich, ob eine Enumeration von Ausnahmetatbeständen, für die das Gesetz nicht gelten soll, weiterhelfen könnte. Abgesehen davon, daß die notwendige Konkretisierung ähnliche Definitionsschwierigkeiten wie beim Dateibegriff bereiten würde, wären Umgehungsmöglichkeiten nur schwer vermeidbar.

Es würde hingegen einen Rückschritt bedeuten, wenn man den Anwendungsbereich des Gesetzes auf die auotmatisierte Datenverarbeitung beschränkte. In diesem Falle blieben durchaus riskante Verarbeitungsformen, wie etwa umfangreiche Papierkarteien, ungeregelt und die Betroffenen insoweit schutzlos.

Um in dieser Frage zu einem tragfähigen Vorschlag zu gelangen, erscheint es mir vordringlich, eine Bestandsaufnahme der Probleme vorzunehmen, die unter dem geltenden Dateibegriff entstanden sind. Das besondere Augenmerk muß dabei auf der Frage liegen, ob Informationsbestände und Verarbeitungsformen, für die ein Regelungsbedürfnis vorliegt, vom BDSG nicht erfaßt werden und dadurch ein Defizit an Datenschutz für die Betroffenen entsteht, das durch bereichsspezifische Bestimmungen nicht ausgeglichen wird.

4.3.2 Zulässigkeit der Datenerhebung

Die Erhebung der Daten sollte in die Zulässigkeitsbestimmung des Gesetzes einbezogen werden (vgl. Art. 25 des französischen Datenschutzgesetzes und Nr. 2 der Empfehlungen des Europäischen Parlaments, BT-Drucks. 8/2928). Da die Datenerhebung nicht unter den vom Gesetz geschützten Phasen der Datenverarbeitung genannt ist (§ 1 Abs. 1), wird sie von der Zulässigkeitsregelung des § 3 nicht erfaßt. Doch liegt schon in der Erhebung von Daten ein Eingriff in Rechte des Betroffenen, der der gesetzlichen Grundlage bedarf. § 9 Abs. 2 BDSG beruht auf derselben Überlegung, macht dies aber nicht hinreichend deutlich. Die Bestimmung ist nachträglich eingefügt und befindet sich an einer systematisch unbefriedigenden Stelle; sie hat auch zu einer Mißdeutung Anlaß gegeben, die durch eine Neufassung vermieden werden könnte: unter Hinweis auf § 1 Abs. 2 Satz 1 wird die Ansicht vertreten, § 9 Abs. 2 gelte nur, wenn die erhobenen Daten zur Speicherung in Dateien oder zur Übermittlung aus Dateien bestimmt seien. Diese Einschränkung ist schon deshalb nicht haltbar, weil bei der Erhebung oft noch gar nicht feststeht, ob eine solche Speicherung erfolgen wird oder nicht. Bei Novellierung des BDSG sollte das Anliegen des § 9 Abs. 2 vorn geregelt und entsprechend auch auf den privaten Bereich erstreckt

werden. Dabei muß klar zum Ausdruck kommen, daß die Vorschrift nicht auf in Dateien gespeicherte Daten beschränkt ist. Außerdem sollte die Aufklärungspflicht noch verstärkt werden: Der Bürger sollte erfahren, für wen die Daten bestimmt sind und welches die Folgen sind, wenn er sie nicht angibt. Auch insofern enthält das französische Gesetz ein gutes Vorbild (Artikel 27 und 45 Abs. 1).

Zu erwägen wäre auch, ob nicht eine Bestimmung aufgenommen werden soll, wonach personenbezogene Daten grundsätzlich nur beim Betroffenen unmittelbar erhoben werden sollten. Der Betroffene erhielte damit Kenntnis von dem Bearbeitungsvorgang und der Tatsache, daß Daten über ihn gespeichert werden. Freilich werden auch hier Ausnahmen nicht zu vermeiden sein, doch würde das Prinzip der unmittelbaren Erhebung beim Betroffenen der weit verbreiteten Tendenz entgegenwirken, sich auf vorhandene und damit vielfach veraltete Daten zu verlassen.

4.3.3 Zulässigkeit der Speicherung und Übermittlung

Die Bestimmungen des BDSG über die Zulässigkeit der Speicherung und Übermittlung (§§ 9 ff., 23 f., 32 Abs. 1) haben weitgehend Blankettcharakter, sie verweisen auf die Rechtmäßigkeitsvoraussetzungen der jeweiligen Verwaltungstätigkeit nach den für sie geltenden speziellen Vorschriften und beziehen sich auf die einzelnen dafür erforderlichen Daten. Dabei ist nicht berücksichtigt, daß die Errichtung eines Systems der Speicherung personenbezogener Informationen von einer gewissen Größenordnung an eine neue Qualität erhält, die eine besondere, den jeweiligen Bedingungen gerecht werdende gesetzliche Regelung erforderlich macht. Wenn etwa ein Verwaltungszweig ein Melde- und Auskunftssystem errichtet, das der überregionalen Kontrolle des betroffenen Personenkreises dient, so handelt es sich nicht mehr um einzelne Speicherungen und Übermittlungen, sondern um etwas qualitativ Neues, das weder nach Regeln der Amtshilfe noch nach denen der §§ 9 Abs. 1 und 10 Abs. 1 BDSG voll zu erfassen ist. Zwar müssen die Voraussetzungen der genannten Bestimmungen für die einzelne Verarbeitungsart gegeben sein, doch reicht dies für die Zulässigkeit eines besonderen Informationssystems dann nicht aus, wenn damit eine wesentlich intensivere „Erfassung" der Betroffenen verbunden ist oder eine ständige enge Zusammenarbeit der beteiligten Stellen stattfinden soll. Dies ergibt sich aus einem Rückschluß aus Art. 87 Abs. 1 GG, wo die Errichtung von Zentralstellen für den Nachrichtenaustausch besonderer gesetzlicher Regelung vorbehalten ist, und aus § 2 BKA-Gesetz.

Ein weiteres Petitum ist die Konkretisierung der Zulässigkeitsvoraussetzungen für die Speicherung und Übermittlung von Daten. Die Unbestimmtheit der jetzigen Regelungen geht so weit, daß gelegentlich die Verfassungswidrigkeit der Bestimmungen wegen eben dieser Unbestimmtheit behauptet wird. Zwar wird sich dieses Problem entschärfen, je mehr Sachbereiche durch spezifische Normen erfaßt werden; doch bleibt das Bedürfnis nach Konkretisierung der allgemeinen Bestimmungen bestehen. Hier kann es zumindest hilfreich sein, eine Verordnungsermächtigung einzuführen, wie sie im nordrhein-westfälischen Landesgesetz (§ 14) enthalten ist. Ein anderer Lösungsansatz könnte darin bestehen, daß der Gesetzgeber die Aufgaben der verschiedenen Behörden möglichst präzise festlegt und ergänzend dazu und zu der Übersicht nach § 15 Nr. 1 BDSG (oben 3.1) von der jeweiligen speichernden Stelle Verfahrensregelungen erlassen werden müssen, in denen bei der Einrichtung einer Datei die Maßnahmen zur Gewährleistung des Datenschutzes festgelegt werden. Ohne Anspruch auf Vollständigkeit könnte in einem solchen „Dateistatut" etwa folgendes geregelt werden:

- Bezeichnung der Datei,
- Zweckbestimmung (Haupt- und Nebenzwecke),
- Art der gespeicherten Daten, die zur Erfüllung des Hauptzweckes erforderlich sind (Rechtsgrundlagen),
- Art der gespeicherten Daten, die darüber hinaus für andere Zwecke (Statistik, Forschung, Planung) erhoben und verarbeitet werden,
- Art der Erhebung,
- betroffener Personenkreis,
- Art der Verarbeitung
- Empfänger innerhalb und außerhalb der speichernden Stelle,
- Verfahren bei Übermittlungen ins Ausland,
- Bezeichnung der Dateien, mit denen eine Verknüpfung der gespeicherten Daten möglich und zulässig ist,
- Bezeichnung der Stelle, die Auskunftsersuchen bearbeitet,
- Verfahren bei der Berichtigung von Daten,
- Dauer der Speicherung,
- Verfahren der Löschung,
- Verfahren der Sperrung,
- Verfahren der sonstigen Archivierung,
- Verfahren, nach dem in Einzelfällen von den Richtlinien abgewichen werden kann (z. B. Zustimmung des internen Datenschutzbeauftragten oder/und der Leitung),
- Verfahren bei vermuteten oder festgestellten Verstößen.

Durch die Verpflichtung zum Erlaß derartiger Richtlinien wäre jeder Normadressat gezwungen, sich über den Datenschutz in jeder Datei Gedanken zu machen und Entscheidungen zu treffen. Den Richtlinien könnte eine gewisse selbstbindende Wirkung gegeben werden. Überprüfungen könnten auf deren Grundlage effektiver durchgeführt werden. Der bereichsspezifische Datenschutz würde damit praktisch für jede Einzeldatei verwirklicht. Die Erfahrung wird erweisen müssen, ob es bei diesem Verfahren bleiben kann oder ob stärkere Korrekturen durch Aufsichtsbehörden erforderlich sind.

Gegenstand einer Novelle müßte auch die Regelung für den behördeninternen Datenverkehr sein. Als Vorbild empfiehlt sich das Landesdatenschutzrecht (Bayern, Saarland, Entwurf Hamburg), wonach die Zulässigkeitsvoraussetzungen für eine Datenübermittlung auch dann gegeben sein müssen, wenn Daten innerhalb einer Behörde zwischen Organisationseinheiten ausgetauscht werden, die unterschiedliche Aufgaben wahrnehmen.

In der öffentlichen Diskussion besteht weiterhin Einigkeit darüber, daß es der Verwaltung nicht selbst überlassen bleiben dürfte, welche Aufgaben sie ihrer Datenverarbeitung zugrunde legt, so daß allgemein gefordert wird, die in den §§ 9 bis 11 BDSG vorausgesetzte Aufgabenbestimmung müsse durch Gesetz erfolgen. Bayern hat eine solche Bestimmung in sein Landesdatenschutzgesetz aufgenommen, allerdings mit langer Übergangsfrist. Gegen die Forderung nach gesetzlicher Aufgabenbestimmung kann eingewendet werden, daß dadurch die Verwaltung unflexibel werde und die Folgen nicht absehbar seien; unverzichtbare Formen von Datenverarbeitung könnten auf diese Weise gefährdet werden. Andererseits muß bedacht werden, daß die Forderung nach gesetzlicher Bestimmung der Aufgaben letztlich ebenso wie das Zweckbindungsprinzip aus der verfassungsrechtlich fundierten Lehre folgt, wonach die Verarbeitung personenbezogener Daten einen Eingriff in die Rechte des Betroffenen darstellt, der nur in gesetzlich bestimmtem Umfang zulässig ist. Praktische Erfahrungen aus Bayern liegen noch nicht vor; in Bereichen, die herkömmlicherweise durch gesetzliche Aufgabenzuweisungen geprägt sind — wie dem Polizeirecht —, hat sich die Verwendung von Aufgabennormen bei allerdings recht weiten, generalklauselartigen Formulierungen als durchaus praktikabel erwiesen (nach entsprechenden rechtsstaatlichen Eingrenzungen durch die Rechtsprechung).

Die Datenverarbeitung im privaten Bereich ist vom BDSG in relativ großzügiger Weise zugelassen. Eine stärkere Position des Betroffenen könnte hier dadurch erreicht werden, daß § 23 auf die erste Alternative eingeschränkt wird, so daß das Speichern nur noch im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen zulässig ist; die Wahrung berechtigter Interessen (in Abwägung zu den schutzwürdigen Belangen des Betroffenen) reicht dann nicht mehr aus. Immer wieder erhalte ich Zuschriften von Bürgern, die es unbegreiflich finden, daß Daten über sie bei privaten Unternehmen in Umlauf sind, von deren Existenz und Übermittlung sie nichts wissen. Gewiß lassen sich gewichtige Gründe gegen eine solche Gesetzesänderung vorbringen. Vorerst scheint mir der Erkenntnisstand, auf den sich eine Einschränkung der Zulässigkeitsvoraussetzungen für die Datenverarbeitung im nicht-öffentlichen Bereich stützen müßte, noch unzureichend zu sein. Auch müssen dazu die Erfahrungen der Aufsichtsbehörden der Länder aufbereitet und in die Überlegungen einbezogen werden.

Wollte man der Kritik an § 23 BDSG folgen, so müßte freilich auch § 32 geändert werden, der das Speichern personenbezogener Daten durch private Stellen für fremde Zwecke schon dann zuläßt, wenn kein Grund zur Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden. Es liegt auf der Hand, daß dies eine Entscheidung von großer Tragweite wäre. Ein Abstellen auf den Vertragszweck würde hier nicht weiterhelfen, weil nämlich gar keine vertraglichen oder vertragsähnlichen Beziehungen zwischen dem Betroffenen und dem Datenverarbeiter (Markt- und Meinungsforscher, Auskunftei, Service-Rechenzentrum) bestehen. Dem Bestimmungsrecht der Betroffenen über die sie betreffenden Daten könnte u. U. dadurch entsprochen werden, daß man sie schon bei der Speicherung (nicht erst bei erstmaliger Übermittlung) benachrichtigt und ihnen ein Widerspruchsrecht einräumt. Das wäre zwar nicht einer vollen Zustimmung gleichzusetzen, wäre aber besser als die gegenwärtige Lösung, bei der Dritte über die Zulässigkeit entscheiden.

Die Einschränkung der Zulässigkeit der Datenübermittlung auf den Rahmen eines Vertrages oder vertragsähnlichen Vertrauensverhältnisses sollte jedenfalls für Arbeitsverhältnisse vorgesehen werden. Es ist nicht einzusehen, daß die Weitergabe von Daten über Arbeitnehmer — die sich ohnehin nie ganz verhindern lassen wird — durch die Benutzung von Mitteln der Informationstechnik noch effektiver gemacht werden soll. Im Arbeitsverhältnis gibt es überdies eine praktikable Möglichkeit der Konkretisierung, die einer materiellen gesetzlichen Regelung gleichwertig ist, nämlich die Einschaltung von Mitbestimmungsgremien der Arbeitnehmer.

Ein grundsätzlich anderer Weg der Zulässigkeitsregelung bestünde darin, die gesamte Datenverarbeitung unter ein Verbot mit dem Vorbehalt aufsichtsbehördlicher Erlaubnis zu stellen. So sehen einige ausländische Gesetze und die Empfehlungen des Europäischen Parlaments (Nr. 1) vor, daß Datenverarbeitungsanwendungen von der Datenschutzaufsichtsbehörde genehmigt oder zumindest bei ihr angemeldet werden müssen (vgl. § 32 österr. Datenschutzgesetz, Art. 4 luxemb. Datenschutzgesetz; § 3 Abs. 3, § 21 Abs. 1 dänisches Private Register Act 1978; § 4 Abs. 1 dän. Public Authorities Registers Act 1978; §§ 9, 14, 22, 25, 31, 36 norwegisches Datenschutzgesetz).

Dem Bürger könnte dann ein Recht eingeräumt werden, die Verarbeitung ihn betreffender Daten zu untersagen, wenn die Anmeldegenehmigung oder Anmeldung fehlt (Art. 26 franz. DSG). Erfahrungen mit diesem Modell liegen bisher im wesentlichen nur aus Schweden vor. Dort hat sich die Regelung bewährt, insbesondere nachdem für die Mehrzahl der Anwendungen ein vereinfachtes Verfahren eingeführt worden ist (s. u. 5.1.2). Wie die französische Datenschutzkommission die auf sie zukommende Arbeitslast bewältigen wird, ist noch nicht absehbar; die Kommission nimmt ihre Tätigkeit erst Anfang 1980 auf (s. Art. 46, 48 des Gesetzes). Die dänische Kontrollbehörde ist zur Zeit mit Genehmigungs- und Anmeldeverfahren stark belastet.

Angesichts dieser Ungewißheit über die Auswirkungen eines Genehmigungs- oder Anmeldesystems

kann ich zur Zeit nicht empfehlen, von dem Grundprinzip des BDSG abzugehen, wonach die Zulässigkeit der Datenverarbeitung zunächst von den verarbeitenden Stellen selbst beurteilt werden muß und die Kontrolle durch externe Organe (Datenschutzbeauftragte und Datenschutzaufsichtsbehörden) wahrgenommen wird. Diese Lösung hat immerhin für sich, daß sie der verarbeitenden Stelle eine sorgfältige Prüfung und Abwägung abverlangt. Sie begünstigt zwar diejenigen, die sich über Bedenken leichter hinwegsetzen, diese Gefahr kann aber durch verschärfte Haftungsregelungen wie den jetzt in der Diskussion befindlichen Schadensersatzanspruch ohne Verschuldensvoraussetzung gemindert werden. Den Aufsichtsbehörden gestattet sie die Konzentration auf wichtige Fälle, vor allem solche, die von dem Betroffenen selbst vorgebracht werden; hier wird erneut die Bedeutung des Auskunftrechts sichtbar. Insgesamt ist die deutsche Lösung um so eher vertretbar, je weniger sich die Kontrolle auf nachträgliche Beanstandungen beschränkt und je mehr sie statt dessen als vorangehende und begleitende Beratung praktiziert wird.

4.3.4 Zulässigkeit sonstiger Nutzung von Daten

Die neben Übermittlung und Veränderung denkbare anderweitige Nutzung von Daten sollte ebenfalls bestimmten Zulässigkeitsregelungen unterworfen werden. Um den Schutz des Betroffenen zu vervollständigen, muß er auch gegen die Kenntnisnahme Unbefugter und gegen zweckwidrige Verwendung seiner Daten geschützt werden. Das BDSG bewirkt einen solchen Schutz nicht mit der wünschenswerten Deutlichkeit. Zwar untersagt § 5 BDSG es den bei der Datenverarbeitung beschäftigten Personen, geschützte Daten unbefugt zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu verarbeiten, bekanntzugeben, zugänglich zu machen oder sonst zu nutzen; die Vorschrift kann aber zu Mißverständnissen führen, weil sie nur den Begriff „bei der Datenverarbeitung beschäftigt" benutzt. Das Verbot der unbefugten Nutzung von Daten muß allgemein für das Personal der Stellen gelten, die in den Bestimmungen des 2. bis 4. Abschnittes angesprochen sind, und darf sich nicht nur an die Personen richten, denen eine Tätigkeit in der Datenverarbeitung übertragen ist. Interne Einschränkungen des Kreises der „bei der Datenverarbeitung beschäftigten Personen" dürfen im Außenverhältnis, also für die Zulässigkeit der Datenverarbeitung im Verhältnis zu den Betroffenen, keine Bedeutung haben.

4.3.5 Verbot von Persönlichkeitsprofilen

Es sollte geprüft werden, ob nicht ein Verbot der Verarbeitung (einschließlich Nutzung) besonders empfindlicher Daten in das BDSG aufgenommen werden kann. Ausländische Datenschutzgesetze haben Vorschriften, nach denen Daten über Rasse, Hautfarbe, Glaube, politische Überzeugung, sexuelles Verhalten, Vorstrafen oder Gesundheitszustand entweder grundsätzlich nur mit Zustimmung des Betroffenen (Frankreich, Dänemark, Norwegen) oder aber unter anderen erschwerten Voraussetzungen (z. B. Genehmigung) verarbeitet werden dürfen (Schweden, Luxemburg, Norwegen). Das BDSG enthält nur eine periphere Bestimmung über solche sensiblen Daten (§ 27 Abs. 3 Satz 3).

Ausnahmen etwa zugunsten von Vereinigungen, die bei der Aufnahme neuer Mitglieder zulässigerweise auf deren Anschauungen abstellen, wären unvermeidbar. Gewerkschaften, Parteien, Religionsgesellschaften und „Tendenzbetriebe" haben ein Recht auf derartige Differenzierung. Gleichwohl hätte eine entsprechende Einschränkung erheblichen Signalwert.

Erst recht gefährlich wäre die Erstellung umfassender Persönlichkeitsbilder oder Persönlichkeitsprofile, deren Unzulässigkeit bereits aus dem Grundgesetz folgt (BVerfGE 27, 1, 6). Die technische Möglichkeit, durch Verbund verschiedener Informationssysteme beliebig Daten über Bürger aus verschiedenen Verwaltungs- und Wirtschaftsbereichen zusammenzuführen, darf aus rechtlichen Gründen nicht Realität werden. Allerdings werden Teilabbilder der Persönlichkeit bereits bei verschiedenen Stellen gesammelt; so fallen in der ärztlichen Praxis vielfältige Lebensdaten an, bei den Sicherheitsbehörden lassen sich aus Daten über äußeres Verhalten Schlüsse auf persönliche Anschauungen ziehen und noch in manchen anderen Zusammenhängen, z. B. in Personalverwaltungen, mögen Daten vorhanden sein, die solche Bilder der Persönlichkeit vermitteln können. Dieser Entwicklung muß Einhalt geboten werden.

Von Interesse ist in diesem Zusammenhang die Bestimmung des Artikel 2 des französischen Datenschutzgesetzes, die lautet:

> „Keine richterliche Entscheidung, die eine Bewertung eines menschlichen Verhaltens enthält, darf auf einer automatischen Datenverarbeitung gründen, die eine Bestimmung des Profils oder der Persönlichkeit des Betroffenen vornimmt.
>
> Keine Entscheidung einer öffentlichen oder privaten Stelle, die eine Bewertung eines menschlichen Verhaltens enthält, darf ausschließlich auf einer automatischen Datenverarbeitung gründen, die eine Bestimmung des Profils oder der Persönlichkeit des Betroffenen vornimmt."

Die Vorschrift verbietet zwar nicht allgemein die Herstellung von Persönlichkeitsprofilen, sie schränkt aber immerhin die Nutzung der mittels der automatischen Datenverarbeitung so weit verdichteten Informationen ein.

Der Begriff des Persönlichkeitsprofils ist hier wie in den meisten Überlegungen zu diesem Thema nicht definiert. Einen Definitionsversuch enthält jedoch der vom „Arbeitskreis Polizeirecht" herausgegebene Alternativentwurf einheitlicher Polizeigesetze des Bundes und der Länder. Dort heißt es in § 12:

> „Die Erstellung eines Persönlichkeitsprofils eines Betroffenen ist das systematische Erheben von Informationen über eine Vielzahl von Lebensbereichen des Betroffenen durch rechnerunterstützte Ausschöpfung von Informationsquellen."

Indem hier auf eine „Vielzahl von Lebensbereichen" abgestellt wird, bleiben die bisher bestehenden Sammlungen, die Teilabbilder der Persönlichkeit enthalten, unangetastet. Würden aber nur zwei dieser Sammlungen miteinander verbunden, so wären die Betroffenen einer ganz erheblichen und nicht mehr vertretbaren „Durchleuchtung" ausgesetzt. Der Begriff des Persönlichkeitsprofils muß daher wohl noch strenger gefaßt werden als in der zitierten Definition des Arbeitskreises Polizeirecht. Das ändert aber nichts an der grundsätzlichen Eignung des Begriffes, in eine Grundsatzbestimmung aufgenommen zu werden. Eine angemessene Formulierung ist gewiß nicht einfach, aber nicht unmöglich. Anzuknüpfen wäre an das Gebot der Zweckentfremdung, das — wie ausgeführt — aus der Verfassung folgt und hier mit dem Grundgebot der Achtung vor der Menschenwürde zu verbinden wäre. Ausdrücklich zu verbieten wäre also die Zusammenführung von Teilabbildern der Persönlichkeit, die aus zwei oder mehr Verwaltungsbereichen stammen, wenn diese ihrerseits nicht durch gleichen oder verwandten Zweck miteinander verbunden sind. Entsprechend wäre für die Datenverarbeitung im nicht-öffentlichen Bereich zu fordern, daß Daten über Verhaltensweisen in bestimmten privaten Lebensbereichen nicht mit solchen eines völlig andersartigen, davon abgrenzbaren verknüpft werden, also z. B. nicht Beschreibungen von Konsumgewohnheiten mit denen des Verhaltens im Arbeitsprozeß zusammengeführt werden.

4.3.6 Transparenz der Datenverarbeitung

Die allgemeine Beunruhigung über die Zunahme und Intensivierung von Datenverarbeitungsprozessen rührt zu einem wesentlichen Teil daher, daß die Verhältnisse für das breite Publikum undurchschaubar geworden sind. Die Computer und ihre Fähigkeiten wirken auf viele Mitbürger einschüchternd und furchterregend. In dem Maße, wie die Datenverarbeitung für die Betroffenen transparent wird, können auch unbegründete Ängste abgebaut werden. Dies ist ein wichtiges Anliegen — im Interesse des Gemeinwesens wie auch der Instanzen, die öffentliche Aufgaben wahrzunehmen haben; es liegt aber auch im Interesse der Unternehmen, die sich dieser Technik bedienen.

Zur Erhöhung der Transparenz sind verschiedene Maßnahmen möglich. Zahlreiche Eingaben, die an mich gerichtet werden, obwohl dafür die Aufsichtsbehörden der Länder zuständig sind (an die ich diese Eingaben abgebe), lassen erkennen, daß Empfänger von Werbesendungen mit allem Nachdruck eine Unterrichtung darüber fordern, woher das werbende Unternehmen ihre Anschrift erhalten hat. Ich habe mich zu dieser Frage bereits im ersten Tätigkeitsbericht (1. TB, 4.4) geäußert und vorgeschlagen, daß der Auskunftsanspruch gegenüber werbenden Unternehmen erweitert wird. Ich wiederhole diesen Vorschlag: Werden personenbezogene Daten zu Werbezwecken verwendet, so sollte die werbende Stelle verpflichtet sein, die Herkunft der Daten anzugeben, und zwar nicht nur im Rahmen des Auskunftsanspruchs des Betroffenen, sondern schon zugleich mit der Werbesendung. Dieser Vorschlag scheint mir vor allem dann leicht realisierbar, wenn das werbende Unternehmen sein Adressenmaterial nur aus einer Quelle bezieht; mit einer Beilage zur Werbesendung kann das Informationsbedürfnis des Empfängers auf einfache Weise befriedigt werden. Entsprechendes sollte für Organisationen gelten, die zur Mitgliederwerbung fremdes Adressenmaterial verwenden.

Es gibt Vorschläge, auch für den öffentlichen Bereich eine Benachrichtigungspflicht bei erstmaliger Speicherung und/oder Übermittlung einzuführen (so auch Nr. 4 und 8 a der Empfehlungen des Europäischen Parlaments). Ich halte diese Vorschläge nicht für zweckmäßig. Ich vermute, daß dadurch Benachrichtigungen in solchen Massen erforderlich würden, daß die öffentliche Verwaltung in unvertretbarem Maße belastet würde, die Betroffenen andererseits aber eher irritiert als auf die wirklich bedeutsamen Fälle aufmerksam gemacht würden. Transparenz läßt sich meines Erachtens auch auf andere Weise herstellen, insbesondere durch wesentlich verbesserte Formulare, durch Merkblätter und sonstige Formen der allgemeinen Unterrichtung über Informationswege und Speicherungsmethoden.

Eine damit nicht unmittelbar zusammenhängende Anregung geht dahin, den Betroffenen zu verständigen, wenn seine Daten berichtigt oder gelöscht werden. Ich unterstütze diesen Vorschlag zumindest für die Fälle, in denen die Berichtigung oder Löschung auf Verlangen des Betroffenen erfolgt. Im Grunde sollte es selbstverständlich sein, daß der Betroffene eine Bestätigung darüber erhält, daß seinem Antrag entsprochen wurde.

Ich habe bereits mehrfach betont, für wie wichtig ich das Auskunftsrecht des Betroffenen über die zu seiner Person gespeicherten Daten erachte. Leider wird von diesem Auskunftsrecht nicht viel Gebrauch gemacht. Offenbar fühlen sich viele Bürger durch die Gebührenpflichtigkeit bzw. Entgeltlichkeit der Auskunft abgeschreckt; die von mir bereits früher (vgl. 1. TB, 4.5.2) geforderte Unentgeltlichkeit ist nunmehr in verschiedenen Novellierungsvorschlägen enthalten und sollte bald verwirklicht werden. Darüber hinaus müßten die Ausnahmen von der Auskunftspflicht, die das BDSG enthält (§ 13 Abs. 2 und 3, § 26 Abs. 4 und § 34 Abs. 4), überdacht werden. Ein generelles Auskunftsverweigerungsrecht der Sicherheitsbehörden (§ 13 Abs. 2) erscheint mir nicht angemessen. An seine Stelle sollte eine Verpflichtung treten, im Einzelfall das Geheimhaltungsinteresse gegen das Interesse des Betroffenen an der Auskunft abzuwägen. Vereinzelt geschieht dies bereits jetzt, was die Praktikabilität einer solchen Auflockerung beweist (oben 2.8.8).

Neben der individuellen Information hat aber die allgemeine Publizität erhebliche Bedeutung. Ich halte es für erforderlich, die Veröffentlichungen über Datenverarbeitungen zu intensivieren. Ein Ansatz besteht darin, die im BDSG vorgesehenen Veröffentlichungspflichten zu erweitern. Hinzukommen sollte die Zusammenlegung der Zuständigkeiten für Veröffentlichungen und Dateienregister beim Bundesbeauftragten. Das vom Publikum bisher so gut wie

gar nicht genutzte Dateienregister birgt viel interessante Informationen, die mit den veröffentlichten Angaben kombiniert und systematisch ausgewertet werden müssen, so wie umgekehrt die Veröffentlichungen auf der Grundlage des Wissensstandes der Aufsichtsinstanzen wesentlich aussagekräftiger gestaltet werden könnten. Dieser Vorschlag hätte auch den Vorteil, daß dem Datenschutzbeauftragten die für seine Kontrolltätigkeit notwendigen Informationen über die speichernden Stellen vollständig selbst zur Verfügung stehen. Freilich sollte er dann auch dafür verantwortlich sein, daß die bisher nur aus dem Dateienregister zu ersehenden Datenverarbeitungen nicht nur zur Einsichtnahme bereitstehen, sondern gemeinsam mit den bisher zur veröffentlichenden Angaben in verständlicher Form öffentlich bekanntgemacht werden.

4.3.7 Stellung des Bundesbeauftragten

Das BDSG verpflichtet den Bundesbeauftragten, den Datenschutz in der gesamten Bundesverwaltung zu kontrollieren. Gleichwohl läßt es das Gesetz zu, daß seine Befugnisse, Auskünfte zu verlangen, Akten einzusehen und Überprüfungen vor Ort vorzunehmen, eingeschränkt werden, wenn die „zuständige oberste Bundesbehörde im Einzelfall feststellt, daß die Einsicht in Unterlagen und Akten die Sicherheit des Bundes oder eines Landes gefährdet" (§ 19 Abs. 3 Satz 4). In der Praxis ist dieser Sicherheitsvorbehalt von kontrollierten Behörden hin und wieder angesprochen worden, von einer Anwendung der Vorschrift haben die betreffenden Stellen jedoch bisher stets abgesehen (oben 2.8.1). Tatsächlich bringt die Vorschrift die zuständigen obersten Bundesbehörden in ein erhebliches Dilemma. Die Zurückweisung des Kontrollorgans, das die Bundesregierung selbst eingesetzt hat, um die korrekte Einhaltung des Datenschutzes zu sichern, muß zwangsläufig in der Öffentlichkeit Argwohn erregen und die Frage provozieren, ob nicht ein Versuch vorliegt, die Aufdeckung von Mißständen auf dem Gebiet des Datenschutzes zu verhindern. Dabei ist zu berücksichtigen, daß das Kontrollorgan nicht zuletzt deshalb eingerichtet wurde, um eine unabhängige Überprüfung des Datenschutzes im Interesse des Betroffenen gerade auch dort sicherzustellen, wo diesem selbst wegen vorrangiger Gemeinwohlinteressen keine unmittelbare Kontrollmöglichkeit eingeräumt wird (vgl. § 13 Abs. 2 und 3). Sobald aber die Öffentlichkeit wahrnimmt, daß nicht nur die Form der Kontrolle wechselt, sondern bestimmte Bereiche von jeder Kontrolle ausgespart bleiben, muß das Vertrauen in die Korrektheit der Datenverarbeitung leiden. Bei einer Novellierung sollte die Regelung, der sich auch die Länder nicht einheitlich angeschlossen haben, unter diesen Gesichtspunkten noch einmal überdacht werden.

Die Wirksamkeit der Kontrolle kann durch weitere Gesetzesänderungen verstärkt werden. Wenn dem Bundesbeauftragten ein Zeugnisverweigerungsrecht eingeräumt und die Befugnis, Aussagegenehmigungen für seine Mitarbeiter zu erteilen, ihm selbst übertragen würde, würde damit nicht nur der Schutz der Betroffenen verstärkt, sondern auch die Unabhängigkeit seiner Stellung betont werden. Eine Klarstellung seiner Befugnisse wäre ferner notwendig im Verhältnis zur Finanzverwaltung und zu anderen Behörden und Beamten, die sich auf Berufs- oder besondere Amtsgeheimnisse (§ 45 Satz 2 Nr. 1, Satz 3 BDSG) berufen könnten. Ich verweise auf die Kontroverse der Datenschutzbeauftragten von Bund und Ländern mit der Finanzverwaltung (oben 2.3). Durch eine geringfügige Ergänzung von § 19 Abs. 3 BDSG könnte hier Klarheit geschaffen werden.

An anderer Stelle ist ausgeführt, daß die Beratungsaufgabe des Bundesbeauftragten ständig an Bedeutung zunimmt. Sie kann um so effektiver wahrgenommen werden, je früher ich über Automationsprojekte und Planungen für Informationssysteme informiert werde. Wünschenswert ist daher eine Bestimmung, die den Behörden des Bundes eine Anzeige bei meiner Dienststelle für den Fall zur Pflicht macht, daß sie derartige Projekte in Angriff nehmen.

In der parlamentarischen Debatte über meinen ersten Tätigkeitsbericht ist die Einsetzung eines parlamentarischen Beirats für den Bundesbeauftragten nach dem Vorbild der im Bayerischen Datenschutzgesetz getroffenen Regelung angeregt worden. Ich halte diesen Vorschlag für sehr beachtenswert. In einem solchen Beirat wäre die Gelegenheit gegeben, anstehende Probleme frühzeitig in einem Kreis von engagierten Abgeordneten zu besprechen. Dabei könnten mehr Informationen ausgetauscht werden als dies gegenwärtig — in Sitzungen von Bundestagsausschüssen und informellen Gesprächen — möglich ist. Eine Alternative zu einem besonderen Beirat wäre, daß der Bundestag einen besonderen Ausschuß für Fragen des Datenschutzes einsetzt, dessen Mitglieder den Informationsaustausch mit den für bereichsspezifische Fragen zuständigen Ausschüssen sicherstellen können.

4.3.8 Aufsichtsbehörden für den nicht-öffentlichen Bereich

Nach einem Novellierungsvorschlag, den die CDU-Fraktion des Deutschen Bundestages vorgelegt hat, sollen die Befugnisse der Aufsichtsbehörden für den privaten Bereich verstärkt werden. Ohne die im einzelnen vorgeschlagenen Verbesserungen werten zu wollen, teile ich die diesen Vorschlägen zugrunde liegende Auffassung, daß die Handlungsmöglichkeiten der Aufsichtsbehörden hinter denen der Datenschutzbeauftragten des Bundes und der Länder erheblich zurückbleiben.

Dies zeigt sich einmal darin, daß die Aufsichtsbehörden nach dem BDSG die Einhaltung des Gesetzes und anderer Vorschriften über den Datenschutz lediglich im Einzelfall überprüfen können und auch nur dann, „wenn ein Betroffener begründet darlegt, daß er bei der Verarbeitung seiner personenbezogenen Daten . . . in seinen Rechten verletzt worden ist". Soll die Datenverarbeitung nicht-öffentlicher Stellen in annähernd gleicher Weise kontrolliert werden wie die der Behörden, so muß die Beschränkung der Aufsichtsbehörden auf die „Anlaßaufsicht" wegfallen. Die Aufsichtsbehörden müssen befugt sein, auch aus eigener Initiative und systematisch Prüfungen vor-

nehmen zu können. Das würde bedeuten, daß sie Ermittlungen nicht nur im Einzelfall durchführen, sondern den gesamten Datenverarbeitungsbetrieb in allen rechtlichen und organisatorischen Beziehungen überprüfen dürften. Damit wären sie auch besser als bisher in der Lage, sich einen genauen Eindruck von Umfang und Qualität der Datenverarbeitung in ihrem Kontrollbereich zu verschaffen und durch entsprechende Darstellung gegenüber der Öffentlichkeit für mehr Transparenz der Datenverarbeitung zu sorgen.

Zum anderen fehlt es den Aufsichtsbehörden an Durchsetzungsmöglichkeiten, wenn sie auf Grund ihrer Überprüfungen Rechtsverletzungen feststellen oder Vorschläge zur Verbesserung des Datenschutzes machen wollen. Während die Datenschutzbeauftragten des Bundes und der Länder Verstöße gegen Datenschutzvorschriften gegenüber der obersten Bundes- bzw. Landesbehörde beanstanden können und durch ihr Recht, sich jederzeit an die Parlamente zu wenden, letztlich die politische Verantwortung der jeweiligen Regierung als Kontrollmittel einsetzen können, fehlt es den Aufsichtsbehörden an vergleichbaren Instrumenten. Die Strafvorschrift des § 41 läßt die unbefugte Datenspeicherung straflos; eine Strafverfolgung nach § 41 BDSG setzt außerdem einen Strafantrag voraus, der von der Aufsichtsbehörde nicht gestellt werden kann. Der Katalog der Ordnungswidrigkeiten im BDSG erfaßt nicht den Fall der fehlenden Zulässigkeitsvoraussetzungen für die Datenverarbeitung.

Der gelegentlich gemachte Vorschlag, auch im nichtöffentlichen Bereich für alle Dateien, also auch für solche, die der Datenverarbeitung für eigene Zwecke dienen, eine Anmeldepflicht zu begründen und ein öffentliches Register anzulegen, bedarf weiterer Prüfung (oben 4.3.3). Für eine solche Ausdehnung der Registerpflicht sprechen die ausländischen Vorbilder; dagegen spricht der Umstand, daß von dem Einsichtsrecht in das Dateienregister für den öffentlichen Bereich bisher so gut wie kein Gebrauch gemacht wird. Die Frage muß auch im Zusammenhang mit dem bisher ganz ungelösten Problem des grenzüberschreitenden Datenverkehrs gesehen werden; möglicherweise ist hier die Anmeldung oder sogar Genehmigung der einzige Weg, eine effektive Datenschutzkontrolle zu garantieren (unten 5.2).

4.3.9 Betrieblicher Datenschutzbeauftragter

Zwischen Unternehmensleitungen und Betriebsräten hat es wiederholt Kontroversen um die Bestellung des betrieblichen Beauftragten für den Datenschutz gem. § 28 BDSG gegeben. Auch die Aufsichtsbehörden der Länder haben sich mit dieser Problematik befaßt und sich eine Meinung darüber gebildet, welche Anforderungen an den betrieblichen Datenschutzbeauftragten zu stellen, insbesondere welche Funktionen mit denen eines Datenschutzbeauftragten unvereinbar sind. Die Vertreter der Arbeitnehmer betrachten den Datenschutzbeauftragten des Betriebes vielfach als „Mann der Unternehmensleitung" und befürchten, daß er unangemessenen Einfluß auf die Betriebsratsarbeit nehmen werde. Mangels eigener Kontrollzuständigkeit kann ich nicht beurteilen, inwieweit die von Arbeitnehmervertretern erhobenen Vorwürfe zutreffen oder andererseits die Betriebsräte ihre gesetzlichen Verpflichtungen nicht erfüllen. Die mir zugänglichen Sachdarstellungen lassen aber zumindest eines erkennen: Die Stellung des betrieblichen Datenschutzbeauftragten ist deshalb besonders schwierig, weil er einerseits im Auftrage der Unternehmensleitung für die Erfüllung von Pflichten mitverantwortlich ist, die das Unternehmen gegenüber Dritten hat, andererseits aber auch Interessen der Arbeitnehmer gegenüber der betrieblichen Personalverwaltung schützen soll. In der letztgenannten Funktion verfolgt er gleiche Ziele wie der Betriebsrat, und es wäre gut, wenn umgekehrt auch dieser in dem betrieblichen Datenschutzbeauftragten insofern einen „Verbündeten" sehen könnte. Als rechtspolitische Empfehlung folgt für mich hieraus, daß die Basis für eine vertrauensvolle Zusammenarbeit zwischen dem betrieblichen Datenschutzbeauftragten und dem Betriebsrat gestärkt werden muß. Dies könnte wohl am besten dadurch geschehen, daß dem Betriebsrat ein Mitbestimmungsrecht bei der Auswahl und Abberufung des Datenschutzbeauftragten eingeräumt wird. Auch die Absicherung des Datenschutzbeauftragten durch einen besonderen Kündigungsschutz könnte dazu beitragen, daß er die Interessen des Personals gegenüber der Unternehmensleitung nachdrücklich vertritt. Die Wahrnehmung der anderen Funktion, nämlich für das Unternehmen eine rechtmäßige Verarbeitung der Daten Dritter sicherzustellen, brauchte unter solchen Umständen keineswegs zu leiden; im Gegenteil könnte auch hier eine verstärkte Unabhängigkeit durch Kündigungsschutz und Mitbestimmung des Betriebsrates der Aufgabe Datenschutz insgesamt nützen.

4.4 Abweichendes Landesrecht

Die Datenschutzgesetze der Länder (das Hamburgische Gesetz steht noch aus) sind, jedenfalls in der geltenden Fassung, erst nach Erlaß des BDSG entstanden. Sie haben die Grundkonzeption des BDSG übernommen und stimmen in den Vorschriften über die Schutzrechte der Betroffenen und über die Zulässigkeit der Datenverarbeitung zum Teil wörtlich mit dem BDSG überein. Der wesentliche Unterschied besteht darin, daß sich ihr Geltungsbereich auf Grund der Kompetenzlage auf die Regelung der Datenverarbeitung der Behörden und sonstigen öffentlichen Stellen der Landesverwaltung beschränkt. Die Datenverarbeitung im nicht-öffentlichen Bereich bestimmt sich also ausschließlich nach dem BDSG.

Abgesehen von landesspezifischen Sondervorschriften (z. B. Übergangsvorschriften zum Meldewesen) und geringfügigen Abweichungen in Einzelformulierungen sind einige Länder auf Grund erster Erfahrungen mit dem BDSG, das bis zum Inkrafttreten der Landesgesetze bei der Ausführung von Bundesrecht auch für die Landesverwaltung galt (§ 7 Abs. 2 BDSG), auch im materiellen Regelungsinhalt ihrer Gesetze über die Vorschriften des BDSG hinausgegangen, um eine Verbesserung des Datenschutzes zu

erreichen. Teilweise haben die Länder auch zusätzliche Regelungen aufgenommen. Die Abweichungen können hier nicht vollständig — etwa in Form einer umfassenden Synopse — wiedergegeben werden. Ich beschränke mich im folgenden auf die Darstellung der mir wichtig erscheinenden Abweichungen, sehe aber davon ab, sie an dieser Stelle im einzelnen zu werten. Meine Beurteilung ist zum Teil schon in die oben unter 4.3 gemachten Vorschläge eingegangen; zum anderen Teil scheint mir eine eingehende Erörterung mit den Landesbeauftragten für den Datenschutz anhand deren Erfahrungen notwendig, bevor Empfehlungen zur Übernahme in das Bundesrecht gegeben werden können.

4.4.1 Zulässigkeit der Datenverarbeitung

In den Datenschutzgesetzen ist die Zulässigkeit der Datenverarbeitung an die Voraussetzung geknüpft, daß das Datenschutzgesetz selbst oder eine andere Rechtsvorschrift sie erlaubt oder daß der Betroffene eingewilligt hat. Nach den Datenschutzgesetzen Baden-Württembergs, Bayerns und Nordrhein-Westfalens ist darüber hinaus der Betroffene über die Bedeutung der Einwilligung aufzuklären. In Baden-Württemberg und Rheinland-Pfalz ist ferner bestimmt, daß ihm keine Rechtsnachteile aus einer Verweigerung der Einwilligung entstehen dürfen; Hessen, Nordrhein-Westfalen und Rheinland-Pfalz haben diese Bestimmung (auch) im Zusammenhang mit der Datenerhebung eingefügt.

In Bayern setzt (ab 1. Januar 1983) die Zulässigkeit der Datenverarbeitung, soweit sie aus dem Landesdatenschutzgesetz selbst hergeleitet wird, eine durch Rechtsnorm zugewiesene Aufgabe voraus, während das BDSG und die übrigen Landesgesetze nur allgemein eine Zuständigkeit zur Erfüllung der betreffenden Aufgabe verlangen.

4.4.2 Freigabe von Datenverarbeitungsverfahren

In der Bundes- bzw. Landesverwaltung haben die jeweiligen obersten Dienst- bzw. Aufsichtsbehörden die Durchführung der Datenschutzgesetze und anderer Rechtsvorschriften über den Datenschutz sicherzustellen. In Bayern und im Saarland bedarf der erstmalige Einsatz von automatisierten Verfahren, in denen personenbezogene Daten verarbeitet werden, hinsichtlich der Datenarten und der regelmäßigen Datenübermittlungen jeweils der schriftlichen Freigabe durch die oberste Dienstbehörde; sollen personenbezogene Daten aus verschiedenen Geschäftsbereichen verarbeitet werden, dann bedarf es der Zustimmung aller beteiligten obersten Dienstbehörden. Im Saarland ist dem Landesbeauftragten für den Datenschutz vor der Freigabe bzw. Zustimmung Gelegenheit zur Stellungnahme zu geben. In Bayern ist die Freigabe bzw. die Zustimmung dem Landesbeauftragten unverzüglich mitzuteilen. Erwähnenswert ist in diesem Zusammenhang, daß in Bremen durch Senatsbeschluß bestimmt wurde, daß Entwürfe von Gesetzen, Rechtsverordnungen oder Verwaltungsvorschriften, die die Verarbeitung personenbezogener Daten regeln, ungeachtet der beabsichtigten Verfahren dem Landesbeauftragten für den Datenschutz zur Prüfung zuzuleiten sind.

4.4.3 Dienst- und arbeitsrechtliche Rechtsverhältnisse

Nach den Datenschutzgesetzen des Bundes und der Mehrheit der Länder gelten für die Datenverarbeitung, die öffentliche Stellen im Zusammenhang mit früheren, bestehenden oder zukünftigen dienst- oder arbeitsrechtlichen Rechtsverhältnissen betreiben, die Vorschriften der §§ 23 bis 27 des Bundesdatenschutzgesetzes über die Datenverarbeitung bei nicht-öffentlichen Stellen entsprechend. Damit soll die datenschutzrechtliche Gleichbehandlung aller Arbeitsverhältnisse im öffentlichen und privaten Bereich gesichert werden.

Die Länder Bayern, Nordrhein-Westfalen, Schleswig-Holstein und das Saarland haben diese Regelung nicht übernommen.

4.4.4 Datenverarbeitung für wissenschaftliche Zwecke und für die amtliche Statistik

Die Datenschutzgesetze von Baden-Württemberg, Hessen, Nordrhein-Westfalen und Rheinland-Pfalz enthalten eine Sondervorschrift über die Datenverarbeitung für wissenschaftliche Zwecke. Danach können Hochschulen und andere öffentliche Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung im Rahmen ihrer Aufgaben für bestimmte Forschungsvorhaben personenbezogene Daten speichern und verändern; dazu können die Behörden und öffentlichen Stellen ihnen Daten übermitteln. Voraussetzung ist die Einwilligung der Betroffenen. Die Einwilligung ist aber entbehrlich, wenn schutzwürdige Belange der Betroffenen wegen der Art der Daten, wegen ihrer Offenkundigkeit oder wegen der Art der Verwendung nicht beeinträchtigt werden. Eine Weiterübermittlung ist nur mit Einwilligung der Betroffenen zulässig.

Die Zulässigkeit der Verarbeitung personenbezogener Daten für Zwecke der amtlichen Statistik ist in den Datenschutzgesetzen der Länder Bayern, Rheinland-Pfalz und des Saarlandes sowie nach dem Entwurf für ein Hamburgisches Datenschutzgesetz ausdrücklich geregelt. Die praktische Bedeutung dieser Sondervorschriften liegt dort, wo die statistischen Rechtsvorschriften des Bundes nicht anwendbar sind, d. h. bei amtlichen Statistiken, die nur auf Landesrecht beruhen. Es handelt sich insbesondere um Übermittlungsregelungen, die den Kreis der Empfänger personenbezogener Daten eng eingrenzen.

4.4.5 Datenverarbeitung im Auftrag

Die Datenschutzgesetze der Länder Bremen, Hessen, Nordrhein-Westfalen und des Saarlandes verpflichten in den Fällen der Datenverarbeitung im Auftrag den Auftraggeber sicherzustellen, daß der Auftragnehmer — sofern auf diesen die Vorschriften des Landesdatenschutzgesetzes keine Anwendung finden — die Bestimmungen des Landesdatenschutzgesetzes beachtet und sich der Kontrolle des Landesbeauftragten für den Datenschutz unterwirft. Das

Landesdatenschutzgesetz Rheinland-Pfalz enthält die gleiche „Verpflichtungsklausel", nicht dagegen die „Unterwerfungsklausel" hinsichtlich der Kontrolle des Landesbeauftragten für den Datenschutz.

4.4.6 Datenübermittlungen innerhalb des öffentlichen Bereichs

Während das BDSG und die meisten Landesgesetze davon ausgehen, daß eine Datenübermittlung nur dann vorliegt, wenn Daten an einen Dritten, d. h. eine Person oder Stelle außerhalb der abgebenden Stelle, weitergegeben werden, gelten in Bayern und im Saarland die Übermittlungsvorschriften auch dann, wenn der Datenempfänger andere Aufgaben oder einen anderen räumlichen Zuständigkeitsbereich hat als die abgebende Stelle. Das bedeutet, daß Datenempfänger unter diesen Voraussetzungen auch Teile derselben Stelle sein können mit der Folge, daß die Übermittlungsvorschriften dann auch für den behördeninternen Datenverkehr anzuwenden sind. Nach dem Datenschutzgesetz Nordrhein-Westfalen ist die Datenübermittlungsvorschrift zwar nicht unmittelbar auf die Datenweitergabe innerhalb einer Behörde anwendbar, jedoch sind dabei die Grundsätze dieser Vorschrift zu beachten.

Der Entwurf des Hamburgischen Datenschutzgesetzes enthält eine ähnliche Regelung, wie sie in Bayern und im Saarland besteht. Andererseits behandelt der Entwurf eine Stelle, bei der Daten mehrerer speichernder Stellen zusammengeführt und in einer „Gesamtdatei" verarbeitet werden, als eine einzige speichernde Stelle.

4.4.7 Datenübermittlungen an nicht-öffentliche Stellen

Die Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs ist allgemein zulässig, wenn dies zur rechtmäßigen Erfüllung der Aufgaben der übermittelnden Stelle erforderlich ist oder der Empfänger ein berechtigtes Interesse glaubhaft macht und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden. In Berlin setzt die Übermittlung zusätzlich die Einwilligung des Betroffenen voraus. Nach dem Entwurf des Hamburgischen Datenschutzgesetzes kann der Betroffene verlangen, daß die Übermittlung gesperrt wird, wenn er ein berechtigtes Interesse an der Sperrung darlegt.

In Rheinland-Pfalz sind verschärfte Zulässigkeitsvoraussetzungen der Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs vorgesehen, wenn die Daten in automatisierten Verfahren verarbeitet werden; sie dürfen dann nur übermittelt werden, wenn und soweit dies gesetzlich zugelassen ist oder wenn der Betroffene mit der Übermittlung einverstanden ist.

In den meisten Landesgesetzen ist bestimmt, daß der Empfänger die übermittelten Daten nur für den Zweck verwenden darf, zu dessen Erfüllung sie ihm übermittelt wurden. In Baden-Württemberg und im Saarland sehen die Landesgesetze zusätzlich vor, daß die übermittelnde Stelle die Datenübermittlung mit Auflagen versehen kann, die den Datenschutz beim Empfänger sicherstellen.

Die Landesgesetze in Bayern und in Nordrhein-Westfalen enthalten Verordnungsermächtigungen, auf Grund deren die Landesregierung — in Bayern auch die Staatskanzlei und die Staatsministerien — näher regeln können, unter welchen Voraussetzungen Datenübermittlungen stattfinden dürfen. In den Rechtsverordnungen sind die für die Übermittlung bestimmten Daten, deren Empfänger und der Zweck der Übermittlung zu bezeichnen.

In Rheinland-Pfalz besteht eine Sondervorschrift für die Übermittlung personenbezogener medizinischer Daten. Die Übermittlung ist nur mit Zustimmung des Betroffenen zulässig, es sei denn, daß eine gesetzliche Erlaubnis gegeben ist. Ist die Zustimmung nicht rechtzeitig zu erlangen, weil der Betroffene zu einer Willensäußerung nicht in der Lage ist, so hat der behandelnde Arzt darüber zu entscheiden, ob eine Datenübermittlung dem mutmaßlichen Willen des Betroffenen entspricht und in seinem wohlverstandenen Interesse geboten ist. Die Regelung gilt übrigens auch für die Übermittlung medizinischer Daten innerhalb des öffentlichen Bereichs. Die Datenschutzgesetze des Bundes und der übrigen Länder haben eine solche Regelung nicht.

4.4.8 Auskunft an den Betroffenen

Nach den Datenschutzgesetzen des Bundes und aller Länder ist dem Betroffenen auf Antrag Auskunft über die zu seiner Person gespeicherten Daten zu erteilen. Nach den Landesdatenschutzgesetzen mit Ausnahme derer der Länder Hessen, Niedersachsen und Schleswig-Holstein ist dem Betroffenen außerdem Auskunft über die Stellen zu erteilen, denen Daten regelmäßig übermittelt werden. Abweichend davon ist in Baden-Württemberg und in Berlin bestimmt, daß die Auskunft sich auch auf die Empfänger der nicht regelmäßigen Übermittlungen der letzten zwei Jahre bezieht. Nach dem Datenschutzgesetz des Landes Baden-Württemberg ist die Auskunftserteilung gebührenfrei.

4.4.9 Verschuldensunabhängiger Schadensersatzanspruch

Schadensersatz kann der Betroffene nach den gesetzlichen Regelungen in den meisten Ländern — in der Regel bis zum Betrag von 250 000 DM für jedes schädigende Ereignis — verlangen, wenn er durch eine nach dem jeweiligen Datenschutzgesetz oder nach anderen Vorschriften über den Datenschutz unzulässige, rechtswidrige oder unrichtige Datenverarbeitung in seinen schutzwürdigen Belangen beeinträchtigt wird. Ein Verschuldensnachweis wird nicht gefordert. Einige Länder beschränken den Ersatzanspruch auf Schäden, die durch automatische Datenverarbeitung verursacht sind. Das Bundesdatenschutzgesetz und die Datenschutzgesetze der Länder Baden-Württemberg und Schleswig-Holstein sowie des Saarlandes sehen eine Gefährdungshaftung nicht vor.

4.4.10 Berichtigung, Sperrung und Löschung von Daten

Nach dem Bayerischen und dem Saarländischen Datenschutzgesetz kann der Betroffene verlangen, daß seine Daten gesperrt werden, wenn er ein berechtigtes Interesse an der Sperrung darlegt und — so im Saarland — keine überwiegenden Interessen der Allgemeinheit entgegenstehen.

Nach dem Bremischen Datenschutzgesetz sind bestrittene Daten, deren Richtigkeit die speichernde Stelle nicht beweisen kann, zu löschen. Eine ähnliche Regelung besteht in Rheinland-Pfalz.

Die Datenschutzgesetze von Baden-Württemberg, Bayern, Berlin, Bremen und Nordrhein-Westfalen sehen vor, daß im Falle einer Berichtigung, Sperrung und Löschung von Daten die Stellen zu verständigen sind, denen die Daten regelmäßig übermittelt wurden.

In den Ländern Bayern, Nordrhein-Westfalen und Rheinland-Pfalz ist gesetzlich verankert, daß der Betroffene verlangen kann, daß eine Beeinträchtigung seiner schutzwürdigen Belange unterlassen oder beseitigt wird, wenn diese nach einer Berichtigung, Sperrung oder Löschung gespeicherter Daten noch andauert.

4.4.11 Landesbeauftragter für den Datenschutz

In allen Ländern — mit Ausnahme des Landes Rheinland-Pfalz — ist jeweils ein in Ausübung seines Amtes unabhängiger Landesbeauftragter für den Datenschutz berufen worden oder noch zu bestellen. In Rheinland-Pfalz ist statt dessen eine Datenschutzkommission beim Landtag, bestehend aus drei Abgeordneten und zwei Beamten oder Richtern des Landes, gebildet.

Die Rechtsstellung der Landesbeauftragten ist unterschiedlich geregelt. Sie stehen teils — wie der Bundesbeauftragte — in einem besonderen öffentlich-rechtlichen Amtsverhältnis, teils sind sie Beamte auf Zeit oder auf Lebenszeit. Sie werden überwiegend von den jeweiligen Landesregierungen ernannt; in Berlin, Bremen, Hessen, Nordrhein-Westfalen und nach dem Hamburger Gesetzentwurf wird der Landesbeauftragte vom Abgeordnetenhaus, von der Bürgerschaft bzw. dem Landtag gewählt.

Während in Berlin der Landesbeauftragte als besondere oberste Landesbehörde eingerichtet ist, sind die Dienststellen der übrigen Landesbeauftragten überwiegend den Innenministern, in Bayern der Staatskanzlei und in Hessen dem Landtag zugeordnet. In Bayern, Hessen und Nordrhein-Westfalen haben die Landesbeauftragten ein ausdrücklich festgelegtes Vorschlagsrecht in Personalangelegenheiten ihrer Dienststelle; in Hamburg ist dies im Gesetzentwurf vorgesehen. In Baden-Württemberg und im Saarland können die Personalstellen nur im Einvernehmen bzw. Benehmen mit dem Landesbeauftragten besetzt werden.

Die gesetzliche Aufgabenzuweisung und die Befugnisse der Landesbeauftragten entsprechen im wesentlichen denen des Bundesbeauftragten. Auf die im BDSG und in den meisten Landesgesetzen vorgesehene Einschränkung der Kontrollbefugnis bei Sicherheitsbehörden im Fall einer Gefährdung der Sicherheit des Bundes oder eines Landes ist in Nordrhein-Westfalen verzichtet worden. Der saarländische Landesbeauftragte ist nicht befugt, die Verfassungsschutzbehörde zu kontrollieren. Der bayerische Landesbeauftragte kontrolliert auch die Einhaltung des Datenschutzes bei öffentlich-rechtlichen Religionsgesellschaften, soweit diesen von Behörden personenbezogene Daten übermittelt werden.

In Berlin, Bremen, Hessen, Nordrhein-Westfalen und Rheinland-Pfalz ist den Landesbeauftragten bzw. der Datenschutzkommission die Aufgabe übertragen, die Auswirkungen der automatisierten Datenverarbeitung dahingehend zu beobachten, ob sie zu einer Verschiebung der Gewaltenteilung zwischen den Verfassungsorganen, der gesetzlichen Aufgaben der Gemeinden und der Aufgabentrennung zwischen staatlicher Verwaltung und der kommunalen Selbstverwaltung führen. Die Landesbeauftragten können Maßnahmen anregen, die geeignet erscheinen, derartige Auswirkungen zu verhindern.

In Bayern wird bei dem Landesbeauftragten zu dessen Unterstützung zusätzlich ein Beirat aus Mitgliedern des Landtags, des Senats, der Staatsregierung, der kommunalen Spitzenverbände und des Verbandes freier Berufe e. V. gebildet. In Bremen wählt die Bürgerschaft (Landtag) zur Durchführung der parlamentarischen Kontrolle des Datenschutzes einen ständigen Parlamentsausschuß.

4.4.12 Dateienregister, Veröffentlichungen über die Dateien

Jeder Landesbeauftragte und die Datenschutzkommission in Rheinland-Pfalz führen Register der Dateien, in denen personenbezogene Daten gespeichert sind. Jedermann kann in die Register Einsicht nehmen.

Bei einem Teil der Länder werden, wie beim Bundesbeauftragten, in das Register nur die automatisch betriebenen Dateien aufgenommen, bei einem anderen Teil der Länder alle Dateien der Behörden. In Bayern und Schleswig-Holstein hat der Landesbeauftragte den Inhalt des Dateienregisters zu veröffentlichen; in Baden-Württemberg, Rheinland-Pfalz, im Saarland und nach dem Hamburger Entwurf sind überhaupt keine Veröffentlichungen durch die speichernden Stellen über die vorhandenen Dateien vorgesehen.

4.4.13 Ordnungswidrigkeiten und Straftaten

Mehrere Länder haben in den Bußgeldbestimmungen der Datenschutzgesetze Sanktionen vorgesehen, wenn private Empfänger von Daten diese entgegen dem Übermittlungszweck verwenden. Im Saarland handelt auch ordnungswidrig, wer sich durch unwahre Angaben gegenüber einer Behörde Daten, die nicht offenkundig sind, verschafft. Nach dem Datenschutzgesetz des Landes Rheinland-Pfalz ist neben der unbefugten Übermittlung und Veränderung nicht

offenkundiger Daten — so das BDSG und die übrigen Landesgesetze — auch die sonstige unbefugte Verwendung unter Strafe gestellt; strafbar macht sich dort auch, wer unbefugt den Zugriff auf solche Daten gewährt.

Die in den Datenschutzgesetzen bezeichneten Straftaten werden jeweils nur auf Antrag des Betroffenen verfolgt. In den Ländern Baden-Württemberg, Bremen, Nordrhein-Westfalen, Rheinland-Pfalz und im Saarland ist neben den Betroffenen auch der Datenschutzbeauftragte bzw. die Datenschutzkommission antragsberechtigt. In Niedersachsen kann die Strafverfolgungsbehörde von Amts wegen tätig werden, wenn sie wegen des besonderen öffentlichen Interesses ein Einschreiten für geboten hält.

4.4.14 Informationsrecht des Landtags

In den Datenschutzgesetzen der Länder Baden-Württemberg, Berlin, Bremen, Hessen, Rheinland-Pfalz und des Saarlandes sind unterschiedlich ausgestaltete Informations- und Auskunftsrechte des Landtags bzw. Abgeordnetenhauses, zum Teil auch der kommunalen Vertretungsorgane, festgelegt. Danach sind die Behörden und sonstigen öffentlichen Stellen verpflichtet, die von den vorgenannten Stellen im Rahmen ihrer Zuständigkeit verlangten Auskünfte aus automatisiert betriebenen Dateien zu geben, soweit Programme zur Auswertung vorhanden sind. Die Auskünfte dürfen allerdings keine personenbezogenen Daten enthalten; in Baden-Württemberg ist dies in beschränktem Umfange zulässig.

5 Datenschutz im Ausland, internationale Zusammenarbeit

5.1 Stand der Datenschutzgesetzgebung im Ausland

Stand und Entwicklung des Datenschutzrechts in anderen Staaten habe ich in meinem ersten Tätigkeitsbericht (5.2) ausführlich beschrieben. Ich ergänze diesen Bericht in Bezug auf die USA und beschränke mich im übrigen auf die Darstellung der seitdem eingetretenen Änderungen und erlassenen Neuregelungen.

5.1.1 USA

Im Oktober 1979 habe ich mich mit Unterstützung des Auswärtigen Amtes über den Stand des Datenschutzes in den USA informiert. In Gesprächen mit Parlamentariern und ihren Mitarbeitern, Regierungsstellen, Wissenschaftlern und Vertretern der Wirtschaft habe ich zahlreiche Informationen über vorhandene und geplante Datenverarbeitungssysteme und die Methoden des Datenschutzes erhalten. Beim Vergleich mit den deutschen Verhältnissen ist zu berücksichtigen, daß sowohl die Strukturen von Wirtschaft und Verwaltung wie auch die Rechts- und Verfassungstraditionen sich erheblich voneinander unterscheiden. Gleichwohl sind Gemeinsamkeiten unverkennbar. So sind die typischen Gefahren für die Rechte des einzelnen, die aus dem intensiven Einsatz technischer Geräte für Datenübermittlung und -verarbeitung mit ihrer enormen Kapazität, Schnelligkeit und Vielseitigkeit entstehen, im wesentlichen gleich, und dem Schutzbedürfnis wird zumindest teilweise durch gleiche oder ähnliche Maßnahmen Rechnung getragen,

Die Gesetzgebungskompetenz ist in den Vereinigten Staaten stärker aufgesplittert. Daher besteht z. B. keine abschließende Regelung des Bundes für die Informationsverarbeitung in der Wirtschaft. Der Federal Fair Credit Reporting Act begründet bundesweit nur Minimalanforderungen und gestattet den Staaten zusätzliche Anforderungen, die damit vereinbar sind, einzuführen. Davon ist in unterschiedlichem Maße Gebrauch gemacht worden. Auch für die Informationspraxis von Banken und anderen Institutionen des Finanzwesens gibt es einzelstaatliche Gesetze unterschiedlichen Inhalts. Nur wenige Staaten haben Datenschutzrecht für die Versicherungswirtschaft und für das Arbeitsverhältnis geschaffen. Für die eigene staatliche Verwaltung haben verschiedene Staaten „Landesdatenschutzgesetze" („Privacy Acts" oder „Fair Information Practices Acts") beschlossen, die die Sammlung, Aufbewahrung, Verwendung und Offenbarung von personenbezogenen Informationen über einzelne durch staatliche — in einzelnen Fällen auch örtliche — Verwaltungsstellen regeln. Einige wenige weitere Staaten haben bereichsspezifische Datenschutzbestimmungen geschaffen. Die National Conference of Commissioners on Uniform State Laws hat den Entwurf eines einheitlichen Datenschutzgesetzes für die Einzelstaaten fast fertiggestellt.

Auf der Ebene des Bundes besteht der Privacy Act von 1974, der für die meisten Verwaltungsstellen des Bundes gilt. Daneben schützen mehrere Bundesgesetze die Vertraulichkeit bestimmter Dateien, z. B. der Steuerverwaltung, der Statistischen Ämter und der Stellen, die den Drogenmißbrauch bekämpfen. Strenge Datenschutzbestimmungen sind für Schulen und Hochschulen eingeführt worden. Der Datenschutz innerhalb der Kreditwirtschaft wird durch den bereits erwähnten Fair Credit Reporting Act und weitere Gesetze (Equal Credit Opportunity Act, Fair Credit Billing Act, Fair Debt Collection Practices Act und — gegenüber der Verwaltung — Right to Financial Privacy Act) gewährleistet.

Die Regelungstechnik ist sehr viel kasuistischer als in kontinental-europäischen Gesetzen; Tatbestand wie Rechtsfolge der Datenschutznormen sind daher

in aller Regel enger; umfassende Gesetze sind selten. Dies hat den Vorteil größerer Konkretheit und Lebensnähe. Der Privacy Act wird als unmittelbare Antwort auf die Enthüllungen von „Watergate" angesehen, und auch für Geheimhaltungsbestimmungen z. B. im Steuerrecht und für die Kreditwirtschaft gab es konkrete Anlässe in Gestalt von Mißbräuchen.

In manchen Einzelvorschriften wie auch in Verwaltungsrichtlinien und einigen unternehmensinternen Verhaltenscodices finden sich Anregungen für praktische Verbesserungen des Datenschutzes in Einzelbereichen, die auch im Rahmen des deutschen Rechts Beachtung verdienen, z. B. Verfahrensregeln für die Übermittlung von Daten aus dem privaten und öffentlichen Bereich (Einschaltung von Gerichten, Fristen, Mitteilungspflichten gegenüber dem Betroffenen) und für den „Abgleich" von Dateien verschiedener Stellen der öffentlichen Verwaltung (Guidelines for the Conduct of Matching Programes, herausgegeben vom Office of Management and Budget am 30. 3. 1979, wo u. a. die vorherige Untersuchung und ausführliche Darstellung der Vor- und Nachteile einschließlich der Kosten solcher Abgleichsprogramme vorgeschrieben wird).

Eine Reihe bemerkenswerter Gesetzgebungsvorschläge sind gerade in jüngster Zeit im Kongreß eingebracht worden. Sie gehen zum Teil auf die Initiative des Präsidenten zurück, die in dessen weithin beachteter Botschaft an den Kongreß vom 2. April 1979 dargelegt ist; zum Teil sind einzelne besonders engagierte Abgeordnete und Senatoren aktiv geworden. So sind derzeit z. B. drei konkurrierende Gesetzentwürfe zum Schutze medizinischer Daten anhängig. Lösungsvorschläge für Probleme einer ganz neuen Technologie, die noch gar nicht voll eingesetzt wird, enthält der Entwurf für einen Fair Financial Information Practices Act; hier geht es u. a. darum, die Daten zu schützen, die bei elektronischem Zahlungsverkehr anfallen, wie er künftig von Heimterminals aus möglich sein soll. Von besonderem Interesse ist auch die Forderung nach einer „Charter" für das FBI, zu der Senator Edward Kennedy einen Entwurf eingebracht hat. Über Einzelheiten dieser und anderer Regelungsvorschläge — die zum Teil auch ohne die Entscheidung des Gesetzgebers durch die Exekutive durchgeführt werden können — kann hier nicht berichtet werden.

Auch über den Grad der Verwirklichung von Datenschutzmaßnahmen — sei es innerhalb der Wirtschaft, sei es in der öffentlichen Verwaltung — kann hier nicht referiert werden. Während offenbar einzelne Unternehmen und manche Verwaltungszweige sich der Bedeutung der Privacy voll bewußt sind und entsprechende Maßnahmen für ihren Bereich vorgesehen haben, ergeben Umfragen, wie sie u. a. der frühere Vorsitzende der Privacy Protection Study Commission, Prof. Linowes, hat durchführen lassen, daß es bei der Verwirklichung von Datenschutz noch große Lücken gibt. Prof. Linowes, den ich an der Universität von Illinois (Urbana-Champaign) aufgesucht habe, berichtete aber auch, daß die Empfehlungen seiner Kommission im allgemeinen sehr positiv aufgenommen worden seien und man sich bei Abweichungen von der dort für richtig gehaltenen Praxis zumindest zu rechtfertigen suche. Einen Eindruck davon, wie sich Beamte eines Einzelstaates, der in der Datenschutzgesetzgebung führend ist, für die Umsetzung liberaler Vorstellungen in die Verwaltungspraxis engagieren, konnte ich in Boston (Massachusetts) gewinnen, wo ich mit Mitgliedern des Privacy Security Council sprechen konnte.

Die Datenschutzdiskussion in den USA wird nach Auskunft meiner Gesprächspartner durch die zunehmende Bürokratiekritik beeinflußt, die nicht nur die unkoordinierte Parallelarbeit mancher Regierungsstellen rügt, sondern sich gegen jede Ausweitung der staatlichen Aktivität wendet. An solchen Tendenzen scheitert bisher auch die u. a. von der Privacy Protection Study Commission vorgeschlagene Einrichtung eines zentralen Datenschutzaufsichtsgremiums. Nur in einigen Einzelstaaten gibt es solche Boards. Das Fehlen einer zentralen Kontrollinstanz hat übrigens auch bewirkt, daß die USA an der internationalen Kooperation der Datenschutzkontrollinstanzen bisher nicht teilgenommen haben.

Es entspricht der herrschenden amerikanischen Sozialphilosophie, darauf zu vertrauen, daß der einzelne seine Rechte wahrnimmt, daß er sie notfalls gerichtlich durchsetzt, sich dabei aber nicht von Verwaltungsstellen helfen läßt. Tatsächlich scheint es so, daß von dem Auskunftsrecht des Betroffenen sehr viel häufiger Gebrauch gemacht wird als bei uns. Hierzu ist noch auf eine weitere Besonderheit des amerikanischen Rechts hinzuweisen, die von großer Bedeutung ist: Neben dem Recht auf Auskunft über die eigenen Daten nach den Datenschutzgesetzen (Privacy Acts) gibt es das allgemeine Akteneinsichtsrecht nach dem Informationsfreiheitsgesetz (Freedom of Information Act — FOIA —) des Bundes und entsprechender einzelstaatlicher Gesetze (siehe dazu schon 1. TB, zu 3.4.7.3 und 3.4.7.4). Obwohl der dadurch begründete Aufklärungsanspruch als ein Gegenkonzept zum Datenschutz angesehen werden könnte, ergänzen sich in der Praxis beide rechtlichen Ansätze. Das Datenschutzrecht gewährt nämlich Auskunftsrechte nur in geringerem Umfang als der FOIA, und so wird insbesondere im Bereich der Sicherheitsbehörden die Mehrzahl der Auskunftsersuchen nach dem FOIA von Betroffenen gestellt. Der Auskunftsanspruch Nichtbetroffener endet dort, wo die Offenlegung die „personal privacy" verletzen würde. Die auskunftspflichtigen Behörden machen von ihrem Auskunftsverweigerungsrecht in der Regel nur noch dann Gebrauch, wenn dieses Recht nach beiden in Betracht kommenden Gesetzen, also dem Privacy Act und dem FOIA gegeben ist. Ich habe mich wegen dieses engen Zusammenhanges zwischen Datenschutz und Informationsfreiheit auch über die Praxis der Auskunftserteilung nach dem FOIA unterrichtet. Sie ist von Ressort zu Ressort sehr unterschiedlich. Selbstverständlich gibt es etwa beim FBI oder anderen Sicherheitsbehörden besondere Probleme; sie sind jedoch nach der Auskunft der verantwortlichen Beamten weitgehend gelöst oder lösbar. Ich halte das allgemeine Akteneinsichtsrecht für eine wichtige Ergänzung des Datenschutzes.

5.1.2 Schweden

In meinem 1. Tätigkeitsbericht habe ich über die wesentlichen Ergebnisse einer zur Überprüfung des schwedischen Datenschutzgesetzes gebildeten Kommission berichtet. Deren Vorschläge sind inzwischen umgesetzt und in das schwedische Datenschutzgesetz, das mit Wirkung vom 1. Juli 1979 geändert wurde, aufgenommen worden.

Folgende Änderungen verdienen hervorgehoben zu werden:

Bei etwa 70 % der automatisiert geführten Dateien ist es offenkundig, daß durch die Speicherung schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden. Diese Dateien bedürfen nicht mehr der Genehmigung durch die Dateninspektion. Für sie wird ein vereinfachtes Registrierungsverfahren entwickelt, welches gewährleistet, daß die Daten dem Kontrollzugriff der Dateninspektion nicht entzogen werden. Für die Genehmigung der sonstigen Dateien sind die Prüfkriterien präzisiert worden: Es ist abzustellen auf die Art der gespeicherten Daten und die Anzahl der Personen, deren Daten gespeichert werden sollen. Ferner ist festgelegt, daß der Zweckbestimmungsgrundsatz Grenzen setzt im Hinblick auf die Personen, deren Daten erhoben werden sollen und die Daten, die gespeichert werden dürfen. Will eine speichernde Stelle Daten über andere Personen als die eigenen Mitglieder, Arbeitnehmer oder Kunden führen, darf die Genehmigung nur erteilt werden, wenn besondere Rechtfertigungsgründe dafür vorgetragen werden. Diese Vorschrift bezieht sich in erster Linie auf die Dateien, die Unternehmen der Direktwerbung (Adressenhandel) führen. Über diese gesetzliche Regelung hinaus hat die schwedische Regierung im Frühjahr 1979 beschlossen, daß ab 1. Juli 1981 nur mehr der Staat selbst Anschriftenverzeichnisse der Bevölkerung anlegen und Auskünfte daraus geben darf. Entsprechende Einschränkungen gelten für Dateien, in denen besonders empfindliche Daten (z. B. Angaben über die Gesundheit, die Sozialhilfe, den Alkoholismus, über politische oder religiöse Anschauungen) gespeichert werden sollen. Andere als die zuständigen Fachbehörden dürfen solche Dateien nur bei Vorliegen zwingender Gründe führen.

Neu aufgenommen ist auch eine Regelung, die den Halter einer Datei verpflichtet, bestehende Eintragungen zu ergänzen oder Angaben über weitere Personen aufzunehmen, wenn dies von der Zweckbestimmung der Datei her geboten erscheint. Die Dateninspektion ist jetzt ausdrücklich ermächtigt, die weitere Führung einer Datei zu untersagen, wenn dadurch schutzwürdige Belange beeinträchtigt werden oder wenn Grund zur Annahme besteht, daß dies der Fall sein könnte. Das Auskunftsrecht des Betroffenen ist erweitert worden. Es umfaßt neben der Auskunft über die gespeicherten Daten auch das Recht, darüber unterrichtet zu werden, daß über ihn keine Daten gespeichert sind. Nicht in das Datenschutzgesetz aufgenommen wurde ein Vorschlag der Kommission, Register, die für Zwecke der Forschung oder Statistik angelegt worden sind, durch Datenschutzerwägungen nicht in ihrer Funktionsfähigkeit zu beeinträchtigen.

5.1.3 Luxemburg

In Luxemburg sind im Frühjahr 1979 zwei wichtige den Datenschutz betreffende Gesetze erlassen worden, nämlich am 30. März 1979 ein Gesetz, durch das ein Personenkennzeichen eingeführt wurde (Loi du 30 mars 1979 organisant l'identification numerique des personnes physiques et morales) und am folgenden Tag ein Datenschutzgesetz (Loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques) (veröffentlicht im Amtsblatt des Großherzogtums Luxemburg Nr. 29 vom 11. April 1979 S. 581)

Gesetz über das Personenkennzeichen

Jeder in Luxemburg geborenen oder eingewanderten natürlichen und jeder dort ansässigen juristischen Person wird ein Personenkennzeichen zugewiesen. In einem zentralen Register werden alle Personenkennzeichen zusammen mit weiteren der Identifizierung dienenden personenbezogenen Daten gespeichert. Das Personenkennzeichen wird dem Betroffenen und denjenigen öffentlichen Stellen zugeleitet, denen die Benutzung durch Gesetz oder andere Regelungen gestattet ist. Es ist ferner durch besondere Regelungen festzulegen, welche offiziellen Urkunden, Dokumente und Akten das Personenkennzeichen enthalten dürfen. Nur für diese verwaltungsinternen Zwecke und für die Kontakte der Verwaltung zum Betroffenen darf das Personenkennzeichen genutzt werden. Weitere Einzelheiten über die Art des Personenkennzeichens und seine Handhabung werden in besonderen Rechtsvorschriften festgelegt.

Das Datenschutzgesetz

Das Gesetz schützt natürliche und juristische Personen gegen den Mißbrauch ihrer Daten, soweit diese zum Zwecke der automatisierten Verarbeitung erhoben, in Datenbanken gespeichert und verarbeitet werden.

Das Gesetz gilt für alle in Luxemburg installierten Datenbanken, auch dann, wenn die Daten ausschließlich im Ausland genutzt werden. Ausgenommen sind lediglich Datenbanken, die durch Gesetz für jedermann öffentlich zugänglich sind, sowie solche, die nur den Eigentümer der Datenbanken selbst betreffende Daten enthalten, und schließlich Datenbanken, die von Institutionen des internationalen öffentlichen Rechts eingerichtet worden sind.

Die Aufgabe der Datenschutzkontrolle wird einem Minister übertragen. Er führt ein nationales Register aller Datenbanken, und er hat dafür Sorge zu tragen, daß die Vorschriften des Gesetzes eingehalten werden. Er kann Kontrollen durchführen, Auskünfte verlangen und Empfehlungen sowie Warnungen erteilen. Zur Erfüllung seiner Aufgaben bedient er sich eines Beratungsausschusses, der aus mindestens 5 vom Großherzog bestellten Persönlichkeiten aus dem privaten Bereich besteht. Ihre Amtszeit beträgt 5 Jahre.

Datenbanken in Bereichen, die nicht der staatlichen Kontrolle unterliegen, benötigen eine Genehmigung

durch den für den Datenschutz zuständigen Minister. Dieser erteilt die Genehmigung nach Anhörung des Beratungsausschusses, sofern kein Grund zur Annahme besteht, daß die Daten mißbraucht werden. Die Genehmigung kann mit Auflagen z. B. im Hinblick auf die Datensicherung und die Dauer der zulässigen Datenspeicherung verbunden werden.

Datenbanken aus dem öffentlichen Bereich dürfen nur aufgrund eines Gesetzes oder einer anderen Rechtsvorschrift des Großherzogtums errichtet werden. Vor dem Erlaß entsprechender Rechtsvorschriften ist der Beratungsausschuß anzuhören.

Das nationale Register enthält Angaben zur Identifizierung der Datenbank und ihres Betreibers sowie über die Rechtsgrundlagen der gespeicherten Daten. Darüber hinaus werden die Zwecke der Datenbank, die Art und Herkunft der gespeicherten Daten sowie bei Übermittlungen die Empfänger aufgeführt. Datenbanken, die die staatliche Sicherheit, die nationale Verteidigung oder die Kriminalitätsbekämpfung betreffen, können durch Beschluß der Regierung von der Veröffentlichung im nationalen Register ausgenommen werden.

Nach den Vorschriften über die Zulässigkeit der Verarbeitung ist es verboten, Daten durch betrügerische, unfaire oder ungesetzliche Mittel zu erheben. Daten, die den intimen Bereich des Privatlebens, politische oder religiöse Überzeugungen oder die Gewerkschaftszugehörigkeit betreffen, dürfen grundsätzlich nicht erhoben und gespeichert werden. Ausnahmen sind nur für entsprechende Vereinigungen im Hinblick auf ihre Mitglieder gestattet. Daten über Vorstrafen und Anordnungen nach dem Jugendschutzgesetz dürfen nur von staatlichen Stellen auf der Basis einer Rechtsgrundlage gespeichert und verarbeitet werden.

Der Betroffene, bei dem personenbezogene Daten erhoben werden sollen, ist zu informieren

— über den Zweck der automatisierten Datenverarbeitung,

— darüber, ob er zur Hergabe der Daten verpflichtet ist oder nicht,

— über die Folgen einer Auskunftsverweigerung,

— über Dritte, denen die Daten zugänglich gemacht werden,

— und über seine Rechte auf Auskunft und Berichtigung.

Werden die Daten mittels eines Fragebogens erhoben, sind die vorstehenden Angaben dort aufzuführen.

Jedermann hat das Recht, gegen eine Gebühr Auskunft über die über ihn gespeicherten Daten zu verlangen. Die Fälle, in denen eine Auskunft verweigert werden kann, sind durch Rechtsvorschrift festzulegen. Daten über den Gesundheitszustand sind dem Betroffenen durch den Arzt seines Vertrauens zugänglich zu machen. Der Betroffene kann ferner die Berichtigung, Vervollständigung, Aktualisierung oder die Löschung der ihn betreffenden Daten verlangen. Werden Daten berichtigt oder gelöscht, sind alle bisherigen Empfänger zu benachrichtigen.

Das Gesetz enthält sehr einschneidende Strafvorschriften gegen Verletzungen seiner Regelungen.

5.2 Grenzüberschreitender Datenverkehr

Die Gewährleistung des Datenschutzes beim grenzüberschreitenden Transport personenbezogener Daten gewinnt zunehmend an Bedeutung. Es sind nicht nur Bundesbürger, die sich dafür interessieren, was mit ihren Daten im Ausland geschieht. Ich habe im Berichtsjahr aufgrund der zwischen mir und den übrigen nationalen Datenschutz-Kontrollbehörden vereinbarten Zusammenarbeit auch Ersuchen von im Ausland lebenden Betroffenen bearbeitet, die sich gegen die Verarbeitung ihrer Daten in der Bundesrepublik zur Wehr setzten, und umgekehrt die Kontakte nutzen können, um Deutschen bei der Durchsetzung ihrer Rechte im Ausland zu helfen. Mögen Eingaben dieser Art gegenwärtig auch zahlenmäßig noch nicht ins Gewicht fallen, so ist dies kein Indiz dafür, daß das Problem nicht existierte oder bedeutungslos sei. Auch hier gilt: Die Tendenz beim grenzüberschreitenden Datenverkehr ist steigend. Dem Datenschutz ist daher bereits in den Anfängen der ihm gebührende Stellenwert beizumessen.

5.2.1 Gegenwärtige Sach- und Rechtslage

Wie ein Überblick über die nationalen Datenschutzgesetze zeigt, sind in wachsendem Maße Ansätze dafür erkennbar, den grenzüberschreitenden Transport personenbezogener Daten gesetzlichen Beschränkungen zu unterwerfen, sei es durch materielle Regelungen, sei es durch administrative Kontrollmaßnahmen (z. B. Exportlizenzen). Die bisher vorliegenden Entwürfe für internationale Übereinkommen zielen indes darauf ab, auf eine Harmoniesierung der nationalen Datenschutzgesetze in wichtigen Grundprinzipien hinzuwirken. Deutlich erkennbar ist das Bestreben, den freien Datenfluß so weitgehend wie möglich zu erhalten.

5.2.2 Nationale Datenschutzgesetze

Im einzelnen ist der Stand der Regelungen des grenzüberschreitenden Datenverkehrs innerhalb der nationalen Datenschutzgesetzgebung wie folgt zu kennzeichnen:

Bundesrepublik Deutschland

Die Regelungen des Bundesdatenschutzgesetzes über die Zulässigkeit der Übermittlung personenbezogener Daten gelten auch für den Fall der Übermittlung ins Ausland. Dabei ist der Tatsache, ob es im Empfängerland ein Datenschutzgesetz gibt oder nicht, Rechnung zu tragen. Es gibt bisher kein Genehmigungs- oder Registrierungsverfahren, das den grenzüberschreitenden Transport personenbezogener Daten einer Datenschutzkontrolle unterwirft.

Frankreich

In Frankreich ist nach dem Datenschutzgesetz vom 6. Januar 1978 eine Kontrollkommission gebildet worden, der es obliegt, bestimmte Formen automatisierter Datenverarbeitung zu genehmigen oder zu registrieren. In den Anträgen ist auch anzugeben, ob die zu verarbeitenden Daten ganz oder teilweise ins Ausland übermittelt werden sollen. Weitergehende Einschränkungen gibt es z. Z. noch nicht. Der Staatsrat kann aber auf Vorschlag oder nach Stellungnahme der Datenschutzkommission eine Verordnung erlassen, durch die der grenzüberschreitende Transport personenbezogener Daten genehmigungspflichtig oder anderen Beschränkungen unterworfen wird.

Österreich

Das österreichische Datenschutzgesetz vom 18. Oktober 1979 enthält einen eigenen Abschnitt, der den internationalen Datenverkehr regelt. Der Export von automationsunterstützt verarbeiteten Daten in das Ausland bedarf grundsätzlich der Genehmigung der Datenschutzkommission. Die Ausnahmen und die Kriterien, nach denen eine Genehmigung zu erteilen ist, sind im Gesetz festgelegt. Diese Beschränkungen gelten auch, wenn nur ein Arbeitsgang der Verarbeitung z. B. in einem im Ausland gelegenen Rechenzentrum durchgeführt wird, oder wenn aus einer in Österreich gelegenen Datenverarbeitungsanlage personenbezogene Daten aus dem Ausland abgerufen werden können.

Luxemburg

Das luxemburgische Datenschutzgesetz vom 31. März 1979 gilt für sämtliche in Luxemburg installierten Datenbanken, und zwar auch dann, wenn die gespeicherten Daten ausschließlich im Ausland genutzt werden. Kann eine im Ausland befindliche Datenbank von einem Terminal in Luxemburg genutzt werden, so gilt das Gesetz für den Benutzer dieses Terminals. Die Datenbanken unterliegen einer staatlichen Genehmigungspflicht. Auch der Benutzer des in Luxemburg gelegenen Terminals bedarf dieser Genehmigung.

Schweden

Sollen personenbezogene Daten ins Ausland übermittelt werden und besteht Grund zu der Annahme, daß sie dort automatisiert verarbeitet werden sollen, bedarf die Übermittlung der Genehmigung durch die Dateninspektion.

Dänemark

Nach dem dänischen Datenschutzgesetz gibt es Regelungen für den Export besonders empfindlicher Daten (Rasse, religiöse Überzeugung, Hautfarbe, politische Ansichten, Vorstrafen). Diese Daten dürfen grundsätzlich nur mit Genehmigung der Datenschutzkontrollbehörde ins Ausland übermittelt werden. Erleichterungen sind möglich, wenn im Empfängerstaat ausreichende Datenschutzvorkehrungen getroffen worden sind.

Norwegen

Personenbezogene Daten, deren Verarbeitung im Inland genehmigungspflichtig ist, dürfen auch nur mit Genehmigung des Königs ins Ausland exportiert werden. Auch hier sind Ausnahmeregelungen für den Fall des Exports in Länder mit eigener Datenschutzgesetzgebung möglich.

5.3 Internationale Übereinkommen

Gegenüber der Darstellung in meinem ersten Tätigkeitsbericht hat sich nur wenig verändert. Die Entwürfe für internationale Übereinkommen, die im Europarat und in der OECD vorbereitet werden, haben ein konkretes Stadium erreicht. Beiden ist gemeinsam, daß sie keine unmittelbar anwendbaren Regelungen für den grenzüberschreitenden Verkehr personenbezogener Daten enthalten. Sie sind vielmehr auf eine Harmonisierung des nationalen Datenschutzrechts ausgerichtet.

5.3.1 Europarat

Der Entwurf einer Datenschutz-Konvention (siehe 1. TB, 3.5.1) ist im Verlaufe des Berichtsjahres von einer Expertenkommission fertiggestellt worden. Er muß nun noch von weiteren Gremien innerhalb des Europarats gebilligt werden, ehe er von den Regierungen der Mitgliedstaaten unterzeichnet und den Parlamenten zur Ratifizierung zugeleitet werden kann. Inhaltlich enthält er im wesentlichen die Punkte, die ich in meinem ersten Tätigkeitsbericht aufgeführt habe. Erwähnt sei noch, daß das Übereinkommen zwar für den öffentlichen und den privaten Bereich gelten soll, daß es aber nur auf die automatisierte Verarbeitung personenbezogener Daten anwendbar ist. Es wird ferner nach der Ratifizierung nicht unmittelbar geltendes Recht, sondern es verpflichtet die Gesetzgeber der Mitgliedstaaten, die Datenschutzgrundsätze in der eigenen nationalen Gesetzgebung zu verwirklichen. Hervorzuheben ist unter den aufgeführten Datenschutzprinzipien der Grundsatz der Zweckbestimmung: Personenbezogene Daten, die für die automatisierte Verarbeitung bestimmt sind, sollen für festgelegte und rechtmäßige Zwecke gespeichert und nicht für Zwecke verwendet werden, die hiermit unvereinbar sind. Dieser Grundsatz ist im Bundesdatenschutzgesetz zwar auch enthalten, aber nicht durchgängig verankert. Hier wird sicher ein Schwerpunkt bei der Fortentwicklung des Datenschutzrechts zu sehen sein.

5.3.2 Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD)

Innerhalb der OECD sind von einer Expertengruppe Leitlinien im Entwurf fertiggestellt worden. Es handelt sich dabei um Empfehlungen an die Mitgliedstaaten ohne bindenden Charakter. Die politische Bedeutung sollte jedoch nicht unterschätzt werden. Die Leitlinien werden möglicherweise als erste verabschiedet werden. Sie richten sich dann praktisch an sämtliche westlichen Industrienationen. Adressat

sind einmal die Mitgliedstaaten, die aufgefordert werden, ihre nationale Gesetzgebung den in den Leitlinien niedergelegten Grundsätzen anzupassen. Adressat sind aber auch die in den Mitgliedstaaten tätigen Wirtschaftsunternehmen. Auch sie sind aufgefordert, die Datenschutzgrundsätze im Rahmen ihrer Möglichkeiten zu verwirklichen. Inhaltlich entsprechen die Grundsätze weitgehend denjenigen der Europaratskonvention. Im Bundesdatenschutzgesetz sind sie größtenteils verwirklicht.

5.3.3 Europäische Gemeinschaft

Aus dem Bereich der Kommission der Europäischen Gemeinschaften sind aus dem vergangenen Jahr keine neuen Entwicklungen zu berichten. Das Europäische Parlament hingegen hat in der letzten Sitzung der vergangenen Legislaturperiode einen Entschließungsantrag des Rechtsausschusses angenommen, in dem die Kommission u. a. aufgefordert wird, eine Richtlinie zur Harmonisierung des Datenschutzrechts auf höchstem Schutzniveau für die Gemeinschaftsbürger vorzubereiten. Der Datenschutz soll sich auf juristische Personen und andere Vereinigungen erstrecken.

Der Entschließung des Parlaments sind Empfehlungen beigefügt, die neben den wichtigsten Datenschutzgrundsätzen auch die Forderung enthalten, daß Dateien mit personenbezogenen Daten einer vorherigen Anmelde- oder Genehmigungspflicht unterworfen werden müssen. Die Europäischen Gemeinschaften sollen ferner ein Datenschutzorgan schaffen, dem die nationalen Datenschutzkontrollinstitutionen alljährlich zu berichten haben und das auch über eigene Kontrollbefugnisse in Fällen des grenzüberschreitenden Datentransports verfügen soll.

5.4 Internationale Zusammenarbeit in Fragen des Datenschutzes

In meinem 1. Tätigkeitsbericht (Nr. 5.3.2) hatte ich auf die Bedeutung der internationalen Zusammenarbeit in Fragen des Datenschutzes hingewiesen. Die von mir aufgenommenen Kontakte mit der schwedischen und der dänischen Datenschutzbehörde boten dafür erste Ansatzpunkte. Sie erwiesen sich als so nützlich, daß vorgeschlagen wurde, die bestehenden nationalen Datenschutzkontrollinstitutionen zu einem Gedanken- und Erfahrungsaustausch einzuladen. Ich habe diese Anregung gern aufgegriffen und die für die Kontrolle des Datenschutzes zuständigen Stellen in Kanada, Dänemark, Frankreich, Österreich, Neuseeland, Norwegen und Schweden zu einer Konferenz am 3./4. Mai 1979 nach Bonn eingeladen.

Aus Norwegen konnte niemand entsandt werden; zwar gibt es dort ein Datenschutzgesetz, die darin vorgesehene Kontrollbehörde ist jedoch noch nicht eingerichtet worden. Der neuseeländische Datenschutzbeauftragte war wegen anderweitiger vorrangiger Dienstgeschäfte an der Teilnahme verhindert. Kanada war durch den Privacy-Commissioner, Frau Inger Hansen, vertreten. Die französische Delegation wurde von dem Vizepräsidenten der französischen Datenschutzkommission (Commission Nationales de l'Informatique et des Libertés), Herrn Senator Tyraud, geleitet. Aus Dänemark waren der Direktor der dänischen Datenschutzkontrollbehörde, Herr Jørgen Paulsen und aus Schweden der Generaldirektor der Dateninspektion, Herr Jan Freese, gekommen. Die österreichische Datenschutzkommission war durch ihren Exekutivsekretär, Herrn Dr. Gerhard Stadler, vertreten. An der Konferenz nahmen ferner einige Vertreter von Bundesministerien und Datenschutzkontrollbehörden der Bundesländer teil.

Der erste Teil der Konferenz diente dem Erfahrungsaustausch. Die Repräsentanten der einzelnen Kontrollinstitutionen berichteten über deren Aufgaben und Befugnisse. Diese sind sehr unterschiedlich ausgestaltet: sie reichen von der bloßen Ombudsman-Funktion im Sinne eines Tätigwerdens nur auf Beschwerden Betroffener hin (Kanada) bis zu weitreichenden Mitwirkungsbefugnissen bei der Errichtung von Datenbanken (z. B. Dänemark, Schweden).

Einen Schwerpunkt der Beratungen bildete die Frage, wie der Datenschutz beim grenzüberschreitenden Datentransport personenbezogener Daten zu gewährleisten ist. Schweden verfügt insoweit über die längsten Erfahrungen. Dort bedarf der Export personenbezogener Daten der Genehmigung durch die Dateninspektion, wenn die Daten im Ausland automatisiert verarbeitet werden sollen. Die Genehmigung wird erteilt, wenn die Dateninspektion sich vergewissert hat, daß die Sicherheit der Daten ausreichend gewährleistet ist. Feste Kriterien für die Erteilung oder die Versagung der Exportlizenz gibt es nicht. Die dänische Aufsichtsbehörde wird entsprechend verfahren. Dort ist es allerdings möglich, den Export in bestimmte Länder (die z. B. über eine eigene Datenschutzgesetzgebung verfügen) lizenzfrei zu gestalten. Auch in Österreich bedarf der Datenexport einer Lizenz. Sie wird erteilt, wenn der Exporteur gewährleistet, daß die Daten im Empfängerland einen gleichwertigen Schutz erhalten. Er muß dies u. U. vertraglich sicherstellen. In Frankreich ist es gesetzlich möglich, den Datenexport von einer staatlichen Genehmigung abhängig zu machen. Davon wird z. Z. noch kein Gebrauch gemacht. In der eingehenden Diskussion wurden Zweifel geäußert, ob das Verfahren der Lizenzierung von Datenexporten tatsächlich eine zusätzliche Sicherheit erbringe, weil der Gebrauch der Daten im Empfängerland nicht kontrollierbar sei. Hier eröffnet sich für die Staaten, die über Datenschutzkontrollinstitutionen verfügen, eine Möglichkeit der Kooperation in der Weise, daß vor der Erteilung der Exportlizenz die Kontrollbehörde des Empfängerstaates eingeschaltet wird.

Einen weiteren Schwerpunkt der Konferenz bildete die Frage, wie bei international arbeitenden Informationssystemen der Datenschutz zu gewährleisten ist. So ist z. B. geplant, das Interpol-System dahingehend zu erweitern, daß auch personenbezogene Daten eingegeben werden. Bisher ist das System auf Sachinformationen (z. B. gestohlene Sachen) beschränkt. Da die Daten mit der Eingabe in das

System grundsätzlich jedem Staat, der an Interpol angeschlossen ist, verfügbar sind, ist der Datenschutz nur in der Weise zu gewährleisten, daß die eingebende Stelle in vollem Umfang Herr der Daten bleibt und allein über die Verwendung, z. B. über eine Änderung oder Löschung der Daten entscheidet. Zum Datenschutz im Bereich des internationalen Arbeitsmarktes und der Sozialversicherung bestand Einvernehmen darüber, daß die zunehmende Integration der europäischen Wirtschaft sich auch auf den Datentransfer auswirken werde. Dies werde nicht ohne Konsequenzen für den Datenschutz bleiben können. Der Datenschutz beim internationalen Bankeninformationssystem (SWIFT) ist durch die schwedische Dateninspektion eingehend geprüft worden, ehe den schwedischen Banken eine Exportlizenz erteilt wurde. Nach den Überprüfungen ist die Datensicherung in der Zentrale in Brüssel sehr gut ausgestaltet. Bisher wurden nur wenige personenbezogene Daten in das System eingegeben. Es ist aber damit zu rechnen, daß deren Anteil erheblich zunimmt. In der Diskussion bestand weitgehende Übereinstimmung, daß der Datenschutz mit dem Instrumentarium des internationalen Rechts allein nur unzulänglich zu gewährleisten ist. Hier wird der Zusammenarbeit der Datenschutzkontrollinstitutionen eine wichtige Rolle zuzumessen sein.

Die Notwendigkeit der internationalen Kooperation wurde von allen Beteiligten hervorgehoben. Eine wesentliche Voraussetzung dafür ist der Informationsaustausch. Alle wichtigen Entscheidungen und Verlautbarungen der Kontrollinstitutionen sollten den übrigen Teilnehmern der Konferenz zugänglich gemacht werden. Um allen Beteiligten das Verfahren zu erleichtern, habe ich mich dazu bereit erklärt, daß meine Dienststelle die Funktion eines Sekretariats übernimmt. Die Informationen und Unterlagen werden mir zugeleitet. Ich sorge sodann für die weitere Verteilung unter den übrigen Teilnehmern der Konferenz.

Der Gedanken- und Erfahrungsaustausch soll im Jahr 1980 — voraussichtlich in Kanada — fortgeführt werden.

Bonn, den 10. Januar 1980

Prof. Dr. Bull

Abkürzungsverzeichnis

AFG	Arbeitsförderungsgesetz
AO	Abgabenordnung
AZR	Ausländerzentralregister
BA	Bundesanstalt für Arbeit
BAföG	Bundesausbildungsförderungsgesetz
BayDSG	Bayerisches Datenschutzgesetz
BDSG	Bundesdatenschutzgesetz
BfV	Bundesamt für Verfassungsschutz
BGBl.	Bundesgesetzblatt
BGS	Bundesgrenzschutz
BKA	Bundeskriminalamt
BKA-Gesetz	Gesetz über das Bundeskriminalamt
BMI	Bundesminister des Innern
BND	Bundesnachrichtendienst
BStatG	Gesetz über die Statistik für Bundeszwecke
BT-Drucksache	Bundestags-Drucksache
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerwG	Bundesverwaltungsgericht
BVerwGE	Entscheidungen des Bundesverwaltungsgerichts
BWO	Bundeswahlordnung
BZR	Bundeszentralregister
BZRG	Bundeszentralregistergesetz
DEVO	Datenerfassungsordnung
DSRV	Datenstelle der deutschen Rentenversicherung
DÜVO	Datenübermittlungsverordnung
DV	Datenverarbeitung
DVDIS	Datenerfassung, Verarbeitung, Dokumentation und Informationsverbund in den sozialärztlichen Diensten mit Hilfe der EDV
ed-	erkennungsdienstlich
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaften
EGStGB	Einführungsgesetz zum Strafgesetzbuch
EheG	Ehegesetz
E-VZRG	Entwurf für ein Verkehrszentralregistergesetz
GG	Grundgesetz
GMBl.	Gemeinsames Ministerialblatt
GSD	Grenzschutzdirektion
GSK	Grenzschutzkommando
INPOL	Informationssystem der Polizei

KBA	Kraftfahrt-Bundesamt
KpS-Richtlinien	Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen
MAD	Militärischer Abschirmdienst
MiStra	Anordnung über Mitteilungen in Strafsachen
NADIS	Nachrichtendienstliches Informationssystem
PIOS	Auskunftssystem über Personen, Institutionen, Objekte, Sachen beim Bundeskriminalamt (Terrorismus und Rauschgift)
Saarl.DSG	Saarländisches Datenschutzgesetz
Schufa	Schutzgemeinschaft für allgemeine Kreditsicherung e. V.
SGB	Sozialgesetzbuch
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
StVZO	Straßenverkehrszulassungsordnung
T.B.	1. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz
VDR	Verband deutscher Rentenversicherungsträger
VZR	Verkehrszentralregister
VZRG	Verkehrszentralregistergesetz
WEWIS	Wehrinformationssystem
ZEVIS	Zentrales Verkehrsinformationssystem
ZPO	Zivilprozeßordnung

Sachregister