Deutscher Bundestag
10. Wahlperiode

Drucksache 10/877

13. 01. 84

Sachgebiet 204

Unterrichtung

durch den Bundesbeauftragten für den Datenschutz

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

Gliederung

Zugeleitet mit Schreiben des Bundesbeauftragten für den Datenschutz — I — 192 111/8 — vom 13. Januar 1984 gemäß § 19 Abs. 2 des Bundesdatenschutzgesetzes.

1. Einleitung und Gesamtüberblick

1.1 Arbeitsschwerpunkte

Beherrschendes Thema in der Arbeit des Bundesbeauftragten für den Datenschutz im Berichtsjahr 1983 war die geplante Volkszählung. Die mit dem Heranrücken des Zählungstermins sich stetig und rasch steigernde, häufig emotional geführte öffentliche Diskussion in den Medien und im politischen Raum verursachte eine Flut von Eingaben, in denen in erster Linie Aufklärung über Sinn und Zweck der beabsichtigten Maßnahme verlangt wurde. Die Dienststelle wurde dadurch in eine Rolle gedrängt, die an sich anderen Stellen zugekommen wäre und die nur durch Herausgabe eines auf die wichtigsten Fragen eingehenden Merkblatts zu bewältigen war. Nicht abzuschlagende Einladungen zu öffentlichen Veranstaltungen und Diskussionen belasteten die Arbeitskapazität der Dienststelle zusätzlich. Nachdem beim Bundesverfassungsgericht Verfassungsbeschwerden erhoben waren, wurde der Bundesbeauftragte am Verfahren beteiligt und hat sowohl im Verfahren der einstweiligen Anordnung wie auch im Hauptverfahren in umfangreichen Schriftsätzen seine Rechtsauffassung zum Volkszählungsgesetz 83 dargelegt. In den in beiden Verfahrensabschnitten anberaumten mündlichen Verhandlungen hat er Erklärungen abgegeben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich mit dem Thema befaßt und eine Entschließung mit einem umfassenden Forderungskatalog für die Durchführung der Volkszählung erarbeitet, die auch dem Gericht zugeleitet wurde.

Das am 15. Dezember 1983 verkündete und für mich keineswegs überraschende Urteil hat u. a. folgende Grundsatzaussagen zum Datenschutz erbracht, die ich diesem Bericht voranstelle, weil sie nach meiner Überzeugung weitreichende Auswirkungen auf die weitere Gestaltung des Datenschutzes und die anstehende Novellierung des BDSG haben werden:

— Das Grundgesetz garantiert dem Bürger ein informationelles Selbstbestimmungsrecht, das nur im überwiegenden Allgemeininteresse eingeschränkt werden darf.

— Der Staat muß dem Bürger klar sagen, für welche Zwecke er Daten von ihm verlangt, und er ist an diese Verwendungszwecke gebunden.

— Der Bürger muß bei der Datenerhebung über seine Rechte schriftlich belehrt werden.

— Für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung ist die Kontrolle der Datenverarbeitung durch unabhängige Datenschutzbeauftragte von erheblicher Bedeutung.

Eine eingehende Analyse der umfangreichen Urteilsbegründung war mir bis zur Drucklegung dieses Berichts noch nicht möglich. Ich werde eine solche einschließlich der daraus zu ziehenden Konsequenzen erstellen und sie dem Deutschen Bundestag vorlegen.

Eine tendenziell vergleichbare und mit kaum minderer Heftigkeit geführte öffentliche Diskussion hat die Verabschiedung des Vierten Gesetzes zur Änderung des Gesetzes über Personalausweise vom 25. Februar 1983 ausgelöst. Das Gesetz sieht die Einführung neuer fälschungssicherer und maschinenlesbarer Personalausweise ab November 1984 vor. Insbesondere die automatische Lesbarkeit der Ausweise hat bei vielen Bürgern Befürchtungen hervorgerufen, der Staat könne sich durch verstärkte Ausweiskontrollen und deren Registrierung in automatisierten Verfahren zusätzliche Überwachungsmöglichkeiten verschaffen und Bewegungsbilder über den einzelnen aufzeichnen. Da ich solche Absichten nicht erkennen kann, bin ich der sich ausbreitenden Beunruhigung durch eine Presseerklärung entgegengetreten und habe die zahlreichen von Rat suchenden Bürgern an mich gerichteten Eingaben auch in diesem Sinne beantwortet. Zugleich habe ich aber in vielen Gesprächen mit dem Bundesministerium des Innern auf die noch bestehenden Mängel, insbesondere auf die in diesem Zusammenhang bedeutsamen Defizite bei den vom Deutschen Bundestag schon vor Jahren geforderten flankierenden Maßnahmen vor allem im Recht der öffentlichen Sicherheit hingewiesen.

Hervorzuheben ist als weiteres markantes Ereignis in der Tätigkeit der Dienststelle im Jahr 1983 schließlich auch die Vorlage eines neuen Referentenentwurfs zur Novellierung des Bundesdatenschutzgesetzes, der wesentlichen Arbeitsgrundlage des Bundesbeauftragten für den Datenschutz. Aus der Sicht des Datenschutzes ist festzustellen, daß der Entwurf den Erwartungen nicht entspricht. Er gab mir Anlaß zu Beratungen mit den verschiedensten Stellen, insbesondere auch mit den Datenschutzbeauftragten der Länder und führte zu einer umfangreichen Stellungnahme gegenüber dem federführenden Bundesministerium des Innern. Gerade auch nach der Konkretisierung von Datenschutzprinzipien im Volkszählungsurteil des Bundesverfassungsgerichts gehe ich davon aus, daß meine zum Teil in die gleiche Richtung zielende Kritik am Entwurf und meine angebotenen Ergänzungsvorschläge nunmehr Beachtung finden werden.

Zu allen drei erwähnten Komplexen — Volkszählung, Personalausweis, BDSG-Novellierung — wird in diesem Bericht noch Näheres ausgeführt. Ich erwähne sie bereits hier, um die Arbeitsschwerpunkte der Dienststelle im Berichtszeitraum zu kennzeichnen.

Wenn in manchen Veröffentlichungen über diese Ereignisse an der Schwelle des Orwell-Jahres

„1984" Bezüge zu dem in diesem Roman geschilderten Überwachungsstaat hergestellt werden, so möchte ich in Erinnerung rufen, was mein Amtsvorgänger bei der Vorstellung des Fünften Tätigkeitsberichts im Januar 1983 gegenüber der Presse erklärt hat:

„1. Die Technologien für eine umfassende Überwachung der Bevölkerung sind zu einem erheblichen Teil entwickelt. Meine Bewertung muß sich auf die Informationsverarbeitung beschränken, die Gegenstand von Datenschutzrecht ist ...

2. Allerdings bedeuten technische Möglichkeiten noch keineswegs, daß die Überwachung auch wirtschaftlich, sozial und politisch „machbar" ist. Glücklicherweise bestehen insofern Hemmschwellen: So wären die Kosten eines perfekten Überwachungsapparates trotz gesunkener Datenverarbeitungskosten enorm, und der Nutzen wäre fragwürdig. Bei der Diskussion um „1984" sollten die wirtschaftlichen oder machtpolitischen Anreize für eine Perfektionierung der Datenverarbeitung in Verwaltung und Wirtschaft nicht überschätzt werden.

3. Vor allem aber sind die rechtlichen Hindernisse für einen Überwachungsstaat eindeutig. Sie ergeben sich aus der Verfassung, insbesondere den Grundrechten und dem Rechtsstaatsprinzip, zu dem auch das Verhältnismäßigkeitsgebot gehört, und aus einer Vielzahl von gesetzlichen Bestimmungen über den Datenschutz — auch außerhalb des Bundesdatenschutzgesetzes."

Auch aufgrund der Erfahrungen im abgelaufenen Jahr teile ich diese Beurteilung.

1.2 Kontrollen und Beratungen

Datenschutzkontrollen unterschiedlicher Intensität und Beratungsgespräche zur Verbesserung des Datenschutzes haben bei folgenden Behörden und öffentlichen Stellen des Bundes stattgefunden:

Bundesminister für Verkehr
Bundesminister für Raumordnung, Bauwesen und Städtebau
Bundesakademie für öffentliche Verwaltung
Fachhochschule des Bundes für öffentliche Verwaltung
Bundeskriminalamt
Bundesamt für Verfassungsschutz
Bundesnachrichtendienst
Militärischer Abschirmdienst
Grenzschutzdirektion
Bundeszentralregister
Kraftfahrt-Bundesamt
Hauptverwaltung der Deutschen Bundesbahn
Statistisches Bundesamt
Bundesamt für Ernährung und Forstwirtschaft
Gesamtdeutsches Institut
Bundesamt für den Zivildienst
Bundesanstalt für Arbeit und ein Arbeitsamt
drei große Betriebskrankenkassen
Bundespost-Ausführungsbehörde für Unfallversicherung
Institut für Wehrmedizinalstatistik
eine Wehrbereichsverwaltung und ein Rechenzentrum der Bundeswehr
ein Postsparkassenamt
ein Hauptzollamt
Filmförderungsanstalt Berlin
Deutsche Genossenschaftsbank
Deutsche Pfandbriefanstalt.

Ich beschränke mich in den einzelnen Abschnitten dieses Berichts auf die Darstellung derjenigen Prüfungsergebnisse, die mir besonders wichtig erscheinen, zu Beanstandungen geführt haben oder wegen ihrer politischen Bedeutung nach meiner Auffassung in besonderem Maße das Interesse des Deutschen Bundestages finden könnten. Wenn darüber hinaus vereinzelt auch weitere Feststellungen mitgeteilt werden, dann deshalb, weil sie möglicherweise auf allgemeine übergreifende Probleme und Lösungen hinweisen und damit auch für nicht kontrollierte Stellen Handlungsmaßstäbe setzen können. In manchen Bereichen, wie beispielsweise in der inneren Verwaltung oder im Rechtswesen, lag der Schwerpunkt der Tätigkeit mehr in der Beratung als in der Kontrolle. Oft ging es dabei um Regelungsmaterien, die in ihrer Wirksamkeit über die Bundesebene hinausgreifen und die vollziehende Verwaltung in den Ländern betreffen oder mitumfassen. Dies machte oft sorgfältige Abstimmungsprozesse nicht nur zwischen den Ressorts beim Bund und in den Ländern, sondern auch zwischen mir und den Landesbeauftragten für den Datenschutz notwendig.

1.3 Amtswechsel

Nach Ende der fünfjährigen Amtszeit und vorübergehender Fortführung der Amtsgeschäfte gemäß § 18 Abs. 1 Satz 6 BDSG wurde der erste Bundesbeauftragte für den Datenschutz, Prof. Dr. Hans Peter Bull, am 17. Mai 1983 aus seinem Amt verabschiedet. Nach meiner Ernennung zum Bundesbeauftragten durch den Herrn Bundespräsidenten am 16. Mai 1983 bin ich insbesondere von Journalisten vielfach nach meinen Vorstellungen zu dieser neuen Tätigkeit gefragt worden. Ich habe mein Amtsverständnis auch später noch einmal in einem Vortrag auf der Datenschutz-Fachtagung in Köln am 9. November 1983 (DAFTA) wie folgt zusammengefaßt:

„Vor einem halben Jahr — als der Wechsel im Amt des Bundesbeauftragten für den Datenschutz feststand oder auch bereits vollzogen war — wurde die Vermutung, Befürchtung oder auch der Verdacht geäußert, daß nun auch im Bereich des Datenschutzes die Wende eingeläutet worden sei. Die Sorge ging um, daß sich die politische, sachliche und inhaltliche Qualität des Daten-

schutzes in Zukunft — speziell unter dem neuen Datenschutzbeauftragten — verändern werde, selbstverständlich zum Nachteil des Datenschutzes.

Ich bin solchen Meinungen und Spekulationen stets entgegengetreten ... Die Aufgaben des Datenschutzbeauftragten sind im Gesetz festgelegt: Er hat den Bürger vor Mißbrauch seiner personenbezogenen Daten zu schützen und für die Einhaltung der Datenschutzvorschriften zu sorgen. Wer hier von einer Wende spricht, müßte gleichzeitig unterstellen, daß der Datenschutzbeauftragte seine Pflichten vernachlässigen wolle. Dies konnte und kann ernstlich wohl nicht angenommen werden. Aus meiner Sicht kommt es darauf an, die Interessen der Behörden, die in einer wirksamen Erfüllung ihrer gesetzlich vorgeschriebenen Aufgaben liegen, mit den schutzwürdigen Belangen und den Rechten der Bürger in Übereinstimmung zu bringen. Wo dies nicht möglich ist, werde ich — wie dies auch von meinem Amtsvorgänger gehandhabt wurde — die mir gesetzlich eingeräumten Möglichkeiten voll ausschöpfen."

Ich möchte diese Aussagen — nicht zuletzt mit Blick auf das außerordentlich erfolgreiche Wirken meines Amtsvorgängers — auch als ein Bekenntnis zur Kontinuität in der Führung dieses wichtigen Amtes verstanden wissen.

1.4. Öffentlichkeitsarbeit

Die Nachfrage nach Informationsmaterial zum Datenschutz hat auch im Berichtsjahr unvermindert angehalten. Die beiden dafür vorrätig gehaltenen Broschüren „Bürgerfibel Datenschutz" und „Der Bürger und seine Daten" mußten deshalb in unveränderter Neuauflage nachgedruckt werden. Mit den im Jahr 1983 verteilten mehr als 80 000 Exemplaren sind von beiden Schriften seit ihrem Erscheinen nunmehr insgesamt nahezu 370 000 Stück versandt worden.

Ein Informationsbedarf hat sich speziell auch auf dem Gebiet des Sozialdatenschutzes gezeigt. Vor drei Jahren sind mit dem Zehnten Buch des Sozialgesetzbuches wichtige und in dieser Form neuartige Vorschriften über die Geheimhaltung und den Schutz der Sozialdaten in Kraft getreten. Obwohl 90 Prozent der Bevölkerung in dem System der sozialen Sicherung erfaßt sind, sind den Bürgern diese Vorschriften, die zu ihrem Schutz erlassen worden sind, weitgehend unbekannt oder unverständlich geblieben. Um hier Abhilfe zu schaffen und den Betroffenen das zu diesem Thema Wissenswerte in einer — wie ich hoffe — leicht verständlichen Form zu vermitteln, habe ich eine allgemeine Informationsschrift zum Sozialdatenschutz herausgegeben. In der 86 Seiten starken Broschüre „Der Bürger und seine Daten im Netz der sozialen Sicherung" wird versucht, Inhalt und Wirkungen des Sozialdatenschutzes aus der Sicht des Bürgers darzustellen und ihn auf seine Rechte hinzuweisen. Auch diese Broschüre wird von mir kostenlos auf Anforderung zugeschickt.

Zu Einzelfragen des Datenschutzes, die in der Öffentlichkeit ein starkes Echo gefunden haben, habe ich im Berichtsjahr mehrfach Presseerklärungen herausgegeben, so beispielsweise zur geplanten Volkszählung, zu der dazu ergangenen Entscheidung des Bundesverfassungsgerichts und zum neuen maschinell lesbaren Personalausweis.

Aber auch im engeren Rahmen wurde von meiner Dienststelle wirksame Öffentlichkeitsarbeit geleistet. So gaben zahlreiche Veranstaltungen, in denen vor allem die geplante Volkszählung behandelt wurde, Gelegenheit für mich und meine Mitarbeiter, die damit verbundenen Datenschutzaspekte darzustellen. Besuchergruppen von Abgeordneten des Deutschen Bundestages informierten sich in meiner Dienststelle über Grundfragen des Datenschutzes und über die Praxis der Datenschutzkontrolle. Ich nutze diese Gelegenheiten zur Diskussion mit interessierten Bürgern gern, um das auch für meine Arbeit unerläßliche Datenschutzbewußtsein in der Bevölkerung weiterzuentwickeln und zugleich an der Reaktion der Besucher abzuschützen, wo noch Informationsbedarf besteht. Mancher in diesen Zusammenkünften vorgebrachte Sachverhalt hat schon zu weiteren Anstößen bei den zuständigen Stellen zur Verbesserung des Datenschutzes geführt. Den gleichen Effekt erzielen geschlossene Fortbildungsveranstaltungen über den Datenschutz, an denen meine Mitarbeiter aktiv mitgewirkt haben.

1.5 Dateienregister

Das allgemeine Dateienregister nach § 19 Abs. 4 Satz 1 BDSG umfaßt zur Zeit rd. 1 200 Dateimeldungen. Die Zahl der *tatsächlich* in der Bundesverwaltung geführten automatisierten Dateien ist damit jedoch nicht zuverlässig bestimmt und liegt höher. Eine größere Zahl der Meldungen betrifft nämlich Dateien, die zwar nur einmal gemeldet, aber in identischer Form bei vielen Stellen mit gleicher oder gleichartiger Aufgabenstellung (z. B. bei Postämtern) geführt werden.

Das nach § 19 Abs. 4 Satz 5 BDSG zu führende besondere Register für die Dateien der Sicherheitsbehörden und der Bundesfinanzverwaltung umfaßt derzeit 122 Meldungen.

Zur Effizienz der Regelung über die Führung des Dateienregisters verweise ich auf meine Ausführungen im Fünften Tätigkeitsbericht, S. 9 f. Meine dort dargelegte Auffassung hat sich auch nach den Erfahrungen im Berichtszeitraum nicht geändert.

1.6 Kooperation

Die mir in § 19 Abs. 5 BDSG aufgegebene Pflicht zur Zusammenarbeit mit den für die Datenschutzkontrolle in den Ländern zuständigen Stellen wurde auch im Berichtsjahr wirkungsvoll wahrgenommen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit verschiedenen Arbeitskreisen, in denen die Beratungsergebnisse vor-

bereitet werden, erweist sich weiterhin als unentbehrliches Instrument zur Abstimmung des Vorgehens in gemeinsam berührenden Fragen. Durch das geschlossene Eintreten für gemeinsame Anliegen wird den in den Beschlüssen der Konferenz niedergelegten Forderungen zum Datenschutz in bestimmten Angelegenheiten mehr Nachdruck verliehen als einzelnen Initiativen. So hat sich beispielsweise der am 22. 3. 1983 gefaßte Beschluß der Datenschutzbeauftragten zur Volkszählung 83 in der Entscheidung des Bundesverfassungsgerichts nachhaltig ausgewirkt. Die wichtigsten Beratungspunkte der Konferenz und die dazu gefundenen Ergebnisse werden in diesem Bericht jeweils bei der Behandlung der entsprechenden Sachthemen dargestellt.
Auch an den regelmäßig stattfindenden Sitzungen des „Düsseldorfer Kreises", in dem die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich (§§ 30, 40 BDSG) übergreifende Probleme diskutieren und einheitliche Lösungen anstreben, nehmen Mitarbeiter meiner Dienststelle teil.

2. Innere Verwaltung

2.1 Neue Personalausweise und Pässe

Das am 15. März 1983 in neuer Fassung bekanntgemachte Gesetz über Personalausweise, durch das zum 1. November 1984 neue fälschungssichere und maschinenlesbare Personalausweise eingeführt werden, war im Berichtsjahr — neben dem Volkszählungsgesetz — eines der beherrschenden Themen in der öffentlichen Diskussion. Hier wie dort geht es um Fragen des Datenschutzes, aber eben nicht nur um solche: Die Frage, ob ein fälschungssicherer und maschinenlesbarer Ausweis überhaupt notwendig ist, ist eine politische Frage, die nicht von den Datenschutzbeauftragten zu beantworten ist. Die datenschutzrechtlichen Fragen setzen beim Personalausweisgesetz selbst an und hinterfragen, ob die schutzwürdigen Belange der Bürger hinreichend berücksichtigt sind. Datenschutzrechtliche Fragen stellen sich aber nicht nur in bezug auf das Gesetz selbst, sondern auch für Bereiche, in denen die Nutzung des Ausweises eine Rolle spielt. Zum gleichen Themenkreis gehören auch die in Vorbereitung befindlichen Ausführungsgesetze der Länder.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich am 13. September 1983 mit dieser Problematik befaßt und die datenschutzrechtlichen Anforderungen an den fälschungssicheren und maschinenlesbaren Personalausweis bzw. Paß aktualisiert. Die Datenschutzbeauftragten weisen in diesem Beschluß darauf hin, daß sie bereits im November 1979 datenschutzrechtliche Anforderungen an die Einführung des fälschungssicheren und maschinenlesbaren Personalausweises gestellt haben. In das Bundespersonalausweisgesetz sind daraufhin entsprechende datenschutzrechtliche Regelungen aufgenommen worden.

Ich nenne insbesondere:

— Es wurde abschließend festgelegt, welche Daten in den Ausweis aufgenommen werden dürfen.

— Die Aufnahme eines Fingerabdrucks oder anderer verschlüsselter Angaben über die Person des Ausweisinhabers ist untersagt.

— 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 darf personenbezogene Angaben nur vorübergehend und ausschließlich zur Herstellung des Personalausweises speichern; danach muß sie lediglich feststellen können, an welche Behörde sie bestimmte Seriennummern vergeben hat.

— Die Seriennummern dürfen nicht zur Einrichtung oder Erschließung von Dateien verwendet werden. Eine Ausnahme gilt lediglich für die örtlichen Personalausweisbehörden zur Erschließung ihrer Dateien und für ungültig erklärte oder abhanden gekommene bzw. für solche Ausweise, bei denen der Verdacht mißbräuchlicher Benutzung besteht.

— Die Nutzung der Maschinenlesbarkeit des Ausweises ist ausdrücklich auf Dateien beschränkt, die für Zwecke der Grenzkontrolle und der Fahndung aus Gründen der Strafverfolgung und der Gefahrenabwehr durch die hierfür zuständigen Behörden betrieben werden. Allen anderen Behörden ist die Verwendung des Ausweises zur automatischen Einrichtung oder Erschließung von Dateien ausdrücklich untersagt.

— Im nicht-öffentlichen Bereich darf die Seriennummer nicht zur Einrichtung oder Erschließung von Dateien verwendet werden. Das Gesetz verbietet die Verwendung zur automatischen Erschließung von Dateien, läßt die Nutzung zur automatischen Einrichtung von Dateien aber offen.

Schon 1979 betonten die Datenschutzbeauftragten, daß ein maschinenlesbarer Personalausweis nur in Verbindung mit einem datenschutzgerechten Melderecht und bereichsspezifischen Datenschutzregelungen für den Sicherheitsbereich hinnehmbar sei. Anknüpfend an diese Forderungen nahm der Deutsche Bundestag bei der Verabschiedung des Personalausweisgesetzes am 17. Januar 1980 den nachstehenden Entschließungsantrag an (vgl. BT-Drucksache 8/3498):

„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."

Die Anwendung moderner Informationstechnologien hat inzwischen zunehmend zur Kombination und Integration neuer und vorhandener Informationssysteme geführt. Die Entwicklung der Informationstechnologie ist gekennzeichnet durch die Verknüpfung von Daten, Text, Sprache, Schriftzügen und Bildern, die eine umfangreiche Darstellung und Überprüfung von Personen möglich machen können. Die Einführung des maschinenlesbaren Personalausweises bzw. Passes muß im Zusammenhang mit dieser Entwicklung gesehen werden. Die Aussage, daß ein maschinenlesbarer Personalausweis unter Datenschutzgesichtspunkten hinnehmbar ist, kann nur dann aufrechterhalten werden, wenn die bereits 1979 erhobenen Forderungen in ausreichendem Maße erfüllt werden und auch im übrigen bei der Ausführung des Personalausweisgesetzes den Datenschutzbelangen Rechnung getragen wird. Das bedeutet, daß weitere Regelungen getroffen werden müssen, um inzwischen zu Tage getretene Unklarheiten und Mißverständnisse auszuräumen und eine datenschutzgerechte Anwendung des Gesetzes sicherzustellen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern im einzelnen:

A. Zum Personalausweisgesetz

— Soweit bei polizeilichen Personenkontrollen Anfragen in polizeilichen Informationssystemen vorgenommen werden, dürfen diese Anfragen nicht personenbezogen protokolliert werden, damit insbesondere keine Bewegungsbilder entstehen können. Da solche Protokollierungen, die als „Einrichtung von Dateien" anzusehen sind, nicht Zwecken der Grenzkontrolle und der Fahndung im Sinne des § 3 Abs. 5 Satz 2 Personalausweisgesetz dienen, sind sie nach § 3 Abs. 5 Satz 1 Personalausweisgesetz unzulässig. Im übrigen läßt sich aus der Entstehungsgeschichte dieser Vorschrift ableiten, daß der Gesetzgeber eine Verwendung des Ausweises zur automatischen Einrichtung von Dateien grundsätzlich nicht gestatten wollte.

— Die Datenschutzbeauftragten gehen davon aus, daß die Nutzung des Personalausweises durch die Polizei nach § 3 Abs. 5 Satz 2 Personalausweisgesetz nicht auch die Verwendung der Seriennummer einschließt; hierfür ist § 3 Abs. 4 Personalausweisgesetz die Spezialvorschrift.

— Die unterschiedliche Formulierung in § 3 Abs. 5 Satz 1 und § 4 Satz 2 Personalausweisgesetz gibt zu Mißverständnissen Anlaß. Die Regelung in § 4 muß deshalb der in § 3 angeglichen werden.

— Die internationale Lesbarkeit des Personalausweises erfordert für deutsche Staatsangehörige die gleiche Schutzintensität auch im grenzüberschreitenden Reiseverkehr. Die Konferenz bittet daher die Bundesregierung, sich dafür einzusetzen, daß die datenschutzrechtlichen Anforderungen an die innerstaatliche Verwendung des Ausweises auch im internationalen Bereich umgesetzt werden.

B. Zu den Ausführungsvorschriften der Länder

— Im Ausführungsgesetz oder in den Verwaltungsvorschriften muß festgelegt werden, daß ein Personenfeststellungsverfahren nur durchzuführen ist, wenn Zweifel an der Identität des Ausweisbewerbers nicht ausgeräumt werden können, und daß in diesem Verfahren erkennungsdienstliche Maßnahmen nur als letztes Mittel zulässig sind. Eine Weiterleitung dieser Unterlagen an das Bundeskriminalamt darf nur für den Vergleich mit anderen Unterlagen zugelassen werden.

— Im Ausführungsgesetz muß bestimmt werden, daß die erkennungsdienstlichen Unterlagen zu vernichten sind, sobald die Identität festgestellt ist.

— In das Personalausweisregister dürfen nur die im Personalausweis enthaltenen personenbezogenen Daten (§ 1 Abs. 2 Personalausweisgesetz) sowie Vermerke über Anordnungen nach § 2 Abs. 2 Personalausweisgesetz aufgenommen werden. Von der Aufnahme der Angabe „unveränderliche Kennzeichen" muß abgesehen werden.

— Der Zweck des Personalausweisregisters ist im Landesgesetz selbst festzulegen. Hierbei ist zu berücksichtigten, daß es nicht Aufgabe dieses Registers sein kann, eine weitere umfassende Identifizierungsdatei neben dem Melderegister zu eröffnen, zumal dadurch weitere Daten (Lichtbild und Unterschrift) mit den Meldedaten verknüpft werden können. Datenübermittlungen an andere öffentliche Stellen und an Private sind auszuschließen. Eine Ausnahme darf nur für Übermittlungen an die Polizei zugelassen werden, wenn es im Einzelfall für deren Aufgabenerfüllung erforderlich ist.

— Spätestens fünf Jahre nach Ablauf der Gültigkeit des Personalausweises sind die Daten im Personalausweisregister ohne Einschränkung zu löschen.

Für die Ausstellung eines vorläufigen Personalausweises reicht eine kürzere Aufbewahrungs-

dauer aus. Entsprechend § 10 Abs. 4 des Entwurfs des Niedersächsischen Ausweisgesetzes sollten die Daten höchstens bis zu einem Jahr nach Ablauf des Jahres der Gültigkeitsdauer aufbewahrt werden.

— Für Daten der Personen, die im Fall der Entmündigung, wegen Geisteskrankheit oder im Fall dauernder Anstaltsunterbringung von der Ausweispflicht befreit worden sind, ist wegen der damit gegebenen Sonderstellung eine strenge Verwendungsbeschränkung vorzusehen.

— In den Verwaltungsvorschriften zum Ausführungsgesetz der Länder müssen das Verfahren bei Mitteilungen über den Verlust des Personalausweises geregelt und das Formular festgelegt werden.

C. Zu bereichsspezifischen Datenschutzregelungen

— Soweit die Regelungen in den Meldegesetzen der Länder dem Melderechtsrahmengesetz entsprechen, sind die datenschutzrechtlichen Anforderungen erfüllt. Die Speicherung der Seriennummer, die in einigen Landesmeldegesetzen in den Datenkatalog aufgenommen wurde, widerspricht dem in § 3 Abs. 4 Satz 1 Personalausweisgesetz festgelegten Nutzungsverbot, erhöht die mit der Maschinenlesbarkeit des Personalausweises verbundenen Gefahren und ist überdies im Hinblick auf die Fälschungssicherheit des Ausweises überflüssig.

— Durch die Maschinenlesbarkeit des Ausweises werden die nachfolgend aufgeführten datenschutzrechtlichen Probleme verschärft, deren Lösung die Datenschutzbeauftragten von Bund und Ländern bereits früher gefordert haben, die aber durch die bisher erlassenen polizeilichen Richtlinien (insbesondere KpS- und Dateienrichtlinien sowie die Regelung über die Amtshilfe zwischen Bundesgrenzschutz und Nachrichtendiensten) noch nicht erreicht ist:

  — Im Polizeirecht des Bundes und der Länder und im Strafverfahrensrecht sind gesetzliche Grundlagen für die Informationsverarbeitung der Polizei, insbesondere für die polizeiliche Beobachtung und die Identitätsfeststellung zu schaffen. Ziel dieser Regelung muß es auch sein, den Umfang der Personenkontrollen im Hinblick auf die Nutzung des maschinenlesbaren Ausweises zu begrenzen.

  — Zulässigkeit und Grenzen des Informationsaustausches zwischen Polizei und den Nachrichtendiensten sind gesetzlich zu regeln.

  — Der Beschluß der Innenministerkonferenz vom 2. September 1977, der vorsieht, daß alle Personen, die der Polizei bei der Erfüllung ihrer Aufgaben bekannt werden, durch Abfrage in der Personenfahndungsdatei überprüft werden, muß aufgehoben werden. Die vorhandenen Rechtsgrundlagen lassen eine derart umfassende Überprüfung nicht zu. Das gleiche gilt für einen routinemäßigen Abgleich mit den Fahndungsdateien im Rahmen von Verkehrskontrollen.

  — Eine Rechtsgrundlage für den Anschluß der Länderpolizeien an die zollrechtliche Überwachung ist nicht ersichtlich. Dieser Anschluß ist zu lösen.

— Für die Praxis der Polizeikontrollen, insbesondere unter Verwendung des maschinenlesbaren Personalausweises, sind Richtlinien zu erlassen, die den Grundsatz der Verhältnismäßigkeit konkretisieren.

Zur Erläuterung und Realisierung dieser Forderungen stehe ich mit dem für das Personalausweisgesetz federführenden Bundesminister des Innern in Kontakt; in den Bemühungen um die Ausführungsgesetze der Länder gilt gleiches für die Landesbeauftragten für den Datenschutz und die Innenminister bzw. -senatoren der Länder. Soweit sich die Forderungen der Datenschutzbeauftragten auf das Personalausweisgesetz beziehen, habe ich den Bundesminister des Innern auf die Möglichkeit hingewiesen, diesen in § 24 des Entwurf eines Paßgesetzes Rechnung zu tragen, der bereits einige Änderungen des Pesonalausweisgesetzes vorsieht. Ich habe in diesem Zusammenhang auch darauf hingewiesen, daß ein Widerspruch besteht zwischen dem oben bereits angesprochenen § 4 des Personalausweisgesetzes, der — wie erwähnt — für den nichtöffentlichen Bereich die Nutzung der Maschinenlesbarkeit für die Einrichtung von Dateien nicht ausschließt, und dem durch Verordnung zur Bestimmung des Personalausweismusters festgelegten Hinweis auf der Ausweisrückseite, der das Gegenteil annehmen läßt.

In einer ersten Reaktion auf den Beschluß der Konferenz der Datenschutzbeauftragten hat mich der Bundesminister des Innern über Überlegungen informiert, einigen Vorschlägen durch Regelungen in Verwaltungsvorschriften zu entsprechen. Er stimmt mit mir darin überein, daß § 3 Abs. 5 Satz 1 des Personalausweisgesetzes eine Protokollierung von Anfragen in polizeilichen Informationssystemen aus Gründen des Datenschutzes nicht zuläßt. Zu den besonders wichtigen Forderungen nach bereichsspezifischen gesetzlichen Regelungen im Sicherheitsbereich (vgl. oben C) fehlt leider bisher eine klare Reaktion (s. hierzu auch unter Nr. 17.4.3).

D. Zum Entwurf eines Paßgesetzes

Das Bundeskabinett hat am 13. Juli 1983 den Entwurf eines Paßgesetzes verabschiedet, der sich im wesentlichen an die Regelungen des Personalausweisgesetzes des Bundes anlehnt, zugleich aber auch Bestimmungen enthält, die bezüglich des Personalausweises Gegenstand von Ausführungsgesetzen der Länder sind. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrem im September 1983 gefaßten Beschluß deutlich gemacht, daß die in bezug auf den Personalausweis erhobenen datenschutzrechtlichen Forderungen auch für die mit dem Entwurf eines Paßgesetzes vorgesehene Einführung eines maschinenlesbaren Passes gelten, soweit die Regelungen inhaltlich identisch sind.

2.2 Neukonzeption des Ausländerzentralregisters

Das Ergebnis meiner früheren Prüfung des beim Bundesverwaltungsamt geführten Ausländerzentralregisters (AZR) und die hierauf gestützten Fragestellungen zur Rechtsgrundlage und Konzeption des Registers, die ich schon in meinen früheren Berichten erwähnt habe (3. TB S. 16, 5. TB S. 15f.), haben den Bundesminister des Innern zu der Feststellung veranlaßt, daß „das Register in inhaltlicher, verfahrensmäßiger und rechtlicher Hinsicht den heutigen und besonders den künftig absehbaren Bedürfnissen nur noch unvollkommen zu entsprechen vermag". Ich begrüße seine Zusage, mich an der Neugestaltung des AZR im Rahmen einer Arbeitsgruppe zu beteiligen; sein Hinweis, daß sich „seit Bestehen des AZR die Einstellung zum Schutz personenbezogener Daten grundlegend gewandelt" habe, ist für mich ein positives Signal. Die mir übersandte Auflistung „wünschbarer Inhalte" für neue Datensätze ist ein sinnvoller Ansatz für die notwendigen grundlegenden Überlegungen zur Neukonzeption des AZR.

Der dem AZR alter Konzeption teilweise anhaftende Mangel an Aktualität wird sich für die Zukunft nur durch Beschränkung auf das unabweislich Erforderliche vermeiden lassen.

2.3 Asylverfahren

Rechtsanwälte, die in Asylverfahren tätig sind, haben in Eingaben an mich ihr Befremden darüber ausgedrückt, daß Verwaltungsgerichte Auskünfte des Auswärtigen Amtes erhalten haben, die mit Angabe des vollen Namens das Verfolgungsschicksal von Betroffenen wiedergeben, die mit dem jeweiligen Prozeßbeteiligten nichts zu tun haben. Die Frage der Entstehung und des Übermittlungsweges von Auskünften des Auswärtigen Amtes in Asylverfahren erschien mir so wichtig, daß ich sie im Rahmen meiner beratenden Aufgabe aufgegriffen und mit dem Auswärtigen Amt und den Bundesministern des Innern und der Justiz erörtert habe. Ich vertrete die Auffassung, daß zur Vermeidung einer Beeinträchtigung schutzwürdiger Belange von Asylsuchenden dem Rechtsgedanken des § 10 BDSG auch dann Rechnung getragen werden sollte, wenn es sich nicht um in Dateien gespeicherte Daten handelt.

Mit den genannten Ressorts besteht Einvernehmen, daß zu unterscheiden ist zwischen solchen Fällen, in denen zur Sachverhaltsaufklärung *in einem konkreten Einzelverfahren* einem Verwaltungsgericht oder dem Bundesamt für die Anerkennung ausländischer Flüchtlinge auf entsprechende Ersuchen Auskünfte erteilt werden, und solchen, in denen zur Erleichterung der Entscheidung *bei gleich oder ähnlich gelagerten Sachverhalten* Informationen von genereller Bedeutung übermittelt und gesammelt werden.

— In einer Vielzahl von Fällen ist die Namensnennung des Asylsuchenden unerläßlich, um den behaupteten Verfolgungstatbestand durch die Auslandsvertretungen des Auswärtigen Amtes überprüfen zu können; auch die Einzelauskunft, die den besonderen Umständen des Einzelfalles Rechnung trägt, wird daher notwendigerweise in der Regel personenbezogene Daten enthalten müssen.

— Davon sind aber solche Fälle zu unterscheiden, in denen es nicht um die Beantwortung eines Ersuchens zu einem einzelnen Asylverfahren, sondern um die Übermittlung von Auskünften von genereller Bedeutung zwecks Verfahrensbeschleunigung und Vermeidung von Mehrfachanfragen in Fällen gleicher oder ähnlicher Sachverhalte geht. Es liegt im Wesen einer — wie sie auch der Bundesminister des Innern nennt — „Information von genereller Bedeutung", daß sie über den individuellen Fall hinaus relevant ist und ihre Verwertbarkeit einen Bezug auf personenbezogene Daten nicht voraussetzt. Die Übermittlung *personenbezogener* Daten im Rahmen der Weiterleitung von solchen Informationen ist nicht erforderlich. Ich habe daher die Mitteilung des Bundesministers des Innern begrüßt, daß in solchen Fällen künftig personenbezogene Daten vor der Weiterleitung geschwärzt werden.

Offengeblieben ist in dem Dialog mit den genannten Ressorts aber die Frage, warum bei Weiterleitungen von Auskünften des Auswärtigen Amtes von genereller Bedeutung an die für die Verwaltungsgerichtsbarkeit zuständigen obersten Landesbehörden bzw. an die Verwaltungsgerichte selbst eine Schwärzung erst durch den Bundesminister der Justiz und nicht schon durch das Auswärtige Amt erfolgt. Die mir gegebene Begründung, der Bundesminister der Justiz habe „aufgrund seiner ministeriellen Zuständigkeit ein Recht darauf, voll informiert zu werden", leuchtet mir nicht ein, da es sich bei dieser Zuständigkeit nur um die formale Kompetenz zur Weiterleitung handelt, die die Frage der Erforderlichkeit nicht berührt.

2.4 Zivildienst

Zivildienstleistende haben mich um datenschutzrechtliche Prüfung der Behandlung von Vorgängen gebeten, die entstehen, wenn gegen einen Zivildienstleistenden wegen eigenmächtiger Abwesenheit, schuldhaftem Fernbleiben vom Dienst oder Dienstverweigerung ein Disziplinarverfahren eingeleitet und eine Disziplinarmaßnahme nach den Vorschriften des sechsten Abschnitts des Zivildienstgesetzes ausgesprochen wird. Wie ich in Erfahrung gebracht habe, werden die hierbei entstehenden Disziplinarvorgänge in einer Beiakte zur Personalakte geführt, die nicht Bestandteil der Personalakte ist und davon getrennt aufbewahrt wird. Diese Beiakte wird nach den Tilgungsvorschriften des § 69a des Zivildienstgesetzes vernichtet, d. h. grundsätzlich nach Ablauf eines Jahres nach Verhängung der Disziplinarmaßnahme.

Über die bei einem solchen Verhalten des Zivildienstleistenden entstehenden Nachdienstzeiten wird ein Nachdienensbescheid erstellt, der entspre-

chend § 36 Zivildienstgesetz Bestandteil der Personalakte wird. Der Nachdienensbescheid enthält zwar die Begründung, warum die Zeiten nachzudienen sind, jedoch keinerlei Hinweis auf das durchgeführte Disziplinarverfahren. Die Personalakte des Zivildienstleistenden wird nur mit dessen Einverständnis an öffentliche oder sonstige Arbeitgeber zur Einsichtnahme übersandt oder weitergegeben.

Den Belangen der Zivildienstleistenden wird durch diese Handhabung der bestehenden Vorschriften in m. E. befriedigender Weise Rechnung getragen.

2.5 Auskünfte an den Internationalen Suchdienst

Die Zulässigkeit der Übermittlung von Auskünften an den Internationalen Suchdienst (ISD) war und ist auch weiter Gegenstand von Kontakten zum Bundesminister des Innern, zum Auswärtigen Amt, zum Internationalen Suchdienst und — da es sich zu einem wesentlichen Teil um Übermittlungen aus Dateien im Bereich der Länder handelt — zu meinen Kollegen in den Ländern. Schwerpunkt der Tätigkeit des ISD ist die Auffindung und Bereitstellung von Daten über das Schicksal ehemaliger KZ-Insassen und Verschleppter, die auch heute noch namentlich zur Geltendmachung von Renten- und Entschädigungsansprüchen für die Betroffenen bzw. deren Hinterbliebene von Bedeutung sind. Wie mir der ISD in einem kürzlich geführten Gespräch verdeutlicht hat, beläuft sich die Zahl der ihm vorliegenden nicht erledigten Suchaufträge auf rd. 500 000; jährlich kommen ca. 40 000 hinzu. Der ISD ist daran interessiert, nicht nur mit gezielten Ersuchen entsprechende Einzelauskünfte zu erhalten, sondern auch in Betracht kommende Karteien „global" auszuwerten, um Anhaltspunkte zu finden, die bei der Bearbeitung der konkreten Suchaufträge weiterhelfen (allgemein als „Schleppnetz-Auskünfte" bezeichnet).

Alle an der Diskussion Beteiligten gehen davon aus, daß es sich beim ISD, einer Stelle des Internationalen Roten Kreuzes, um eine zwischenstaatliche Einrichtung und nicht um eine öffentliche Behörde handelt und der ISD, der seinen Sitz in Arolsen hat, keinen bundesrechtlichen oder landesrechtlichen Datenschutzvorschriften unterliegt. Die beteiligten Regierungen haben den ISD — wie es in den zugrunde liegenden Vereinbarungen heißt — „im Rahmen ihrer Rechtsvorschriften" zu unterstützen; hierzu zählen die Vorschriften des Datenschutzes.

Die Problematik liegt nicht in den Einzelauskünften, denen ein Ersuchen der Betroffenen zugrunde liegt, sondern darin, daß Globalauskünfte zwangsläufig auch Daten von Personen umfassen, für die der ISD keinen konkreten Auftrag hat. Es handelt sich also um eine Vorratsspeicherung zumindest bis zu dem Zeitpunkt, zu dem die übermittelten Daten daraufhin ausgewertet werden, ob sich Anhaltspunkte finden, die für die Bearbeitung von dem ISD vorliegenden Suchaufträgen hilfreich sind. Die datenschutzrechtliche Beurteilung hat sich an den konkreten Gegebenheiten zu orientieren, d. h. es muß geprüft werden, um welche Art von Dateien es sich jeweils handelt, deren Auswertung der ISD anstrebt, und inwieweit schutzwürdige Belange Betroffener berührt sein könnten. Die von mir mit der Angelegenheit befaßte Konferenz der Datenschutzbeauftragten hat dem Internationalen Suchdienst empfohlen, sich bei auftretenden Schwierigkeiten bei Übermittlungsersuchen an den jeweils zuständigen Datenschutzbeauftragten zu wenden.

Die Datenschutzbeauftragten haben damit zu erkennen gegeben, daß sie bereit sind, von Fall zu Fall in bestmöglicher Weise und ihrem gesetzlichen Auftrag gemäß zu einem Ausgleich zwischen dem humanitären Anliegen des ISD und den Datenschutzbelangen Dritter beizutragen. Das Interesse der Verfolgten bzw. ihrer Hinterbliebenen an der Aufklärung ihrer Schicksale und der Geltendmachung ihrer Ansprüche hat einen hohen rechtlichen und humanitären Stellenwert. Soweit nicht besondere Geheimnisbereiche berührt sind, können daher schutzwürdige Belange Außenstehender der Datenübermittlung im Rahmen von Globalauskünften an den ISD grundsätzlich nur dann entgegenstehen, wenn sie einen entsprechend hohen Stellenwert haben.

Für solche Abwägungen, wie sie in Anwendung des § 11 Satz 3 i. V. m. Satz 1 (2. Alternative) des Bundesdatenschutzgesetzes bzw. entsprechender landesrechtlicher Bestimmungen Platz greifen müssen, ist aber kein Raum, wenn es sich um Sozialdaten handelt. Zwischen dem Bundesarbeitsministerium, dem Bundesinnenministerium, dem Auswärtigen Amt und mir besteht Übereinstimmung darin, daß die geltenden Regelungen über den Sozialdatenschutz in §§ 67 ff. SGB X Globalauskünfte dieser Art an den ISD nicht zulassen.

Vor diesem Hintergrund waren die folgenden Anliegen des ISD im Oktober 1983 Gegenstand eines mit mir geführten Gesprächs:

— Der ISD sieht Anlaß für die Befürchtung, daß seine Bemühungen (nicht nur um Global-, sondern auch um Einzelauskünfte) zunehmend durch Vernichtung in Betracht kommender Unterlagen unmöglich werden. Er ist um eine offizielle Entscheidung bemüht, die die Vernichtung bis zur Prüfung aufschiebt, ob sie für den ISD relevant sind. Dagegen bestehen aus meiner Sicht keine Bedenken.

— Angesichts der Tatsache, daß Globalauskünften, soweit es sich um Sozialdaten handelt, die strengen Vorschriften des Sozialgesetzbuchs entgegenstehen, ist dem ISD daran gelegen, andere in Betracht kommende Unterlagen — so Melderegister, Strafvollzugsregister, Beschäftigungsregister etc. — voll auszuschöpfen. Der ISD denkt hierbei an eine Aufforderung von öffentlicher Seite an die zuständigen Behörden und Unternehmen, Materialien durch eigenes Personal zu sichten, und Unterlagen, die für den ISD von Interesse sein könnten, auszusondern und bereitzustellen. So würde die Arbeit des ISD z. B.

durch eine Auswahl von Unterlagen, die sich auf Ausländer beziehen, erleichtert.
Ich habe darauf hingewiesen, daß eine solche Vorauswahl von Materialien zwar an der datenschutzrechtlichen Problematik im Prinzip nichts ändere. Da eine Vorauswahl aber das Übermittlungsvolumen und den Anteil solcher Fälle, zu denen dem ISD keine konkreten Suchaufträge vorliegen, verringere, sei sie datenschutzrechtlich zu begrüßen. Eine andere Frage sei freilich, ob die in Betracht kommenden Stellen und Unternehmen haushalts- und personalwirtschaftlich bereit und in der Lage seien, den Wünschen des ISD zu entsprechen.

Zu beiden Anliegen habe ich deutlich gemacht, daß ich — beschränkt auf Behörden und Stellen des Bundes — lediglich beratende und kontrollierende, aber keinerlei regelnde Zuständigkeiten habe. Ich rechne damit, daß der ISD mit seinen Anliegen auch an den Bundesminister des Innern herantreten wird, und habe daher den Bundesminister des Innern über den Inhalt des mit dem ISD geführten Gesprächs unterrichtet.

3. Rechtswesen

3.1 Bundeszentralregister

Das Bundeszentralregister (BZR) stellt nicht nur nach dem Volumen der Dateien und nach der Zahl der täglichen Datenübermittlungen (täglich ca. 30 000 Auskünfte), sondern auch im Hinblick auf die Sensibilität der gespeicherten Daten eines der bedeutendsten Datenverarbeitungssysteme im Bundesbereich dar. Zwei Besuche, die meine Mitarbeiter zur datenschutzrechtlichen Kontrolle einer Reihe von Arbeitsabläufen beim BZR im Jahre 1983 durchführten, haben ein insgesamt erfreuliches Niveau des Datenschutzes erkennen lassen. Diese Besuche haben aber auch einige problematische Punkte aufgezeigt. In Zukunft wird es daher notwendig sein, enge Kontakte zu halten und auf der Suche nach praktischen Verbesserungen den Dialog weiterzuführen.

Eine Reihe meiner Vorschläge und Hinweise hat beim Generalbundesanwalt, zu dessen Zuständigkeit das BZR zählt, eine positive Aufnahme gefunden:

— Hinsichtlich der nach § 15 BDSG zu führenden Übersicht habe ich auf den Zweck der Transparenz hingewiesen sowie auf einzelne Lücken (so z. B. bezüglich der Verwendung des amtlichen Vordrucks „Unbeschränkte Auskunft aus dem Bundeszentralregister" auch für BZR-interne Arbeitsabläufe). Nach Mitteilung des Generalbundesanwalts ist die Erstellung der internen Übersicht in der dazu notwendigen Differenzierung eingeleitet und wird in Kürze abgeschlossen sein.

— Zur Organisation der Datenverarbeitung habe ich empfohlen, ein förmliches Freigabeverfahren für ADV-Programme einzuführen, das sicherstellt und dokumentiert, daß das Programm den Vorgaben des Fachreferates entspricht. Wie mir mitgeteilt wurde, bereitet das BZR entsprechende Organisationsregeln vor.

— Nach meinen Feststellungen sind die Schutzvorkehrungen gegen eine unbefugte Registereinsicht nicht ausreichend. Der Generalbundesanwalt hat zugesagt, weitere technisch-organisatorische Maßnahmen zu treffen, um eine mißbräuchliche Registereinsicht zu verhindern. Insbesondere soll jeder Bedienstete vor der regelmäßig oder aus besonderem Anlaß erfolgenden Vergabe eines neuen Bearbeiter-Kennzeichens durch schriftliche Belehrung nochmals an die Pflicht erinnert werden, das Bearbeiter-Kennzeichen nur zu benutzen, wenn dies zur Erledigung der ihm obliegenden Aufgaben erforderlich ist.

Besondere Aufmerksamkeit verdient die Problematik der automatisierten Anfrage- und Auskunftsverfahren. Einer Online-Abfrage durch auskunftsberechtigte Behörden stehen — wie ich bei meinen Besuchen verdeutlicht habe — erhebliche datenschutzrechtliche Bedenken entgegen. Sie gelten vor allem Fragen der Authentizitätsprüfung des Anfragenden durch das System, der Prüfung der Zulässigkeit einer bestimmten Registerauskunft sowie der Zugriffskontrolle bezüglich der Terminals und der ausgedruckten Auskünfte. Ich teile nicht nur die Skepsis der Mitarbeiter des BZR hinsichtlich der Möglichkeiten einer zuverlässigen technischen Lösung dieser Probleme. Ich habe darüber hinaus auch erhebliche Zweifel, ob die derzeitige Rechtslage eine Online-Abfrage zuläßt. Meine datenschutzrechtlichen Bedenken gegen eine Online-Abfrage werden vom Bundesminister der Justiz und vom Generalbundesanwalt geteilt. Zunächst soll deshalb lediglich ein Datenträgeraustausch erprobt werden.

Auch bei meiner jüngsten Kontrolle der Datenübermittlung aus dem Register stellte die schon in meinem vorigen Tätigkeitsbericht (5. TB S. 18) angesprochene Vorschrift des § 39 Abs. 1 Nr. 2 BZRG, die den obersten Bundes- und Landesbehörden, nicht aber nachgeordneten Behörden, ein Recht unbeschränkter Auskunft aus dem Register gewährt, einen Schwerpunkt dar. Nach wie vor geht es darum, daß die nach geltendem Recht bestehende Beschränkung des Auskunftsrechts nicht dadurch umgangen wird, daß die obersten Bundes- oder Landesbehörden über den durch § 41 BZRG gezogenen Rahmen hinaus Auskünfte für nachgeordnete oder ihrer Aufsicht unterstehende Behörden einholen

und an diese weiterreichen. Zur Prüfung habe ich mir erneut für bestimmte Zeitabschnitte Aufstellungen über die Ersuchen oberster Bundes- und Landesbehörden vorlegen lassen.

In der Auswertung ist der Fall, in dem „Verwaltungsangelegenheit" als Zweck der Anfrage angegeben wird, von solchen Fällen zu unterscheiden, in denen „Feststellung der Eignung als Kleinsiedler", „Bürgschaftseinzelsache" bzw. „Aufnahme in die freiwillige Feuerwehr" als Zweckangaben erscheinen.

„Verwaltungsangelegenheit" ist lediglich eine allgemeine Umschreibung von Behördentätigkeit, aber keine Zweckangabe im Sinne von § 39 Abs. 4 BZRG und steht damit der Zeichenfolge „XXXXX" gleich, die nach der technischen Auslegung des Systems die Auslösung einer unbeschränkten Auskunft erlaubt. Ich habe daher gefordert, durch Dienstanweisung klarzustellen, daß „Verwaltungsangelegenheit" als Zweckangabe für eine unbeschränkte Auskunft an oberste Bundes- und Landesbehörden nicht ausreicht.

Ich bedaure, daß in diesem Punkt ein Einvernehmen mit dem Bundesminister der Justiz bislang nicht erzielt ist. Der vom Bundesminister der Justiz unterstützten Auffassung des Generalbundesanwalts, daß „Verwaltungsangelegenheit" den Verwendungszweck „nur allgemein bezeichne", dieser im übrigen aber durch die Geschäftsnummer hinreichend konkretisiert werde, vermag ich nicht zu folgen. Abgesehen davon, daß die Geschäftsnummer in Auskunftsersuchen nicht immer angegeben wird, kann sie die geforderte verbale Zweckangabe nicht ersetzen. Der Generalbundesanwalt hält es für zweifelhaft, ob § 39 Abs. 4 Satz 2 BZRG, der die Zweckangabe verlangt, für Auskünfte an oberste Bundes- und Landesbehörden überhaupt Anwendung findet, da insoweit eine Beschränkung auf bestimmte Zwecke nicht vorgesehen ist. Auch diese Argumentation halte ich — angesichts des Zweckes wie des Wortlauts der geltenden Gesetzesvorschrift — nicht für zutreffend.

Auch die übrigen der oben genannten Zweckangaben für Auskünfte an oberste Landesbehörden verfehlen m. E. das vom Gesetzgeber gewollte Ziel, unbeschränkte Auskünfte nur für Verwaltungsangelegenheiten von einem gewissen Gewicht zuzulassen. Das Problem ließe sich dadurch lösen, daß das BZR eine Schlüssigkeitsprüfung des Auskunftsersuchens vornimmt. Dabei bereitet allerdings der unterschiedliche Verwaltungsaufbau zwischen Stadt- und Flächenstaaten Schwierigkeiten. Ich werde daher den Datenschutzkontrollinstitutionen der Länder nahelegen, für ihren Zuständigkeitsbereich entsprechende Initiativen zu ergreifen und namentlich bei den Senatoren der Stadtstaaten als oberste Landesbehörden auf eine gewisse Selbstbeschränkung in den Auskunftsersuchen hinzuwirken.

Der zwischenstaatliche Datenaustausch, namentlich die Übermittlung von Daten des BZR an Behörden und Gerichte außerhalb der Bundesrepublik ist auch Gegenstand meiner Kontroll- und Beratungstätigkeit gegenüber dem Bundeskriminalamt. Ich teile die Auffassung des BZR, daß im Rahmen des § 53 Satz 1 BZRG i. V. m. § 74 Abs. 1 Satz 3 des Gesetzes über die Internationale Rechtshilfe in Strafsachen (IRG) dem Bundeskriminalamt in bezug auf Auskünfte aus dem Bundeszentralregister lediglich eine Vermittlungsfunktion zukommt. Dem entspricht auch die vom BZR verwandte Übermittlungsformel „Ich bitte diese Auskunft des BZR als solche (d. i. als Auskunft des BZR) an die ersuchende ausländische Dienststelle weiterzuleiten". In Einzelfällen wegen besonderer Eilbedürftigkeit aus eigenen Unterlagen des Bundeskriminalamtes gegebene Vorstrafen-Auskünfte müssen daher vom Bundeskriminalamt mit dem Hinweis auf die Vorläufigkeit solcher Informationen erteilt und gegebenenfalls nach Übermittlung der offiziellen Auskunft des BZR revidiert werden.

Hilfreich hat sich das mit dem BZR geführte Gespräch auch für die Beurteilung solcher Auskunftsersuchen erwiesen, in denen die ausländische Polizeidienststelle lediglich angegeben hat, daß es sich um eine „Personenüberprüfung" handelt. Mit dem BZR besteht nunmehr Einvernehmen, daß diese Angabe nicht ausreicht, um von einem Strafvorwurf (vgl. Artikel 13 des Europäischen Übereinkommens über die Rechtshilfe in Strafsachen: „für eine Strafsache erbetene Auskünfte") auszugehen.

Die geschilderten Probleme geben mir keinen Anlaß, von der früheren Aussage abzugehen, daß es sich bei dem Bundeszentralregistergesetz um das Beispiel eines gelungenen bereichsspezifischen Datenschutzes handelt. Meine Bemühungen bezwekken aber nicht nur eine angemessene Datenschutzpraxis, sondern auch eine Verbesserung der Rechtsgrundlagen. Insoweit bleiben meine schon im Fünften Tätigkeitsbericht skizzierten Vorschläge zur Novellierung des Bundeszentralregistergesetzes (5. TB S. 18) weiterhin aktuell. In den Beratungen zu einem Zweiten Gesetz zur Änderung des Bundeszentralregistergesetzes sind meine Vorschläge nicht berücksichtigt worden. Nachdem der Bundesminister der Justiz aber mitgeteilt hat, daß er einem wesentlichen Teil meiner Überlegungen „nicht ohne Sympathie gegenüberstehe", sollten die Vorschläge auch Berücksichtigung finden.

3.2 Personenstandswesen

Auf die Problematik der in diesem Bereich bestehenden Mitteilungspflichten habe ich schon in früheren Tätigkeitsberichten hingewiesen (2. TB S. 19, 4. TB S. 44, 5. TB S. 21). Es ist zu begrüßen, daß — unbeschadet der Länderzuständigkeit für die Ausführung personenstandsrechtlicher Vorschriften — Bund und Länder nunmehr gemeinsam prüfen, ob und in welchem Umfang die in der Dienstanweisung für die Standesbeamten und ihre Aufsichtsbehörden (DA) geregelten Mitteilungspflichten in einer Rechtsvorschrift verankert werden können. Der hohe Sensibilitätsgrad der im Personenstandswesen geführten Daten und die auf langen Erfahrungen beruhende Kenntnis des Übermittlungsbedarfs legen es nahe, für diesen Bereich spezifische *Rechts*grundlagen zu schaffen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat deshalb im Juni 1983 empfohlen, die einzelnen Datenübermittlungen in einer Rechtsvorschrift konkret zu regeln; allerdings sollte sie sich nicht in einer bloßen Übernahme der DA erschöpfen. Entsprechende Bemühungen sollten vielmehr mit einer Prüfung der Erforderlichkeit der bislang praktizierten Mitteilungen Hand in Hand gehen. Diese Prüfung muß sich am Maß unabweislicher Bedürfnisse der Empfänger der Mitteilungen orientieren. Vorschriften, deren Vollzug eine Übermittlung von Personenstandsdaten voraussetzt, müssen einer Überprüfung unterzogen werden, ob sie im Hinblick auf das heutige Verständnis des verfassungsrechtlich garantierten Persönlichkeitsschutzes noch Bestand haben können. Eine Reihe von Regelungen hat angesichts eines veränderten gesellschaftlichen Umfeldes und eines Wandels der Verwaltungsaufgaben ihren Sinn verloren. Außerdem sollte darauf Bedacht genommen werden, daß

- Datenübermittlungen den betroffenen Bürgern im Hinblick auf Inhalt, Adressat und zugrundeliegende Rechtsgrundlage transparent gemacht werden,
- übermittelte Daten nur im Rahmen des Zwecks, zu dem sie übermittelt wurden, genutzt werden,
- die notwendigen technisch-organisatorischen Maßnahmen der Datensicherung vorgesehen werden und
- die Aufbewahrungsdauer unter Berücksichtigung auch der Belange der Betroffenen auf das erforderliche Maß beschränkt wird.

Die Bemühungen um eine Abstimmung zwischen den verschiedenen Bundesressorts und den Ländern dauern noch an.

Ich begrüße die mir nunmehr zugegangene Mitteilung der Bundesregierung, daß sie die von mir wiederholt (2. TB S. 19, 5. TB S. 21) am öffentlichen Aufgebotsverfahren geäußerten Zweifel teilt und vorgesehen sei, das Aufgebot in seiner derzeitigen Form abzuschaffen und durch eine Anmeldung — ohne Veröffentlichungspflicht — zu ersetzen.

Aufgrund meiner Bemühungen (vgl. 4. TB S. 44, 5. TB S. 21) scheint sich unter den beteiligten Behörden auch mehr und mehr die Einsicht durchzusetzen, daß die Pflicht des Standesbeamten, bei Eintragungen über umherziehende Personen ohne festen Wohnsitz die Kriminalpolizei zu unterrichten (§§ 103 und 201 DA), entfallen kann.

Die Datenschutzbeauftragten haben außerdem empfohlen, auf Angaben über empfangene Versorgungsleistungen und deren Mitteilung an das Versorgungsamt (§§ 203 und 353 DA) zu verzichten. Das Personenstandsgesetz enthält hierfür keine Rechtsgrundlage; auch sonst ist eine solche nicht ersichtlich. Es handelt sich bei der Erhebung dieser Angaben um Tätigkeiten, die mit den eigentlichen Aufgaben des Standesbeamten nichts zu tun haben.

Die Datenschutzbeauftragten haben weiterhin angeregt, Sterbeurkunden im Hinblick auf die übliche Vorlage dieser Urkunden auch bei Banken etc. von solchen Angaben zu entlasten, die mit detaillierten Orts- und Zeitangaben z. B. Hinweise darauf enthalten, daß der Verstorbene den Freitod gewählt hat (§ 336 DA). Solche Angaben bzw. der Rückschluß auf solche Fakten sind nicht erforderlich und durch das Personenstandsgesetz (§§ 37, 64) m. E. nicht geboten. Hilfsweise sollte erwogen werden, zur Vorlage bei Banken etc. ein Papier zu schaffen, daß sich auf die für diesen Zweck notwendigen Daten beschränkt.

Angesichts der gegenwärtig zwischen den zuständigen Bundes- und Landesressorts geführten Diskussion zur Unterrichtung der Meldebehörden über das Erlöschen des Verwandtschaftsverhältnisses bei Inkognito-Adoption Minderjähriger sind die Datenschutzbeauftragten der Ansicht, daß die DA eine Mitteilung des Standesbeamten über die Adoption an die Meldebehörde der leiblichen Eltern des adoptierten Kindes nicht vorsieht und auch nicht vorsehen sollte, um Nachforschungen über das Kind auszuschließen. Die zuständigen Stellen scheinen sich überwiegend dieser Auffassung anzuschließen und halten eine Mitteilungspflicht des Standesbeamten an die für den Wohnort der leiblichen Eltern zuständige Meldebehörde mit dem Offenbarungsverbot des § 1758 BGB nicht für vereinbar. Dies soll in einer Rechtsvorschrift und in der DA (§ 98) klarer zum Ausdruck gebracht werden.

3.3 Mitteilungen in Zivilsachen

Die Vorschläge der Datenschutzbeauftragten (vgl. 5. TB S. 20 f.) haben es bisher nicht vermocht, die Justizverwaltungen zu der geforderten umfassenden Prüfung der rechtlichen Begründung und praktischen Notwendigkeit bestehender Mitteilungspflichten nach der Anordnung über Mitteilungen in Zivilsachen (MiZi) zu veranlassen. Gemeinsam mit den Landesbeauftragten für den Datenschutz habe ich mich bei den jeweiligen Justiz- und Sozialministerien darum bemüht, eine Aufhebung der Mitteilungspflicht über Klagen auf Räumung von Wohnraum bei Zahlungsverzug des Mieters (MiZi IV 1) zu erreichen. Während sich zunächst eine Mehrheit der Justizverwaltungen — namentlich auch der Bundesminister der Justiz — für die Streichung ausgesprochen hatte, haben die obersten Sozialbehörden der Länder dem widersprochen. Daraufhin hat mir der Bundesminister der Justiz mitgeteilt, daß das Vorhaben, MiZi IV 1 aus datenschutzrechtlichen Gründen zu streichen und durch ein lediglich dem Beklagten zu übersendendes Formblatt zu ersetzen, nunmehr als gescheitert anzusehen sein dürfte. Neuerdings wurde indessen aus Rheinland-Pfalz bekannt, daß bei den Trägern der Sozialhilfe eine Umfrage über die Auswirkungen der Mitteilung der Gerichte gehalten werde und das Ministerium für Soziales aus sozialhilferechtlicher Sicht ein gut gestaltetes Informationsblatt für den Räumungs-Beklagten für ausreichend halte.

Dies ist nur ein Beispiel für die Schwierigkeit der Diskussion im Rahmen der komplexen Gesamtproblematik einer Vielzahl von Mitteilungspflichten.

3.4 Mitteilungen in Strafsachen

Zur Problematik der Anordnung über Mitteilungen in Strafsachen (MiStra) habe ich in meinem Fünften Tätigkeitsbericht (S. 19) Stellung genommen. Inzwischen hat eine Arbeitsgruppe der Justizverwaltungen Vorschläge für die Neufassung der MiStra erstellt. Diese liegen nunmehr den Justizverwaltungen zwecks weiterer Abstimmung vor. Allerdings sind noch viele Fragen offen; so enthält der Entwurf noch keine Antwort auf die vom Rechtsausschuß des Deutschen Bundestages gestellte Frage (vgl. 5. TB a. a. O.), inwieweit die Bestimmungen der MiStra — bislang Verwaltungsvorschriften — Rechtsnormcharakter erhalten sollten.

Die Vorschläge der Arbeitsgruppe sind von den Landesjustizverwaltungen den Landesbeauftragten für den Datenschutz und vom Bundesminister der Justiz auch mir zur Stellungnahme zugeleitet worden. Kritischer Betrachtung bedürfen insbesondere die Bestimmungen über Mitteilungen bezüglich der Personen, die einer Dienst-, Staats- oder Standesaufsicht unterliegen. Unter Heranziehung der Regelungen des jeweiligen Aufsichts- bzw. Disziplinarrechts sollten sie noch eingehender geprüft und diskutiert werden. Ich werde dem Bundesminister meine Auffassung zu den Vorschlägen der Arbeitsgruppe darlegen.

3.5 Richtlinien für das Strafverfahren und das Bußgeldverfahren

Zu meinen im Fünften Tätigkeitsbericht (S. 19f.) wiedergegebenen Vorschlägen zur Überarbeitung der Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV) sind erste Erfolge zu verzeichnen:

Zur Frage des Akteneinsichtsrechts für den Beschuldigten ist — wie mir der Bundesminister der Jusitz mitgeteilt hat — in dem Referentenentwurf eines Gesetzes zur Änderung strafverfahrensrechtlicher Vorschriften die Regelung vorgesehen, daß dem Beschuldigten Akteneinsicht auf der Geschäftsstelle des Gerichts, der Staatsanwaltschaft oder bei einer anderen Behörde unter Aufsicht gestattet werden kann, soweit nicht wichtige Gründe entgegenstehen. Gegenüber dem bisherigen Rechtszustand grundsätzlicher Verweigerung der Akteneinsicht durch den Beschuldigten (§ 147 StPO, Nr. 185 RiStBV) sehe ich in der vorgesehenen Regelung insofern einen entscheidenden Fortschritt, als nunmehr das Einsichtsrecht des Beschuldigten zum Regelfall gemacht werden soll. Ich habe dem Bundesminister der Justiz vorgeschlagen, bei Ausschluß entgegenstehender wichtiger Gründe keinen Ermessensspielraum des Gerichts bzw. der Staatsanwaltschaft, sondern einen Anspruch des Betroffenen vorzusehen.

Bezüglich der schon im Fünften Tätigkeitsbericht angesprochenen Frage der Übersendung von Urteilsabschriften an die in Nr. 236 Abs. 1 RiStBV genannten Einrichtungen hat mich der Bundesminister der Justiz noch nicht davon überzeugen können, daß dies in nicht-anonymisierter Form erforderlich ist. Um weitere Erfahrungen zu gewinnen hat er diese Frage zum Gegenstand näherer Beobachtung und Beratung mit den Ländern gemacht.

3.6 Bekanntmachung von Verurteilungen wegen falscher Verdächtigung bzw. wegen Beleidigung

Bei Straftatbeständen der Beleidigung (§§ 185ff. StGB) und der falschen Verdächtigung (§ 164 StGB), ist auf Antrag des Verletzten oder des zur Stellung eines Strafantrags Berechtigten die öffentliche Bekanntgabe der Verurteilung vom Gericht anzuordnen, wenn die Tat öffentlich begangen wurde (§§ 165 und 200 StGB). Entsprechende Veröffentlichungen in der Berliner Tagespresse haben in mehreren Fällen zu Anfragen von Bürgern geführt, ob diese Praxis nicht gegen den Datenschutz verstoße. Die Veröffentlichung in einer Tageszeitung erscheint problematisch, wenn — etwa bei der Beleidigung von Polizeibeamten — die Tat zwar „öffentlich", also auf einem öffentlichen Platz, aber lediglich in Gegenwart eines sehr kleinen Personenkreises geschah.

In Übereinstimmung mit dem Berliner Datenschutzbeauftragten bin ich der Auffassung, daß aus Gründen des Datenschutzes dem Richter bei solchen Verurteilungen ein Entscheidungsspielraum zustehen sollte, ob eine öffentliche Bekanntgabe der Verurteilung angemessen ist oder nicht. Das Gericht sollte im Rahmen des Ermessens zwischen dem Genugtuungsinteresse des Verletzten einerseits und dem Interesse des Täters am Schutz vor unnötiger Bloßstellung andererseits abwägen können.

Der Bundesminister der Justiz hat auf meine Vorschläge ausgeführt, dem sei bereits dadurch ausreichend Rechnung getragen, daß die *Art* der Bekanntmachung grundsätzlich im pflichtgemäßen Ermessen des Gerichtes stehe. Eine Bekanntmachung in einer Zeitung oder Zeitschrift bzw. im Rundfunk sei nur dann obligatorisch, wenn der Täter selbst sich dieser Publikationsmittel bedient habe; auch andere Veröffentlichungsmittel, z. B. Aushang am Schwarzen Brett einer Polizeidienststelle, kämen in Betracht. Meines Erachtens werden diese Alternativen in der praktischen Anwendung der Gesetzesvorschriften nicht genutzt. Ich habe dem Bundesminister der Justiz daher empfohlen, im Zusammenwirken mit den Justizverwaltungen der Länder die Praxis der Handhabung der genannten Gesetzesbestimmungen zu beobachten und gegebenenfalls deren Änderung zu erwägen, um dem Richter einen Entscheidungsspielraum nach Schwere und Form der Tat einzuräumen. Der Bundesminister der Justiz sieht hierfür jedoch kein Bedürfnis.

3.7 Hinweise auf die „andere Tat" bei Einstellung der Strafverfolgung

Ein Rechtsanwalt hat mir folgenden Fall geschildert: Ein von einem Hund gebissener Spaziergänger habe seine Mandantin verdächtigt, diesen Hund nicht ordnungsgemäß geführt zu haben, und gegen

sie Strafantrag gestellt. Die Staatsanwaltschaft habe das Verfahren gemäß § 154 Abs. 1 StPO vorläufig mit dem Hinweis an den Anzeigeerstatter eingestellt, gegen die Beschuldigte werde „bei dem Generalbundesanwalt ein Ermittlungsverfahren wegen Landfriedensbruchs geführt". Die Strafe, zu der die Verfolgung der angezeigten Tat führen könnte, falle neben der Strafe, die die Beschuldigte wegen der genannten Tat zu erwarten habe, nicht ins Gewicht.

Der Sachverhalt ist zwar nicht nach dem BDSG zu beurteilen. Im Rahmen meiner Beratungsaufgabe habe ich jedoch gegenüber dem Bundesminister der Justiz den Standpunkt vertreten, daß der Inhalt eines Bescheides der Staatsanwaltschaft an einen Strafantragsteller (§ 171 StPO, Nr. 89 RiStBV) schützwürdige Belange des Beschuldigten und des Antragstellers berücksichtigen sollte. Der Antragsteller, zumal wenn er zugleich der Verletzte ist, hat ein berechtigtes Interesse zu erfahren, ob die Staatsanwaltschaft seinem Antrag Folge gibt und falls sie dies nicht tut — welche Gründe hierfür maßgebend sind. Der Beschuldigte hat ein berechtigtes Interesse daran, nicht schon gebrandmarkt zu werden, ehe auch nur die Ermittlungen abgeschlossen sind. In diesem Rahmen ist eine Abwägung geboten. Dem Antragsteller mitzuteilen, welche anderen Straftaten, die mit der Anzeigeerstattung nichts zu tun haben, Gegenstand der Strafverfolgung sind, geht m. E. über das berechtigte Informationsbedürfnis hinaus, verletzt Belange des Beschuldigten und ist durch § 171 StPO ebensowenig geboten wie durch Nr. 89 RiStBV.

Der Bundesminister der Justiz will die Landesjustizverwaltungen auf diese Problematik aufmerksam machen. Er ist mit mir der Auffassung, daß Hinweise auf die „andere Straftat" — da in der Sache nicht weiterführend — unterbleiben sollten.

3.8 Grundbuchwesen

Über eine mögliche Verletzung schutzwürdiger Belange der Miteigentümer gemeinsam genutzter Grundstücke wie Garagenflächen und Zufahrtswege durch Bekanntgabe des Inhalts von Grundbuchauszügen, die u. a. Darlehensbelastungen der übrigen Miteigentümer wiedergeben, habe ich im vorigen Tätigkeitsbericht (5. TB S. 22) berichtet. Ich begrüße es, daß der Bundesminister der Justiz nach Abstimmung mit den Landesjustizverwaltungen meinem Anliegen entgegenzukommen sucht und im Rahmen der von ihm in Aussicht genommenen Novellierung der Grundbuchordnung eine Änderung des § 3 der Grundbuchordnung anstrebt. Eine nähere Beurteilung dieses Vorhabens wird erst möglich sein, wenn konkrete Formulierungen vorliegen.

3.9 Handbuch der Justiz

Seit 1979 erörtere ich mich mit dem Bundesminister der Justiz die Zulässigkeit der Übermittlung von Personaldaten an den Deutschen Richterbund, der unter Mitwirkung der Justizverwaltungen des Bundes und der Länder sowie der Verwaltungen der Verfassungs- und Finanzgerichte das „Handbuch der Justiz" herausgibt. Aufgrund einer Reihe von Eingaben von Betroffenen und in Übereinstimmung mit den Landesbeauftragten für den Datenschutz habe ich wiederholt Bedenken dagegen erhoben, daß außer Namen, auch Geburts- sowie Ernennungs- und Beförderungsdaten ohne Einwilligung der Betroffenen übermittelt werden. Meine Einwände gegen dieses Verfahren gründen sich einmal auf § 24 Abs. 1 Satz 1 i. V. m. § 7 Abs. 3 BDSG, wonach solche Übermittlungen nur zulässig sind, wenn feststeht, daß schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden, und zum anderen auf die höchstrichterliche Rechtsprechung zur Geheimhaltung des Inhalts von Personalakten.

Der Bundesminister der Justiz hat mir nunmehr mitgeteilt, daß er künftig Ernennungs- und Beförderungsdaten von Angehörigen des Bundesministeriums der Justiz dem Deutschen Richterbund nur übermitteln werde, wenn der Betroffene einwilligt. Auch Geburtsdaten sollen — wie bisher schon — nur mit Zustimung der Betroffenen übermittelt werden. Diese Praxis berücksichtigt bereits, daß schon in naher Zukunft in den öffentlichen Verwaltungen Personaldaten weitgehend in Dateien geführt und auf Datenträgern gespeichert sein werden.

Ich habe diese Entscheidung des Bundesministers der Justiz begrüßt und hoffe, daß sie nicht nur für die Justizverwaltungen in den Ländern, sondern für Handbücher ähnlicher Art auch in anderen Bereichen außerhalb der Justiz orientierend wirkt.

4. Finanzverwaltung

4.1 Änderung der Abgabenordnung

In meinem letzten Tätigkeitsbericht (5. TB S. 25 f.) habe ich zu dem damaligen Referentenentwurf des Bundesministers der Finanzen zur Änderung der Abgabenordnung Stellung genommen. Der Bundesminister der Finanzen hat den Entwurf später zurückgezogen und im August 1983 in überarbeiteter Form wieder vorgelegt. Er stellt gegenüber der früheren Fassung eine wesentliche Verbesserung dar.

Der neue Entwurf verzichtet auf zwei Vorhaben, die Schwerpunkte der Kritik der Datenschutzbeauftragten bildeten:

— Er läßt die vorgesehene Ergänzung des § 16 der Abgabenordnung (AO) fallen, nach der unterschiedliche Finanzbehörden im Verwaltungsverfahren in Steuersachen nicht als Dritte im Sinne des Datenschutzrechts sondern als Verwaltungseinheit anzusehen wären, was zur Folge gehabt hätte, daß z. B. die gesetzlichen Zulässigkeitsregeln für Datenübermittlungen nicht greifen.

— Der neue Entwurf enthält nicht mehr die ursprünglich geplante Ergänzung des § 112 AO, nach der über Auskünfte im Einzelfall hinaus Auskünfte „allgemein" zum Gegenstand der Amtshilfe gemacht würden. Hiermit ist auf den Versuch verzichtet worden, die Amtshilfe in einer Weise auszudehnen, die von der datenschutzrechtlichen Erforderlichkeitsprüfung des Einzelfalls weggeführt hätte.

In dem letztgenannten Zusammenhang verdient in dem neuen Entwurf die in § 93 Abs. 7 AO vorgesehene Regelung besondere Aufmerksamkeit. Um sicherzustellen, daß Steuern nicht verkürzt und Steuererstattungen und Steuervergütungen nicht zu Unrecht gewährt werden, soll danach der Bundesminister der Finanzen durch Rechtsverordnung bestimmen können, daß Gerichte und Behörden bestimmte Maßnahmen ohne vorheriges Ersuchen der zuständigen Finanzbehörde mitzuteilen haben, soweit der Inhalt dieser Mitteilungen für die Besteuerung und das Besteuerungsverfahren von Bedeutung ist. Diese Regelung trägt der von mir wiederholt erhobenen und auch von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder formulierten Forderung Rechnung, daß steuerbehördliche Aufklärungsmaßnahmen wegen ihres Eingriffscharakters auf eine eindeutige Rechtsgrundlage gestützt werden müssen. Als eine Verbesserung gegenüber dem früheren Referentenentwurf betrachte ich es, daß die Pflicht von Gerichten und Behörden zu Kontrollmitteilungen nicht ein für alle Mal festgeschrieben wird, sondern in einer nicht zwingend auszuübenden Verordnungsermächtigung enthalten ist, die bedarfsgerecht anzuwenden ist. In diesem Zusammenhang ist wichtig, daß durch die Einfügung dieser Vorschrift in § 93 (anders der frühere Referentenentwurf) die Zuordnung zum Subsidiaritätsprinzip des § 93 Abs. 1 Satz 3 unterstrichen wird. Das bedeutet, daß die Heranziehung „anderer Personen" nur hilfsweise zugelassen wird und als andere Personen im Sinne dieser Vorschrift auch Behörden anzusehen sind.

Allerdings sollten, wie ich schon wiederholt gefordert habe, die schutzwürdigen Belange der Betroffenen auch dadurch berücksichtigt werden, daß die auskunftsgebende Stelle die Betroffenen durch Übersendung einer Durchschrift der Mitteilung oder in anderer geeigneter Form unterrichtet. Ich habe dem Bundesminister der Finanzen empfohlen, den vorgesehenen Absatz 7 dementsprechend zu ergänzen. Eine Unterrichtung des Betroffenen durch die übermittelnde Stelle würde dem Zweck der Mitteilung nicht zuwiderlaufen; sie ist vielmehr geeignet, den Steuerpflichtigen anzuhalten, von sich aus die notwendigen Auskünfte zu geben.

Aufmerksamkeit verdient auch eine Ergänzung des § 30 AO, die den Schutz des Steuergeheimnisses gegen unbefugte Offenbarung oder Verwertung auf den „automatisierten Abruf" von Daten ausdehnt. Sie trägt den mit der elektronischen Datenverarbeitung verbundenen besonderen Risiken Rechnung, und ist von mir unterstützt worden.

In der Frage der Kontrollbefugnisse der Datenschutzbeauftragten halte ich auch in meiner jüngsten Stellungnahme gegenüber dem Bundesminister der Finanzen an der Auffassung fest, daß die Steuerverwaltungen den Datenschutzbeauftragten nicht unter Berufung auf das Steuergeheimnis (§ 30 AO) Auskünfte und Einsicht in Akten verweigern können (vgl. 5 TB S. 23 f). Eine entsprechende Klarstellung in der Abgabenordnung darf jedoch nicht dazu führen, daß in Bereichen anderer Geheimhaltungsvorschriften (z. B. des Sozial- oder des Statistikgeheimnisses) das Fehlen entsprechender ausdrücklicher Regelungen den Datenschutzbeauftragten entgegengehalten werden kann. Ich habe daher empfohlen, die Klarstellung, die sich gleichermaßen auch auf andere Geheimhaltungsvorschriften beziehen würde, in die anstehende Novelle des Bundesdatenschutzgesetzes aufzunehmen, und würde dem auch weiterhin den Vorzug geben. Eine Regelung in der Abgabenordnung würde ich gleichwohl begrüßen, kann sie jedoch nur unter der Voraussetzung befürworten, daß im Wortlaut wie auch in der Begründung unmißverständlich zum Ausdruck gebracht wird, daß es sich um eine Vorschrift deklaratorischen Charakters handelt.

Als erfreulich ist schließlich noch eine in den neuen Referentenentwurf aufgenommene Ergänzung des § 309 AO zu nennen, wonach an Drittschuldner zuzustellende Pfändungsverfügungen künftig nicht mehr Angaben über die Arten der Steuerschulden enthalten sollen. Der Bundesminister der Finanzen folgt damit Empfehlungen, die ich wiederholt — u. a. in meinem letzten Tätigkeitsbericht (5. TB S. 26) — gemacht habe.

4.2 Prüfung eines Hauptzollamtes

Die Kontrolle eines Hauptzollamtes hat dort keine Speicherung von Daten erkennen lassen, die nicht zur rechtmäßigen Erfüllung der in der Zuständigkeit dieses Amtes liegenden Aufgaben erforderlich sind. Einige Schwachstellen und Problemfelder, zu denen ich Hinweise gegeben habe, waren im Bereich der Datensicherung sowie bezüglich der nach § 15 BDSG zu führenden Übersicht festzustellen. Der Bundesminister der Finanzen hat meine Vorschläge zur Führung der Übersicht akzeptiert und zum Gegenstand eines Erlasses an die Behörden der Bundesfinanzverwaltung gemacht.

Daneben wurden einige Einzelprobleme sichtbar, die nach meinem Eindruck ebenfalls über den Bereich eines einzelnen Hauptzollamtes hinausreichen:

— Nach § 39 Abs. 1 Ziff. 4 Bundeszentralregistergesetz (BZRG) dürfen Finanzbehörden für die Verfolgung von Straftaten, die zu ihrer Zuständig-

keit gehört, unbeschränkte Auskünfte aus dem Bundeszentralregister erhalten. Dem Zweck und dem Wortlaut dieser Vorschrift widerspricht es, in Bußgeldangelegenheiten, die schon nach erster Prüfung erkennen lassen, daß ein Strafverfahren nicht in Betracht kommt, eine unbeschränkte Auskunft einzuholen.

Ich habe daher empfohlen, von der bisherigen Praxis abzusehen, schon im Rahmen der vorbereitenden Prüfung (Eintragung in die Strafliste oder Bußgeldliste und Anlegung einer entsprechenden Karteikarte) routinemäßig auch für *Bußgeldsachen* Ersuchen auf Erteilung einer unbeschränkten Auskunft an das Bundeszentralregister zu richten. Im Rahmen der weiteren Bearbeitung im Einzelfalle kann eine Auskunft selbstverständlich dann eingeholt werden, wenn sich ergibt, daß eine Verfolgung im Rahmen eines Strafverfahrens in Betracht kommt. Tatsächlich hat meine Kontrolle auch keinen Bedarf erkennen lassen, im Regelfalle für Bußgeldangelegenheiten Auskünfte aus dem Bundeszentralregister einzuholen.

— Die nach § 39 Abs. 4 BZRG in Auskunftsersuchen an das Bundeszentralregister zu machende Zweckangabe sollte — dem Inhalt des § 39 Abs. 1 Ziff. 4 BZRG entsprechend — korrekterweise nicht „Steuersache" sondern „Steuerstrafsache" lauten. Ich werde gegenüber dem Bundeszentralregister darauf hinwirken, daß Ersuchen von Finanzbehörden mit der Zweckangabe „Steuersache" künftig zurückgewiesen werden.

— Die Karteikarten zur Straf- und Bußgeldliste des Hauptzollamtes werden nach 10 bis 15 Jahren ausgesondert und nach Ablauf von insgesamt 30 Jahren vernichtet. Aus den zugehörigen Akten werden nach 10 Jahren alle Unterlagen bis auf die Entscheidungen entfernt und vernichtet. Diese Handhabung entspricht den geltenden Aufbewahrungsvorschriften für die Bundesfinanzverwaltung.

  Ich habe empfohlen, diese Verwaltungsvorschrift mit dem Ziel zu überprüfen, namentlich im Straf- und Bußgeldbereich die Aufbewahrungsfristen für personenbezogene Daten deutlich zu reduzieren. Ich habe festgestellt, daß für die praktische Arbeit frühere Entscheidungen spätestens nach 10 Jahren jedenfalls dann entbehrlich sind, wenn zwischenzeitlich nicht neue Erkenntnisse hinzugetreten sind. Die geltenden Verwaltungsvorschriften bedürfen zudem einer Überprüfung unter dem Gesichtspunkt, sie mit den Vorschriften des Bundeszentralregistergesetzes in Einklang zu bringen, die darauf abzielen, durch Tilgung von Eintragungen den Betroffenen nach Ablauf bestimmter Fristen vom Makel der Verfehlung zu lösen und damit die Resozialisierungschancen zu verbessern.

— Die „Kartei der von der Abfindung ausgeschlossenen Personen" ist eine alphabetisch geordnete Datei von Personen, die wegen strafrechtlicher Verfehlungen gegen das Branntweinmonopol von dem Recht, als sogenannte Stoffbesitzer oder Brenner Branntwein herzustellen oder herstellen zu lassen, ausgeschlossen sind. Rechtsgrundlage ist die Brennereiordnung, eine Rechtsverordnung aus dem Jahre 1922. Je nach Schwere der Verfehlung ist die Dauer des Verlustes der Befugnis unterschiedlich. Eine Wiederzulassung und damit eine Gleichstellung mit unbescholtenen Stoffbesitzern bzw. Brennern erfolgt nur auf Antrag. Der Rechtsverstoß bleibt bis zu dem Zeitpunkt einer Wiederzulassung auf Antrag und, wenn ein solcher nicht gestellt wird, lebenslang gespeichert.

  Die genannte Vorschrift sollte an Ziel und Inhalt des Bundeszentralregistergesetzes angepaßt werden. Unter Gesichtspunkten des Datenschutzes dürfte sich eine Regelung des Inhalts empfehlen, daß nach Ablauf bestimmter Ausschlußfristen der Betroffene unbescholtenen Bürgern automatisch gleichgestellt und dementsprechend die Karteikarte aus der Kartei der Ausgeschlossenen entfernt wird. Dies würde nach meiner Überzeugung auch praktischen Erfordernissen entsprechen.

4.3 Datenerfassung bei den Bundeskassen

Bei den Bundeskassen und der Sonderkasse Berlin sind elektronische Datensammelsysteme eingesetzt, die über Bildschirmerfassungsplätze verfügen. Im Verlauf der datenschutzrechtlichen Kontrolle einer Bundeskasse wurde festgestellt, daß mit Hilfe dieser Systeme zusätzlich zu den Beleginhalten auch Daten zur Tätigkeit der Erfasserinnen, wie z. B. Soll- und Ist-Arbeitszeit, Schreibleistung und Korrekturen, registriert wurden. Monatlich wurden diese Angaben nach Erfasserinnen geordnet in Listenform ausgedruckt. Nach Auskunft des Bundesministers der Finanzen dient dieses Verfahren in erster Linie der Dokumentierung aller Arbeitsvorgänge zur Absicherung des automatisierten Kassenverfahrens, außerdem zur Gewinnung von Planungswerten für Personalberechnungen. Dieses Verfahren mit seiner detailierten Registrierung personenbezogener (Leistungs-)Daten erschien aus datenschutzrechtlicher Sicht bedenklich. Ich begrüße daher die Entscheidung des Bundesministers der Finanzen, die Programme der Datensammelsysteme bei den Bundeskassen so zu ändern, daß kein Bezug auf eine bestimmte Erfasserin mehr möglich ist.

5. Personalwesen

5.1 Allgemeines

Während des Berichtsjahres hatte ich mich im Bereich Personalwesen aufgrund von Bürgereingaben und von Datenschutzkontrollen mit Problemen der Erhebung von Personaldaten, der Führung von Personalakten, Anträgen auf Auskunft, Einsicht in und Kopien aus Personalakten, Fällen der Verletzung des Personalaktengeheimnisses durch Übermittlung von Personaldaten aus Personalakten und schließlich mit Fragen der automatisierten Personaldatenverarbeitung in Personalinformationssystemen zu befassen.

Generell läßt sich feststellen, daß ich mit keinem der in diesem Zusammenhang aufgetretenen Probleme erstmalig konfrontiert wurde. Ich hatte mich mit ihnen bereits in den Vorjahren mehr oder minder eingehend beschäftigt und dazu meine Auffassung in früheren Tätigkeitsberichten niedergelegt.

Mit Ausnahme einiger Einzelfragen im Zusammenhang mit der Erhebung und Übermittlung von Personaldaten, in denen es zu übereinstimmenden Lösungen mit den betroffenen Behörden kam, wurden in anderen Problembereichen erneut erhebliche Unsicherheiten in der Beurteilung der Rechtslage auf seiten der betroffenen Behörden offenbar.

Diese Erfahrungen haben mich in meiner Überzeugung bestärkt, daß gesetzgeberische Aktivitäten im Bereich des Personalwesens dringend geboten erscheinen. Dies gilt zum einen für die umfassende Regelung des Personalaktenrechts, dessen Ziel es sein sollte, die von der Rechtsprechung und Lehre entwickelten Grundsätze in Gesetzesrang zu heben und dabei auch von der Rechtsprechung bisher nicht abschließend geklärte Zweifelsfragen zu erfassen. Meine Forderung deckt sich insoweit inhaltlich mit Empfehlungen des Bundesrechnungshofs, der in seinen Prüfungsfeststellungen zu Einzelplan 06 den Erlaß einheitlicher Richtlinien für das Führen und Verwalten von Personalakten für notwendig hält (BT-Drucksache 10/574, S. 22 f.).

Der andere gesetzgebende Schwerpunkt sollte in einer bereichsspezifischen Grundsatzregelung von Aufgaben, Funktionen und Grenzen von Systemen der Personaldatenverarbeitung liegen. Deren Einsatz nimmt auch in der öffentlichen Verwaltung zu. Die neueste Darstellung der Entwicklung auf diesem Gebiet gibt der „Zwischenbericht der Enquete-Kommission ‚Neue Informations- und Kommunikationstechniken'" vom 28. März 1983, S. 191 bis 206 (BT-Drucksache 9/2442). Die dort angesprochenen Nutzungsmöglichkeiten automatisierter Personaldatensysteme und die hierin begründeten datenschutzrechtlichen aber auch gesellschaftspolitischen Risiken machen den Regelungsbedarf besonders deutlich. Betriebsvereinbarungen reichen im Hinblick auf die begrenzte und im einzelnen umstrittene Reichweite der Mitbestimmungstatbestände und die mit der Durchführung von Betriebsvereinbarungen verbundenen Probleme nicht aus.

5.2 Neuregelung des Personalaktenrechts

In meinem Dritten (S. 26, 27) und Fünften Tätigkeitsbericht (S. 27) habe ich mich ausführlich mit dem Problem der Unvollständigkeit des Personalaktenrechts des Bundes auseinandergesetzt. Der Bundesminister des Innern hat meine Anregungen aufgegriffen und mir den ersten Rohentwurf einer Neufassung des § 90 BBG übersandt. Diese frühzeitige Beteiligung hat mich in die Lage versetzt, bereits im Entstehungsstadium der Neuregelung Vorschläge zu machen. Ich habe insbesondere angeregt, sie so umfassend wie möglich zu gestalten. Neben dem Personalaktengeheimnis sollten insbesondere auch die Abgrenzung und Abschottung der verschiedenen Personalaktenteile voneinander geregelt werden, ein besonderer Schutz für hochsensible Personaldaten, wie z. B. Gesundheitsdaten vorgesehen, und Vorschriften über die Führung verschiedener Personalakten bzw. Personaldatensammlungen bei mehreren Stellen aufgenommen werden.

Darüber hinaus müßten die neuen Vorschriften aber vor allem dem spezifischen Regelungsbedarf der automatisierten Personaldatenverarbeitung gerecht werden.

Ich habe dem Bundesminister des Innern meine Bereitschaft zu weiterer Mitarbeit mitgeteilt.

5.3 Automatisierte Personaldatenverarbeitung

5.3.1 Zur Planung von Personalinformationssystemen

Eine oberste Bundesbehörde hat mir mitgeteilt, daß sie beabsichtige, eine ADV-Personaldatei einzuführen. Sie hat mir gleichzeitig den ersten Entwurf ihrer konzeptionellen Vorstellungen einer solchen Datei übersandt und mich gebeten, diese zu überprüfen und aus der Sicht des Datenschutzes Stellung zu nehmen.

Ich habe diese frühzeitige Beteiligung sehr begrüßt; denn sie gibt mir Gelegenheit, schon im Planungsstadium organisatorischer Neuerungen Empfehlungen zur Verbesserung des Datenschutzes zu geben und die jeweiligen Bundesbehörden in Fragen des Datenschutzes zu beraten (§ 19 Abs. 1 BDSG).

Für die umfassende datenschutzrechtliche Bewertung von ADV-Personaldateien sind insbesondere Klarstellungen zu folgenden Punkten notwendig:

— Welche personenbezogenen Daten werden erfaßt (komplette Datenübersicht)?

Jede personenbezogene Angabe, die in ein Verarbeitungssystem aufgenommen wird, muß Gegenstand der datenschutzrechtlichen Überprüfung sein. Besonders sensible Daten, wie z. B. Gesundheits- oder Beurteilungsdaten, bedürfen dabei einer besonders eingehenden Betrachtung.

— Welche Programme sind im einzelnen vorgesehen (komplette Programmübersicht)?

In diesem Zusammenhang ist vorrangig zu prüfen, inwieweit die vorgesehenen Programme Verhaltens- oder Leistungskontrollen oder Personalentscheidungen ermöglichen; darüber hinaus ist von besonderer Bedeutung, ob das geplante System Verknüpfungsmöglichkeiten bietet bzw. vorsieht, mit denen Persönlichkeitsprofile erstellt werden können. Die genannten Anwendungsmöglichkeiten bedürfen aus datenschutzrechtlicher Sicht einer besonders eingehenden Prüfung, weil ihre grundrechtliche Zulässigkeit fraglich sein kann.

— Welche Daten bzw. Programme sollen wem zur Verfügung gestellt werden?

Da der Kreis der Datenempfänger so klein wie möglich zu halten ist, geht es hier insbesondere um die Notwendigkeit des Zugangs zu den Daten unter dem Aspekt der jeweiligen Zuständigkeiten.

— Wozu dient das Verfahren hinsichtlich jedes einzelnen Datums und jedes einzelnen Programms bzw. jeder Auswertung (Zweck-/Verwendungszusammenhang)?

— Sind Datenerhebung und -verarbeitung im einzelnen erforderlich?

In diesem Zusammenhang geht es vor allem um den Erforderlichkeitsnachweis unter dem Aspekt des Verhältnismäßigkeitsprinzips; Gesichtspunkte wie Wirtschaftlichkeit und Nutzen für den Betroffenen spielen ebenfalls eine Rolle.

— Welcher Speicherungszeitraum ist erforderlich (Löschungsfristen)?

Daten sollen grundsätzlich nicht länger gespeichert bleiben, als es für den Zweck, für den sie verarbeitet werden, erforderlich ist. Für jede Datenart sind daher von vornherein Löschungsfristen festzulegen.

— Beschreibung des technischen Systems

Von Bedeutung sind in diesem Zusammenhang u. a. die technischen Möglichkeiten der Protokollierung aller Benutzungsvorgänge und der übrigen Kontrollmaßnahmen.

— Welche Vorkehrungen sind im einzelnen zu den in Anlage zu § 6 Abs. 1 Satz 1 BDSG aufgeführten Kontrollmaßnahmen tatsächlich vorgesehen?

Die detaillierte Darstellung der organisatorischen und technischen Vorkehrungen zu jeder der in Betracht kommenden zehn Kontrollmaßnahmen ist notwendig, um feststellen zu können, ob die geplanten Maßnahmen in einem angemessenen Verhältnis zum angestrebten Schutzzweck stehen.

Die von der obersten Bundesbehörde beabsichtigte umfassende Beteiligung der Personalvertretung schon in der Planungsphase habe ich aus datenschutzrechtlicher Sicht begrüßt. Ich betrachte die Mitbestimmung bei Einführung von Personaldatenverarbeitungssystemen als ein wesentliches Instrument zur Sicherung des Datenschutzes.

Ich erwähne die vorstehenden Fragestellungen deshalb im einzelnen, weil sie auch anderen Stellen als Orientierungshilfe dafür dienen können, welche Gesichtspunkte bei der Umstellung auf automatisierte Personaldatenverarbeitung zu beachten sind. Im vorliegenden Fall habe ich darüber hinaus auch zu anderen Punkten Stellung genommen und mich zu weiterer Mitarbeit bei der Vorbereitung der geplanten Maßnahme bereiterklärt.

5.3.2 AWV-Arbeitskreis „Personalinformationssysteme"

Mit dem Thema „Personalinformationssysteme" befaßt sich auch ein zu diesem Zweck gegründeter Arbeitskreis der AWV-Arbeitsgemeinschaft für wirtschaftliche Verwaltung e. V., in dem ich vertreten bin. Die Aktivitäten dieses Arbeitskreises zielen darauf ab, ein Arbeitspapier zu ertellen, in dem Entwicklungsstand und -tendenzen von Personalinformationssystemen in der Bundesrepublik Deutschland und deren Bewertung aus der Sicht von Arbeitgebern und Arbeitnehmern, der Wissenschaft, Rechtsprechung und der Aufsichtsbehörden für den Datenschutz dargestellt und Empfehlungen für Planung, Funktionen, Grenzen, Einsatz und Kontrolle von Personalinformationssytemen gegeben werden sollen. Erst bei Vorliegen der Arbeitsergebnisse werde ich darüber entscheiden, ob ich diese aus datenschutzrechtlicher Sicht mittragen kann.

5.4 Einzelfragen

5.4.1 Abschottung der Beihilfeakten

Das Problem der mangelnden Abschottung der Beihilfestelle von der Personalverwaltung im übrigen habe ich in meinem Vierten Tätigkeitsbericht ausführlich dargestellt (s. dort S. 38, 39). In diesem Zusammenhang berichtete ich, daß ich den Bundesminister der Innern um Stellungnahme zu meinen Vorschlägen gebeten habe, die insbesondere auf eine Änderung des Personalaktenführungserlasses vom 21. Juni 1966 abzielten. Eine Stellungnahme des Bundesministers des Innern aus dem Jahre 1982 geht auf meine Argumente nur unzureichend ein und in einem weiteren Schreiben vom 2. Juni 1982 zieht er insbesondere meine Kontrollkompetenz in Personalaktenangelegenheiten in Zweifel und stellt eine Antwort „in Kürze" in Aussicht, die indes noch nicht eingegangen ist.

Da ich im Berichtsjahr in Eingaben aber auch persönlich mehrfach auf dieses Problem von betroffenen Beihilfeberechtigten angesprochen wurde, die

wegen der als mangelhaft empfundenen Abschottung der Beihilfeverwaltung darauf verzichten, bestimmte Rechnungen für ärztliche Leistungen zur Beihilfegewährung einzureichen, bedauere ich es um so mehr, daß diese Frage noch immer nicht zufriedenstellend geregelt werden konnte.

Die Daten im Beihilfebereich entsprechen von ihrer Geheimhaltungsbedürftigkeit her den Sozialdaten im Bereich der sozialen Sicherung. Ich halte es daher für erforderlich, die „Beihilfedaten" einem dem Sozialgeheimnis entsprechenden Schutz zu unterstellen. Einige Stellen meines Zuständigkeitsbereichs führen bereits eine entsprechende Trennung durch, andere prüfen gegenwärtig, wie dies organisatorisch zu realisieren ist. Eine verbindliche Regelung für alle Bereiche des öffentlichen Dienstes halte ich für dringend geboten.

5.4.2 Personalaktengeheimnis

Das Bundesministerium für das Post- und Fernmeldewesen hat in seiner Antwort vom 9. Februar 1983 auf eine allgemein gehaltene Anfrage eines Bundestagsabgeordneten personenbezogene Daten eines Postbediensteten offengelegt. Es handelte sich dabei u. a. um Namen, Geburtsdaten, Dienstrang, Noten und sonstige Einzelheiten dienstlicher Beurteilungen und Angaben über die Häufigkeit von Bewerbungen um Beförderungsdienstposten (BT-Drucksache 9/2408 S. 40, 41).

Ich sehe in dieser Publizierung personenbezogener Daten eine schwerwiegende Verletzung des Personalaktengeheimnisses als besonderes Amtsgeheimnis im Sinne des Datenschutzrechts und habe daher den Bundesminister für das Post- und Fernmeldewesen um Unterrichtung über die zugrundeliegenden Vorgänge und um Stellungnahme gebeten. In seiner Antwort vom 24. März 1983 hat der Bundespostminister mir lediglich mitgeteilt, die Veröffentlichung des Namens beruhe auf einem Mißverständnis und entspreche keineswegs der Praxis bei der Deutschen Bundespost. Auf Einzelheiten ist er nicht eingegangen, da er mir meine Kontrollkompetenz in diesem Fall bestreitet.

5.4.3 Personalrat

— *Kontrollrechte der Dienststelle*

In einem Fall hatte ich mich mit der Frage zu befassen, ob und gegebenenfalls inwieweit der interne Datenschutzbeauftragte einer Behörde gegenüber deren Personalrat Kontrollbefugnisse besitzt. Schon in meinem Ersten Tätigkeitsbericht (s. dort S. 15, 16) hatte ich unter Hinweis auf eine Entscheidung des Bundesverfassungsgerichts die Auffassung vertreten, daß die Rechtsstellung des Personalrats auch gegenüber der Dienststelle abschließend durch das Personalvertretungsrecht geregelt ist. Ergänzend hierzu hat das Bundesverfassungsgericht in einem Beschluß vom 27. März 1979 (BVerfGE 51, S. 77, 87) betont, die durch die Wahlentscheidung der Beschäftigten erlangte Mitgliedschaft im Personalrat sei ohne Bindung an Weisungen und Aufträge in persönlicher Unabhängigkeit eigenverantwortlich als Ehrenamt wahrzunehmen und gehöre jedenfalls auch zur persönlichen Rechtsstellung der einzelnen Personalratsmitglieder gegenüber dem Staat.

Aus diesen Entscheidungen des Bundesverfassungsgerichts läßt sich m. E. ableiten, daß die Behördenleitung — der interne Datenschutzbeauftragte ist ein Organ der Behördenleitung — gegenüber dem Personalrat hinsichtlich der diesem durch das Personalvertretungsgesetz übertragenen Aufgaben keine Kontrollkompetenzen hat. Insbesondere darf die Unabhängigkeit des Personalrats nicht beeinträchtigt werden. Nicht ausgeschlossen sind indessen Kontrollbefugnisse, die diese Rechtsposition nicht tangieren. Dies bedeutet, daß sich die Kontrollrechte des internen Datenschutzbeauftragten gegenüber dem Personalrat zumindest auf die technischen und organisatorischen Maßnahmen im Sinne des § 6 BDSG beziehen. Inwieweit die Beachtung auch anderer BDSG-Vorschriften kontrolliert werden kann, ist im jeweiligen Einzelfall zu entscheiden.

Hiervon unberührt bleibt, daß das BDSG und die anderen Vorschriften über den Datenschutz auch für den Personalrat gelten. Dieser hat ihre Durchführung sicherzustellen und unterliegt insoweit der Kontrolle der Datenschutzbeauftragten von Bund und Ländern.

— *Telefonkontrolle*

Die Bundesregierung hat ihre bisherige ablehnende Haltung zu meinen Vorschlägen, auf die Aufzeichnung der Zielnummern zu verzichten (vgl. 5. TB S. 29f.), in ihrer Stellungnahme zu meinem Fünften Tätigkeitsbericht erneut bekräftigt. Der Hinweis auf Nr. 9 der Dienstanschlußvorschriften vom 1. Juni 1976 (— DAV —, MinBlFin. S. 487) bietet jedoch m. E. keine überzeugende Begründung dafür, daß die Aufzeichnung der Zielnummer für den vorgeschriebenen Nachweis abgehender dienstlicher Ferngespräche sowie für die Abrechnung von Privatgesprächen zwingend notwendig ist. Vor allem die dadurch mögliche Kontrollierbarkeit von Gesprächen des Personalrats und anderer Einrichtungen mit besonderer Vertrauensstellung und mit besonderen Schweigepflichten erscheinen mir äußerst bedenklich.

Beispielgebend ist insoweit ein Fall im Bereich einer Bundesbehörde. Dort ist ohne förmliche Festlegungen zwischen den Beteiligten der Fernsprechanschluß des Personalrats stillschweigend so geschaltet worden, daß Telefongespräche — auch außerhalb des Ortsbereichs — ohne Einschaltung der Telefonzentrale geführt werden können. Ich würde es sehr begrüßen, wenn sich dies als Beginn einer allgemeinen Entwicklung erweisen sollte.

— *Auskunfts- und Einsichtsrecht von Bediensteten*

An mich ist die Frage herangetragen worden, ob hinsichtlich derjenigen Personalunterlagen, die

der Personalrat zur Erfüllung seiner in § 67 Abs. 1 Bundespersonalvertretungsgesetz umschriebenen Aufgaben aufbewahrt bzw. gespeichert hat, den betroffenen Bediensteten ein Auskunfts- und Einsichtsrecht zukommt.

Diese Frage ist zu bejahen. Zwar ist das Auskunftsrecht der Bediensteten gegenüber dem Personalrat nirgends ausdrücklich geregelt. Es erscheint aber fraglich, ob der Gesetzgeber dies überhaupt als ein besonderes Problem angesehen hat. Deshalb ist davon auszugehen, daß die Vorschriften der §§ 90 BBG, 13 BAT und 13 a MTB II einen allgemeinen, aus dem allgemeinen Persönlichkeitsrecht abgeleiteten Rechtsgrundsatz enthalten, der auf alle Beziehungen innerhalb des öffentlichen Dienst- bzw. des Arbeitsverhältnisses anwendbar ist. So erscheint es zulässig und angemessen, den Auskunftsanspruch gegenüber dem Personalrat aus einer entsprechenden Anwendung der vorgenannten Bestimmungen abzuleiten. Bei einem Dateibezug ergeben sich Auskunfts- und Einsichtsrechte zusätzlich aus §§ 7 Abs. 3, 26 BDSG.

5.4.4 Erhebung von Personaldaten

— *Angaben über die Religionszugehörigkeit*

Aufgrund einer Eingabe hatte ich den Bundesminister des Innern um Stellungnahme zur Frage der Erforderlichkeit von Angaben über die Religionszugehörigkeit in Personalbögen gebeten. Ich hatte diese schon in meinem Dritten Tätigkeitsbericht (S. 26) in Frage gestellt.

Der Bundesminister des Innern hat inzwischen mitgeteilt, er sehe prinzipiell keine Veranlassung, in standardisierten Fragebögen nach der rechtlichen Zugehörigkeit zu einer Religionsgemeinschaft zu fragen. Eine andere Beurteilung komme nur für die Angehörigen geschlossener Verbände, wie z. B. des Bundesgrenzschutzes, in Betracht, für die eine eigenständige und stetige seelsorgerliche Betreuung eingerichtet ist. Hier wäre gegebenenfalls der Hinweis „Beantwortung freigestellt" geboten. Er habe inzwischen veranlaßt, daß in dem künftigen einheitlichen Personalbogen des Bundesministeriums des Innern (Haus- und Geschäftsbereich), der demnächst eingeführt werden soll, die Frage nach der Religionszugehörigkeit vollständig gestrichen wird. Der Bundesminister des Innern hat mir darüber hinaus mitgeteilt, daß auch der Bundesminister für Verkehr seine Bereitschaft erklärt habe, künftig auf die Angabe der Religionszugehörigkeit allgemein zu verichten; die Vordruckmuster des Bundesministers für das Post- und Fernmeldewesen hätten das Merkmal „Religionszugehörigkeit" schon bisher nicht enthalten.

So erfreulich das Ergebnis in dieser Einzelfrage ist, so muß doch auch darauf hingewiesen werden, daß der vom Bundesminister des Innern in dem vorstehenden Zusammenhang erwähnte „künftige einheitliche Personalbogen des Bundesministeriums des Innern" in der Zwischenzeit mit dem Personalrat abgestimmt und eingeführt, mir indessen vorher nicht zur Stellungnahme zugeleitet worden ist.

— *Angabe über die Zugehörigkeit zu extremistischen Organisationen*

In mehreren Eingaben waren Zweifel an der Zulässigkeit der Datenerhebung zu dieser Frage geäußert worden. Datenschutzrechtliche Bedenken gegen die Erhebung als solche bestehen im Grundsatz nicht; das entsprechende Fragerecht der anstellenden Behörde halte ich mit dem Bundesarbeitsgericht (NJW 1981, S. 71 f.) für gegeben.

Hiervon abgesehen, schien mir indessen die Art und Weise der Datenerhebung in einem Personalfragebogen der Bundesversicherungsanstalt für Angestellte nicht zufriedenstellend gelöst zu sein, da der Bewerber durch die Art der Fragestellung verleitet werden könnte, Organisationen anzugeben, die objektiv nicht unter den Kreis extremistischer Organisationen fallen, deren Angabe folglich für den angestrebten Zweck auch nicht erforderlich wäre. Ich habe der Bundesversicherungsanstalt für Angestellte daher empfohlen, die entsprechende Frage mit dem Hinweis zu versehen: „Bei Zweifeln über die korrekte Beantwortung bitte rückfragen." Die Bundesversicherungsanstalt für Angestellte hat mir inzwischen mitgeteilt, sie habe in den Text des Anschreibens, mit dem der Bewerberfragebogen versandt werde, den Hinweis aufgenommen, der Bewerber möge sich bei Zweifeln — zu allen Fragen — an die Personalabteilung wenden. Diese Lösung erscheint mir akzeptabel; ich hätte es allerdings vorgezogen, wenn der Hinweis wegen des mit der Falschbeantwortung gerade dieser Frage verbundenen Risikos für den Bewerber ausdrücklich auf die Frage nach der Zugehörigkeit zu extremistischen Organisationen bezogen worden wäre.

6. Deutsche Bundespost

6.1 Allgemeines

Da wohl jeder Bürger auch Postkunde ist, ist nicht überraschend, daß sich im Berichtszeitraum wieder zahlreiche Bürger mit Eingaben an mich wandten, die den Bereich des Post- und Fernmeldewesens betrafen. Dabei ging es aber nicht nur um die herkömmlichen Dienstleistungen. Auch zu den neuen Kommunikationstechniken wurden Besorgnisse geäußert, die die Gewährleistung des Datenschutzes bei der Übermittlung von Nachrichten betrafen.

Häufiger als die Nachrichteninhalte waren es jedoch die Tatsache und die näheren Umstände der

Nachrichtenübermittlung (Einzelverbindungsdaten, wie z. B. Datum, Uhrzeit und Dauer), deren Bekanntgabe den Bürgern Anlaß zu Fragen gaben. In einzelnen Fällen ging es auch um die Übermittlung von Personaldaten von Postbediensteten an Stellen außerhalb der Deutschen Bundespost.

Der Schwerpunkt meiner Arbeit in bezug auf die Deutsche Bundespost lag weniger in datenschutzrechtlichen Kontrollen, als vielmehr — mit Blick auf die fortschreitende Entwicklung neuer Kommunikationstechniken — in zahlreichen informellen und beratenden Gesprächen sowohl mit dem Ministerium als auch den nachgeordneten Stellen.

6.2 Datenschutzrechtliche Kontrollen

6.2.1 Kontrolle eines Fernmeldeamtes

Durch die steigende Inanspruchnahme, aber auch durch die Ausweitung des Dienstleistungsangebotes wächst die Bedeutung des Fernmeldewesens als Mittel der Kommunikation zwischen den Bürgern und zugleich auch hinsichtlich Umfang und Sensibilität der diesem Medium anvertrauten personenbezogenen Daten. Betrieb, Instandhaltung und Gebührenberechnung der Fernmeldedienstleistungen sind im wesentlichen Aufgabe der Fernmeldeämter der Deutschen Bundespost. Da diese alle nach einheitlichen zentral vorgegebenen Richtlinien organisiert sind, gab die datenschutzrechtliche Kontrolle eines größeren Fernmeldeamtes nicht nur einen Überblick über den Stand des Datenschutz in diesem speziellen Amt, sondern darüber hinaus in allen Fernmeldeämtern. Mir ist bewußt, daß die gewonnenen Erkenntnisse — zumindest zum Teil — Fragen betreffen, die sich auch in anderen Fernmeldeämtern stellen und die schon deshalb eines weiteren Dialoges mit dem Bundesminister für das Post- und Fernmeldewesen bedürfen.

Die Kontrolle erstreckte sich hauptsächlich auf die Abwicklung der kundenbezogenen Dienstleistung, schloß aber auch die Verarbeitung der Personaldaten der Bediensteten ein. Der Stand des Datenschutzes im Bereich des untersuchten Fernmeldeamtes ist allgemein als hoch anzusehen. Schwachstellen und Problemfelder, die einer weiteren Prüfung und verbesserten Lösung bedürfen, waren namentlich im Bereich der Datensicherung, bezüglich der nach § 15 BDSG zu führenden Übersicht, sowie hinsichtlich einzelner Aspekte der Personaldatenverarbeitung festzustellen.

Im einzelnen:

Die Dateien, in denen personenbezogene Daten verarbeitet werden, sind in Bestandsnachweisen erfaßt. Diese sind nicht genügend detailliert, um den Ansprüchen der Übersicht gemäß § 15 Nr. 1 BDSG zu genügen. Dadurch wird sowohl die lückenlose Sicherung der beim Fernmeldeamt verarbeiteten personenbezogenen Daten als auch die Gewährleistung des Auskunftsrechts der Betroffenen in Frage gestellt.

Die festgelegten Mängel im Bereich der Datensicherung betrafen sowohl die Gebäude- und Raumsicherung als auch die Sicherung einzelner besonders sensibler Dateien.

Als problematisch im Bereich der Personaldatenverarbeitung erwies sich der Umstand, daß Personalakten bzw. personalaktenähnliche Vorgänge über die Bediensteten des Fernmeldeamtes an vier verschiedenen Stellen geführt werden (siehe auch 5. TB S. 28). Dies vervielfacht nicht nur die Probleme der Datensicherung, sondern erschwert auch die Durchsetzung des Rechtes eines jeden Bediensteten auf Einsicht in seine vollständigen Personalakten, wie es sich u. a. aus § 90 BBG ergibt. Ich bin hierüber mit dem Bundesminister für das Post- und Fernmeldewesen im Gespräch.

6.2.2 Kontrolle eines Postsparkassenamtes

Die Deutsche Bundespost setzt zur Bewältigung der umfangreichen Datenmengen im Postsparkassen- und Giroverkehr in zunehmendem Maße elektronische Datenverarbeitung ein. Nachdem ich bereits früher ein Postscheckamt kontrolliert habe, ist nunmehr ein Postsparkassenamt geprüft worden.

Die Verarbeitung personenbezogener Daten durch das Postsparkassenamt beschränkt sich im wesentlichen auf Angaben zur Identifizierung der Sparer sowie auf Angaben über die Kontenbewegungen. Für die Verarbeitung der Daten bestehen detaillierte Anweisungen. Die Überprüfung hat keine Anhaltspunkte dafür ergeben, daß nicht erforderliche Daten erhoben, Daten unsachgemäß bearbeitet, Daten unberechtigt offenbart oder Dritten übermittelt werden. Stichproben an verschiedenen Arbeitsplätzen lassen auf einen sorgfältigen Umgang mit personenbezogenen Daten schließen.

Lediglich im Bereich der Organisation des Datenschutzes und der Datensicherung habe ich angeregt, durch geeignete Maßnahmen eine gezielte Verbesserung anzustreben.

6.3 Bekanntgabe von Telefonverbindungsdaten

Zur Thematik der Aufzeichnung und Herausgabe von Einzelverbindungsdaten an den Telefonteilnehmer habe ich mich ausführlich schon in meinem Fünften Tätigkeitsbericht (S. 32 f.) geäußert. Einen Schwerpunkt meiner Gespräche mit dem Bundesminister für das Post- und Fernmeldewesen bildete neuerdings die spezielle Frage der Herausgabe der Zielnummer (Telefonnummer des Angerufenen) in solchen Fällen, in denen die Deutsche Bundespost die Einzelverbindungsdaten von Telefongesprächen registriert. Ausgangspunkt der gegenwärtigen Diskussion, die nun auch im Ausschuß für das Post- und Fernmeldewesen des Deutschen Bundestages geführt wird, war die in meinem Fünften Tätigkeitsbericht (S. 33) aufgeworfene Frage, ob nicht das geltende Verfahren der Post, die Zielnummer dem Inhaber des anrufenden Anschlusses nur auf richterliche Anordnung herauszugeben, eine zu hohe Schwelle bildet. Im Einklang mit entsprechenden Überlegungen der Post habe ich vorgeschlagen, von dieser Praxis abzurücken und Zielnummern

den Teilnehmern auf Antrag aus Gründen der Kostenkontrolle oder -aufteilung bzw. aus Anlaß von Gebührenbeanstandungen mitzuteilen.

Ganz wesentlich kommt es hierbei allerdings darauf an, daß die Post das bislang schon praktizierte Verfahren zum Schutze der Belange der Mitbenutzer des Anschlusses beibehält. Wichtig ist auch, daß es bei den Voraussetzungen für das Erfassen und Speichern von Einzelverbindungsdaten bleibt. Eine vorratsmäßige Speicherung ohne bestimmten Anlaß, die — sei es auch nur für einen bestimmten, zurückliegenden Zeitraum — Auskunft darüber gibt, welche beiden Anschlüsse zu welchem Zeitpunkt miteinander verbunden waren, darf es nicht geben. Dies gilt auch, wenn künftig das Elektronische Wählsystem (EWS) bzw. das geplante digitale System die Aufzeichnung von Einzelverbindungsdaten erleichtern. Als berechtigte Anlässe für eine Speicherung sehe ich lediglich Gebührenbeanstandungen, ferner den Antrag des Postkunden, ihm zwecks Kostenkontrolle oder -aufteilung einen Einzelgebührennachweis zu erstellen und die Fälle der Betriebsstörung und Belästigung.

Die Diskussion dieser Problematik dauert an. Einem Wunsche des Ausschusses für das Post- und Fernmeldewesen entsprechend bereite ich gegenwärtig im Benehmen mit dem Bundespostministerium einen Formulierungsvorschlag für die künftige Handhabung der Herausgabe von Einzelverbindungsdaten vor.

6.4 Neue Techniken im Post- und Fernmeldebereich

6.4.1 Prüfkompetenz des BfD

Sowohl bei der Modernisierung konventioneller Dienste als auch bei neuen Kommunikationstechniken werden ADV-Anlagen eingesetzt. Hierzu gehören auch DATEX-P und das Elektronische Fernsprechsystem EWS. Bei der Durchführung der Dienste verbleiben die zu übermittelnden Daten zum Teil nur kurze Zeit im Speicher des Rechners. Unter Hinweis auf diese kurze Speicherungsdauer hat die Deutsche Bundespost die Anwendbarkeit des BDSG wegen Nichterfüllung des Speicherungsbegriffs nach § 2 Abs. 2 Nr. 1 BDSG verneint. Diese Ansicht ist jedoch weder durch den Wortlaut noch durch den Sinn des Gesetzes gerechtfertigt. Zwar kann z. B. das Auskunftsrecht des Betroffenen bei extrem kurzer Speicherdauer nicht wirksam werden, es bestehen aber zumindest die Sicherungspflichten. Die besondere Gefährdung, die sich für personenbezogene Daten aus ihrer dateimäßigen Verarbeitung ergibt, wird durch eine kurze Speicherdauer nicht etwa aufgehoben. Angesichts der hohen Verarbeitungsgeschwindigkeiten und der daraus resultierenden vielfältigen Auswertungs- und Verknüpfungsmöglichkeiten moderner EDV-Anlagen werde ich mich um den Datenschutz bei rechnergesteuerten Kommunikationsdiensten besonders bemühen.

6.4.2 Bildschirmtext

Der Bildschirmtext-Staatsvertrag der Länder (5. TB S. 38f.) wurde am 18. März 1983 von den Ministerpräsidenten der Länder unterzeichnet; das Ratifizierungsverfahren läuft. Die Datenschutzregelungen im Staatsvertrag entsprechen im wesentlichen den von mir schon früher erhobenen Forderungen. Unbefriedigend ist m. E. die Regelung des Abrechnungsverfahrens. Hier hätte ich ein striktes Verbot der Registrierung von Art und Inhalt in Anspruch genommener Angebote vorgezogen. Außerdem halte ich eine gesetzgeberische Entscheidung für notwendig, inwieweit gesetzliche Durchbrechungen des Fernmeldegeheimnisses (z. B. Gesetz zu Artikel 10 GG) auch für Btx gelten.

Die Deutsche Bundespost hat mit der 22. Änderungsverordnung der Fernmeldeordnung diese um Vorschriften ergänzt, die das Teilnehmerverhältnis im Bildschirmtextdienst regeln. Diese Regelungen, an deren Zustandekommen ich zu meinem Bedauern nicht beteiligt wurde, enthalten nur unvollkommene Bestimmungen zum Datenschutz. Der für 1983 geplante Übergang vom (örtlich begrenzten) Feldversuch zum bundesweiten Wirkbetrieb, in dem auch ein neues EDV-Konzept verwirklicht werden soll, hat sich verzögert. Das neue Btx-Verfahren wird nun voraussichtlich erst Mitte 1984 eingesetzt werden. Eine datenschutzrechtliche Beurteilung, die sowohl die Vorschriften als auch die Wirkungsweise des Systems einbeziehen muß, war mir bisher noch nicht möglich, da die Bundespost meine Fragen nach den für die Beurteilung wesentlichen Einzelheiten der beabsichtigten Datenspeicherungen, -übermittlungen und sonstigen Nutzungen unzureichend bzw. mit störenden Verzögerungen beantwortet hat.

6.4.3 Automatisierung am Postschalter

In einem Praxistest betreibt die Deutsche Bundespost sechs automatisierte Postschalter, die die Kundenbedienung und die Arbeitsbedingungen am Postschalter verbessern sollen. Bei diesem Schalterterminalsystem (STS) handelt es sich um autonome Kleinrechner, die über Standleitungen im Online-Betrieb auf zentral geführte Dateien zugreifen können. Im Rahmen der computermäßigen Abwicklung bestimmter Schaltervorgänge werden — neben Zahlungsdaten — z. B. auch die Nummern von Ausweispapieren, deren Ausstellbehörden sowie die Nummern von Eurocheques und Eurocheque-Karten registriert.

Nach einer bereits erfolgten ersten Information über das STS werde ich prüfen, durch welche technischen und organisatorischen Vorkehrungen der Datenschutz der Betroffenen sichergestellt ist, insbesondere auch welche Datensicherungsmaßnahmen getroffen wurden.

6.5 Sicherheit des Fernsprechnetzes

Bei der Benutzung der Einrichtungen des Fernsprechdienstes der Deutschen Bundespost geht der Bürger davon aus, daß weder vom Inhalt der Nachricht noch von den näheren Umständen der Übermittlung ein anderer als der von ihm angerufene Partner Kenntnis erhält. Sinngemäß gilt dies auch für die Betreiber elektronischer Rechenanlagen, die

Daten auf Leitungen des öffentlichen Fernsprechnetzes übertragen. Ebenso vertraut der Bildschirmtext-Teilnehmer auf die Sicherheit des Fernsprechnetzes (s. auch Nr. 6.4.2). Auch im Berichtszeitraum hat es im In- und Ausland Berichte über gesetzwidriges Mithören von Telefongesprächen oder „Anzapfen" von Computern unter Zuhilfenahme des Fernsprechnetzes gegeben. Ich habe daher wiederholt die Frage gestellt, ob das historisch gewachsene Fernsprechnetz, das in seiner grundsätzlichen Struktur seit Jahrzehnten unverändert geblieben ist, den höheren Anforderungen nach Sicherheit bei der Datenübertragung genügt und ob angesichts der Leistungsfähigkeit und der weiten Verbreitung elektronischer Geräte sowie des hohen technischen Wissenstandes immer noch eine ausreichende Sicherheit gegen unbefugtes Mithören bzw. Aufzeichnen von Nachrichten gegeben ist. Es sollte auch überlegt werden, ob die Deutsche Bundespost besonders sensible (z. B. aus geographischen Gründen) Nachrichtenverbindungen grundsätzlich verschlüsselt durchführen sollte. Ich begrüße daher eine Initiative der Bundesversicherungsanstalt für Angestellte, Daten, die von Berlin (West) an die Beratungsstellen in der Bundesrepublik übermittelt werden, grundsätzlich zu verschlüsseln.

Der Bundesminister für das Post- und Fernmeldewesen hat mich darüber informiert, daß die „Organisation Betriebssicherung im Fernmeldewesen" der Deutschen Bundespost alle geeigneten organisatorischen und betrieblichen Vorkehrungen gegen Eingriffe Unbefugter trifft. In Ergänzung dieser Maßnahmen sollten auch kryptographische Verschlüsselungsverfahren intensiv mit dem Ziel untersucht werden, diese Methoden stärker als bisher zur Sicherung von Datenübertragungen zu nutzen.

6.6 Beschränkung des Brief-, Post- und Fernmeldegeheimnisses

Nach Maßgabe des § 100 a StPO können durch richterliche Anordnung Maßnahmen zur Überwachung und Aufnahme des Fernmeldeverkehrs getroffen werden. Aufgrund einer solchen Anordnung hat die Deutsche Bundespost den zuständigen Stellen das Abhören des Fernsprechverkehrs und das Mitlesen des Fernschreibverkehrs zu ermöglichen. Die Sorgen mancher Bürger hinsichtlich der Gewährleistung des Fernmeldegeheimnisses und des Datenschutzes bei der Deutschen Bundespost haben mich veranlaßt, mir bei einer datenschutzrechtlichen Kontrolle eines Fernmeldeamtes (s. auch Nr. 6.2.1) auch die bei der Bundepost intern zur Durchführung solcher Verfahren erlassenen Arbeitsanweisungen darlegen zu lassen. Als Ergebnis eingehender Erläuterungen habe ich den Eindruck gewonnen, daß jedenfalls bei diesem Fernmeldeamt dem Schutzbedürfnis der Betroffenen soweit wie möglich Rechnung getragen wird. Durch das Verfahren ist insbesondere sichergestellt, daß

— die Anordnung der Maßnahme den rechtlichen Bestimmungen entspricht,

— Irrtümer bzw. Verwechslungen hinsichtlich der Identität des betroffenen Teilnehmeranschlusses ausgeschlossen sind,

— der Deutschen Bundespost die Gesprächsinhalte nicht zugänglich sind.

Ich werde auch bei dem demnächst anstehenden Besuch einer Oberpostdirektion dieser Problematik nachgehen.

7. Verkehrswesen

Der Schwerpunkt meiner Kontroll- und Beratungstätigkeit auf dem Gebiet des Verkehrswesens bezog sich wiederum auf die Arbeit des Kraftfahrt-Bundesamtes in Flensburg (KBA). Kontrollen habe ich beim KBA und beim Bundesministerium für Verkehr durchgeführt. Die Kontrollen erstreckten sich auch auf Fragen der Personaldatenverarbeitung; mit dem Bundesminister für Verkehr habe ich zudem die Datenschutzanforderungen erörtert, die bei der Verarbeitung von personenbezogenen Daten für Zwecke der Verkehrsforschung, insbesondere bei der Verwertung von Einzalangaben aus Bundesstatistiken durch den BMV und von ihm beauftragte Stellen zu beachten sind (s. u. Nr. 9.2).

Weiterhin habe ich mich im Verkehrsbereich mit folgenden Fragen befaßt:

— Zulässigkeit der Speicherung der Namensangaben in Untersuchungsberichten der Flugunfalluntersuchungsstelle beim Luftfahrt-Bundesamt in Braunschweig,

— rechtzeitige Tilgung von Mitteilungen an die Wasser- und Schiffahrtsdirektion Mitte, Hannover, welche Tatsachen betreffen, die eine Entziehung des Sportbootführerscheins oder ein Fahrverbot rechtfertigen können,

— Zulässigkeit der Übermittlung von Personaldaten an Gewerkschaften,

— Behandlung von Personaldaten bei der Bundesanstalt für Flugsicherung und ihrer Regionalstellen.

Aus dem Bereich des Kraftfahrt-Bundesamtes sind folgende Probleme zu erwähnen:

a) bezüglich des Verkehrszentralregisters (VZR)

— Zulässigkeit der Nutzung der VZR-Daten für Zwecke der wissenschaftlichen Forschung,

— Zulässigkeit der Eintragung der Versagung der Fahrerlaubnis sowie der Erteilung der Fahrerlaubnis nach vorangegangener Versagung oder

Entziehung sowie Tilgung solcher Eintragungen,

— Zulässigkeit der Verwertung strafrechtlicher Verurteilungen (§ 50 Abs. 2 BZRG), die sowohl im Bundeszentralregister als auch im Verkehrszentralregister eingetragen sind,

— Sicherstellung der fristgerechten Entfernung tilgungsreifer Eintragungen aus dem Verkehrszentralregister,

— Notwendigkeit der Unterscheidung nach Entziehungsgründen bei Eintragung der Entziehung einer Sonderfahrerlaubnis,

— geplanter Entwurf eines VZR-Gesetzes;

b) *bezüglich der zentralen Erfassung der Kraftfahrzeuge (Zentrales Fahrzeugregister)*

— Zulässigkeit der Erhebung und Speicherung von Berufs- und Gewerbeangaben bei der Zulassung von Fahrzeugen,

— Modalitäten der Nutzung des Adressenmaterials durch Verlage, die nicht mehr zum Kreis der Bezieher von Halteradressen gehören,

— Sicherung der Aktualität des Zentralen Fahrzeugregisters,

— Zulässigkeit der Übermittlung von sogenannten Befassungsdaten (Daten der Zulassung, Umschreibung, Löschung usw. von Fahrzeugen) an Hersteller und Alleinvertriebsberechtigte auf besondere Anforderung oder aufgrund vertraglicher Vereinbarung mit dem KBA,

— Zulässigkeit der Angabe des Löschungsgrundes bei der Abmeldung des Fahrzeugs,

— Zulässigkeit der Übermittlung von Fahrzeug- und Halterdaten an Funkkontrollmeßstellen der Deutschen Bundespost,

— Arbeitsentwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes (Fahrzeugregistergesetz).

Ich verzichte auf die Darstellung von Einzelheiten zu diesen Problemen.

Den breitesten Raum meiner Tätigkeit im Verkehrswesen nahmen wiederum die Fragen der Zulässigkeit und der Ausgestaltung des Zentralen Verkehrsinformationssystems des KBA (ZEVIS) ein. Hierzu ist folgendes zu berichten:

Wie ich im Mai des Berichtsjahres aufgrund eines Sachstandsberichtes des Verkehrsministers erfahren habe, wurde die Pilotphase Ende 1982 abgeschlossen und die Aufbauphase begonnen. Zum Zeitpunkt der Abfassung des Berichts (Nov. 83) enthielt ZEVIS die Fahrzeugbestände der Länder Baden-Württemberg, Schleswig-Holstein, Bayern, Rheinland-Pfalz, des Saarlandes sowie aus Nordrhein-Westfalen die Bestände der Zulassungsbezirke Bonn und Düsseldorf. Damit sind die Daten von annähernd der Hälfte aller zulassungspflichtigen Fahrzeuge sowie alle Fahrzeuge mit Versicherungskennzeichen im Zentralen Verkehrsinformationssystem gespeichert. Daneben enthält das System auch die Grunddaten der im Verkehrszentralregister eingetragenen Personen sowie Hinweise, sofern diesen Personen die Fahrerlaubnis entzogen, versagt oder wieder erteilt oder ein Fahrverbot gegen sie ausgesprochen wurde. Auf diesen Datenbestand greifen zur Zeit die Polizeibehörden der Länder Baden-Württemberg, Bayern, Schleswig-Holstein, Saarland, Hamburg sowie das Bundeskriminalamt und die Grenzschutzdirektion Koblenz im Online-Verfahren zu. Weiteren Ländern sowie 16 Grenzzolldienststellen ist der Zugriff angeboten worden.

Ich habe bereits 1980 in meinem Zweiten Tätigkeitsbericht und erneut in meinem Fünften Tätigkeitsbericht darauf hingewiesen, daß ich den Übergang zum Dauerbetrieb — und dieser wurde mit dem Eintritt in die Aufbauphase vollzogen — nicht für zulässig halte, solange die notwendigen Rechtsgrundlagen fehlen. Die bereichsspezifische Rechtsgrundlage für Auskünfte über Kraftfahrzeughalter, § 26 Abs. 5 StVZO, besteht nur für die örtlichen Zulassungsstellen und gestattet nur Einzelauskünfte. Auch unter Rückgriff auf § 10 BDSG ist ein Online-Anschluß nicht zu rechtfertigen, weil die nach § 2 Abs. 2 Nr. 2 BDSG damit verbundene Übermittlung des gesamten Datenbestandes nicht erforderlich ist.

Der Eintritt in die Aufbauphase und der vorgesehene vollständige Ausbau bis zum Jahre 1984 machte deutlich, daß anscheinend nicht oder nicht mehr die Absicht bestand, die Entscheidung des Gesetzgebers abzuwarten, um die Systemplanungen an den Vorgaben des Gesetzgebers zu orientieren; vielmehr dürfte der Ausbau vollständig vollzogen sein, wenn sich der Deutsche Bundestag anläßlich eines entsprechenden Gesetzentwurfs mit der Angelegenheit befaßt. Abgesehen von der Gefahr, daß der Gesetzgeber präjudiziert wird, ist diese Verfahrensweise aus der Sicht des Datenschutzes nicht zu akzeptieren.

Im Hinblick auf die angestrebten Entscheidungen des Gesetzgebers konnte ich von einer Beanstandung absehen, solange sich das Projekt im Pilotstadium befand. Nach dem Übergang zum Vollausbau ist mir dies nicht mehr möglich gewesen. Ich habe daher das Bereithalten personenbezogener Daten zum Abruf im Rahmen des ZEVIS gemäß § 20 Abs. 1 BDSG beanstandet, weil darin mangels besonderer gesetzlicher Ermächtigung eine unzulässige Übermittlung liegt (Verstoß gegen §§ 3, 2 Abs. 2 Nr. 2, 10 BDSG). Einen Abdruck meines Beanstandungsschreibens habe ich dem Vorsitzenden des Innenausschusses des Deutschen Bundestages zur Aktualisierung meiner Ausführungen im Fünften Tätigkeitsbericht zur Kenntnis gegeben.

Der Bundesminister für Verkehr hält die Beanstandung nicht für gerechtfertigt. Er leitet eine Rechtsgrundlage für ZEVIS aus § 2 Nr. 2 des Gesetzes über die Errichtung eines Kraftfahrt-Bundesamtes vom 4. 8. 1951 (BGBl. I S. 488) ab und betrachtet auch § 10 BDSG als ausreichende Basis für eine Übermitt-

lung im Online-Verfahren. Unbeschadet dessen hält der Bundesminister für Verkehr jedoch eine Verbesserung der Rechtsgrundlagen für ZEVIS für geboten.

Das geltende Straßenverkehrsrecht sieht für das Kraftfahrt-Bundesamt die Aufgabe der Erteilung von Auskünften nur für den Einzelfall und nur für die Daten des Verkehrszentralregisters (§ 30 StVG, § 13c StVZO) sowie die Daten der Fahrzeuge mit Versicherungskennzeichen (§ 29f. Abs. 2 StVZO) vor. Für die Datei der Kraftfahrzeuge mit amtlichen Kennzeichen sind gemäß § 26 Abs. 5 StVZO die Kraftfahrzeugzulassungsstellen befugt, im Einzelfall auf Antrag Auskunft zu erteilen. Weitere Regelungen zur Verwertung der Daten des KBA gibt es zur Zeit nicht.

Im Herbst wurde mir ein erster Arbeitsentwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes vorgelegt, zu dem ich Stellung genommen habe. In den weiteren Beratungen — an denen mich der Verkehrsminister beteiligen will — werde ich auf eine ausreichende rechtliche Regelung hinwirken.

Der Abschluß der Aufbauphase des Zentralen Verkehrsinformationssystems war ursprünglich für 1984 geplant. Das Kraftfahrt-Bundesamt hat mir jedoch inzwischen versichert, bis zu einer Äußerung des Deutschen Bundestages, aus der die Bereitschaft erkennbar ist, die geplanten Informationsstrukturen gesetzlich zu legitimieren, keine weiteren Online-Anschlüsse zu schalten.

Ich habe in meinem Fünften Tätigkeitsbericht angekündigt, mich gemeinsam mit den Landesbeauftragten für den Datenschutz davon zu überzeugen, ob Anhaltspunkte für unbefugte Datenabrufe erkennbar sind. Die Verpflichtung, die Kontrollierbarkeit des Zugriffs auf ZEVIS sicherzustellen, trifft in erster Linie das KBA. Hierzu gehören nicht nur die rein technische Kontrollierbarkeit des Zugriffs, sondern auch Abreden zwischen den am Verfahren beteiligten Stellen über die tatsächliche Handhabung solcher Kontrollen und gegebenenfalls Einzelheiten des Verfahrens.

Im Oktober des Berichtsjahres hatte ich Gelegenheit, zusammen mit dem Bayerischen Datenschutzbeauftragten an einer Demonstration der Nutzung des Zentralen Verkehrsinformationssystems durch die bayerische Landespolizei beim Bayerischen Landeskriminalamt teilzunehmen. Dabei bin ich insbesondere der Frage nachgegangen, ob die vom KBA und vom LKA erstellten Protokolle ausreichen, um feststellen zu können, welche Polizeidienststellen mittels Terminal zu welchem Zeitpunkt welche Daten aus dem Zentralen Verkehrsinformationssystem erhalten haben. Dies erwies sich zum Teil als unmöglich. Die Protokolle wichen sowohl vom Aufbau als auch vom Inhalt her so stark voneinander ab, daß eine Zuordnung der Anfragen nicht möglich war. Ich habe das KBA entsprechend unterrichtet und auf seine Verantwortung hingewiesen.

Strittig ist nach wie vor die Frage der Zulässigkeit der P-Anfrage im Online-Verfahren, d. h. der Möglichkeit, den zentralen Bestand der Kraftfahrzeuge und der Fahrzeuge mit Versicherungskennzeichen mittels Namensangabe im Online-Verfahren zu erschließen (s. 5. TB S. 42f.). Die Erforderlichkeit dieser Zugriffsmöglichkeit, die ich in Frage gestellt habe, wurde bisher nur sehr allgemein begründet. Eine eingehende Begründung der spezifischen polizeilichen Informationsbedürfnisse ist jedoch wegen der großen Tragweite dieser Maßnahme unerläßlich. Eine solche mit den Ländern abgestimmte Begründung wurde mir vom Bundesminister des Innern vor längerer Zeit zugesagt, aber bisher noch nicht zugeleitet.

8. Bildung und Ausbildung

Im vergangenen Jahr habe ich eine Prüfung bei der Bundesakademie für öffentliche Verwaltung und bei der Fachhochschule des Bundes durchgeführt.

Bei der Bundesakademie waren nur geringfügige Verbesserungen zu empfehlen. Dagegen hatte die Fachhochschule des Bundes die gesetzlich vorgeschriebenen Maßnahmen zur Durchführung des Datenschutzes erst im unmittelbaren zeitlichen Zusammenhang mit der Prüfungsankündigung in die Wege geleitet. Inzwischen hat mir der Bundesminister des Innern mitgeteilt, daß die meisten der beanstandeten Mängel beseitigt seien und noch ausstehende Verbesserungen kurzfristig vorgenommen werden sollen.

9. Statistik

9.1 Volkszählung

Die für 1983 geplante Volkszählung war das zentrale Datenschutzereignis des vergangenen Jahres. Das Vorhaben bewirkte, daß das Thema Datenschutz die Schlagzeilen auch der überregional erscheinenden Presseorgane, die Berichterstattung in Rundfunk und Fernsehen und die öffentliche Diskussion beherrschte. Die Verfassungsbeschwerden gegen das Volkszählungsgesetz haben dazu geführt,

daß Fragen des Datenschutzes vor dem Bundesverfassungsgericht eingehend erörtert wurden. Das am 15. Dezember 1983 verkündete Urteil hat für die datenschutzrechtlichen Bedingungen staatlicher Informationsbeschaffung entscheidende Maßstäbe gesetzt.

Diese Entwicklung, insbesondere das Ausmaß und die Vielfalt an Meinungsäußerungen, kam für die meisten Beteiligten überraschend, obwohl der Bundesbeauftragte für den Datenschutz in seinem Ersten Tätigkeitsbericht (für das Jahr 1978) die gleichen Mängel aufgezeigt hatte, die jetzt die Diskussion bestimmt haben.

Für viele Kenner der Materie stand die Intensität des Protests in keinem angemessenen Verhältnis zu dem tatsächlichen Ausmaß der von dieser Volkszählung ausgehenden Gefahr für die Rechte des Bürgers. Daran ist sicher richtig, daß nicht nur die realen Datenschutzprobleme der Volkszählung, wie Mängel des Volkszählungsgesetzes oder Mängel der staatlichen Aufklärungsarbeit, ursächlich für diesen Protest waren. Vielmehr dürften allgemeine, irrationale Ängste vor neuen Informationstechniken, verstärkt durch den Mangel an Transparenz staatlichen Handelns, hinzugekommen sein. Bei manchen Beteiligten kam auch der Eindruck auf, daß einige Gegner der Volkszählung mit ihrem Boykott nicht vorrangig Datenschutzinteressen, sondern andere politische Ziele verfolgten.

Dies ist aber auch nicht entscheidend. Von maßgeblicher Bedeutung ist m. E. vielmehr, daß die Auseinandersetzung um die Volkszählung auch einen Mangel an Vertrauen von Teilen der Bevölkerung zum Staat deutlich gemacht hat. Nur so ist verständlich, daß die Ablehnung der Volkszählung eine so breite Basis in fast allen Schichten der Bevölkerung finden konnte. Wie die Diskussion um die Einführung des maschinenlesbaren Personalausweises gezeigt hat, können vergleichbare Manifestationen dieser Vertrauenskrise in neuen Zusammenhängen immer wieder auftreten. Sie behindert zum einen staatliche Funktionen, zum anderen beeinträchtigt sie — und das ist jedenfalls im Hinblick auf den Datenschutz besonders wichtig — die Ausübung von verfassungsrechtlich verbürgten Grundrechten: Bürger, die befürchten, daß ihre Lebensäußerungen — für sie nicht wahrnehmbar oder in ihren Konsequenzen für sie nicht abschätzbar — registriert werden, werden ihr Verhalten danach ausrichten und möglicherweise ihr verfassungsrechtlich verbürgtes Recht auf freie Entfaltung der Persönlichkeit nur eingeschränkt nutzen.

Richtig verstandener Datenschutz erfordert deshalb nicht nur einen Schutz der Daten vor ihrer mißbräuchlichen Verwendung, sondern — wie jetzt auch das Bundesverfassungsgericht bestätigt hat — außerdem Transparenz, genauer gesagt, die Erkennbarkeit der materiellen Legitimation staatlicher Informationsbeschaffung und -verarbeitung. Es muß zumindest im Grundsatz allgemein erkennbar sein, welche Stellen welche personenbezogenen Daten erhalten und für welche Zwecke die Daten tatsächlich genutzt werden können. Es muß nachvollziehbar sein, daß keine Stelle mehr Informationen erhält, als tatsächlich erforderlich ist, und daß kein Bürger dadurch unverhältnismäßig beeinträchtigt wird. Zu der Sorge vor einer gesetzlich nicht zugelassenen Verwendung der Daten, also vor ihrem Mißbrauch, kommt im übrigen auch die Befürchtung, schon das Gesetz könne unverhältnismäßig belastende Wirkungen haben. Dies hat die Volkszählungsdiskussion deutlich gezeigt.

Diese Umstände habe ich auch bei der Arbeit des letzten Jahres berücksichtigt:

Vorrangig haben die Datenschutzbeauftragten des Bundes und der Länder in zahlreichen gemeinsamen Gesprächen und in Verhandlungen mit den zuständigen Stellen beim Bund und in den Ländern versucht, die tatsächlichen und wesentlichen Datenschutzprobleme im Zusammenhang mit der Volkszählung zu lösen, soweit dies auf der Grundlage des Volkszählungsgesetzes 1983 möglich war. Das Ergebnis war der gemeinsame Forderungskatalog der Datenschutzbeauftragten vom 22. März 1983, der alle realisierbaren Datenschutzforderungen noch einmal zusammenfaßte.

Darüber hinaus habe ich mich bemüht, den Mangel an Verständlichkeit beim Volkszählungsgesetz und die Defizite an öffentlicher Aufklärung auszugleichen. In den drei Monaten vor dem vorgesehenen Erhebungstermin wurden teils individuell, teils durch Zusenden einer Informationsschrift hunderte von Eingaben beantwortet. Die Informationsschrift mit dem Titel „Zwölf Fragen zum Thema: Datenschutz bei der Volkszählung" wurde in zwei Auflagen gedruckt. Sie gab Antworten zu den am häufigsten an mich herangetragenen Fragen und lieferte den Betroffenen erstmals einen Abdruck des Fragebogens mit Erläuterungen und die maßgeblichen gesetzlichen Bestimmungen. Diese Informationsschrift habe ich zusammen mit einer Presseerklärung in mehreren hundert Exemplaren auch den Medien zur Verfügung gestellt. Außerdem haben mein Amtsvorgänger und die Mitarbeiter der Dienststelle in vielen Interviews von Presse und Rundfunk und in zahlreichen abendlichen Veranstaltungen von Verbänden und Parteien Fragen zum Thema Datenschutz bei der Volkszählung beantwortet. Diese Aufklärungsarbeit sollte zu einer objektiven Sicht der Problematik beitragen und auch Ängste, soweit sie unbegründet oder übertrieben erschienen, abbauen helfen. Das war mitunter deshalb schwierig, weil die von den Medien geprägte öffentliche Meinung von den Datenschutzbeauftragten weitgehend eine bedingungslose Ablehnung der gesamten Volkszählung erwartete und weil Persönlichkeiten des öffentlichen Lebens sich teilweise — ohne Differenzierung und Begründung — der Volkszählungskritik anschlossen.

Eingehend hat der Bundesbeauftragte für den Datenschutz dann auch gegenüber dem Bundesverfassungsgericht zu den Problemen der Volkszählung Stellung genommen. Im Verfahren zum Erlaß einer einstweiligen Anordnung hat sich mein Amtsvorgänger schriftlich und mündlich geäußert; ich selbst habe dies nach der Amtsübernahme im Hauptver-

fahren getan. Diese Stellungnahmen machten deutlich, daß die speziellen Datenschutzprobleme der Volkszählung wegen der schnellen Entwicklung der Informationstechnologie und der damit parallel verlaufenden Bewußtseinsänderung in der Bevölkerung vor allem in der fehlenden Transparenz für den Bürger liegen, und daß der vorgesehene Melderegisterabgleich zugleich eine Verletzung seines Vertrauens in eine rein statistische Verwendung seiner Daten bewirkt. In meiner mündlichen Stellungnahme sind die wesentlichen Gesichtspunkte zusammengefaßt. Sie ist als Anlage 1 zu diesem Bericht wiedergegeben.

Das Bundesverfassungsgericht hat in seinem Urteil meine Einschätzung bestätigt und fast alle Empfehlungen der Datenschutzbeauftragten aufgegriffen. Dabei ist zunächst festzuhalten, daß das Gericht nicht nur die Zulässigkeit der Volkszählung beim derzeitigen Stand der Technik bejaht hat, sondern gerade auch unter Berücksichtigung der besonderen Bedeutung solcher Erhebungen für rationale politische Entscheidungen einen Weg aufgezeigt hat, wie das für eine funktionsfähige Statistik notwendige Vertrauen des Bürgers in die Erforderlichkeit und Verhältnismäßigkeit der Befragung und in eine rein anonyme Verwendung seiner Daten wiedergewonnen werden kann.

Die in diesem Zusammenhang aus meiner Sicht wichtigsten Aussagen sind — in Grundzügen — folgende:

Zunächst wird durch das Urteil erneut deutlich, daß die Verhältnismäßigkeit einer Auskunftspflicht des Bürgers nicht immer schon deshalb bejaht werden kann, weil die Angaben nur für statistische Zwecke (also nicht personenbezogen) verwendet werden sollen. Der Verhältnismäßigkeitsgrundsatz verbietet nach Aussage des Gerichts vielmehr auch lediglich zur statistischen Auswertung bestimmte Fragen, wenn sie für den Betroffenen die Gefahr der sozialen Abstempelung hervorrufen können. Das Gericht weist im Zusammenhang mit der für die Volkszählung vorgesehenen Frage, ob man Insasse einer Anstalt ist (oder zum Personal gehört), darauf hin, daß eine personenbezogene Erhebung für diesen Fall nicht notwendig sei, weil diese Angaben summenmäßig erhoben werden könnten. Ich hatte das Gericht auf meine Bedenken gegen diese Frage hingewiesen.

Als eine weitere wichtige Voraussetzung für eine verfassungskonforme Statistik nennt das Gericht besondere Vorkehrungen für Durchführung und Organisation der Datenerhebung und -verarbeitung. Die Vorkehrungen, die das Gericht im einzelnen für erforderlich hält, entsprechen im wesentlichen den Empfehlungen aus dem Forderungskatalog der Datenschutzbeauftragten vom 22. März 1983, zu dessen Beachtung sich jedenfalls einige Länder verpflichtet hatten und der dem Gericht vorgelegen hat:

— Durch Aufklärung und Belehrung müsse der Bürger auf seine Rechte hingewiesen werden, etwa darauf, daß jeder einen eigenen Erhebungsbogen erhalten und ihn auf verschiedenen Wegen zurücksenden kann; freiwillige Angaben müßten deutlich als solche kenntlich gemacht werden.

— Die jeweils frühestmögliche Abtrennung und Löschung der zur Identifizierung dienenden Merkmale sei zur Grundrechtssicherung erforderlich und könne daher nicht im Ermessen der Verwaltung stehen. Die Sollvorschrift des § 11 Abs. 7 BStatG genügt dem Gericht hier offensichtlich nicht.

— Bei der Auswahl der Zähler müßten Interessenkollisionen möglichst vermieden werden. Außerdem sei ein Einsatz in unmittelbarer Nähe ihrer Wohnung auszuschließen.

— Der Gesetzgeber müsse auch dafür Sorge tragen, daß der Inhalt des Fragebogens mit dem Gesetz übereinstimmt. Das Gericht läßt ausdrücklich offen, in welcher Weise der Gesetzgeber diese Pflicht erfüllt, nennt als Möglichkeit aber die Ermächtigung, den Inhalt des Fragebogens durch Rechtsverordnung festzulegen.

Mindestens ebenso wichtig ist, daß das Gericht die Übermittlung von personenbezogenen Angaben, die für eine Statistik gemacht wurden, allenfalls unter strengen Voraussetzungen für zulässig hält und die Bestimmungen des § 9 Abs. 1 bis 3 VZG danach als nicht verfassungsgemäß aufgehoben hat. Das Gericht hat also nicht die sonst häufig gewählte Methode der verfassungskonformen Auslegung gewählt, sondern die Verfassungswidrigkeit dieser Bestimmungen bereits darin erkannt, daß der Bürger aus ihnen nicht hinreichend deutlich erkennen kann, welche Verwendungen zu Verwaltungsvollzugszwecken erlaubt und welche ausgeschlossen sind. Daraus wird deutlich, daß die für eine funktionsfähige Statistik und für eine reale Grundrechtsgewährleistung notwendige Vertrauensgrundlage zwischen Bürger und Staat nicht Zweckmäßigkeits- oder Wirtschaftlichkeitserwägungen geopfert werden darf und Forderungen des Datenschutzes sich aus wirtschaftlichen Gründen nicht einfach reduzieren lassen.

Den in § 9 Abs. 1 VZG vorgesehenen Melderegisterabgleich hält das Gericht im übrigen schon deshalb mit der Verfassung nicht für vereinbar, weil durch ihn tendenziell Unvereinbares miteinander verbunden wird. Das Gericht weist darauf hin, daß einerseits die Effizienz der Statistik eine strenge Beachtung des Statistikgeheimnisses verlangt, während andererseits das Melderecht sehr weitreichende und in ihren Auswirkungen von den Betroffenen nicht abschätzbare Datenübermittlungen vorsieht. Damit ist das Bundesverfassungsgericht Bedenken gefolgt, die der Bundesbeauftragte für den Datenschutz schon in seinem Ersten Tätigkeitsbericht (S. 20) geäußert hatte.

Noch größere Auswirkungen als die Aussagen des Gerichts, die sich speziell auf den Bereich der amtlichen Statistik und hier der Volkszählung beziehen, werden die Aussagen haben, die allgemein die Ver-

arbeitung personenbezogener Daten durch den Staat zu den Grundrechten des einzelnen in Beziehung setzen und daraus in jedem Fall zu beachtende Rahmenbedingungen für die staatliche Informationsbeschaffung und -verarbeitung herleiten.

Von fundamentaler Bedeutung für jede staatliche Datenverarbeitung ist vor allem, daß das Gericht aus Artikel 2 Abs. 1 i. V. m. Artikel 1 Abs. 1 des Grundgesetzes ein Recht des einzelnen auf informationelle Selbstbestimmung hergeleitet hat. Der einzelne hat danach grundsätzlich die Befugnis, nicht nur über die Preisgabe, sondern auch über die Verwendung seiner persönlichen Daten selbst zu bestimmen. Die Diskussion, ob der Grundrechtskatalog (nach ausländischem und nordrhein-westfälischem Vorbild) um ein Grundrecht auf Datenschutz erweitert werden soll, dürfte durch die Anerkennung dieses Rechts gegenstandslos geworden sein.

Das bedeutet zwar keinen Verlust an wirklich notwendigen Informationen für Staat und Gesellschaft, weil das Gericht auch die Schranken des informationellen Selbstbestimmungsrechts betont und die Möglichkeiten der Grundrechtseinschränkung im überwiegenden Allgemeininteresse aufgezeigt hat, es macht aber eine eingehende Prüfung erforderlich, ob nicht in vielen Bereichen eine Neuorientierung des Datenschutzes erforderlich ist. Es stehen Fragen von grundlegender, auch politischer Bedeutung mit weitreichenden Konsequenzen an: Etwa die Frage, ob sich aus dem Bundesdatenschutzgesetz Voraussetzungen und Umfang der Beschränkungen des informationellen Selbstbestimmungsrechts für den Bürger klar erkennbar ergeben, wie das Gericht es gefordert hat.

Von noch größerer Tragweite dürfte die Feststellung des Gerichts sein, daß die Verarbeitung personenbezogener Daten durch den Staat jedenfalls dann, wenn die Daten unter Zwang erhoben werden, nach unserer Verfassung nur dann zulässig ist, wenn der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt hat.

Erhebliche Auswirkungen auf die Praxis der Datenübermittlungen im staatlichen Bereich wird schließlich die Aussage haben, daß die Verfassung einen amtshilfefesten Schutz personenbezogener Daten gegen Zweckentfremdung durch Weitergabe- und Verwertungsverbote fordert.

Zu einer Verbesserung der Rechtsstellung des einzelnen wird das Votum des Gerichts für eine unabhängige Datenschutzkontrolle beitragen. Das Gericht hat darauf hingewiesen, daß die Tätigkeit unabhängiger Datenschutzbeauftragter von erheblicher Bedeutung für einen effektiven Schutz des durch die Verfassung verbürgten Rechts auf informationelle Selbstbestimmung ist. Damit wird bestätigt, daß wirksame Datenschutzkontrolle eine wesentliche Bedingung verfassungsmäßiger Datenverarbeitung ist. Indem das Gericht diese Feststellung für einen Bereich getroffen hat, für den eine besondere Geheimhaltungspflicht — das Statistikgeheimnis — gilt, hat es zugleich auch verdeutlicht, daß spezielle Berufs- und Amtsgeheimnisse einer Datenschutzkontrolle, die gerade die Einhaltung dieser Geheimhaltungspflichten mit gewährleisten soll, nicht entgegengehalten werden können. Aus gegebenem Anlaß weise ich darauf hin, daß es mit diesen Feststellungen nicht zu vereinbaren wäre, die Befugnis der Datenschutzbeauftragten, die Einhaltung z. B. des Steuergeheimnisses durch Einsicht in die Datenbestände der Finanzverwaltung zu prüfen, unter Hinweis auf diese Geheimhaltungspflichten zu verneinen.

Damit sind nur einige Sätze des Urteils von offenkundig übergreifender Bedeutung genannt. Eine erschöpfende Darstellung der aus dem Urteil folgenden Konsequenzen ist der Analyse vorbehalten, die ich dem Bundestag vorlegen werde.

9.2 Datenschutz bei Empfängern statistischer Einzelangaben

Einige Gesetze, die eine Bundesstatistik anordnen, gestatten es den Statistischen Ämtern, gemäß § 11 Abs. 3 Bundesstatistikgesetz (BStatG) nicht vollständig anonymisierte Daten aus Bundesstatistiken an oberste Bundes- und Landesbehörden oder an von diesen bestimmte Stellen zu übermitteln. Solche Regelungen enthält auch das Volkszählungsgesetz 1983.

Ich habe deshalb zunächst bei zwei Ministerien, die in besonderem Maße als Empfänger von Statistikdaten in Frage kommen, die Vorkehrungen überprüft, die die Einhaltung des Statistikgeheimnisses (§ 11 BStatG) gewährleisten sollen. In einem Fall waren dem Ministerium nur geringfügige Verbesserungen vorzuschlagen. In dem anderen Fall konnte mir das Ministerium zunächst nur einen Fall nennen, in welchem Einzelangaben aus Bundesstatistiken auf Veranlassung des Ministeriums an ein Forschungsinstitut übermittelt worden sind. Nunmehr wurde mir mitgeteilt, daß eine Reihe weiterer Übermittlungsvorgänge, die teilweise periodisch wiederholt werden, bekanntgeworden seien. Zu der Frage, ob der Schutz weitergeleiteter statistischer Einzelangaben in dem aufgezeigten Bereich gewährleistet ist, kann ich unter diesen Umständen noch keine Aussage machen.

10. Sozialverwaltung — Allgemeines

10.1 Beachtung des Sozialgeheimnisses

Bei den Leistungsträgern der sozialen Sicherung wird dem Datenschutz, wie ich bei vielen Gelegenheiten feststellen konnte, schon traditionell wegen der Schutz- und Geheimhaltungsbedürftigkeit der ihnen anvertrauten Sozialdaten ein hoher Stellenwert eingeräumt. Das hauptsächliche Problem besteht deshalb nicht darin, durch die Kontrolle der Einhaltung datenschutzrechtlicher Vorschriften (§ 19 Abs. 1 BDSG) „Mißbräuche" zu verhindern oder aufzudecken; vielmehr sind es oft nur mangelnde Überlegung oder bloße Nachlässigkeiten, die in der täglichen Verwaltungsroutine Verstöße gegen die recht komplizierten Vorschriften über das Sozialgeheimnis und über den Schutz der Sozialdaten verursachen. Sie können aber im Einzelfall durchaus eine nicht unerhebliche Beeinträchtigung schutzwürdiger Belange des Betroffenen bewirken.

Zur Verdeutlichung seien als Beispiele hierfür genannt:

— Eine Krankenkasse hat das Arbeitsgericht um Auskunft über den Ausgang eines dort anhängigen Verfahrens gebeten und zur Begründung angegeben, daß der Versicherte Arbeitsunfähigkeitszeiten teilweise ohne Vorlage einer ärztlichen Bescheinigung gemeldet habe; auch seien Untersuchungen beim vertrauensärztlichen Dienst erschwert worden, weil der Versicherte sich geweigert habe, Angaben über Vorerkrankungen zu machen.

  Die Offenbarung dieser Einzelheiten war für die Aufgabenerfüllung der Krankenkasse nicht erforderlich (§ 69 Abs. 1 Nr. 1 SGB X) und daher unzulässig. Auf die Klage des Betroffenen hat das Sozialgericht in seinem Urteil festgestellt, daß die beklagte Krankenkasse durch ihre Mitarbeiter dem Arbeitsgericht unbefugt ein Sozialgeheimnis des Klägers offenbart habe.

— Eine Betriebskrankenkasse teilte der Zahlstelle bei ihrer Trägerfirma mit standardisierten Schreiben in den zutreffenden Fällen regelmäßig mit, daß Krankengeld nicht mehr zu zahlen sei, weil der Betreffende zur amtsärztlichen Untersuchung nicht erschienen ist, oder daß Mutterschaftsgeld ab einem bestimmten Zeitpunkt wegen vorzeitiger Niederkunft zu zahlen sei.

  In beiden Fällen ist die Angabe des Grundes für die Einstellung bzw. für den Beginn der Zahlung für die Aufgabenerfüllung der Krankenkasse nicht erforderlich (§ 69 Abs. 1 Nr. 1 SGB X) und stellt damit eine unzulässige Offenbarung von Sozialdaten dar. Auf meine Beanstandung hin wurden diese Mitteilungen eingestellt.

10.2 Aufklärungs- und Hinweispflichten

Ein anderes Defizit bei der Umsetzung datenschutzrechtlicher Vorschriften, das bereits im letzten Tätigkeitsbericht (5. TB S. 51/52) näher beschrieben wurde, ist die mangelhafte Aufklärung des Bürgers über seine Mitwirkungs- und Mitteilungspflichten. Auch in diesem Jahr habe ich häufig derartige Fälle festgestellt. Nach wie vor scheint man in diesem Zusammenhang die Vorschriften über die Aufklärungs- bzw. Hinweispflichten (§§ 14, 66 Abs. 3 SGB I, § 9 Abs. 2 BDSG) mehr als lästige Formalie denn als Aufgabe zu sehen. Als Hinweis gemäß § 9 Abs. 2 BDSG reicht es nicht aus, wenn ein Leistungsträger auf einem Fragebogen lediglich den Stempelaufdruck „die Daten werden aufgrund § 21 des Zehnten Buches Sozialgesetzbuch (SGB X) erhoben" anbringt (der in dem konkreten Fall einer Bürgereingabe auch noch unterlassen worden war). Dieser Hinweis klärt den Betroffenen nicht auf; er konfrontiert ihn mit einer Vorschrift, deren Inhalt er nicht kennt und deren Tragweite selbst für den Rechtskundigen problematisch ist.

Ständig wird viel Zeit und Mühe aufgewendet für die Bewältigung der vielfältigen Aufgaben und für die Entwicklung neuer Formblätter zur Anpassung an veränderte Rechtslagen. Ein vergleichsweise geringer Teil dieses Aufwandes würde genügen, um den Betroffenen über seine Auskunfts- und Mitwirkungspflichten richtig und verständlich zu beraten, wie dies das Gesetz, nicht etwa der Bundesbeauftragte für den Datenschutz, verlangt.

Um auch von meiner Seite im Rahmen meiner Möglichkeiten zum Abbau dieses Aufklärungsdefizits beizutragen, habe ich zur Unterrichtung des Bürgers eine allgemeine Informationsschrift über Inhalt und Wirkungen des Sozialdatenschutzes herausgegeben (s. auch oben Nr. 1.4). In dieser Broschüre „Der Bürger und seine Daten im Netz der sozialen Sicherung" sind u. a. die allgemeinen Grundsätze der Auskunfts- und Mitwirkungs*pflichten* des Bürgers bei der Inanspruchnahme von Sozialleistungen bzw. bei der Durchführung der Sozialversicherung sowie seine Auskunfts- und Einsichts*rechte* in jeweils besonderen Kapiteln erläutert.

10.3 Datenschutzdefizite im Sozialrecht

Gelegentlich sind Datenschutzprobleme nicht das Ergebnis einer schlechten Verwaltungspraxis, sondern mittelbare Folge gesetzgeberischer Entscheidungen. Diese Feststellung mit einem Beispiel dafür steht bereits im letzten Tätigkeitsbericht (5. TB S. 52). Ein weiteres Beispiel ist § 205 Abs. 4 der Reichsversicherungsordnung, wonach für ein Kind die Krankenkasse desjenigen Elternteils leistungspflichtig ist, für den im letzten Monat vor Eintritt des Leistungsfalles der höhere Beitrag zu entrichten war. Diese Regelung führt in manchen Fällen zu einer zwar rechtmäßigen, nach dem Grundsatz der Verhältnismäßigkeit aber nicht zu vertretenden Offenbarung von Sozialgeheimnissen:

Im Falle eines nichtehelichen Kindes wurde durch den zur Durchführung dieser Vorschrift geführten

Schriftwechsel der Krankenkasse der Mutter die bis dahin streng geheimgehaltene Identität des Vaters bekannt; der Krankenkasse des Vaters wurde die Existenz eines nichtehelichen Kindes sowie Name und Anschrift der Mutter (und weitere unter das Sozialgeheimnis fallende Einzelangaben) offenbart. In diesem Einzelfall konnte ich wenigstens erreichen, daß die personenbezogenen Daten des Vaters bei der Krankenkasse der Mutter gelöscht wurden (§ 84 SGB X); die Krankenkasse des Vaters untersteht nicht meiner Zuständigkeit.

Das System der Familienhilfe in der gesetzlichen Krankenversicherung führt darüber hinaus in manchen Fällen zu einer Diskrepanz der Geheimhaltungsvorschriften des § 35 SGB I: Nach § 205 Abs. 1 RVO erhält der Versicherte für den unterhaltsberechtigten Ehegatten Krankenhilfe und sonstige Hilfen; der Ehegatte selbst hat keinen Anspruch aus eigenem Recht. Das bedeutet beispielsweise, daß die Mehrkosten bei aufwendigeren Hilfsmitteln (§ 182b RVO) für die Ehefrau der versicherte Ehemann zu tragen hat. Dabei hat er der Kasse die notwendigen Verschreibungs- und Rechnungsunterlagen vorzulegen; die Abrechnung der Kasse mit in der Regel genauer Bezeichnung der Hilfsmittel wird ihm zugestellt.

In einem Fall ist auf diese Weise dem Versicherten offenbart worden, daß seine getrennt lebende Ehefrau eine Brustprothese trägt. Diese zunächst unvermeidbar erscheinende Offenbarung steht im Widerspruch zu Sinn und Zweck des § 35 SGB I. Danach hat *jeder* Anspruch darauf, daß Einzelangaben über seine persönlichen (besonders seine gesundheitlichen) und sachlichen Verhältnisse von den Leistungsträgern als Sozialgeheimnis gewahrt werden. Die betreffende Kasse hat zwar eine organisatorische Lösung gefunden, die künftig derartige Offenbarungen ausschließt. Eine generelle Lösung würde m. E. jedoch eine gesetzliche Regelung voraussetzen, z. B. durch Begründung eines eigenen Leistungsanspruches für den Angehörigen.

11. Arbeitsverwaltung

11.1 Eingaben

Die laufende Arbeit im Bereich der Arbeitsverwaltung, insbesondere aufgrund von Bürgereingaben, hat sich auf Probleme konzentriert, über die schon mehrfach, zuletzt im Fünften Tätigkeitsbericht (S. 58) berichtet wurde:

— Nach wie vor erreichen mich viele Eingaben, in denen über das Verfahren bei der Gewährung von Arbeitslosenhilfe Beschwerde geführt wird. Meiner eindringlichen Bitte, das Verfahren betroffenengerecht zu gestalten — was unschwer möglich wäre — hat sich die Bundesanstalt für Arbeit in ihrer Stellungnahme zum Fünften Tätigkeitsbericht nach wie vor verschlossen. Ich kann deshalb nur nochmals eindringlich bitten, das Verfahren zu ändern.

— In der Praxis gibt es weiterhin Schwierigkeiten bei der Handhabung des Akteneinsichtsrechts gemäß § 25 SGB X bzw. des Auskunftsrechts gemäß § 13 BDSG. Der Erlaß, den die Bundesanstalt hierzu 1982 angekündigt hat, ist bisher nicht fertiggestellt.

  Drei diesbezügliche Eingaben habe ich vor Ort überprüfen lassen. In einem Fall, der die Aufbewahrung von veralteten ärztlichen Gutachten betraf, habe ich eine Beanstandung gemäß § 20 BDSG ausgesprochen. Eine Antwort der Bundesanstalt hierzu steht noch aus. In einem anderen Fall habe ich erreicht, daß bestimmte, aus der Sicht des Betroffenen diskriminierende medizinische Feststellungen aus den Unterlagen entfernt wurden.

  Allerdings hat sich in diesen Fällen auch gezeigt, daß die Kenntnis aller Unterlagen und die Aushändigung von Kopien allein noch nicht ausreicht, um das Mißtrauen der Arbeitslosen gegen das Arbeitsamt abzubauen.

11.2 Entwicklung der Datenverarbeitung

Wie ich in meinem Fünften Tätigkeitsbericht (S. 55) ausführlich berichtet habe, wird der Einsatz der Informationstechnik vor allem im Bereich der Arbeitsvermittlung mit großer Kraft vorangetrieben. Hierzu fühlt sich die Bundesanstalt insbesondere durch mehrere Gutachten von Unternehmensberatungen ermutigt, die seit Mitte des Jahres vorliegen.

Im Jahre 1984 werde ich mich vorrangig mit den durch die neuen Informationstechniken auftretenden Problemen befassen.

11.3 Kindergeld

Am 1. Januar 1983 ist die neue Kindergeldregelung mit einer einkommensabhängigen Staffelung der Kindergeldbeträge für das zweite und jedes weitere Kind in Kraft getreten. Seither erreichte mich eine große Zahl von Bürgereingaben, die sich mit Fragen des Datenschutzes bei der Durchführung dieser neuen Regelung, insbesondere hinsichtlich der Erforderlichkeit und des Umfanges der Ermittlung und des Nachweises des maßgeblichen Einkommens befassen.

Infolge mangelnder Aufklärung der Betroffenen über bestehende Auskunfts- bzw. Mitwirkungspflichten (vgl. auch oben Nr. 10.2) wurde in fast allen Eingaben die Frage gestellt, ob eine rechtliche Verpflichtung bestehe, die Einkommensverhältnisse in dem verlangten Umfang offenzulegen. Ich habe die Bundesanstalt für Arbeit und die zuständigen obersten Bundesbehörden auf die Belehrungspflicht des § 9 Abs. 2 BDSG hingewiesen und dazu einen Formulierungsvorschlag gemacht, der in der notwendigen Ausführlichkeit die Mitwirkungspflichten und die Folgen fehlender Mitwirkung darstellt. In die entsprechenden Fragebögen der Arbeitsämter wurde dann aber lediglich folgender Hinweis aufgenommen:

„Nach den Vorschriften zum Datenschutz müssen Sie darauf hingewiesen werden, daß Ihre Angaben freiwillig sind. Sie brauchen keine Angaben zu machen; allerdings kann bei fehlenden Angaben oder Nachweisen das Kindergeld ganz oder teilweise entzogen werden."

Dieser im Ergebnis zwar richtige, aber in seiner Kürze wenig bürgerfreundliche und von manchen Bürgern als „erpresserisch" empfundene Hinweis hat zu weiteren Eingaben an mich geführt.

Materiell stand und steht die Frage im Mittelpunkt, ob es erforderlich (und damit zulässig) ist, die nach § 10 Abs. 2, § 11 Abs. 2 BKGG maßgebliche Summe der positiven Einkünfte (Jahreseinkommen) bei der Erhebung in die einzelnen Einkunftsarten — getrennt nach Ehegatten — aufzuschlüsseln und dazu als Nachweis in allen Fällen die Vorlage des Einkommenssteuerbescheids zu verlangen. Ich habe dazu die Auffassung vertreten, daß aufgrund des Wortlauts der genannten Vorschriften eine Aufschlüsselung nach Einkunftsarten nicht verlangt werden kann. Wegen der möglichen Schwierigkeiten für viele Betroffene, das maßgebliche Jahreseinkommen in einer Summe richtig anzugeben, habe ich angeregt, den Betroffenen für den eigenen Gebrauch ein Berechnungsschema anzubieten.

Die Datenschutzbeauftragten des Bundes und der Länder haben in einem gemeinsamen Beschluß ebenfalls gefordert, nur die maßgebliche Summe der positiven Einkünfte zu erheben, nicht aber deren Aufschlüsselung in einzelne Einkunftsarten zu verlangen, sowie ferner die Überprüfung der angegebenen Einkommensverhältnisse durch Vorlage des Steuerbescheids oder durch Einholung von Auskünften bei den Finanzämtern auf solche Einzelfälle oder Fallgruppen zu beschränken, bei denen konkrete Anhaltspunkte für Mißbrauch gegeben sind oder Unstimmigkeiten vorliegen, die mit dem Antragsteller nicht geklärt werden können.

Diesen Forderungen haben die zuständigen obersten Bundesbehörden mit der Begründung widersprochen, die Berechtigten wären mit der Nennung der Summe häufig überfordert, da sie hierzu Rechenoperationen anstellen müßten, die nicht ganz einfach seien; das Risiko unbewußt falscher Angaben wäre sehr groß. Auf einen förmlichen Nachweis könne in aller Regel nicht verzichtet werden, um das Risiko von Überzahlungen auf das vertretbare Maß zu mindern.

Im Ergebnis wird nunmehr in den für das Berechnungsjahr 1984 neu entwickelten Fragebogen die Angabe der Einkommenshöhe nicht mehr verlangt, in jedem Fall aber die Vorlage des Einkommensteuerbescheids bzw. eines geeigneten Nachweises über lediglich lohnsteuerpflichtige Einkünfte gefordert. Der Berechtigte wird darauf hingewiesen, daß Angaben im Steuerbescheid (bzw. der Fotokopie), die der Kindergeldstelle nicht bekannt werden sollen, unleserlich gemacht werden können; das gilt nicht für Angaben über die Einkünfte, die Steuernummer und die zugunsten des Berechtigten absetzbaren Beträge.

Vergleichbares gilt auch für den Bereich des öffentlichen Dienstes, an dessen Angehörige das Kindergeld nach § 45 BKGG nicht durch die Arbeitsverwaltung, sondern durch die für die Festsetzung der Bezüge bzw. des Arbeitsentgelts zuständigen Stellen gezahlt wird. Aus dieser speziellen Situation heraus wurde von Angehörigen des öffentlichen Dienstes über die allgemeinen Fragen hinaus vielfach die Befürchtung geäußert, die durch die detaillierte Darlegung dem Dienstherrn/Arbeitgeber bekanntgewordenen Einkommensverhältnisse könnten Personalentscheidungen in unzulässiger Weise zum Nachteil des Bediensteten beeinflussen. Dies hat die Datenschutzbeauftragten veranlaßt, in dem o. a. gemeinsamen Beschluß hierauf aufmerksam zu machen und zu fordern, daß die Kindergeldstellen des öffentlichen Dienstes auf folgende Rechtslage ausdrücklich hingewiesen werden: Die für die Kindergeldbearbeitung erhobenen Daten unterliegen einer strengen Zweckbindung. Diese verbietet es demjenigen, der im Bereich des öffentlichen Dienstes nach § 45 des Bundeskindergeldgesetzes mit der Bearbeitung von Kindergeldangelegenheiten betraut ist, Kindergelddaten an die mit der Bearbeitung von Personalsachen Betrauten weiterzugeben oder, wenn er selbst auch mit der Bearbeitung von Personalsachen betraut ist, hierfür die Kindergelddaten zu verwenden. Die gehalts- bzw. lohnzahlenden Stellen der öffentlichen Verwaltung haben bei der Erfüllung von Aufgaben nach dem Bundeskindergeldgesetz das Sozialgeheimnis zu wahren.

Ein entsprechender Hinweis wurde in das gemeinsame Rundschreiben des BMJFG und des BMI vom 26. Oktober 1983 aufgenommen.

Die nunmehr getroffenen Verfahrensregelungen stellen unter Datenschutzaspekten zweifellos eine Verbesserung dar. Unbefriedigend bleibt jedoch die von der Verwaltung nach wie vor für notwendig gehaltene Feststellung der einzelnen Einkunftsarten. Maßgebend ist nach §§ 10, 11 BKGG die Summe der positiven Einkünfte.

Erfahrungsgemäß ist ein Großteil der Betroffenen geneigt und bereit, auf freiwilliger Basis und von sich aus den vollständigen Steuerbescheid vorzulegen. Es sollte jedoch dem mündigen Bürger nicht von vornherein die Fähigkeit abgesprochen werden, die richtige Summe anzugeben, noch dazu dann, wenn ihm entsprechend meiner früheren Anregung dafür ein Berechnungsschema zur Verfügung gestellt würde.

12. Rentenversicherung

12.1 Online-Anschluß zwischen der Bundesversicherungsanstalt für Angestellte und der Pensionsversicherungsanstalt der Angestellten in Wien

Die Pensionsversicherungsanstalt der Angestellten (PVAng) und die Bundesversicherungsanstalt für Angestellte (BfA) haben im Oktober 1983 einen Vertrag über den Anschluß an und die Nutzung des Teleprocessing-Auskunfts-Systems der BfA über einen Bildschirmarbeitsplatz bei der PVAng in Wien geschlossen.

Nach dieser Vereinbarung übermittelt die PVAng auf Anforderung einen Versicherungsverlauf mit den bei der BfA gespeicherten Versicherungsdaten. Darüber hinaus wird der PVAng ein Direktzugriff auf das bei der BfA maschinell geführte Versichertenkonto ermöglicht.

Die Vereinbarung stützt sich auf Artikel 35 des Abkommens vom 22. Dezember 1966 zwischen der Bundesrepublik Deutschland und der Republik Österreich über soziale Sicherheit in Verbindung mit Artikel 10 der Durchführungsvereinbarung zu diesem Abkommen.

Der Bundesminister für Arbeit und Sozialordnung hatte die Einrichtung dieses Online-Anschlusses ursprünglich für unzulässig gehalten. Die Vorschriften über den Schutz der Sozialdaten stünden Datenübermittlungen an öffentliche Stellen, für die das Sozialgesetzbuch (SGB) nicht gilt, grundsätzlich entgegen, weil die Prüfung der Erforderlichkeit eines Datenabrufs weder generell-abstrakt im voraus möglich sei, noch den Empfänger überlassen bleiben darf. Der Datenabruf sei deshalb gemäß § 77 SGB X unzulässig.

Der Bundesminister für Arbeit und Sozialordnung hat seine Bedenken später zurückgestellt, falls der Direktabruf von der Einwilligung des Versicherten im Sinne des § 67 SGB X abhängig gemacht und dies ausdrücklich in den Vereinbarungstext übernommen wird. Dies ist auch geschehen.

Wie die Diskussionen um die Vorschrift über den Direktabruf im Rahmen der Novellierung des Bundesdatenschutzgesetzes zeigen, ist dieses Problem schon innerstaatlich strittig. Im vorliegenden Fall halte ich es darüber hinaus auch für zweifelhaft, ob Abkommen und Verwaltungsvereinbarung mit der Republik Österreich eine geeignete rechtliche Grundlage für Online-Verbindungen zwischen zwei Staaten darstellen. Ich hätte es daher vorgezogen, wenn die Vereinbarung, deren sozialrechtlichen und praktischen Sinn ich nicht bestreite, unter weniger Zeitdruck zustandegekommen wäre und man die Novellierung des BDSG abgewartet hätte.

12.2 Sicherheitsbereich der Bundesversicherungsanstalt für Angestellte

Das Bundesarbeitsgericht hat im Mai 1983 zur Sicherheitsüberprüfung im Bereich der Bundesversicherungsanstalt für Angestellte (BfA) entschieden, daß der im Rahmen einer von der Bundesregierung angeordneten Sicherheitsüberprüfung von den zu überprüfenden Bediensteten auszufüllende Fragebogen nicht der Mitbestimmung des Personalrates nach § 75 Abs. 3 Nr. 8 BPersVG unterliege. Das Gericht hat ferner ausgeführt, daß die Weiterleitung des von dem Bediensteten in Kenntnis seiner Bedeutung und seiner Funktion ausgefüllten Fragebogens an das Bundesamt für Verfassungsschutz (BfV) zum Zwecke der Sicherheitsüberprüfung nicht das allgemeine Persönlichkeitsrecht des Bediensteten verletze.

In meinem Fünften Tätigkeitsbericht (dort S. 60) hatte ich die Meinung vertreten, daß die Mitarbeiter, die Zugang zu den bei der BfA gespeicherten sensiblen Daten haben, sorgfältig auszuwählen seien. Der Sicherheitsbereich sei jedoch möglicherweise falsch zugeschnitten. Eine gewissermaßen „automatische" Überprüfung aller Mitarbeiter eines Funktionsbereiches erscheine unangemessen.

Im Berichtszeitraum habe ich in der Angelegenheit mehrere Gespräche mit dem Bundesminister für Arbeit und Sozialordnung (BMA) geführt; im August fand ein Gespräch mit Vertretern des BMA, der BfA und des BfV statt. Dabei wurde folgendes Ergebnis erzielt:

- Der BMA wird nach Inkrafttreten der neuen Sicherheitsrichtlinien eine Verfügung erlassen, die das künftige Verfahren bei der BfA regelt.
- Darin wird der Sicherheitsbereich der BfA neu definiert mit dem Ziel, den Kreis der Betroffenen so weit wie möglich einzuschränken. Die Funktionen, deren Träger sicherheitsüberprüft werden, werden dabei aufgeführt.

Eine solche Neuregelung entspräche meinen Vorstellungen. Datenschutzrechtliche Bedenken hinsichtlich des einbezogenen Personenkreises bestehen dann nicht mehr.

13. Krankenversicherung

13.1 Kontrollen

Im Berichtsjahr habe ich bei zwei Trägern der gesetzlichen Krankenversicherung umfangreichere Kontrollen durchführen lassen.

— Bei der *Bundespost-Betriebskrankenkasse* habe ich weder konkrete Verletzungen des Sozialgeheimnisses, noch mißbräuchliche Verwendungen von Sozialdaten festgestellt. Gleichwohl hatte ich mehrere Mängel hinsichtlich des Datenschutzes zu beanstanden, so vor allem bei der Organisation des Datenschutzes (Führung der Datenübersicht, interne Kontrolle und Überwachung, allgemeine Aufgaben des Datenschutzbeauftragten). Die Beseitigung der beanstandeten sowie weiterer kleinerer Mängel und Unstimmigkeiten in angemessener Zeit hat der Vorstand der Kasse zugesichert.

— Ein erster Besuch und eine Teilkontrolle bei der *Betriebskrankenkasse Volkswagenwerk AG* haben den Eindruck vermittelt, daß dort große Aufgeschlossenheit gegenüber den Belangen des Datenschutzes vorhanden ist. Die Besonderheit bei der Datenverarbeitung im Bereich dieser Betriebskrankenkasse liegt darin, daß die Datenbestände der Kasse und der Volkswagenwerk AG in dem gemeinsamen Personal-Daten-Informations-System der Volkswagenwerk AG (PEDATIS) geführt werden. Hieraus ergeben sich schwierige datenschutzrechtliche Probleme. Es stellt sich vor allem die wichtige Frage nach der Zulässigkeit der Datenverarbeitung im Auftrag der Kasse durch die Volkswagenwerk AG im Hinblick auf § 80 Abs. 5 SGB X. Diese Vorschrift besagt, daß die Verarbeitung personenbezogener Sozialdaten im Auftrag (eines Leistungsträgers) durch nicht-öffentliche Stellen nur zulässig ist, wenn anders Störungen im Betriebsablauf nicht vermieden oder Teilvorgänge der automatischen Datenverarbeitung hierdurch erheblich kostengünstiger besorgt werden können.

  Die Bedeutung und die Tragweite dieser Vorschrift lassen sich aus dem Gesetzeswortlaut und aus der vom zuständigen Bundestagsausschuß dazu gegebenen Begründung nicht eindeutig entnehmen. Zweifelhaft erscheint insbesondere, ob die Abgrenzung der „Teilvorgänge" aufgabenbezogen oder verarbeitungsbezogen vorzunehmen ist. Im letzteren Falle könnte — bei Vorliegen der sonstigen Voraussetzungen — die Zulässigkeit der Auftragsdatenverarbeitung dann angenommen werden, wenn beispielsweise der Auftrag lediglich das „Aufbewahren" der Daten — ein Teilvorgang des Speicherns (§ 2 Abs. 2 Nr. 1 BDSG) — umfaßt, das „Aufnehmen" der Daten mittels Dateneingabegerät aber vom Auftraggeber selbst vorgenommen wird.

  Die Gesamtbeurteilung muß sich m. E. auch an dem Schutzzweck dieser Vorschrift für den Betroffenen ausrichten. Es wird deshalb im konkreten Fall darauf ankommen, wie die Zugriffsberechtigungen auf die gespeicherten Sozialdaten geregelt und abgesichert sind und welche Bestimmungen der Auftraggeber im Einzelfall für die Aufbewahrung und weitere Verwendung der überlassenen Daten getroffen hat (§ 80 Abs. 4 SGB X).

  Diese Fragen sollen in Fortsetzung der Kontrolle bei der Betriebskrankenkasse Volkswagenwerk AG demnächst untersucht werden.

13.2 Bundesknappschaft

Zu der im Jahre 1982 durchgeführten Kontrolle bei der Bundesknappschaft (vgl. 5. TB S. 65) ist nachzutragen, daß die Bundesknappschaft die festgestellten Mängel im wesentlichen anerkannt und beseitigt bzw. ihre Beseitigung zugesichert hat. Dies gilt auch hinsichtlich des Datenschutzes in den Knappschaftskrankenhäusern, obwohl die Bundesknappschaft ihren Rechtsstandpunkt aufrechterhalten hat, mir fehle insoweit die Kontrollkompetenz.

13.3 Einzelprobleme

Im übrigen hatte ich mich insbesondere mit folgenden Fragen und Problemen zu befassen:

— Personenbezogene Hinweise auf das Vorliegen von Suchtkrankheiten in Rundschreiben der Kassenärztlichen Vereinigungen an die Kassenärzte;

— Umfang und Auswirkungen der Ausnahmeregelung nach § 76 Abs. 2 SGB X, wonach eine Offenbarung von unter die ärztliche Schweigepflicht und andere Berufsgeheimnisse fallenden Daten zulässig ist, soweit diese dem Leistungsträger im Zusammenhnag mit einer Begutachtung wegen der Erbringung von Sozialleistungen oder wegen der Ausstellung einer Bescheinigung zugänglich gemacht worden sind;

— Datenübermittlung aus den Dateien der Krankenkassen an den Internationalen Suchdienst (s. oben Nr. 2.5);

— Modellversuche im Rahmen des § 223 RVO; nach dieser Vorschrift kann die Krankenkasse in geeigneten Fällen Krankheitsfälle vor allem im Hinblick auf die in Anspruch genommenen Leistungen überprüfen und den Versicherten und den behandelnden Arzt über die Leistungen und ihre Kosten unterrichten;

— Umfang der Einkommensermittlung und der Auskunftspflichten (§ 317 Abs. 8 RVO) für Zwecke der Krankenversicherung der Rentner;

— Durchführung der Familienkrankenhilfe nach § 205 Abs. 1 und Abs. 4 RVO (s.o. Nr. 10.3).

14. Unfallversicherung

Im Bereich der gesetzlichen Unfallversicherung wurde eine mehrtägige Datenschutzkontrolle bei der *Bundespost-Ausführungsbehörde für Unfallversicherung (AfU)* durchgeführt.

Gegenüber anderen Trägern der gesetzlichen Unfallversicherung weist die AfU einige Besonderheiten auf. Sie ist keine Körperschaft des öffentlichen Rechts, sondern organisatorisch Teil des Sozialamtes der Bundespost (SAP), einer zentralen Mittelbehörde im Geschäftsbereich des Bundesministers für das Post- und Fernmeldewesen. Die organisatorische Einbindung der AfU in die Verwaltung der Post beschränkt sich indessen auf die „innere Verwaltung". Hinsichtlich der Aufgaben der Unfallversicherung besitzt die AfU — insoweit vergleichbar mit den selbständigen Trägern der Unfallversicherung — durchaus eine relative Eigenständigkeit. Dies ergibt sich aus den Vorschriften des SGB IV, wonach bei der AfU entsprechende Selbstverwaltungsorgane, die ihre Befugnisse unabhängig ausüben, zu bilden sind.

Diese organisationsrechtlichen Besonderheiten sind nach meinem Eindruck eine wesentliche Ursache für verschiedene formale Mängel bei der Durchführung des Datenschutzes:

Die AfU hat entgegen § 28 Abs. 1 BDSG i. V. m. § 79 Abs. 1 SGB X einen Datenschutzbeauftragten nicht bestellt. Ich habe zwar keine grundsätzlichen Bedenken dagegen, daß — wie praktiziert — der Datenschutzbeauftragte des SAP auch für die AfU tätig ist, halte aber eine formelle Bestellung durch die zuständigen Organe der AfU mit einer klaren Zuweisung der Verantwortlichkeiten und Aufgaben für erforderlich.

Aus der durchgeführten Kontrolle ist der Eindruck festzuhalten, daß durch die räumliche Trennung der AfU (Tübingen) vom SAP (Stuttgart) einerseits und durch die unzureichend reflektierte Eigenverantwortlichkeit der AfU auch im Hinblick auf den Datenschutz andererseits der Datenschutz bei der AfU nicht so gewährleistet ist, wie dies nach den gesetzlichen Vorgaben zu erwarten ist. Dies gilt insbesondere hinsichtlich der in § 29 BDSG konkretisierten Aufgaben des Datenschutzbeauftragten, nämlich Erstellung und Führung einer Datenübersicht, Überwachung der ordnungsgemäßen Programmanwendung, Vertrautmachen der Mitarbeiter mit den allgemeinen und spezifischen Datenschutzvorschriften, bezogen auf die besonderen Verhältnisse in dem Bereich der gesetzlichen Unfallversicherung.

Datenschutzrelevante Mängel waren auch bei der Führung von Personalunterlagen für die Mitarbeiter der AfU festzustellen.

Die Mitarbeiter der AfU sind Beamte und Angestellte der Bundespost. Dienstvorgesetzter ist der Präsident des SAP, der in dieser Eigenschaft die personalrechtlichen Entscheidungen zu treffen hat. Personalverwaltende Stelle ist ein Referat des SAP. Ein Mitarbeiter dieses Referats, der seinen Arbeitsplatz bei der AfU in Tübingen hat, ist (u. a.) für die Mitarbeiter der AfU zuständig. Er führt für diese Mitarbeiter „Personalpapiere" (personalaktenähnliche Vorgänge) im Sinne des Abschnitts 5 der „Anweisung für die Führung und Verwaltung von Personalakten der Beamten" vom 13. März 1980 des BMP. Bei der stichprobenweisen Kontrolle der Personalpapiere wurde festgestellt, daß diese in großem Umfange Unterlagen enthielten, die nach der genannten Anweisung bzw. nach den allgemeinen Grundsätzen der Personalaktenführung entweder an die personalaktenführende Stelle beim SAP abzugeben oder zu vernichten sind. Die „Anweisung" schreibt dazu ausdrücklich eine Prüfung und Aussonderung in regelmäßigen Zeitabständen vor.

In seiner Stellungnahme hat der BMP in der Mehrzahl der aufgezeigten Mängel zugesagt, meinen Vorschlägen und Anregungen zu ihrer Beseitigung zu folgen. Einzelne Punkte konnten noch nicht endgültig geklärt werden und bedürfen weiterer Erörterung.

15. Gesundheitswesen

15.1 Krebsregister

Im Vordergrund der Datenschutzdiskussion in diesem Bereich standen die rechtlichen Grundsätze für zukünftige *Krebsregister*.

Die Konferenz der für das Gesundheitswesen zuständigen Minister und Senatoren der Länder (GMK) hat auf ihrer letzten Sitzung am 17./18. November 1983 ein Thesenpapier über die Einrichtung von regionalen Krebsregistern zustimmend zur Kenntnis genommen. In ihrer Entschließung empfiehlt die GMK jenen Ländern, die ein regionales Krebsregister einrichten wollen, die in den Thesen festgelegten Grundsätze zu berücksichtigen. Das Thesenpapier hat folgenden Wortlaut:

> „Zur Verbesserung der Krebsbekämpfung muß die epidemiologische Krebsforschung dringend gefördert werden, um ausreichende Kenntnisse über die ursächlichen Zusammenhänge, die zu einer Krebserkrankung führen können, zu erhalten. Eine wichtige Voraussetzung hierfür ist der Auf- bzw. Ausbau von epidemiologischen Krebsregistern.

Da internationale Erfahrungen gezeigt haben, daß Register mit einem zu großen Einzugsbereich nicht mehr praktikabel sind, kommt ein einziges zentrales Register für die Bundesrepublik nicht in Frage. Vielmehr sind regionale epidemiologisch geführte Krebsregister auf Länderebene zu bevorzugen.

Solche Register müssen bestimmte Bedingungen erfüllen, um einerseits dem Schutz der Intimspähre des Patienten Rechnung zu tragen und andererseits eine wissenschaftliche Bearbeitung der gesammelten Daten nach den Erfordernissen der Krebsbekämpfung zu ermöglichen. Sie bedürfen dabei, um wirksam werden zu können, in besonderem Maße der Mitwirkungsbereitschaft der Ärzte.

Thesen zur Errichtung regionaler Krebsregister

1. Regionale epidemiologische Register sind für die Erweiterung der Kenntnisse über die Krebsentstehung und damit zur Ermöglichung präventiver und anderer Maßnahmen der Krebsbekämpfung von Bedeutung.

2. Zum Auf- und Ausbau regionaler Krebsregister und zur wissenschaftlichen Auswertung der dort erfaßten Daten ist die Schaffung rechtlicher Voraussetzungen nötig.

3. Regionale Krebsregister sollen mindestens 15%, besser 30% der Wohnbevölkerung erfassen. Auf lange Sicht ist eine flächendeckende Erfassung innerhalb der Bundesrepublik anzustreben.

4. Regionale Register, die auf Länderebene errichtet werden, müssen untereinander vergleichbar sein und eine Zusammenarbeit ermöglichen (vgl. GMK-Beschluß vom März 1980). Hierfür ist die Erhebung eines einheitlichen Mindestdatensatzes nötig. Neben der Auswertung und Dokumentation der anfallenden Daten durch das jeweilige regionale Register sind Maßnahmen vorzusehen, die eine zusammenfassende Auswertung der anonymisierten Daten aus allen regionalen Krebsregistern ermöglichen.

5. Um aussagekräftige Daten zu erhalten, ist ein ausreichender Bevölkerungsbezug herzustellen. Hierfür sind innerhalb der definierten Regionen die Krebserkrankungsfälle möglichst vollständig zu erfassen.

6. Klinikregister, die der Versorgung von Krebspatienten dienen, können bei entsprechendem Ausbau epidemiologisch nutzbar gemacht werden. Voraussetzung ist die Herstellung eines ausreichenden Bevölkerungsbezugs. Hierfür sind jedoch in ähnlicher Weise rechtliche Regelungen wie bei regionalen Krebsregistern erforderlich.

7. Eine namentliche Meldung der Patienten an das Krebsregister ist unumgänglich.

8. Ärzte und Zahnärzte sollen zur Meldung der Patienten berechtigt werden. Von einer Meldepflicht ist abzusehen.

9. Grundsätzlich soll die namentliche Meldung nur mit Einwilligung des Patienten erfolgen. Ausnahmen von dieser Regelung müssen zulässig sein, jedoch sind ihre Voraussetzungen im Rahmen entsprechender gesetzlicher Regelungen genau zu definieren. Besondere Vorgaben sind für die Meldungen durch pathologische Institute vorzusehen.

   Hat der Patient vorsorglich erklärt, im Falle einer Krebserkrankung mit der Meldung seiner persönlichen Daten nicht einverstanden zu sein, so gilt dieser Einspruch bis zum Widerruf.

10. Eine möglichst frühzeitige Anonymisierung der personenbezogenen Daten muß sichergestellt werden.

11. Für das Krebsregister muß feststellbar sein, ob der gemeldete Patient verzogen oder verstorben ist. Um die personenbezogenen Daten in bestimmten Abständen mit den Daten der Meldebehörden und den Leichenschauscheinen abgleichen zu können, müssen entsprechende rechtliche Voraussetzungen vorhanden sein bzw. geschaffen werden.

12. Es ist festzulegen, an wen und unter welchen Voraussetzungen anonymisierte Daten für wissenschaftliche Zwecke abgegeben werden können.

13. Personenbezogene Daten dürfen nur für Zwecke der Krebsforschung und unter besonderen Vorkehrungen abgegeben werden.

14. Zur Bearbeitung bestimmter Forschungsthemen kann die Befragung des Patienten oder von Dritten erforderlich sein. In gesetzlichen Regelungen zur Krebsregistrierung müssen hierfür entsprechende Modalitäten vorgesehen werden, da die Zustimmung des Patienten zur Meldung an ein Register nicht auch die Zustimmung zur eventuellen Befragung in späteren Forschungsvorhaben beinhaltet.

15. Eine Auskunft über die zu seiner Person erfolgte Eintragung im Register ist dem Patienten nur durch einen von ihm zu benennenden Arzt zu vermitteln.

16. Es muß ausgeschlossen werden, daß das Krebsregister Bescheinigungen des Inhalts ausstellt, daß eine bestimmte Person dort nicht gemeldet ist (Negativ-Attest)."

Diese Thesen decken sich im wesentlichen mit den Forderungen, die ich in meinem Fünften Tätigkeitsbericht (S. 71/72) aufgestellt habe. Sie sind eine geeignete Grundlage für die künftige Gesetzgebung in den Bundesländern. Ich werde beobachten, wie diese Grundsätze im einzelnen in die Praxis, umgesetzt werden, und, soweit meine Zuständigkeit berührt ist, Empfehlungen zur Verbesserung des Datenschutzes geben.

15.2 Einzelprobleme

Darüber hinaus war ich — überwiegend im Rahmen der Zusammenarbeit mit den Landesbeauftragten für den Datenschutz (§ 19 Abs. 5 BDSG) — insbesondere mit folgenden Problemen und Einzelfragen befaßt:

— Datenschutz im Krankenhaus (Umfang der Speicherung und Übermittlung von „Patientendaten")

— Reichweite der innerbehördlichen Schweigepflicht nach § 203 Abs. 1 StGB gegenüber Vorgesetzten

— Fertigung von Fotografien bei der Patientenaufnahme in Nervenkrankenhäusern

— Forschungsvorhaben zum psychiatrischen Maßregelvollzug (§ 63 StGB).

Die Themen sind noch nicht ausdiskutiert.

16. Wirtschaftsverwaltung

16.1 Öffentlich-rechtliche Banken — Allgemeines —

Ein Arbeitsschwerpunkt der letzten Jahre war die Beurteilung der Datenverarbeitung im Bankenbereich. Mit der Prüfung zweier öffentlich-rechtlicher Kreditinstitute in diesem Jahr ist der Bereich nahezu abgeschlossen. Beiden Kreditinstituten konnte ich bestätigen, daß der Umgang mit personenbezogenen Daten im großen und ganzen sorgfältig und verantwortungsbewußt erfolgt. Meine Vorschläge zur Verbesserung des Datenschutzes wurden in fast allen Fällen aufgegriffen und zum Teil bereits in die Praxis umgesetzt. Sie führten teilweise auch zu Vereinfachungen im Arbeitsablauf und zu Einsparungen. Ich nenne hier einige Beispiele, weil sie auch für andere Stellen mit ähnlichen Aufgaben von Bedeutung sein dürften.

— In Antragsvordrucken wird auf die Erhebung solcher Daten verzichtet, die zeitlichen Änderungen unterliegen, aber im Datenbestand nicht gepflegt werden (z. B. die Berufsangabe).

— Die Aufnahme von Dokumenten in den Datenbestand wird unterlassen, wenn die Papiere lediglich dazu bestimmt sind, bei Vertragsabschluß die Richtigkeit von Angaben des Betroffenen zu beweisen (z. B. die Geburtsurkunde).

— Um keinen Anlaß für unzulässige Datenübermittlung zu geben, sollen bei der schriftlichen Befragung Dritter über die Verhältnisse des Betroffenen nur solche Angaben erfragt werden, deren Richtigkeit die übermittelnde Stelle erwartungsgemäß beurteilen und nachweisen kann (z. B. keine allgemeinen Persönlichkeitsbeurteilungen).

— Eine „vertrauliche Behandlung" von Informationen Dritter darf nicht in einer Weise zugesichert werden, als ob damit die Auskunftserteilung an den Betroffenen (nach § 13 Abs. 3 oder § 26 Abs. 4 BDSG) ausgeschlossen wäre. Um derartige Mißverständnisse zu vermeiden, sollen Hinweise, die lediglich Selbstverständlichkeiten zum Ausdruck bringen, unterbleiben oder jedenfalls eindeutig formuliert werden. Eine Formulierung, die neben der Zusicherung der Vertraulichkeit den Zweck der Anfrage zum Ausdruck bringt und damit der übermittelnden Stelle Anhaltspunkte für die Beurteilung nach §§ 24, 32 BDSG gibt, könnte etwa lauten: „Die erbetenen Angaben werden ausschließlich für den benannten Fall zur kreditorischen Beurteilung verwendet".

— Bei der Verwendung von (datenschutzrechtlich nicht vorgeprüften) Fremdvordrucken muß die Zulässigkeit der Bekanntgabe jeder einzelnen Information geprüft werden. So stellt z. B. eine Wirtschaftsauskunftei Kreditinstituten Vordrucke zur Verfügung, mit denen Wirtschaftsauskünfte angefordert werden sollen. Auf dem Vordruck sind aber auch nähere Angaben über die Geschäftsbeziehungen des Kreditinstituts mit dem Betroffenen vorgesehen, die anscheinend nur den Zweck haben, der Auskunftei zusätzliche Erkenntnisse zu liefern.

— Wenn eine Fremdauskunft zu einer negativen Entscheidung des Kreditinstituts führen kann, soll ihr Inhalt dem Betroffenen eröffnet werden, damit er Gelegenheit zur Stellungnahme und gegebenenfalls zur Richtigstellung erhält.

— Zwischen den Vorstellungen der Betroffenen über die Wahrung des sogenannten Bankgeheimnisses und den tatsächlichen Geschäftsgepflogenheiten der Kreditwirtschaft beim Umgang mit Kundendaten klafft mitunter eine beträchtliche Lücke. Die Transparenz von Informationsbeziehungen, die im Zusammenhang mit Bonitätsprüfungen genutzt werden, soll verbessert werden.

16.2 Benachrichtigung und Auskunft bei „stillen Zessionen"

Im Bankenbereich habe ich eine bedenkliche Einschränkung von Datenschutzrechten in folgendem Sachzusammenhang festgestellt:

Im Falle der Refinanzierung von Krediten tritt die Geschäftsbank (Zedent) ihre Forderung gegen den Kreditnehmer ab und gibt dazu im Regelfall die entsprechenden Daten an das refinanzierende Kreditinstitut (Zessionar) weiter. Dieses speichert die Daten und löst damit die Benachrichtigungspflicht nach § 26 Abs. 1 BDSG aus, sofern der Betroffene nicht auf andere Weise Kenntnis von der Speicherung erlangt hat (§ 26 Abs. 1 2. Halbsatz BDSG). Eine entsprechende Aufklärung könnte durch die Geschäftsbank erfolgen. Diese ist jedoch mitunter daran nicht interessiert, weil sie beim Kunden den Eindruck vermeiden möchte, zur Finanzierung des Kredites ohne fremde Hilfe nicht in der Lage zu sein. Man befürchtet, daß daraus geschäftliche Nachteile entstehen könnten. Der Zessionar entspricht dem Wunsch seines Geschäftspartners, die Refinanzierung nicht bekannt werden zu lassen. Er beruft sich dabei auf die Ausnahmeregelungen des § 26 Abs. 4 Nr. 1 und 3 BDSG. Die Kreditwirtschaft hält die Offenlegung der Abtretung für unzumutbar und verweist auf atmosphärische Störungen der Geschäftsbeziehungen („unbegründeter Vertrauensschwund", „Mißverständnisse", „Fehleinschätzungen") und auf das mangelhafte Verständnis des „in geschäftlichen Dingen nicht versierten Kunden".

Mit einer nur auf Empfindlichkeiten und Rücksichtnahme basierenden Argumentation kann man sich jedoch nicht der gesetzlichen Verpflichtung zur Benachrichtigung und zur Auskunftserteilung entziehen. Bei der Beurteilung müssen auch die Konsequenzen für den Betroffenen bedacht werden, die eintreten, wenn die Verarbeitung seiner Daten vor ihm geheimgehalten wird: Korrekturansprüche gemäß § 27 BDSG (Berichtigung, Sperrung, Löschung von Daten) können nicht verwirklicht werden; die strafrechtliche Verfolgung einer unzulässigen Datenverarbeitung, die nur auf Antrag erfolgt, wird nahezu unmöglich. Dem muß die Auslegung der Ausnahmeregelungen des § 26 Abs. 4 BDSG Rechnung tragen. Ob eine Ausnahme hinnehmbar ist, muß sich im Einzelfall erweisen. Es reicht jedenfalls nicht aus, mit einer pauschalen Begründung Ausnahmen für einen ganzen Geschäftstyp zu reklamieren; ebensowenig führt der Hinweis auf die nach dem Privatrecht bestehende Möglichkeit, Forderungen stillschweigend abzutreten, zu einer generellen Freistellung von Datenschutzpflichten.

Es mag durchaus Situationen geben, in denen mit der Offenlegung der Finanzierungszusammenhänge eine erhebliche Geschäftsgefährdung (§ 26 Abs. 4 Nr. 1BDSG) verbunden ist, so daß die Datenschutzinteressen des Betroffenen zurücktreten müssen. Es sind auch Fälle denkbar, in denen das Ergebnis einer Abwägung der beteiligten Interessen (§ 24 Abs. 2 Nr. 3 BDSG) die Geheimhaltung rechtfertigt. In jedem Fall jedoch müssen Fakten oder konkrete Anhaltspunkte vorliegen, die eine Entscheidung, auf wesentliche Teile des Datenschutzrechts zu verzichten, vertretbar erscheinen lassen. In diesem Sinne hat auch der Bundesgerichtshof in einem vergleichbaren Konfliktfall entschieden (BGH, Urteil vom 7. Juli 1983 — III ZR 159/82).

Ich habe die Landesbeauftragten für den Datenschutz und die Landesaufsichtsbehörden unterrichtet und vorgeschlagen, der Kreditwirtschaft Beratung bei der Erarbeitung einer sach- und datenschutzgerechten Lösung anzubieten. Die Problematik kann in die geplanten Verhandlungen mit der Kreditwirtschaft — zum Bankenauskunfts- und zum SCHUFA-Verfahren — einbezogen werden.

17. Öffentliche Sicherheit — Allgemeines

17.1 Tätigkeitsüberblick

Der Schwerpunkt der Tätigkeit im Berichtsjahr lag bei der Prüfung der Abteilung III (Linksextremismus) des BfV. Diese Prüfung erstreckte sich rein zeitlich mit verschiedenen Unterbrechungen von März bis Oktober 1983.

Daneben sind an bedeutenderen und umfangreicheren datenschutzrechtlichen Kontrollen im Berichtsjahr zu erwähnen:

— *Beim Bundeskriminalamt* die Datenverarbeitung unter Einsatz von Videogeräten zum Schutze eines amerikanischen Generals;

der Informationsaustausch des BKA als Nationales Zentralbüro von Interpol;

— *beim Bundesgrenzschutz* die Datenverarbeitung der Fahndungsleitstelle der Grenzschutzdirektion;

— *beim Bundesnachrichtendienst* zwei Querschnittsprüfungen mit Schwerpunkten auf dem Gebiet der generellen Auskunftstätigkeit und den Grundsätzen der Datenverarbeitung in zwei Sonderbereichen.

Aus der Beratungs- und gutachterlichen Tätigkeit sind vor allem die Mitwirkung bei den neuen Richtlinien zur Sicherheitsüberprüfung und dem Beschluß der Datenschutzbeauftragten zum Personalausweisgesetz zu erwähnen, dessen Schwerpunkt im Sicherheitsbereich liegt.

Außerdem gab es eine Reihe von Eingaben, die in vielen Fällen Prüfungen vor Ort veranlaßt haben (vor allem beim BGS, BKA, BfV).

17.2 Übergreifende Probleme

17.2.1 Zur Prüfkompetenz im Sicherheitsbereich

Die Auseinandersetzungen über meine Befugnisse beschränken sich im wesentlichen auf die Prüfungen beim BfV, wo die Kontroverse um mein Recht auf Akteneinsicht ihren Ausgang genommen hatte (vgl. 5. TB S. 77 f.). Im Verlaufe der Prüfungen des Jahres 1983 konnten jedoch die Streitfragen jeweils pragmatisch gelöst werden. Alle Kontrollen wurden in dem erforderlichen Umfang durchgeführt. Die einzige Ausnahme hiervon bezog sich auf eine Prüfung beim Generalbundesanwalt aufgrund einer Eingabe. Dort wurde mir die Auskunft auf meine Fragen verweigert, weil der Generalbundesanwalt der Auffassung war, es sei kein Dateibezug im konkreten Fall gegeben, obwohl die Akte, auf die der Petent verwies, karteimäßig erfaßt ist. Ich habe diese Verweigerung als Verstoß gegen § 19 Abs. 3 Sätze 1 und 2 BDSG gegenüber dem Bundesminister der Justiz beanstandet.

17.2.2 Übergreifende Grundsätze der Datenverarbeitung bei den Sicherheitsbehörden

Die Prüfungen in diesem Jahr geben Anlaß, folgende Gesichtspunkte schwerpunktmäßig hervorzuheben:

— Folgepflichten bei Übermittlungen, insbesondere die Pflicht zum Nachbericht sowie zur Unterrichtung anderer Teilnehmer eines Verbundsystems über Löschungen (a);

— Notwendigkeit der Relevanzprüfung bei Übermittlungsersuchen und ihre Konsequenzen (b);

— Auskunftspraxis gegenüber dem Bürger (c).

(a) Folgepflichten bei Übermittlungen

Eine Behörde, die Daten an andere Stellen übermittelt hat, ist grundsätzlich gehalten, relevante Änderungen des Inhalts der Übermittlung nachzumelden. Im Sicherheitsbereich betrifft dies insbesondere den Abschluß und das Ergebnis von Ermittlungsmaßnahmen, wie etwa die Aufklärung eines Verdachts bereits bei der Ausgangsbehörde (z. B. Polizei oder Verfassungsschutz) oder Beendigung eines Strafverfahrens durch Freispruch oder Einstellung. Das gleiche gilt generell für die Löschung wegen fehlender weiterer Relevanz aus welchen Gründen auch immer. Wird die Behörde, die Daten erhalten hat, über solche Änderungen oder Ergänzungen unterrichtet, so hat sie daraufhin ihrerseits zu überprüfen, ob und inwiefern sich Auswirkungen auf die eigene Datenverarbeitung ergeben. Nur so wird verhindert, daß die ursprünglich zulässige Übermittlung von Daten später zu einer praktisch unkontrollierbaren Perpetuierung von bloßen Verdachtsmomenten oder überholten Angaben führt.

Die Pflicht zum Nachbericht ist Ausfluß des Grundsatzes der Folgenbeseitigung und der Verhältnismäßigkeit. Sie ist auch aus der allgemeinen Bestimmung des § 14 Abs. 1 BDSG abzuleiten, wonach Daten zu berichtigen sind, wenn sie unrichtig (geworden) sind. Für einzelne Bereiche gibt es darüber hinaus entsprechende Verwaltungsvorschriften, wie Nr. 10 und 11 der Anordnung über die Mitteilungen in Strafsachen (MiStra). Dort geht es um die Meldung über den Ausgang eines Verfahrens an die ursprünglich anzeigende Behörde (Nr. 10) und die ermittelnde Polizeidienststelle (Nr. 11), damit letztere ihre eigenen Unterlagen daraufhin berichtigen, ergänzen und auf weitere Erforderlichkeit überprüfen kann, wie es z. B. auch Nr. 5.4.3 der KpS-Richtlinien und Nr. 7.4.3 der Dateienrichtlinien vorsehen. Das jeweilige Ergebnis ist dann gegebenenfalls an andere Stellen nachzuberichten, denen zwischenzeitlich Auskünfte aus den eigenen Unterlagen erteilt wurden. Im Sicherheitsbereich kommen hierfür neben anderen Polizeibehörden vor allem das BKA als Zentralstelle, das Bundesamt oder die Landesämter für Verfassungsschutz in Betracht. Vom Nachbericht gehen ersichtlich auch die Nrn. 6.2 und 8.2 der KpS- bzw. Dateienrichtlinien aus, wenn sie bestimmen, daß die Löschung der Unterlagen einer Polizeidienststelle grundsätzlich für andere Stellen verbindlich ist, an die diese Unterlagen übermittelt wurden.

Die speichernde Stelle ist aber prinzipiell auch von sich aus verpflichtet, stets die weitere Erforderlichkeit im Rahmen des möglichen zu überprüfen. Deshalb muß sich eine Polizeibehörde, die Unterlagen an die Staatsanwaltschaft im Rahmen strafprozessualer Ermittlungen übermittelt hat, nach Ablauf einer bestimmten Zeit von sich aus über den Ausgang des Strafverfahrens erkundigen und so eventuell unterbliebene Mitteilungen nach der MiStra auslösen. Gleiches gilt natürlich auch für andere Behörden mit entsprechenden Datenbeständen (z. B. Nachrichtendienste). Das baden-württembergische Innenministerium hat in den „Richtlinien über Einzelfallöschungen in der Personenauskunftsdatei" vom 30. Oktober 1981 (GABl. S. 1230) entsprechende Regelungen erlassen. Für den *Interpolverkehr*, in dem die Berichtigung von Daten besonders wichtig ist, ist außerdem auf die Artikel 5 und 9 der im Herbst 1982 beschlossenen Richtlinien über die internationale polizeiliche Zusammenarbeit und die Kontrolle der Dateien von Interpol zu verweisen, an deren Zustandekommen BKA, BMI und meine Dienststelle gemeinsam und weitgehend einvernehmlich mitgewirkt haben.

Die Beachtung dieser Pflichten ist also letztlich kein Regelungsproblem, sondern eine Frage der Durchsetzung, wie die Praxis beispielsweise zur Vorschrift der Nr. 11 MiStra zeigt, deren Beachtung offenbar nicht die Regel ist. Fehler, die daraus entstehen, setzen sich dann für alle Stellen fort, die zwischenzeitlich unterrichtet wurden. Meine Prüfungen bei den meiner Kontrolle unterliegenden Sicherheitsbehörden des Bundes haben dies leider immer wieder gezeigt. Ich habe seit Jahren darauf hingewiesen, daß dieser Zustand nicht hingenommen werden kann, weil er verhindert, daß die schutzwürdigen Belange des Betroffenen bei allen Stellen, die von einem belastenden Vorgang erfahren haben, auch wirklich gewahrt werden können.

Insbesondere hat die erneute Prüfung der Tätigkeit des BKA als Nationales Zentralbüro von Interpol im Frühjahr des Berichtsjahres ergeben, daß das BKA bisher die Richtlinien, an denen es selbst entscheidend mitgearbeitet hat, in diesem Punkt in keinem der überprüften Fälle beachtet hat. Für die Zukunft ist es deshalb besonders wichtig, daß diese rechtlichen Pflichten erfüllt werden, um die Verletzung schutzwürdiger Belange zu vermeiden.

In diesen Zusammenhang gehört auch die gegenseitige Unterrichtung innerhalb von Verbundsystemen wie NADIS und INPOL, wenn zu einem Personendatensatz von verschiedenen Stellen Hinweise erteilt wurden. Gleiches gilt innerhalb einer einzelnen speichernden Stelle, soweit sie unter verschiedenen Aspekten in verschiedenen Dateien mit unterschiedlichen Fristen Datenverarbeitung betreibt (was vor allem im INPOL-Bereich in großem Umfang der Fall ist). Hier muß jeweils die Löschungsentscheidung der einen Stelle der anderen mitgeteilt werden, damit diese daraufhin eine eigene Prüfung einleitet.

Solche gegenseitigen Unterrichtungen und Nachberichte sollen freilich keinen Löschungsautomatismus auslösen. Aber sie können dazu beitragen, den Interessen des Betroffenen besser Rechnung zu tragen. Gleichzeitig wird dadurch verhindert, daß wichtige Entscheidungen einer Stelle für andere speichernde Stellen verloren gehen. Das ist von besonderer Bedeutung in Verbundsystemen wie den bereits erwähnten NADIS oder INPOL. Bestehen z. B. im System NADIS, wo dies sehr oft der Fall ist, mehrere Notierungen zu einer Person (z. B. eine des BfV und eine oder weitere von verschiedenen Landesämtern) und wird nur eine Notierung gelöscht (weil die zuständige Stelle sie nicht mehr für erforderlich hält), so bleiben die Notierungen zu der betroffenen Person mit den Aktenfundstellen der anderen Ämter weiterhin gespeichert und für alle angeschlossenen Teilnehmer abrufbar. Wären die anderen Stellen aber von der Löschung unterrichtet worden und hätten sie daraufhin ihre eigenen Unterlagen überprüft, dann wären sie eventuell zu demselben Ergebnis gekommen wie die Stelle, die ihre Notierung gelöscht hat. Denn sehr oft sind die Unterlagen, die bei verschiedenen Stellen zu Speicherungen geführt haben, identisch (z. B. Kopien eines einzigen Benachrichtigungsschreibens, das an verschiedene Verfassungsschutzämter gleichzeitig ging).

Gegenwärtig findet aber eine solche Unterrichtung nicht statt. Das hat zur Folge, daß Verlautbarungen über hohe Löschungszahlen von „Notierungen" theoretisch bedeuten können, daß dennoch alle betroffenen Personen weiterhin gespeichert und lediglich eine oder mehrere Aktenfundstellen entfallen sind.

Ich führe mit den zuständigen Stellen seit längerem Gespräche mit dem Ziel, diese unbefriedigende Situation, die weder im Interesse der Sicherheitsbehörden noch im Interesse des Datenschutzes liegt, zu bereinigen.

(b) Relevanzprüfung bei Übermittlungsersuchen und Konsequenzen

Die Übermittlung personenbezogener Erkenntnisse im Sicherheitsbereich kann die schutzwürdigen Belange des Betroffenen besonders nachhaltig beeinträchtigen, wenn die Voraussetzungen für die Zulässigkeit und die Vertretbarkeit von Übermittlungen weitgehend nicht eingehalten werden. Dies gilt besonders für die Prüfung der Relevanz der Unterlagen für die eigene Tätigkeit der übermittelnden Stelle zum Zeitpunkt der Übermittlung. Ergibt diese Prüfung, daß die Unterlagen

— aus formellen Gründen (z. B. Ablauf der gesetzlich oder verwaltungsintern festgelegten Regelfristen insbesondere bei Altfällen, von denen es bei den Sicherheitsbehörden leider noch relativ viele gibt) oder

— aus materiellen Gründen (zwischenzeitlich erfolgte sachliche Änderungen oder neue Wertungen)

nicht mehr für die Aufgabenerfüllung erforderlich sind, dann ist die Personenakte zu vernichten; personenbezogene Daten sind zu löschen. Die Folge muß sein, daß prinzipiell keine Auskunft mehr erteilt werden darf. Von diesem Grundsatz kann allenfalls in besonderen Ausnahmefällen abgewichen werden.

Meine Kontrollen haben jedoch im Jahre 1983 — also mehr als fünf Jahre nach Inkrafttreten des BDSG und nach mehrjährigen intensiven Diskussionen zu diesen Punkten — ergeben, daß diese Grundsätze noch weitgehend unbeachtet bleiben. Zum Teil war festzustellen, daß Relevanzprüfungen zwar stattfinden, die erforderlichen Konsequenzen jedoch nicht gezogen werden. Als Beispiel dafür sei die Prüfung beim BfV in diesem Jahr angeführt. Dort wird zwar neuerdings in aller Regel eine Relevanzprüfung vor Auskunftserteilung durchgeführt. In vielen Fällen wurde auch die Vernichtung der Unterlagen und Löschung der personenbezogenen Daten angeordnet. Dennoch wurde in aller Regel jeweils vorher die erbetene Auskunft erteilt, und es erfolgte lediglich ein Zusatz, daß das BfV die Unterlagen vernichten bzw. löschen werde.

Bei der Prüfung des Interpolauskunftsverkehrs des BKA wurden vor allem Verstöße gegen eigene Löschungsfristen festgestellt. In zwei Fällen handelte es sich um Straftaten, die die Betroffenen als Jugendliche begangen hatten. Sehr oft wurde auch eine Auskunft erteilt, obwohl nach Aktenlage dringender Anlaß bestanden hätte, vorher Erkundigungen über das weitere Schicksal der zum Teil lange nicht mehr ergänzten Erkenntnisse einzuholen. Hierzu sei auf die Ausführungen zu (a) verwiesen.

Ich gehe jedoch nach den zwischenzeitlichen eingegangenen Stellungnahmen zu meinen Prüfberichten und nach Gesprächen zu den in diesem Jahr aufgezeigten Mängeln davon aus, daß gerade beim Auskunftsverkehr solche Verstöße künftig unterbleiben werden. Dies soll durch Verbesserung der organisatorischen Abläufe bei der Auskunft und durch entsprechende Schulung der für den Aus-

kunftsverkehr zuständigen Mitarbeiter sichergestellt werden.

Ein besonderes Problem ist noch immer die inhaltliche Gestaltung der Auskunft je nach Anfragegrund. Oft sind personenbezogene Daten bei einer Stelle gespeichert, ohne daß die zugrundeliegenden Erkenntnisse für die anfragende Stelle von Bedeutung wären. In solchen Fällen müßte an sich eine reine Negativauskunft („keine Erkenntnisse") erteilt werden. Denn wer kein Recht hat zu wissen, welche Erkenntnisse über eine bestimmte Person gespeichert sind, hat auch kein Recht zu erfahren, ob Daten dieser Person überhaupt bei der angefragten Stelle registriert sind. Bei Verbundsystemen ist dies allerdings nicht möglich, da der Verbundteilnehmer unmittelbar Zugriff auf die gespeicherten Daten hat und damit weiß, ob zu einer bestimmten Person Unterlagen vorhanden sind. Dann ist aber jegliche inhaltliche Auskunft aus den Akten zu vermeiden wenn sie nicht erforderlich ist. Ich muß darauf bestehen, daß dies in Zukunft stärker beachtet wird.

Hinsichtlich der Übermittlung an anfragende Stellen haben die Prüfungen und Gespräche vor allem beim BND, dessen personenbezogenen Datenverarbeitung ohnehin besondere Probleme aufwirft (vgl. 5. TB S. 97 f.), inzwischen zu einem positiven Ergebnis geführt. Ich sehe darin ein Beispiel für die Möglichkeit, Interessen des Datenschutzes und der Sicherheit gleichermaßen zu berücksichtigen. Nunmehr stellt der BND sicher, daß inhaltliche Auskünfte in wesentlich geringerem Umfang erteilt werden, als es bisher der Fall war. Auch bei den anderen Sicherheitsbehörden bemühe ich mich um restriktiveres Auskunftsverhalten, auch wenn einzuräumen ist, daß dort vielfach andere Speicherungsgründe gegeben sind als beim BND.

(c) Auskunftspraxis gegenüber dem Bürger

Realisierung und Durchsetzung des Datenschutzes hängen in großem Umfang von der Erfüllung des Auskunftsanspruchs des Bürgers ab. Dessen Recht auf Kenntnis der Daten, die bestimmte Stellen über ihn gespeichert haben, ist von wesentlicher Bedeutung für die Verwirklichung des Datenschutzes und im BDSG in einer Vielzahl von Vorschriften verankert, die Auskunftsansprüche gewähren oder Maßnahmen vorschreiben, die die Wahrnehmung dieses Rechts ermöglichen (Veröffentlichung der Dateien, Dateienregister, Auskunftspflichten).

Diese Regelungen gehen letztlich auf die verfassungsrechtlich verbürgte Eröffnung des Rechtsweges gegenüber Maßnahmen der öffentlichen Gewalt gemäß Artikel 19 Abs. 4 GG zurück. Denn die Wahrnehmung dieses Grundrechts setzt voraus, daß der Bürger Kenntnis von den ihn betreffenden Maßnahmen hat. Hierzu gehört auch die Speicherung personenbezogener Daten über seine Person durch die für die öffentliche Sicherheit zuständigen Behörden. Die Sicherheitsbehörden sind aber weitgehend von der Auskunftspflicht gegenüber dem Bürger ausgenommen. Dies ist in gewissem Umfang auch hinzunehmen und verfassungsrechtlich vertretbar, wenn und solange eine Auskunft das überwiegende Interesse der Allgemeinheit an der konkreten sicherheitsbehördlichen Maßnahme gefährdet oder gefährden könnte. Dem entsprechen auch verschiedene gesetzliche Regelungen wie § 5 Abs. 5 Gesetz zu Artikel 10 GG, § 101 Abs. 1 und Abs. 3 StPO und auch § 29 Abs. 2 VwVfG (vgl. auch BVerfGE 30, 1, 21 zur Unterrichtungspflicht bei G 10-Maßnahmen nach Wegfall der Zweckgefährdung). Allein der diesen Bestimmungen zugrundeliegende *Abwägungsmaßstab* entspricht dem verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit. Hieran ist daher auch § 13 Abs. 2 BDSG zu messen, der den Sicherheitsbehörden die Verweigerung der Auskunft gestattet. Diese Bestimmung ist somit verfassungskonform restriktiv auszulegen. Dabei ist selbstverständlich den unterschiedlichen Gegebenheiten zwischen Polizeibehörden einerseits und Nachrichtendiensten andererseits Rechnung zu tragen. Die in letzter Zeit jedoch zunehmend geübte Praxis insbesondere der Nachrichtendienste, unter ständiger Berufung auf § 13 Abs. 2 BSDG und gesetzliche oder innerdienstliche Regelungen über die Aufgabenstellung die Auskunft pauschal zu verweigern, wird den vorstehend aufgezeigten verfassungsrechtlichen Grundsätzen in Verbindung mit der überwiegenden Rechtsprechung nicht gerecht. Hierzu sei verwiesen auf die Urteile

- des VG Köln vom 5. Mai 1982, Az. 14 K/8/81, NVwZ 1983, 112;
- des VG Berlin vom 7. Juli 1982, Az. I A 9/81;
- des OVG Hamburg vom 26. August 1982, OVG Bf III 19/81;
- des OVG Bremen vom 26. Oktober 1982, Az. 1 BA 15/81; NVwZ 1983, 358

und jüngst auf den Beschluß des OVG Münster vom 10. Oktober 1983, Az. 18 A 1591/82, in dem das ersterwähnte Urteil des VG Köln vollinhaltlich bestätigt wurde (nicht rechtskräftig).

Vor diesem Hintergrund erscheint es mir auch bedenklich, daß in dem Referentenentwurf des Bundesministers des Innern zur Novellierung des BDSG die Vorschrift des § 13 Abs. 2 trotz der weitergehenden und in der Praxis bisher ohne erkennbare Schwierigkeiten angewandten innerdienstlichen Regelungen für die Polizei (Nr. 4 KpS-Richtlinien, Nr. 6 Dateienrichtlinien) beibehalten und überdies vorgesehen ist, daß die Sicherheitsbehörden die Ablehnung der Auskunftserteilung künftig nicht zu begründen brauchen.

17.3 Neuregelung der Richtlinien für die Sicherheitsüberprüfung

Die Sicherheitsüberprüfung ist ein wichtiges Instrument zur Gewährleistung der legitimen Sicherheitsinteressen des Staates. Andererseits ist die Sicherheitsüberprüfung ein Verfahren, bei dem zahlreiche personenbezogene Daten über die betroffene Person und über Dritte erhoben werden, die unter Umständen deren Privatsphäre sehr stark tangie-

ren können. So hat der Bürger, der sich einer Sicherheitsüberprüfung unterziehen muß, weil er ein bestimmtes sicherheitsempfindliches Amt anstrebt oder auf Anordnung seines Dienstherrn übernehmen soll, eine Vielzahl von Fragen zu beantworten, und zwar auch über dritte Personen, insbesondere nähere Angehörige. Bei erweiterten Überprüfungen richtet das für die Durchführung zuständige Bundesamt für Verfassungsschutz Anfragen an die verschiedensten Stellen, vor allem an andere Nachrichtendienste des Bundes und der Länder, örtliche Polizeidienststellen sowie je nach Fallgestaltung an den Leiter des Bundesnotaufnahmeverfahrens und das Bundesamt für die Anerkennung ausländischer Flüchtlinge. Legitimes Ziel dieser Ermittlungen ist es herauszufinden, ob bei dem Betroffenen davon ausgegangen werden kann, daß er kein Sicherheitsrisiko darstellt und deshalb in einem als sicherheitsempfindlich eingestuften Bereich beschäftigt werden oder Zugang zu Unterlagen mit vertraulichem Charakter haben kann. Dabei entsteht nahezu zwangsläufig ein sehr ausgeprägtes Bild des Berufs- und Privatlebens des Betreffenden.

Wegen der Besonderheiten des Verfahrens und der zum Teil sehr weitgehenden personenbezogenen Ermittlungen kommt es aus datenschutzrechtlicher Sicht darauf an, den Grundsatz der Verhältnismäßigkeit streng zu beachten. Vor allem muß ein Höchstmaß an Transparenz für den Betroffenen gewährleistet sein bei aller Notwendigkeit der Wahrung der Sicherheitsinteressen der Bundesrepublik. Die gegenwärtig noch praktizierten Richtlinien vom 15. Februar 1971 werden diesem Anliegen nicht voll gerecht. Es kommt daher darauf an, bei den zur Zeit in Bearbeitung befindlichen neuen Sicherheitsüberprüfungsrichtlinien die Belange des Datenschutzes besser zu berücksichtigen. Dies sollte auf der Grundlage der Erfahrungen und der geänderten Einschätzungen von Rechtsfragen nach mehr als fünfjähriger Datenschutzpraxis und Prüftätigkeit im Sicherheitsbereich geschehen.

Der Entwurf der neuen Richtlinien, der mir im Sommer des Jahres zur Stellungnahme zugeleitet wurde, enthält bereits verschiedene Ansätze, um das allgemeine Persönlichkeitsrecht des einzelnen mit den Interessen der Allgemeinheit an einer ausreichenden Sicherheitsüberprüfung besser als bisher in Einklang zu bringen. Das betrifft vor allem die beabsichtigte Einführung einer vereinfachten Überprüfungsform, die nur die Anfrage im NADIS und im Bundeszentralregister umfaßt. Zwar wurde sie auch bisher schon neben den geltenden Richtlinien praktiziert, sie wird aber nunmehr verfahrensmäßig festgeschrieben. In einem solchen Fall finden keine besonderen Ermittlungen der vorstehend skizzierten Form statt. Durch die Einbindung der Dateianfrage als Form der Sicherheitsüberprüfung in die Richtlinien ist gleichzeitig sichergestellt, daß die verfahrensmäßigen Garantien der Richtlinien uneingeschränkt gelten.

In verschiedenen Punkten ist es m. E. jedoch erforderlich, die Grundsätze der Transparenz und der Verhältnismäßigkeit noch stärker zur Geltung zu bringen. Hierzu habe ich dem Bundesminister des Innern eine Reihe von Vorschlägen unterbreitet, die noch berücksichtigt werden sollten. Das gilt insbesondere

- für das Recht auf Einsicht in die Sicherheitsüberprüfungsrichtlinien durch den Betroffenen, wenn er dies wünscht,
- für den Hinweis an den Betroffenen auf die eventuelle Speicherung von Daten beim BfV und — je nach Art der Überprüfung — auch der Daten des Ehegatten, des Verlobten oder der Person, mit der der Betroffene in eheähnlicher Gemeinschaft lebt,
- für die Beschränkung der Einbeziehung der Akten des Leiters des Bundesnotaufnahmeverfahrens oder des Bundesamtes für die Anerkennung ausländischer Flüchtlinge auf die Fälle, in denen der Betroffene dem zugestimmt hat, wie dies bereits für die Einsicht des BfV in Unterlagen über das Anerkennungsverfahren von Kriegsdienstverweigerern generell (also über die Sicherheitsüberprüfung hinaus) geregelt ist (vgl. 4. TB S. 28).

Besonders wichtig ist aber auch die uneingeschränkte Kontrolle der Einhaltung der Richtlinien, insbesondere hinsichtlich des Zeitpunktes der Eröffnung des Prüf- und/oder Ermittlungsverfahrens. Dieses darf nämlich erst *nach* Abgabe des Erklärungsbogens durch den Überprüften eingeleitet werden, keinesfalls aber schon vorher und ohne seine Kenntnis. Wie meine Prüfungen im Jahre 1981 ergaben, wurde gegen diesen Grundsatz, der auch schon in den zur Zeit gültigen Richtlinien verankert ist, von verschiedenen Behörden in beträchtlichem Umfang verstoßen. Dies hatte z. B. zur Folge, daß ein Bewerber eine neutrale Absage erhielt, ohne daß die nach den Sicherheitsüberprüfungsrichtlinien vorgesehene Anhörung durchgeführt und ihm damit Gelegenheit zur Rechtfertigung gegeben wurde (vgl. 4. TB S. 29). Nachdem sich zwischenzeitlich Anhaltspunkte für weitere Verstöße gegen die Richtlinien gerade in diesem Punkte ergeben haben (vgl. 5. TB S. 84), beabsichtige ich im nächsten Jahr eine erneute Kontrolle dieses Bereiches. Nach meinen Gesprächen mit dem Bundesministerium des Innern zu den Sicherheitsüberprüfungsrichtlinien gehe ich davon aus, daß die in diesem Punkt früher aufgeworfenen Schwierigkeiten bezüglich meiner Kontrollbefugnis nunmehr bereinigt sind.

Besondere Aufmerksamkeit wird bei dieser und anderen Prüfungen auch darauf zu richten sein, ob der Anfragegrund „Sicherheitsüberprüfung" jeweils zu Recht verwandt wurde. Sowohl anläßlich der erwähnten und im Vierten Tätigkeitsbericht (S. 29 f.) geschilderten Kontrollen, als auch bei anderen Prüfungen mußte ich feststellen, daß dieser Begriff mißbräuchlich verwendet wurde. Bei einer Stelle wurde dies sogar für einen bestimmten Personenkreis generell so gehandhabt. Ich habe erreicht, daß inzwischen diese Praxis aufgegeben wurde, wovon ich mich stichprobenartig bei Kontrollen in diesem Jahr überzeugt habe. Mit einer anderen Stelle, bei der ich diese „Sprachregelung" für eine bestimmte

Fallgruppe erst vor kurzem anläßlich einer Einzelfallprüfung festgestellt habe, bin ich noch im Gespräch; ich gehe davon aus, daß man sich auch dort meiner Auffassung anschließt. Es geht nicht an, einen durch Richtlinien fest umrissenen und verfahrensmäßig definierten Begriff, wie den der Sicherheitsüberprüfung, als Anfragegrund anzugeben, wenn die nach den Richtlinien geforderten Voraussetzungen nicht gegeben sind. Die angefragte Stelle muß sich darauf verlassen können, daß die Anfrage tatsächlich einer Sicherheitsüberprüfung dient, weil sie nur dann zur Auskunft berechtigt ist. Das gilt im übrigen auch für den Begriff „Einstellungsüberprüfung", der für den Bundesbereich in den Grundsätzen für die Einstellungsüberprüfung vom 17. Januar 1979 (BT-Drucksache 8/2482) ebenfalls genau festgelegt ist.

17.4 Entwicklungstendenzen in der Datenverarbeitung und im Recht

17.4.1

Bei fast allen Sicherheitsbehörden des Bundes werden derzeit beträchtliche Anstrengungen für den weiteren Ausbau der elektronischen Datenverarbeitung unternommen. Mehr und mehr kommt den Computern die Aufgabe zu, nicht nur den herkömmlichen Karteikasten zu ersetzen, sondern qualitative Fortschritte in der Datenverarbeitung zu realisieren. Die bloße „Registraturfunktion" der ADV wird zunehmend durch zusätzliche Komponenten ergänzt, wie Freitextverarbeitung, Verknüpfungen und bessere Recherchiermöglichkeiten.

Diese Neuentwicklungen bergen aus datenschutzrechtlicher Sicht auch neue Gefahren in sich. Die Freitextverarbeitung, d. h. die inhaltliche Erschließung nicht formatierter Angaben, kann die Neigung fördern, nicht mehr nach Sachlage, sondern nach „Computerlage" Entscheidungen zu treffen. Verknüpfungen können die gespeicherten Daten in einen mehrdimensionalen Zusammenhang bringen und ihnen dadurch eine neue Qualität geben. Damit wächst die Gefahr, daß Verbindungen zwischen Daten und damit letztlich Aussagen über Personen formalisiert, d. h. nach festen Regeln und im Einzelfall möglicherweise falsch zustande kommen. Neue Recherchiermöglichkeiten bringen die gespeicherten Daten in einen permanenten Auswertungszusammenhang, vervielfachen also ihre Nutzbarkeit, ohne daß die Aktualität und die Zuverlässigkeit der Aussagen diesen Bedeutungszuwachs immer rechtfertigen.

Neben diesen, hier nur skizzenhaft aufgeworfenen Fragen ergibt sich eine Fülle weiterer Probleme. Ihnen gerecht zu werden wird auch deshalb schwierig sein, weil schon bisher bestehende Probleme der Datenverarbeitung noch nicht gelöst sind. Die vor allem in den Anfangsjahren der ADV unbedenklich vorgenommenen umfangreichen Speicherungen sind noch bei keiner Sicherheitsbehörde des Bundes vollständig bereinigt. Auch im Jahre 1983 trifft trotz aller Anstrengungen die Aussage zu, daß praktisch alle Sicherheitsbehörden eine Fülle von Altfällen mit sich „herumschleppen", deren Bereinigung noch Jahre in Anspruch nehmen wird und die ein ständiges Fehlerpotential darstellen.

Es wäre auch nicht richtig, die Bereinigung der Bestände als ein einmaliges Problem anzusehen. Die Bereinigung stellt sich vielmehr den Sicherheitsbehörden als eine permanente Aufgabe. Die jetzt praktisch überall eingeführte Zeitspeicherung erleichtert zwar in Zukunft das Auffinden möglicherweise „bereinigungsreifer" Vorgänge. Gleichwohl muß stets zusätzlich noch eine Relevanzprüfung durchgeführt werden. Aus all diesen Gründen wäre es aus meiner Sicht besser gewesen, man hätte zunächst einmal die Bestandsbereinigung erledigt, bevor neue Verfahren der Datenverarbeitung eingeführt und hierbei zum Teil noch unbereinigte Datenbestände einbezogen werden.

17.4.2

Von den Neuentwicklungen verdient vor allem das System SPUDOK (Spurendokumentationssystem), das bei der Polizei in Anwendung ist, besondere Aufmerksamkeit. Es kann nicht nur, wie sein Name vermuten läßt, zur Dokumentation umfangreichen Spurenmaterials in großen Kriminalfällen eingesetzt werden, sondern es kann auch zum Aufbau beliebiger Sonderdateien, etwa im Bereich der Gefahrenabwehr, verwendet werden (so z. B. die SPUDOK-Datei „Bundestagswahlkampf" 1980, vgl. 3. TB, S. 50 sowie jüngst die Datei „Lage 1", vgl. unten Nr. 18.5). Seine umfangreichen Nutzungsmöglichkeiten, insbesondere die Möglichkeit, nach Begriffen und Namen im gesamten Bestand zu recherchieren, machen ein Durchdenken dieser neuen Formen der Datenverarbeitung notwendig. Da der Nutzen von SPUDOK-Anwendungen gerade auch darin besteht, durch Recherche Verdachtsfälle zu ermitteln, zu dokumentieren oder auszuräumen, ist die Speicherung sogenannter „anderer Personen", d. h. von Personen die noch nicht als Beschuldigte, Verdächtige oder Störer erkannt sind, geradezu ein Wesensmerkmal der SPUDOK-Anwendungen. Aus datenschutzrechtlicher Sicht kommt deswegen der Einhaltung der Nr. 4.5 der Dateienrichtlinien, wonach diese sogenannten „anderen Personen" von der Speicherung zu unterrichten sind, sofern diese ein Jahr überschreitet, besondere Bedeutung zu. Die Bestrebungen der Polizei gehen aber zumindest zum Teil in die entgegengesetzte Richtung. Da nach Nr. 4.5.2 der Dateienrichtlinien die Unterrichtung zurückgestellt werden kann, solange durch sie der mit der Speicherung verfolgte Zweck gefährdet würde, wird mitunter diese Ausnahmevorschrift für SPUDOK-Dateien zur Regel erhoben.

17.4.3

Im Arbeitskreis II der Innenministerkonferenz wurde am 26./27. September 1983 der Antrag behandelt, die nach Nr. 4.5 der Dateienrichtlinien vorgeschriebene Unterrichtung der „anderen Personen" über die Tatsache der Speicherung im Bereich der Terrorismusbekämpfung statt nach einem Jahr erst nach drei Jahren vorzunehmen. Der Antrag wurde an die AG Kripo zur weiteren Begründung zurückverwiesen.

Aus datenschutzrechtlicher Sicht muß diese Entwicklung mit großer Sorge betrachtet werden. Die Speicherung „anderer Personen" als Verdächtiger und Beschuldigter begegnete von Anfang an großen Bedenken der Datenschutzbeauftragten in Bund und Ländern. Die entsprechende Bestimmung in den Dateienrichtlinien wurde letztlich hingenommen, weil die Unterrichtungspflicht nach Nr. 4.5 als ein hinreichendes Korrektiv betrachtet wurde. Die praktische Aushöhlung der Nr. 4.5 würde den in den Dateienrichtlinien gefundenen Ausgleich zwischen Datenschutz und Sicherheit einseitig zu Lasten des Datenschutzes verändern.

Dies wäre um so bedauerlicher, als der neue, maschinenlesbare Personalausweis gerade in diesem Bereich neue Probleme schaffen könnte. Unter den sogenannten „anderen Personen" machen die Begleitpersonen im Rahmen der polizeilichen Beobachtung einen beträchtlichen Anteil aus. Erhöht sich durch die Maschinenlesbarkeit des Ausweises die Zahl der fahndungsmäßigen Überprüfungen, so erhöht sich mit statistischer Gesetzmäßigkeit die Zahl der „Trefferfälle" aus dem Bereich der polizeilichen Beobachtung. In jedem dieser Fälle ist es möglich, daß Begleitpersonen festgestellt, gemeldet und gespeichert werden. Nach Einführung des maschinenlesbaren Ausweises kann sich demnach die Zahl der gespeicherten „anderen Personen" erhöhen. Um so wichtiger ist es aus meiner Sicht, daß die flankierenden datenschutzrechtlichen Vorschriften nicht verschlechtert werden. Die Verschärfung der Probleme durch die Einführung des maschinenlesbaren Personalausweises zwingt vielmehr dazu, daß nunmehr endlich die seit Jahren geforderten klaren und rechtsstaatlich vertretbaren gesetzlichen Grundlagen für diesen Bereich geschaffen werden.

Dies gilt auch für die Vorschriften über die Amtshilfe des Bundesgrenzschutzes für die Nachrichtendienste. Die im Jahre 1981 gefundene Neuregelung berücksichtigt nur einen Teil der seinerzeitigen datenschutzrechtlichen Forderungen. Veränderungen dieser Regelungen zu Lasten des Datenschutzes wären auch im Hinblick auf den neuen maschinenlesbaren Ausweis Anlaß zur Sorge. Ein Teil der neuen Amtshilferegelung, nämlich die sogenannte „benannte Amtshilfe", deren Einzelheiten hier nicht dargelegt werden können, basiert auch auf dem elektronischen Fahndungssystem der Polizei. Mehr Abfragen im INPOL-Fahndungssystem mit Hilfe des maschinenlesbaren Ausweises würden auch insoweit zu mehr „Trefferfällen" und damit zur Erhebung, Übermittlung und Speicherung von mehr Daten führen. Um so mehr besteht deshalb aus meiner Sicht Anlaß, die bestehende Amtshilferegelung datenschutzrechtlich nicht zu verschlechtern.

Insgesamt werden sich für den Datenschutz im Sicherheitsbereich in den kommenden Jahren neue Aufgaben stellen. Die technische Weiterentwicklung hat in jüngster Zeit gerade bei den Sicherheitsbehörden ein beachtliches Tempo angenommen. Dies gilt nicht nur hinsichtlich der Polizei und des hier erwähnten Systems SPUDOK, sondern auch für den MAD und das BfV. Auch dort laufen die Planungen in die vorstehend beschriebene Richtung. Wenn dadurch nicht der Datenschutz ausgehöhlt werden soll, ist eine Weiterentwicklung der bestehenden Datenschutzvorschriften und Richtlinien notwendig, nicht aber deren Abbau.

18. Bundeskriminalamt

18.1 Kontrolle beim Bundeskriminalamt als Nationales Zentralbüro von Interpol

18.1.1

Zweck der diesjährigen Prüfung der Tätigkeit des Bundeskriminalamtes als Nationales Zentralbüro im Rahmen der internationalen kriminalpolizeilichen Organisation (Interpol) war festzustellen,

— ob und inwieweit die von der Generalversammlung von Interpol im Oktober 1982 beschlossenen datenschutzrechtlichen Regelungen den Auskunftsverkehr verbessert haben (vgl. 5. TB S. 91 f. zu b) und

— ob die vom Bundeskriminalamt im Anschluß an die Prüfung 1982 zugesagten Verbesserungsmaßnahmen durchgeführt wurden (vgl. 5. TB S. 92 c).

In den entscheidenden Punkten, die bereits Gegenstand der Erörterungen im Zusammenhang mit der Prüfung im Jahr 1982 waren, hat sich gezeigt, daß die Schwachstellen nicht behoben worden sind. Sie stellen zum Teil allgemeine, auch im Inland auftretende Probleme dar, die unter dem Gesichtspunkt der Nachberichtspflicht und der Relevanzprüfung vor Auskunftserteilung bereits oben zu 17.2.1 und 17.2.2 angesprochen wurden.

Hervorzuheben ist vor allem, daß Erkenntnisse übermittelt wurden

— unter Verstoß gegen die eigenen Löschungsfristen,

— ohne nähere Überprüfung der aktuellen Relevanz,

— trotz fehlender Erforderlichkeit oder unter Verstoß gegen den Grundsatz der Verhältnismäßigkeit.

Darüber hinaus wurden in keinem überprüften Fall Hinweise auf interne Fristenregelungen bei der Übermittlung an die ausländischen Polizeidienststellen gegeben. Dies ist jedoch unerläßliche Voraussetzung dafür, daß innerstaatliche Schutzregelungen auch nach Datenübermittlung an ausländische Dienststellen wirksam bleiben.

In den beiden letztgenannten Fallgruppen liegen gleichzeitig Verstöße gegen die neuen Interpol-Regelungen vor.

Erfreulicherweise haben der Bundesminister des Innern und das Bundeskriminalamt auf meine entsprechenden Beanstandungen zugesagt, durch geeignete Maßnahmen mit Nachdruck für Abhilfe zu sorgen. Ich werde mich hiervon im nächsten Jahr überzeugen.

18.1.2

Die Prüfung beim BKA hat darüber hinaus erneute Hinweise auf mögliche Probleme bei der Datenverarbeitung des Generalsekretariats von Interpol ergeben, die dort dringend einer unabhängigen Überprüfung bedürfen. Es ist daher zu hoffen, daß die in den Richtlinien vorgesehene unabhängige Kontrollkommission baldmöglichst eingerichtet wird und ihre Arbeit aufnimmt. Die Voraussetzung hierfür ist durch die kurz vor Drucklegung dieses Berichts erfolgte Ratifizierung des neuen Sitzstaatabkommens zwischen der Französischen Republik und Interpol durch die Französische Nationalversammlung geschaffen.

Was den Nachrichtenaustausch zwischen den Nationalen Zentralbüros anbelangt, so hat sich auch die Notwendigkeit von Gegenkontrollen bei dem jeweiligen ausländischen Nationalen Zentralbüro des Empfängerstaats gezeigt, die nur durch die zuständige Nationale Datenschutzkontrollbehörde durchgeführt werden können. Um hier zu einem einheitlichen Verfahren zu kommen, soll auf Wunsch der 5. Internationalen Konferenz der Datenschutzbeauftragten in Stockholm die Interpol-Arbeitsgruppe der Konferenz erneut im Frühjahr 1984 einberufen werden, um entsprechende Beschlüsse vorzubereiten. Ich werde bei dieser Gelegenheit auch anregen, daß die Arbeitsgruppe Vorschläge für die Tätigkeit der unabhängigen Interpol-Kontrollinstitution unterbreitet und insbesondere Löschungsrichtlinien für die zentrale Datenverarbeitung beim Generalsekretariat ausarbeitet. Mit der Verabschiedung vertretbarer Löschungsrichtlinien für das Generalsekretariat von Interpol wäre ein wesentlicher Schwachpunkt der bisherigen Regelungen behoben (vgl. 5. TB S. 92). Zu der von mir im letzten Tätigkeitsbericht aufgeworfenen Frage der Bindungswirkung von Entscheidungen des vorgesehenen unabhängigen Kontrollorgans hat mittlerweile die Bundesregierung in ihrer Stellungnahme zum Fünften Tätigkeitsbericht klargestellt, daß sie von einer solchen bindenden Wirkung ausgehe. Ich werde diese Interpretation der Arbeitsgruppe mitteilen und darum bitten, eine entsprechende Klarstellung auch von den anderen Regierungen zu erwirken. Im übrigen muß die Praxis der noch zu konstituierenden Kommission abgewartet werden.

18.2 Einsatz von Videoeinrichtungen im Rahmen der Aktion „PADDY"

Im Zusammenhang mit dem befürchteten Anschlag auf den amerikanischen General Kroesen wurden vom Bundeskriminalamt im Raum Heidelberg-Mannheim Wohnobjekte akut gefährdeter Militärpersonen observiert. Während dieser Zeit hat das Bundeskriminalamt Video-Bandaufzeichnungen gefertigt. Hierdurch wurden vorübergehend alle Bewegungsabläufe von Personen, die sich in dem observierten Raum befanden, aufgezeichnet. Die Aufzeichnungen wurden jeweils kurz nach der Auswertung vernichtet. Daneben wurden noch andere fahndungstaktische Maßnahmen ergriffen. Das Bundeskriminalamt war hier rechtlich zur Unterstützung der für die Gefahrenabwehr zuständigen Landespolizei von Baden-Württemberg tätig.

Nach Abschluß der Aktion „PADDY" habe ich beim Bundeskriminalamt eine datenschutzrechtliche Prüfung durchgeführt, die sich auf die noch bestehenden Unterlagen erstreckte.

Entgegen den vielfach in verschiedenen Pressepublikationen geäußerten Befürchtungen haben sich bei meiner Prüfung keine Anhaltspunkte dafür ergeben, daß personenbezogene Speicherungen in Karteien oder Dateien durch das Bundeskriminalamt vorgenommen worden sind. Die am Einsatzort geführte Kfz-Kennzeichen-Kartei war bereits vernichtet; darüber besteht ein Vernichtungsvermerk. Lediglich in drei Fällen sind aus dieser Kfz-Kennzeichen-Datei Kraftfahrzeugkennzeichen in das System PIOS eingestellt worden. Die Prüfung der Dateiauszüge PIOS ergab, daß diese Hinweise ohne Personenbezug und somit nur als reiner Spurenhinweis gespeichert sind.

Außerdem habe ich ein Tagebuch eingesehen, in dem die Personen und Kfz-Kennzeichen festgehalten waren, die auf polizeiliche Relevanz im Zusammenhang mit der Personenschutzmaßnahme durch den Einsatz von Video-Geräten überprüft worden waren. Anläßlich meiner Prüfung und aufgrund der übereinstimmenden Feststellung, daß die Aufbewahrung dieser Aufzeichnung nach dem Abschluß der Maßnahmen nicht mehr erforderlich ist, ist auch dieses Tagebuch vernichtet worden.

Ob dieses Ergebnis auch für andere Maßnahmen des Bundeskriminalamts gilt, die mit Hilfe von Videoaufzeichnungen durchgeführt wurden, habe ich noch nicht überprüft. In Zukunft wird jedenfalls dem Aspekt des Einsatzes neuer Technologien, deren sich die Polizeibehörden in zunehmendem Maße bedienen, gerade unter datenschutzrechtlicher Sicht größte Beachtung geschenkt werden müssen (s. auch oben Nr. 17.4).

18.3 BKA — Abteilung Staatsschutz

18.3.1

Im Jahre 1982 habe ich die Datenverarbeitung bei der Abteilung Staatsschutz des Bundeskriminalamtes kontrolliert und hierüber im Fünften Tätigkeitsbericht (S. 89 f.) berichtet. Inzwischen hat das Bundeskriminalamt zu meinem Prüfbericht Stellung genommen. Die Beanstandungen wurden im wesentlichen als berechtigt anerkannt. Die Datensätze in den beanstandeten Einzelfällen sind inzwischen bis auf wenige Ausnahmen gelöscht worden.

Zur Bereinigung seiner Bestände hat das Bundeskriminalamt eine Arbeitsgruppe von 15 Mitarbeitern gebildet. Seit Mai 1982 bis Juni 1983 wurden nach Mitteilung des Amtes ca. 50 000 Personendatensätze gelöscht. Dies ist ca. ein Viertel der Gesamtbestände.

Die Arbeitsgruppe des Bundeskriminalamtes, Abteilung Staatsschutz, arbeitet die Vorgänge systematisch durch. Deshalb werden verschiedene, von mir besonders gerügte Gruppen von Speicherungen, z. B. die Speicherung von Zeugen und Hinweisgebern, nicht gezielt vorab bereinigt, sondern in die allgemeine Löschungsaktion sukzessiv einbezogen. Wegen des hohen Arbeitsaufwandes, den es aufgrund der Struktur der Dateien der Abteilung Staatsschutz bedeuten würde, derartige Sondergruppen von gespeicherten Daten vorab zu löschen, bestehen gegen die Vorgehensweise der Abteilung Staatsschutz keine datenschutzrechtlichen Bedenken. Die Löschungsaktion wird nach Mitteilung des Bundeskriminalamtes fortgesetzt, bis die Bereinigung der Aktenbestände abgeschlossen ist.

Das Bundeskriminalamt hat mir ferner mitgeteilt, es werde im Rahmen der Schulung der Mitarbeiter verstärkt darauf hinwirken, daß aus löschungsreifen Vorgängen keine Daten mehr an andere Behörden übermittelt werden.

18.3.2

Indessen möchte das Bundeskriminalamt nicht in allen Fällen meinen geäußerten Bedenken Folge leisten. So hatte ich vorgeschlagen, daß die Abteilung Staatsschutz sich nach einer bestimmten Frist (etwa zwei bis drei Jahre) selbst nach dem weiteren Fort- und Ausgang eingeleiteter Verfahren erkundigt. Der Hintergrund meines Vorschlags war, daß nach meinen Feststellungen das Bundeskriminalamt zu einem ganz überwiegenden Teil nur von der Einleitung eines Verfahrens Kenntnis erhält und daraufhin die Speicherung vornimmt. Die sich daraus ergebende Problematik ist oben unter Nr. 17.2.2 (a) dargestellt. Sie stellt sich beim Bundeskriminalamt als Zentralstelle deshalb in besonderer Weise, weil es selbst nur in vergleichsweise wenigen Fällen die Ermittlungen führt. Zumeist ist es darauf angewiesen, von den Landespolizeibehörden über den Fortgang der Verfahren informiert zu werden. Da diese Information bislang offensichtlich weitgehend nicht stattfindet, habe ich dem Bundeskriminalamt vorgeschlagen, sich nach einer bestimmten Frist selbst zu erkundigen. Ich stehe auf dem Standpunkt, daß es einer allgemeinen datenschutzrechtlichen Pflicht entspricht und das Bundeskriminalamt auch selbst Verantwortung dafür trägt, daß die Datenbestände möglichst aktuell sind und unberechtigte Speicherungen vermieden werden.

Weitere hiermit im Zusammenhang stehende, aus meiner Sicht besonders bedauerliche Meinungsunterschiede ergeben sich bei der Frage, welcher Qualität Daten sein müssen, die an andere Behörden übermittelt werden. Wie an anderer Stelle näher ausgeführt (s. Nr. 17.2.2 [b]), stehe ich auf dem Standpunkt, daß das Bundeskriminalamt Daten an andere Stellen nur dann übermitteln darf, wenn es sich zuvor erkundigt hat, welchen Ausgang das jeweilige Verfahren hat. Ansonsten wird unnötig über den Betroffenen Verdacht gestreut, der sich möglicherweise längst als haltlos erwiesen hat. Umgekehrt kann es für die empfangende Behörde auch von Bedeutung sein zu wissen, daß sich etwa ein Verdacht bestätigt hat.

Leider hat das Bundeskriminalamt meine Vorschläge abgelehnt. Das — auch in diesem Zusammenhang wieder vorgebrachte — Argument der Arbeitsbelastung ist nach meiner Ansicht nicht stichhaltig. Zum einen muß eine speichernde Stelle eine gewisse Arbeitskapazität für die ständige Bestandspflege auch zugunsten der Betroffenen aufwenden. Zum anderen führen die für die Abteilung Staatsschutz geltenden Fristenregelungen dazu, daß eine Vielzahl der vor allem leichteren Fälle bereits nach zwei oder drei Jahren gelöscht wird. Eine aktive Erkundigung wäre also nicht in allen, vermutlich nicht einmal im überwiegenden Teil der Fälle notwendig. Eine derartige Belastung halte ich im Interesse der Betroffenen für zumutbar, zumal auch das Bundeskriminalamt selbst Interesse an möglichst vollständigen Daten haben muß. Das ergibt sich bereits aus § 14 Abs. 1 BDSG. Ich werde daher auch weiterhin versuchen, das Amt zu einer Änderung seiner Haltung zu bewegen. Im Falle der Übermittlungen im Interpolverkehr mußte ich dieses Verhalten des Bundeskriminalamts wegen der besonderen Gefahren bei Übermittlung unüberprüfter Daten an ausländische Polizeibehörden beanstanden (s. o. Nr. 18.1.1). Die daraufhin für den Interpolverkehr zugesagten Verbesserungen sollten auch in anderen Bereichen eingeführt werden.

18.3.3

Differenzen bestehen mit dem Bundeskriminalamt darüber hinaus über den Umfang des Zweckbindungsprinzips. Ich habe in meinem Prüfbericht die Auffassung vertreten, daß Daten, die nur für eine bestimmte Aufgabe erhoben werden, dann auch nur für diese Aufgabe verwendet werden dürfen. Aus der Sicht der Spionageabwehr ist beispielsweise bisweilen die Erhebung und Speicherung von Daten notwendig, die für den allgemeinen Staatsschutz in dieser Form von mir nicht für zulässig erachtet würden. Es kann aber nicht angehen, daß derartige Daten, einmal erhoben, dann für jedwede andere Aufgabenerfüllung, insbesondere auch für die Übermittlung an andere Behörden, zur Verfügung stehen. Ich werde mich deswegen auch weiterhin für eine Beachtung des Zweckbindungsprinzips in dem beschriebenen Sinn einsetzen. Erste Teilerfolge in dieser Hinsicht sind z. B. bei der Formulierung der Errichtungsanordnungen für SPUDOK-Dateien sowie bei der Neuregelung der Häftlingsüberwachung erzielt worden, wo dieser Aspekt besonders dringlich ist (s. o. Nr. 17.4.2 und 5. TB S. 90).

18.3.4

Das Bundeskriminalamt hat mir auch mitgeteilt, daß die beabsichtigte Einrichtung der Datei APIS

(Arbeitsdatei PIOS — Innere Sicherheit) sich verzögert. In der Datei APIS sollen künftig auch die Vorgänge der Abteilung Staatsschutz gespeichert werden (vgl. 5. TB S. 85 f.). Es handelt sich dabei um eine Datei auf der Basis eines verbesserten PIOS-Systems. Diese Datei kann also bei weitem mehr leisten als die bloße Registratur von Vorgängen. So können dort Personen, Institutionen, Objekte und Sachen miteinander verknüpft werden. Anhand des gespeicherten Datenumfangs und mit Hilfe des PIOS-Systems können umfangreiche Recherchen und Querschnittsauswertungen vorgenommen werden.

Meine Bedenken dagegen, daß auf diese Weise Methoden, die für die Terrorismusbekämpfung entwikkelt worden sind, auf den Bereich des allgemeinen Staatsschutzes übertragen werden, habe ich bereits im Fünften Tätigkeitsbericht (S. 86) dargelegt. Die Bedenken gegen die *Struktur* der geplanten Datei und die damit verbundenen Möglichkeiten bestehen fort.

Andererseits würde ich es begrüßen, wenn die Abteilung Staatsschutz des Bundeskriminalamtes nunmehr möglichst bald ein eigenes automatisiertes Aktennachweissystem erhielte. Solange dies nicht der Fall ist — und nach der neuerlichen Verzögerung werden bis zur Realisierung erneut ein bis zwei Jahre vergehen — speichert das Bundeskriminalamt, Abteilung Staatsschutz, seine Vorgänge im Verfassungsschutzsystem NADIS. Die Folge ist, daß, jedenfalls soweit jeweils Vorgänge zu ein und derselben Person bestehen, die Informationen hierüber wechselseitig im Online-Verkehr abgerufen werden können. Das Bundesamt für Verfassungsschutz und die Landesämter für Verfassungsschutz können also durch NADIS-Abfragen im Online-Verkehr feststellen, zu welchen Personen bei der Abteilung Staatsschutz des Bundeskriminalamtes Vorgänge existieren und umgekehrt. Daß dies eine unzulässige, weil nicht in jedem Einzelfall erforderliche, Datenübermittlung ist, die zudem gegen das verfassungsmäßig verankerte Gebot der Trennung von Polizei und Verfassungsschutz verstößt, habe ich bereits früher dargelegt (s. zuletzt 5. TB S. 79). Der erneute Aufschub der Einrichtung eines eigenen Aktennachweissystems der Abteilung Staatsschutz des Bundeskriminalamtes verlängert diesen m. E. rechtswidrigen Zustand.

18.4 BKA — Datei PIOS-TE

Im Jahre 1981 habe ich die Datei PIOS-TE beim Bundeskriminalamt einer datenschutzrechtlichen Kontrolle unterzogen. Über die Ergebnisse der Prüfung habe ich im Vierten Tätigkeitsbericht (S. 22 f.) und im Fünften Tätigkeitsbericht (S. 90) berichtet. Der Bundesminister des Innern hat mir mitgeteilt, daß im Jahre 1983 erneut mehrere tausend Personendatensätze in PIOS-TE gelöscht worden sind. Die zu diesem Zweck seit Anfang 1982 eingesetzte Bereinigungskommission führt ihre Arbeit weiter fort. Ich kann daher die im Fünften Tätigkeitsbericht gegebene insgesamt positive Wertung des Vorgangs wiederholen. In der datenschutzrechtlichen Kontrolle des Systems PIOS-TE und der danach folgenden systematischen Bereinigung des Systems sehe ich ein beispielhaftes Verfahren, das bis zu einem gewissen Grade nunmehr auch im Bereich BKA-Staatsschutz Anwendung findet (s. oben Nr. 18.3.1).

18.5 BKA — Datei „Lage 1"

Im Hinblick auf den erwarteten „heißen Herbst" wurde beim Bundeskriminalamt eine SPUDOK-Anwendung mit der Bezeichnung „Lage 1" eingerichtet. Es handelt sich dabei um eine Sonderdatei, in der Informationen im Zusammenhang mit Aktionen gegen die NATO-Nachrüstung verarbeitet werden. Ich habe gegenüber dem Bundesminister des Innern Bedenken gegen einzelne Ziffern der Errichtungsanordnung sowie Zweifel an der Erforderlichkeit der gesamten Datei geäußert. Auch stellt sich die Frage, ob das Bundeskriminalamt unter Berufung auf seine Zentralstellenkompetenz eine derartige Spezialdatei als Zentraldatei führen darf, und zwar aus folgendem Grund: Die Datei war ursprünglich als Verbunddatei geplant. Von den Ländern hat jedoch nur Bayern von der Möglichkeit eines Anschlusses Gebrauch gemacht. Inzwischen hat auch Bayern auf den Anschluß verzichtet. Aus der ursprünglich geplanten Verbunddatei ist eine Zentraldatei geworden, die überwiegend aus konventionell übermittelten Informationen im Rahmen anderer Meldedienste aus den Ländern aufgebaut ist. Inwieweit dies zulässig ist, könnte auch deshalb fraglich sein, weil verschiedene Länder von Anfang an Bedenken gegen diese Datei hatten und eine Mitarbeit speziell an dieser Datei ablehnten.

Der Meinungsaustausch mit dem Bundesminister des Innern zu diesen Fragen ist noch nicht abgeschlossen. Auch eine Prüfung des Dateiinhalts war mir bislang aus zeitlichen Gründen noch nicht möglich. Da die Datei nicht nur, wie ursprünglich vorgesehen, bis zum 31. Dezember 1983, sondern nun bis zum 31. März 1984 geführt werden soll, beabsichtige ich, im nächsten Tätigkeitsbericht ausführlicher auf die „Lage 1" und insbesondere auf die Frage einzugehen, inwieweit beim BKA auch SPUDOK-Anwendungen zur Gefahrenabwehr betrieben werden können.

19. Bundesgrenzschutz

Im Berichtsjahr habe ich eine größere datenschutzrechtliche Prüfung bei der Grenzschutzdirektion in Koblenz durchgeführt. Diese erstreckte sich schwerpunktmäßig auf die Datenverarbeitung der dortigen Fahndungsleitstelle. Die Prüfung diente primär dem Zweck zu klären, ob die Zusagen, die mir im Jahre 1980 gegeben worden sind (vgl. 4. TB S. 30 f. unter Nr. 2.15.1 b) eingehalten wurden. Ich habe feststellen müssen, daß einige dieser Zusagen bisher nicht umgesetzt worden sind (s. unten dritter und vierter Anstrich). Ich gehe davon aus, daß sie — wie auch andere Prüfungsergebnisse — bei den Arbeiten an der Errichtungsanordnung für den im Aufbau befindlichen Grenzaktennachweis (GAN) noch berücksichtigt werden.

Bei dem Grenzaktennachweis handelt es sich um eine Datei, ähnlich dem beim Bundeskriminalamt bestehenden KAN, in der sämtliche Akten, die bei der Grenzschutzdirektion vorhanden sind, registriert werden sollen. Die Datei soll in einem geschützten Index des Bundesgrenzschutzes beim Bundeskriminalamt geführt werden.

Aufgrund meiner Prüfungsfeststellungen habe ich den Bundesminister des Innern und die Grenzschutzdirektion auf folgende Sachverhalte, die datenschutzrechtlich bedenklich und bei der Errichtung des Grenzaktennachweises änderungsbedürftig sind, hingewiesen:

— Zentrale Registrierung von Strafanzeigen für fünf Jahre, auch soweit keine abschließende Sachbearbeitung durch Stellen des Grenzschutzes erfolgt; fehlende Verkürzung von Fristen für Jugendliche und Kinder

— Registrierung von Anzeigen der Grenzschutzämter über Ordnungswidrigkeiten, obwohl sie bisher selbst bei den Grenzschutzämtern nicht vorgenommen wird

— Registrierung aller kriminaltaktischer Anfragen, auch soweit bei der Grenzschutzdirektion keinerlei grenzrelevante Vorgänge bestehen und/oder die Anfragen im übrigen keinen grenzrelevanten Bezug aufweisen

— Registrierung von nachrichtlich zugeleiteten Hinweisen über Fahndungsausschreibungen von Inlandsbehörden ohne erkennbare Grenzschutzrelevanz.

Allgemein habe ich noch darauf hingewiesen, daß neben der Registrierung von Personenakten im GAN grundsätzlich parallel im Bundeskriminalamt eine Registrierung in der E-Gruppe (erkennungsdienstliche Hinweise) des KAN und/oder in der Daktyloskopie-Datei erfolgt, soweit es um Personen geht, die erkennungsdienstlich behandelt worden sind. Diese Unterlagen, die ebenfalls ausschließlich für Zwecke des Grenzschutzes angefertigt worden sind, sind also zentral für alle Verbundteilnehmer des KAN verfügbar. Die im übrigen abgeschottete Speicherung von Grenzschutzakten ist insoweit durchbrochen. Hier stellt sich daher die gleiche Frage hinsichtlich des Umfangs der Zentralstellenkompetenz des Bundeskriminalamtes, wie ich sie im Verhältnis zu den Ländern mehrfach dargestellt habe (vgl. zuletzt 5. TB S. 88 f.).

Unabhängig davon hatte sich gezeigt, daß die Aufbewahrung der erkennungsdienstlichen Unterlagen verschiedentlich auch dann erfolgte, wenn keinerlei Anhaltspunkte für die Notwendigkeit zu vorbeugender Aufbewahrung der Unterlagen erkennbar waren. Die Fälle sind inzwischen bereinigt.

Anläßlich meiner Prüfung bei der Grenzschutzdirektion habe ich auch bemängelt, daß die Dateienübersicht nicht den gesetzlichen Anforderungen entspricht. Die Überarbeitung der bestehenden Übersicht ist mir kurzfristig zugesagt worden. Ich habe deshalb zunächst auf eine Beanstandung verzichtet.

Mit Schreiben vom 27. Dezember 1983 teilte mir der Bundesminister des Innern mit, daß die Übersicht nunmehr den gesetzlichen Anforderungen entsprechend erstellt worden sei. Ich werde dies bei nächster Gelegenheit überprüfen.

Gleichzeitig wurde mir erstmals der Entwurf eines Grenzaktennachweises vorgelegt. Eine erste Durchsicht ergab, daß mit Ausnahme einer Fristverkürzung für Kinder kaum eines der vorstehend aufgeführten Bedenken berücksichtigt ist, auf die ich in meinen Prüfungsfeststellungen hingewiesen hatte. Das betrifft vor allem auch die Registrierung von Fahndungshinweisen anderer Dienststellen oder kriminaltaktischer Anfragen ohne grenzrelevanten Bezug sowie die zentrale Registrierung aller Ordnungswidrigkeitsanzeigen im gesamten Zuständigkeitsbereich der Grenzschutzdirektion.

Eine eingehende Prüfung des mir erst kurz vor Drucklegung dieses Berichts zugeleiteten Entwurfs war mir noch nicht möglich. Näheres darüber werde ich daher erst im nächsten Jahr berichten.

20. Bundesamt für Verfassungsschutz

20.1 Prüfung beim Bundesamt für Verfassungsschutz

In der Zeit von März bis Oktober 1983 (mit Unterbrechungen) habe ich die Datenverarbeitung bei der Abteilung III des Bundesamtes für Verfassungsschutz (BfV) kontrolliert. Die Abteilung III ist für die Beobachtung linksextremistischer Bestrebungen zuständig. Bei der Prüfung handelt es sich um die bisher zeitaufwendigste Maßnahme dieser Art.

Die Aus- und Bewertung der festgestellten Sachverhalte war bei Drucklegung dieses Berichts noch nicht abgeschlossen. Einzelheiten der getroffenen Feststellungen werde ich deswegen erst in meinem nächsten Tätigkeitsbericht darstellen können.

20.1.1

Schon jetzt ist aber als Gesamteindruck festzuhalten, daß die Prüfung Anhaltspunkte sowohl für erfreuliche datenschutzrechtliche Fortschritte, wie auch für Verstöße gegen Datenschutzrecht erbracht hat. Insgesamt verfährt das BfV, was Neueinspeicherungen angeht, nach meinem Eindruck heute wesentlich zurückhaltender als in früheren Jahren. Die Frage, welche Personen im Rahmen der Extremismusbeobachtung gespeichert werden dürfen, ist in vergleichsweise detaillierten, innerdienstlichen Vorschriften geregelt. Wenngleich daraus das Bestreben erkennbar ist, aus der Fülle der eingehenden Informationen nur die für die Erfüllung der gesetzlichen Aufgaben relevanten zu speichern, so sind diese Richtlinien nach meiner Ansicht an einigen Stellen zu weit gefaßt. Im Ergebnis kann dies dazu führen — wie die Prüfung ergeben hat —, daß auch heute noch Personen gespeichert werden, die meines Erachtens nicht als Träger verfassungsfeindlicher Bestrebungen anzusehen sind. Dabei verstehe ich den Begriff „Träger" nicht nur im Sinne einer Funktionsträgerschaft, sondern auch als Kriterium für eine bedeutsame aktive Betätigung im Sinne eines individuellen Beitrages der betreffenden Person für die beobachtete Bestrebung. Ich werde dem BfV diesbezüglich Vorschläge zu einer noch präziseren und teilweise engeren Fassung der Richtlinien unterbreiten. Durch differenzierende Vorschläge, z. B. abgestufte Zeitspeicherung, kann auch dem Umstand Rechnung getragen werden, daß das BfV auch Verdachtsmomenten nachzugehen hat.

20.1.2

Problematisch sind beim BfV, so wie bei anderen Sicherheitsbehörden auch, die sogenannten „Altfälle", d. h. diejenigen Fälle, die nach den für das BfV geltenden Fristenregelungen zu überprüfen und in der Regel zu löschen wären, aber noch nicht gelöscht sind. Hinzu kommen diejenigen Fälle, die vor Erlaß des Bundesdatenschutzgesetzes und damit unter Zugrundelegung eines teilweise sehr weiten Aufgabenverständnisses gespeichert worden sind. Es wird für das BfV großer Anstrengungen bedürfen, diese Datenbestände zu löschen. Erst seit zwei Jahren wird beim BfV und somit auch bei der Abteilung III des BfV ein Wiedervorlage- bzw. Löschungsdatum in der Datei gespeichert. Bei der Einführung eines entsprechenden Datenfeldes wurde bei den bestehenden Datensätzen anhand einer Protokolldatenauswertung an die letzte Änderung des Datensatzes angeknüpft, auch wenn es sich dabei nur um eine Anschriftenänderung o. ä. handelte. Dies bedeutet im Ergebnis, daß frühestens im Jahre 1996 die sichere Einhaltung der 15-Jahres-Speicherfrist gewährleistet ist, wenn man sich nur auf die Hilfestellung der automatisierten Datenverarbeitung stützt.

Dies ist aus datenschutzrechtlicher Sicht deshalb bedenklich, weil die Prüfung gezeigt hat, daß die zu löschenden Daten noch verwertet werden: Zum einen bleiben sie im Verbundsystem NADIS gespeichert (nämlich die Personengrunddaten, einige Zusatzinformationen sowie das Aktenzeichen) und sind damit insoweit für die anderen NADIS-Teilnehmer direkt abrufbar; zum anderen werden aus derartigen Datenbeständen auch noch auf konventionellem Wege Daten übermittelt, bevor sie gelöscht werden (vgl. auch oben Nr. 17.2.2).

20.1.3

Bereits in früheren Tätigkeitsberichten (4. TB S. 22, 5. TB S. 79) habe ich meine Auffassung dargelegt, daß das verfassungskräftige Gebot der Trennung von Polizei und Nachrichtendiensten einem umfassenden Datenaustausch entgegensteht. Speziell zur Frage der Übermittlung von Daten, die von der Polizei im Wege einer Hausdurchsuchung gewonnen wurden, habe ich ausgeführt (5. TB S. 93 f.), daß auch die Verwertungsvorschriften der Strafprozeßordnung (§§ 108 ff.) einer Übermittlung dieser Daten an den Verfassungsschutz entgegenstehen. In einer Reihe von Fällen sind Daten von der Polizei an den Verfassungsschutz in einem Umfang übermittelt worden, den ich mit dem Trennungsgebot und den vorgenannten Bestimmungen nicht für vereinbar halte.

20.1.4

Bei vielen der von mir festgestellten Sachverhalte stellen sich grundsätzliche Fragen der Zulässigkeit der Speicherung von Personen wegen Verhaltensweisen, die sich als Ausübung von Grundrechten darstellen, etwa die Teilnahme an genehmigten Demonstrationen oder die Äußerung kritischer Mei-

nungen. Zwar wäre der Eindruck unzutreffend, das BfV speichere in massenhaftem Umfang derartige Informationen. Eher ist das Gegenteil der Fall. Es kann auch nicht davon ausgegangen werden, daß die Grundrechtsausübung einem Tätigwerden des BfV von vornherein entgegensteht. Gleichwohl bestehen in einer Reihe der von mir überprüften Fälle Bedenken, ob bei der Entscheidung über die Speicherung hinreichend berücksichtigt worden ist, daß durch eine solche Praxis die Ausübung von Grundrechten beeinträchtigt werden kann (vgl. auch Urteil des Bundesverfassungsgerichts zur Volkszählung 83 vom 15. Dezember 1983, 1 BvR 209/83, S. 45 f.).

20.1.5

Zumeist stellt sich beim Verfassungsschutz unter datenschutzrechtlichen Gesichtspunkten primär die Frage, ob und wie lange eine Person gespeichert sein darf. In einigen in die Prüfung einbezogenen Teilbereichen haben sich darüber hinausgehend Fragen ergeben. Dort werden — z. B. für Zwecke der Identifizierung — auch Daten gespeichert, die in erheblichem Maße in die Intimsphäre hineinreichen. Ich habe zum gegenwärtigen Zeitpunkt Zweifel an der Erforderlichkeit und unabhängig davon an der generellen Zulässigkeit der Speicherung derartiger Merkmale, da diese Daten möglicherweise den Kernbereich des Persönlichkeitsrechts betreffen.

20.1.6

Im Laufe der Kontrolle wurde mir bekannt, daß das Bundesamt für Verfassungsschutz begonnen hat, nach einem sogenannten „Rahmenkonzept für Personenarbeitsdateien" die Datenverarbeitung zu „modernisieren", d. h. insbesondere komfortabler zu gestalten. Dies bedeutet vor allem, daß auch Datenbestände, die bislang nur manuell geführt wurden, nunmehr im automatisierten Verfahren verarbeitet werden sollen. Die Neukonzeption wird die Möglichkeit eröffnen, den Umfang der zu einzelnen Personen gespeicherten Informationen und damit auch die Auswertungsmöglichkeiten zu erweitern. Die Einzelheiten des neuen Konzepts und etwaige datenschutzrechtliche Bedenken hiergegen müssen noch mit dem BfV erörtert werden. Unabhängig davon hätte ich es allerdings begrüßt, wenn zuerst die bestehenden Datenbestände bereinigt würden, bevor an eine Neukonzeption des Systems gegangen wird.

20.2 BfV-Datei NADIS-PET

In meinem Vierten und Fünften Tätigkeitsbericht (S. 28 bzw. 94) habe ich von der Prüfung einer Sonderdatei des BfV im Zusammenhang mit der Terrorismusbekämpfung berichtet. Es handelt sich dabei um die Datei NADIS-PET. Hierzu ist mir inzwischen eine weitere Stellungnahme des Bundesministers des Innern zugegangen. Danach wurden bis auf eine Ausnahme inzwischen die Daten in allen von mir beanstandeten Einzelfällen gelöscht.

In meinem Prüfbericht hatte ich auch ganz allgemein und unabhängig von NADIS-PET an einigen Formen der Datenverarbeitung bei der Abteilung VII des BfV (für die Terrorismusbekämpfung zuständige Abteilung) Kritik geübt. Der Bundesminister des Innern hat mir nunmehr mitgeteilt, daß derzeit in der Abteilung VII eine gezielte und systematische Bereinigungsaktion abläuft. Sie habe von Anfang 1982 bis Anfang 1983 in über 10 000 Fällen die Löschung von Datensätzen in NADIS zur Folge gehabt.

Eine endgültige Stellungnahme zu der von mir ebenfalls aufgeworfenen Frage nach der Erforderlichkeit der gesamten Datei NADIS-PET sowie zu den grundsätzlichen Fragen des Amtshilfeverfahrens unter den Sicherheitsbehörden in Fragen der Terrorismusbekämpfung ist mir bislang noch nicht zugegangen. Der Bundesminister des Innern hat mir kurz vor Drucklegung des Berichts mitgeteilt, daß die von mir veranlaßte Prüfung inzwischen abgeschlossen und hiernach die Erforderlichkeit zu bejahen sei.

Ich werde mich mit den dafür ausschlaggebenden Argumenten befassen, sobald sie mir im einzelnen zugeleitet sind.

20.3 Weitere Bereinigungsaktionen des BfV

Das BfV hat mir mitgeteilt, daß auch im Jahre 1983 verschiedene Bereinigungsaktionen durchgeführt worden sind. Seit 1972 wurden in der NADIS-Personenzentraldatei auch Hinweisdaten der Personen gespeichert, die das Amt für Sicherheit der Bundeswehr einer Sicherheitsüberprüfung der Stufe II, bei Vorliegen besonderer Umstände auch der Stufe I, unterzog. Die Einspeicherung derartiger Daten wurde im September 1983 eingestellt, die bis dahin gespeicherten Daten wurden im November 1983 gelöscht. Dies hat im Ergebnis zur Löschung von ca. 360 000 Personendatensätzen in NADIS geführt.

Daneben wurden ca. 200 000 Notierungen gelöscht Da zu einer Personen mehrere Notierungen bestehen können, bedeutet dies nicht, daß damit auch 200 000 Personendatensätze gelöscht worden sind (vgl. oben Nr. 17.2.1 a)). In dieser Zahl sind auch die durch die Abteilung Staatsschutz des BKA vorgenommenen Löschungen enthalten (vgl. dazu oben Nr. 18.3.1). Zahlen über die im Berichtsjahr vorgenommenen Neueinspeicherungen liegen mir nicht vor.

Außerdem, so hat mir das BfV mitgeteilt, wurden im November 1983 einige Daten in der NADIS-Personenzentraldatei gelöscht, die über den Hinweischarakter dieser Datei hinausgingen.

Beide Vorgänge belegen, daß das Amt auch selbst, unabhängig von meinen Kontrollen und deren Ergebnissen, Anstrengungen unternimmt, nicht mehr erforderliche Daten zu löschen und die Bestände zu bereinigen.

21. Bundesnachrichtendienst

21.1 Gesamteindruck

Beim Bundesnachrichtendienst (BND) ist trotz seiner Sonderstellung und trotz der Probleme, die bei meinen Kontrollen in diesem Jahr aufgetreten sind bzw. nach wie vor bestehen (s. u. Nr. 21.2 und 21.3), eine insgesamt erfreuliche Tendenz zur Fortentwicklung des Datenschutzes erkennbar. Das zeigt sich z. B. daran, daß in einem bestimmten Bereich, in dem noch vor rund zwei Jahren recht „großzügig" gespeichert wurde, eine deutlich höhere Relevanz der Unterlagen gefordert und damit der Umfang der Speicherung reduziert wurde. Wo die Situation noch nicht geklärt ist, wird entsprechend meiner Empfehlung eine in der Regel auf zwei Jahre befristete Wiedervorlage verfügt, um dann in eine erneute Relevanzprüfung einzutreten. Darüber hinaus konnte bei der zuletzt durchgeführten Kontrolle der Übermittlungen an andere Dienststellen eine weitgehende Verbesserung gegenüber der bisherigen Praxis festgestellt werden (s. o. Nr. 17.2.2 b). Dies erhält besonderes Gewicht, weil gerade die *Übermittlung* durch den BND oft problematischer ist als die Speicherung für eigene Zwecke.

Durch die nunmehr festgestellte strengere Beachtung des Grundsatzes der Verhältnismäßigkeit, wie vorstehend beispielhaft gezeigt, wird das Defizit an gesetzlichen Grundlagen für die Tätigkeit des BND weitgehend gemildert. Ich bin jedoch nach wie vor davon überzeugt, daß es besser wäre und auch möglich ist, rechtsstaatlich substantielle Regelungen auch für die Tätigkeit des BND, soweit diese sich innerhalb der Bundesrepublik auswirkt, zu finden. Zumindest sollte der Versuch dazu unternommen werden.

21.2 Neue Grundsatzvereinbarungen

Bei den Kontrollen im Frühjahr dieses Jahres stellte ich mehrere Sachverhalte fest, die zum Teil mit früheren Erklärungen des BND, zum Teil mit den Löschungsrichtlinien und/oder mit dem Grundsatz der Verhältnismäßigkeit nicht vereinbar waren. Es handelte sich schwerpunktmäßig

— um die Frage der Löschung der Daten einer bestimmten Personengruppe nach Ablauf der Regelfrist von 15 Jahren,

— um die Übermittlung von Erkenntnissen über einen bestimmten anderen Personenkreis, der einen sehr bedeutenden Umfang bei der personenbezogenen Speicherung des BND einnimmt (er betrifft rund ein Sechstel der jährlichen Neueinspeicherungen); hier stand der Inhalt der Übermittlung, wie ich ihn mehrfach feststellen mußte, auch im Widerspruch zu anderen schriftlichen Erklärungen des BND;

— um die Frage, unter welchen Voraussetzungen eine weitere Speicherung nach Ablauf der fünfzehnjährigen Regelfrist zulässig ist. Es waren u. a. Fälle festgestellt worden, in denen z. B. reine Routineanfragen anderer Dienste eine Fristverlängerung ausgelöst haben, ohne daß aus der Anfrage Anhaltspunkte irgendwelcher Art erkennbar waren, die eine längere Speicherung rechtfertigen konnten; außerdem wurde festgestellt, daß nach der Struktur der Datenverarbeitung beim BND und der bisherigen Organisation die systematische Einhaltung der fünfzehnjährigen Überprüfungsfristen erst ab 1991 sichergestellt ist, weil das hierfür geeignete Auswertungskriterium, nämlich das Erfassungsdatum, erst seit 1976 gespeichert wird. Vorschläge, diesem Sachverhalt wenigstens teilweise durch organisatorische Maßnahmen abzuhelfen, wurden unter Berufung auf fehlende Arbeitskapazität zunächst abgelehnt.

Teils wegen der besonderen Bedeutung, teils wegen der Abweichung von früheren Absprachen habe ich die Datenverarbeitung in diesen Punkten beanstandet.

Inzwischen wurden für alle Fallgruppen Vereinbarungen getroffen, die meine bisherigen Bedenken weitgehend beseitigen:

Für die beiden ersten Fallgruppen werden die Übermittlungen inhaltlich erheblich eingeschränkt (s. auch Nr. 17.2.2 [b]). Hierdurch ist sichergestellt, daß bisher mögliche Rückschlüsse auf den der Speicherung zugrundeliegenden Sachverhalt bei bestimmten Personengruppen nicht mehr möglich sind. Nach Ablauf von 15 Jahren werden die Hinweise und Unterlagen über diese Personen grundsätzlich gesperrt. Sie stehen dann nur noch für bestimmte interne Zwecke des BND zur Verfügung. Bei Anfragen wird dann prinzipiell Negativauskunft erteilt. Ausnahmen hiervon sind nur möglich, wenn die gemeinsam definierten eng abgegrenzten Voraussetzungen hierfür vorliegen.

Bezüglich der letzten Fallgruppe besteht nunmehr Einigkeit darüber, daß für die Fristverlängerung allein auf die materielle Relevanz der jeweiligen neuen Erkenntnisse abgestellt werden darf. Sogenannte Routineanfragen, wie z. B. eine normale Anfrage im Zusammenhang mit der Sicherheitsüberprüfung entsprechend den hierfür ergangenen Richtlinien der Bundesregierung oder Anschriftenänderungen, können für sich ohne zusätzliche Anhaltspunkte keine Fristverlängerung auslösen. Zum Ausgleich dafür, daß bis 1991 die automatisierte Überprüfbarkeit der 15-Jahresfrist nicht möglich ist, wird in Fällen, die aus Anlaß einer Anfrage oder aus sonstigen Gründen zur Bearbeitung gelangen und bei denen nur noch ein Zeitraum von höchstens einem Jahr bis zum Ablauf der Regelfrist besteht,

sofort die Relevanzprüfung durchgeführt. Ergibt sich dann, daß ohne ein zusätzlich eintretendes Ereignis der Vorgang nach Ablauf der Restzeit vernichtet werden müßte, so wird dies sofort verfügt. Im übrigen wurde mir zugesagt, daß die oben zu Nr. 17.2.2 [b]) geforderte Relevanzprüfung vor jeder Auskunftserteilung künftig in der Regel durchgeführt wird. In Zweifelsfällen sollen auch hier nur dann Auskünfte erteilt werden, wenn sie unter die vorstehend erwähnten Ausnahmekriterien fallen. Ich halte diese Ergebnisse, deren Einhaltung ich überprüfen werde, für einen tragfähigen Kompromiß.

21.3 Noch ungelöste Probleme

Zu den noch offenen Fragen gehört u. a. der Umfang der Speicherung im Bereich der Beobachtung des internationalen Kommunismus. Hier bin ich der Auffassung, daß die personenbezogene Speicherung nur auf wichtigere Persönlichkeiten beschränkt sein, dagegen nicht unterschiedslos auf alle Mitglieder einer einschlägigen Organisation ausgedehnt werden sollte. Hierüber bin ich weiter im Gespräch mit der Dienststelle. Einzuräumen ist jedoch, daß diese Problematik beim BND weniger bedeutsam ist als etwa im Bereich des Verfassungsschutzes, weil es keine externen Online-Anschlüsse zu den Personendateien des Dienstes gibt. Die Auskunft wird zentral erteilt, um organisatorisch besser zu gewährleisten, daß irrelevante Auskünfte unterbleiben. Außerdem handelt es sich überwiegend um Daten von Personen, die sich in aller Regel in der Bundesrepublik nicht um eine Beschäftigung im öffentlichen Dienst bewerben werden, so daß — anders als beim BfV — eine Beeinträchtigung im Zusammenhang mit Einstellungs- oder Sicherheitsüberprüfungen weitgehend ausgeschlossen ist.

Auch die Tatsache, daß der Bestand der Altfälle in den letzten zwei Jahren nicht merklich abgenommen hat, bereitet mir nach wie vor Sorge. Der BND beruft sich demgegenüber stets auf mangelnde Arbeitskapazität. Dies ist ein Argument, das zunehmend weniger durchschlägt, nachdem das Datenschutzgesetz nunmehr seit über fünf Jahren und die Löschungsrichtlinien des BND seit mehr als drei Jahren in Kraft sind. Obwohl die datenschutzrechtliche Gefährdungslage beim BND wesentlich geringer ist als bei Zentralsystemen wie NADIS und INPOL, müssen auch hier die datenschutzrechtlichen Pflichten beachtet werden.

22. Militärischer Abschirmdienst

Das Amt für Sicherheit der Bundeswehr (ASBw), die Zentrale des Militärischen Abschirmdienstes (MAD), hat im wesentlichen die aus meiner Sicht erforderlichen Konsequenzen aus den Ergebnissen meiner umfangreichen datenschutzrechtlichen Prüfung im Jahre 1982 gezogen. Die bereits kurz nach Übersendung meines Prüfberichts als berechtigt anerkannten Einzelbeanstandungen sind inzwischen zum größten Teil ausgeräumt. An der Bereinigung der restlichen Fälle wird gearbeitet.

Zur Durchführung dieser Löschungen wurde im ASBw eine spezielle Arbeitsgruppe eingesetzt. Die inzwischen gelöschten Personendatensätze belaufen sich auf mehrere zehntausend. Aus einer von mir kritisierten manuellen Nebenkartei, die teilweise deckungsgleich mit der automatisierten Personenzentraldatei war, wurden ca. 500 000 Karteikarten vernichtet.

Wichtig an der im ASBw laufenden Bereinigungsaktion erscheint mir vor allem, daß nicht nur nach „formalen" Gesichtspunkten (z. B. Daten aller Personen, die ein bestimmtes Lebensalter haben) gelöscht wird, sondern daß auch unter inhaltlichen Gesichtspunkten Schwerpunkte gesetzt werden. So konnten in von mir als besonders problematisch angesehenen Einzelbereichen bereits Löschungen von Datensätzen in bedeutender Zahl erreicht werden. Dies gilt auch für Fälle, in denen nach meiner Auffassung durch die Speicherung der Kernbereich des Persönlichkeitsrechts tangiert war.

Das ASBw hat mir auch mitgeteilt, daß nunmehr vor der Auskunftserteilung, d h. vor der Übermittlung von Daten an andere Sicherheitsbehörden, eine Zuständigkeits- und Rechtmäßigkeitskontrolle durchgeführt wird. Daten die beim MAD nicht oder nicht mehr gespeichert sein dürfen, werden demnach gelöscht und nicht mehr übermittelt. Dies entspricht meiner oben (s. Nr. 17.2.2 b) näher dargelegten Auffassung zur Notwendigkeit und zu den Konsequenzen einer Relevanzprüfung vor der Datenübermittlung.

Auch bei der Umsetzung der von mir in meinem Prüfbericht ausgesprochenen Empfehlungen und Anregungen wurden nach Mitteilung des ASBw inzwischen ebenfalls Datensätze in beträchtlicher Zahl gelöscht.

Die in den vergangenen Tätigkeitsberichten gegebene positive Grundeinschätzung der datenschutzrechtlichen Situation beim MAD hat sich somit bestätigt. Der MAD steht den aus dem Datenschutzrecht entstehenden Anforderungen sehr aufgeschlossen gegenüber und versucht, die notwendigen Konsequenzen zu ziehen. Ich werde mich im kommenden Jahr vom weiteren Fortgang der Bereinigungs- und Löschungsarbeiten beim MAD überzeugen. Meine Beratungstätigkeit wird sich außerdem auf die Frage konzentrieren, inwieweit bestehende Vorschriften und Verfahrensabläufe geändert werden müssen, damit bedenkliche Datenspeicherungen in Zukunft unterbleiben.

23. Zollkriminalinstitut

Auch im Jahr 1983 war es mir nicht möglich, eine umfassende datenschutzrechtliche Kontrolle beim Zollkriminalinstitut anhand von Einzelfällen durchzuführen, die die Rechtmäßigkeit *personenbezogener* Speicherung einschließt. Das Bundesministerium der Finanzen beruft sich mir gegenüber — mit Ausnahme bei Einzeleingaben, in denen die Einwilligung der Betroffenen unterstellt wird — auf das Steuergeheimnis und schränkt insoweit meine Prüfungsbefugnis ein (vgl. 3. TB S. 21, 4. TB S. 19, 5. TB S. 100). Es bleibt zu hoffen, daß die Novellierung des Bundesdatenschutzgesetzes bald eine eindeutige rechtliche Klarstellung dieser Frage bringt.

Auch im Bereich der zollrechtlichen Überwachung haben meine Ausführungen in meinem Fünften Tätigkeitsbericht (S. 100 f.) zu keiner Änderung der Situation geführt. Der Bundesminister der Finanzen hält trotz meiner Bedenken den Zugriff der Bundes- und Landespolizeibehörden auf steuerliche Daten für zulässig und mit dem Steuergeheimnis vereinbar, obwohl diese Behörden keine Befugnisse nach dem Zollgesetz haben.

Auch hinsichtlich des Auskunftsrechtes des Betroffenen hat sich an der Haltung des Bundesministers der Finanzen nichts geändert. Er beruft sich stets auf das Auskunftsverweigerungsrecht nach § 13 Abs. 2 BDSG und nimmt mir damit die Möglichkeit, Petenten das Ergebnis der Prüfung ihrer Eingaben mitzuteilen. Dies bedeutet m. E. einen deutlichen Widerspruch zur Rechtspflicht der Ermessensabwägung, wie ich oben unter Hinweis auf die einschlägige Rechtsprechung näher dargelegt habe (s. o. Nr. 17.2.2 [c]). Im übrigen ist daran zu erinnern, daß das Zollkriminalinstitut nach den Vorschriften der Abgabenordnung nicht als Finanzbehörde im Sinne von § 12 Abs. 1 Nr. 2 BDSG definiert werden kann, so daß ihm das Auskunftsverweigerungsrecht nach § 13 Abs. 2 BDSG nicht zusteht. Hierzu verweise ich auf meine Ausführungen in meinem Dritten Tätigkeitsbericht (S. 23).

24. Verteidigung

24.1 Wehrersatzwesen

Eine Vielzahl von Eingaben bezieht sich auf den Umgang und den Inhalt von Unterlagen, die im Zusammenhang mit der Wehrpflicht entstehen. Im vorigen Jahr habe ich mehrere Kreiswehrersatzämter beraten und kontrolliert (s. 5. TB S. 101 f.); die hierbei gewonnenen Erkenntnisse und Erfahrungen haben mir geholfen, diese Eingaben sachgerecht beantworten zu können. Auch konnten dadurch über den Einzelfall hinaus Verbesserungen bei der Verarbeitung personenbezogener Daten erreicht werden.

Typisch dafür ist eine Zuschrift, die sich auf die Erhebung der Vorstrafen eines Wehrpflichtigen bezog, die während der Eignungs- und Verwendungsprüfung (EVP-Test) erfolgte. Die Praxis hierzu erwies sich als höchst unterschiedlich. Dabei war nicht immer gewährleistet, daß die Angaben nur von den wenigen Mitarbeitern des psychologischen Dienstes der Kreiswehrersatzämter zur Kenntnis genommen wurden. In einem Gespräch mit den zuständigen Stellen konnte eine Lösung gefunden werden, nach der einerseits nur der psychologische Dienst die für seine Arbeit notwendigen Informationen erhält, und auf der anderen Seite die schutzwürdigen Belange der Betroffenen gewährleistet bleiben.

Die Beratung und Kontrolle einer Wehrbereichsverwaltung und eines Rechenzentrums der Bundeswehr bestätigten und ergänzten die Ergebnisse aus den Kontrollen der Kreiswehrersatzämter; Verstöße gegen den Datenschutz wurden nicht festgestellt. Einige Probleme der Datensicherheit, die aus der Größe dieses Bereichs und aus der notwendigerweise zentralistischen Organisation resultieren, werde ich im Rahmen der für 1984 geplanten Kontrolle des Wehrersatzwesen-Informationssystems (WEWIS) weiterverfolgen.

24.2 Kontrolle des Instituts für Wehrmedizinalstatistik und ärztliches Berichtswesen in Remagen

Eine im Januar 1983 kurzfristig anberaumte Prüfung des Instituts mußte abgebrochen werden, da meinen Mitarbeitern der Einblick in die beim Institut abgelegten Gesundheitsakten verwehrt wurde. Der Bundesminister der Verteidigung war der Auffassung, daß sich das Prüfungsrecht des Bundesbeauftragten für den Datenschutz nicht auf Akten erstreckt und die ärztliche Schweigepflicht der Einsichtnahme entgegensteht. Die mikroverfilmten Akten sind nur über eine vorhandene automatisch geführte Namensdatei zugänglich und stehen nach meiner Auffassung deshalb mit der Verarbeitung personenbezogener Daten im Zusammenhang (§ 19 Abs. 3 Satz 2 Nr. 2 BDSG).

Nachdem eine Anzahl von Bürgern die Mitarbeiter des Remagener Instituts von der ärztlichen Schweigepflicht entbunden hatte, konnte die Prüfung —

unbeschadet weiter fortbestehender unterschiedlicher Rechtsauffassungen — im Sommer 1983 fortgesetzt werden. Die Prüfung hatte folgende Arbeitsschwerpunkte:

— Überprüfung verschiedener Einzeleingaben,

— Überprüfung der Übermittlungspraxis des Instituts,

— Datensicherung im Remagener Institut mit seinen Außenstellen.

Verstöße gegen datenschutzrechtliche Bestimmungen wurden nicht festgestellt; die Ärzte des Instituts handhaben die ihnen anvertrauten Unterlagen sorgfältig und gewissenhaft. Bei der Prüfung und dem anschließenden Schriftwechsel mit dem Bundesminister der Verteidigung sind einige Probleme offengeblieben, die klärungsbedürftig sind:

Das Institut dokumentiert und archiviert sämtliche Gesundheitsdaten aus dem Bereich der Bundeswehr. Das sind zur Zeit ungefähr 10 Mio. Akten, aus denen jährlich etwa 55 000 Auskünfte erteilt werden. Bei den Anfragen Dritter waren folgende Probleme erkennbar:

— Ärzte behaupten, daß die ärztliche Schweigepflicht zwischen Ärzten nicht gilt, und legen deshalb keine Entbindungserklärungen von der ärztlichen Schweigepflicht vor.

— Gerichte, insbesondere Sozialgerichte, fordern ärztliche Unterlagen an, ohne Entbindungserklärungen vorzulegen bzw. deren Notwendigkeit anzuerkennen.

— Private Versicherungen legen aus der Sicht des Instituts zu pauschale Entbindungserklärungen vor.

— Stellen aus der Personalabteilung des Bundesministeriums der Verteidigung verlangen in der Form von Weisungen die Herausgabe der ärztlichen Unterlagen eines Betroffenen.

Es ist zu begrüßen, daß das Institut sich regelmäßig *gezielte* Entbindungserklärungen von der ärztlichen Schweigepflicht vorlegen läßt, die den Zeitraum, den Zweck und die benötigten Daten konkret bezeichnen sollen. Allerdings können die Mitarbeiter des Instituts dann keinen korrigierenden Einfluß ausüben, wenn — wie in der Mehrzahl der Fälle — die Betroffenen selbst derartige gezielte Entbindungserklärungen vorlegen bzw. vorlegen lassen, z. B. beim Abschluß von Versicherungsverträgen. In diesen Fällen müssen sich die Betroffenen häufig zwingenden ökonomischen Interessen beugen, was nicht selten dazu führt, daß sie Nachteile erleiden.

Ich sehe eine wichtige Aufgabe der ärztlichen Standesorganisationen darin, Grundsätze zu entwickeln, die die Betroffenen, die sich in der Regel in einer schwächeren Position befinden, besser als gegenwärtig schützen.

Hinzu kommt, daß die Sammlungen sowohl solche Gesundheitsdaten enthalten, die während ärztlicher Behandlungen entstanden sind, als auch ärztliche Gutachten, die über die Verwendungsfähigkeit des Soldaten Auskunft geben.

Ich habe beim Bundesminister der Verteidigung angeregt zu prüfen, ob beide Datenarten voneinander getrennt werden können. Der Bundesminister der Verteidigung hat dies abgelehnt. Ich halte die hierfür angegebene Begründung nicht für überzeugend und werde die Angelegenheit weiter verfolgen.

Die Datensicherung, insbesondere die Zugangskontrolle, ist sowohl im Hauptgebäude in Remagen als auch — in besonderem Maße — in der nahe gelegenen Außenstelle völlig unzureichend. Daher erscheint die Art und Weise der Lagerung der zur Bearbeitung anstehenden Gesundheitsunterlagen im Hauptgebäude auf Gängen und in unverschlossenen Räumen nicht vertretbar.

Der Bundesminister der Verteidigung hat das Sanitätsamt der Bundeswehr, die vorgesetzte Dienststelle des Instituts, gebeten, diese Feststellungen zu überprüfen und gegebenenfalls Vorschläge zur Verbesserung der Sicherheit vorzulegen.

25. Datensicherung

Wie schon in den vorangegangenen Berichtsjahren wurden bei vielen Prüfungen auch Fragen der Datensicherung einbezogen. Dabei zeigte sich, daß manche der festgestellten Mängel überwiegend deswegen bestehen, weil die Organisation Mängel aufweist und das Sicherheitsbewußtsein nicht immer so ausgeprägt ist, wie es der modernen Datenverarbeitungstechnik angemessen wäre. Gelegentlich läßt auch noch immer die Unterstützung der Anwender durch die Hersteller zu wünschen übrig. So fehlt z. B. in einem modernen Betriebssystem die Protokollierung von Dateizugriffen. Hier hilft es wenig, dem Benutzer die Schnittstelle im Betriebssystem anzugeben, an die er eine eigene Protokollierung anschließen könnte. Denn die Anwender scheuen aus verständlichen Gründen davor zurück, in das vom Hersteller gewartete Betriebssystem eigene Routinen einzubauen.

Neben Problemen dieser — eher alten — Art entstehen neue Probleme durch die Weiterentwicklung der Datenverarbeitungstechnik. So führt der zunehmende Einsatz großer Plattenspeicher und neuer Druckverfahren zum Wegfall manueller Tätigkeiten in den Rechenzentren und Datenträgerarchiven. Das Personal wird entlastet und möglicherweise reduziert, Funktionstrennungen werden aufgegeben. Damit vermindern sich die früher zwangsläufigen gegenseitigen Kontrollen, wodurch neue Schwachstellen entstehen können.

Auf ein weiteres Problem, das künftig an Bedeutung gewinnen wird, möchte ich hier besonders eingehen. Erhebliche Sicherheitsprobleme sind zu lösen, wenn die Zugriffsmöglichkeiten zu automatisiert geführten Daten durch den Anschluß von Terminals „verteilt" werden. Hier muß die Sicherheit der Daten besonders sorgfältig organisiert werden, u. a. weil solche Terminals häufig in wenig gesicherten Bereichen stehen, die technisch gegebenen Möglichkeiten der Terminals oft die Berechtigung übersteigen und — z. B. beim Anschluß über öffentliche Wählnetze — die Identifizierung des Terminals besondere Schwierigkeiten bereitet.

Ein wichtiges Mittel zur Einschränkung der erheblichen Risiken ist der Verzicht darauf, daß von jedem Terminal aus jede Aktivität möglich ist. Zumindest die Nutzung zu Eingriffen in das System, zur interaktiven Programmierung und als Operatorkonsole muß auf wenige, gesichert untergebrachte Terminals beschränkt werden.

Eine weitere Sicherung könnte in der Anwendung kryptographischer Verfahren liegen; eine solche wird aber aus organisatorischen Gründen bis auf weiteres nur in wenigen Systemen möglich sein. Deshalb kommt dem richtigen Einsatz von password-Sicherungen besondere Bedeutung zu. Durch die Vergabe von passwords und ihre Prüfung im System kann erreicht werden, daß die gebotenen Möglichkeiten mit hoher Sicherheit nur von den dazu ausdrücklich berechtigten Personen genutzt werden. Bei der Organisation von Verfahren zur Verwaltung von passwords sollten die folgenden Punkte beachtet werden:

— Ein password für jeden Benutzer

  Jeder einzelne Benutzer sollte ein nur für ihn geltendes password haben. Dies unterstreicht seine Verantwortung für die sichere Handhabung und macht die veranlaßten Datenzugriffe und andere Transaktionen zurechenbar.

— Länge des passwords

  Weil kurze Zeichenfolgen dazu verführen, einfache Begriffe als password zu wählen, werden Folgen aus vier oder noch weniger Zeichen für viele Anwendungen unter Sicherheitsaspekten zu kurz sein, besonders dann, wenn nur Ziffern oder nur Buchstaben gewählt werden. Ein password aus acht Zeichen bietet eine im allgemeinen ausreichende Sicherheit gegen systematisches Probieren und Zufallsfunde. Eine Mischung aus Ziffern und Buchstaben erschwert das Erraten auch dann, wenn das password für den Berechtigten „sinnvoll" und deshalb leichter merkbar aufgebaut ist.

— Auswahl der passwords

  Weil man aus Sicherheitsgründen das password nicht aufschreiben, sondern im Gedächtnis behalten soll, werden einfache, leicht merkbare Zeichenfolgen häufig bevorzugt. „System", „Test", das eigene Geburtsdatum, Vornamen oder Begriffe aus dem Aufgabenbereich sind deshalb beliebte und leicht zu erratende passwords. Weil automatische Kontrollen nur extrem einfache Folgen oder Doubletten als unzulässig abweisen können, helfen außer einer — aus anderen Gründen aber unzweckmäßigen — zentralen Vergabe nur die Belehrung und die Erinnerung der Benutzer an ihre Sorgfaltspflicht. Wenn die Art der Anwendung das rechtfertigt, können auch die durch neue passwords abgelösten Folgen zur Kontrolle ausgedruckt und darauf untersucht werden, ob gezielte Erinnerungen an die Sorgfaltspflicht erforderlich sind.

— Sichere Vergabe von passwords

  Am sichersten ist ein password, das nur der berechtigte Benutzer kennt. Er sollte deshalb sein password selbst bestimmen, wechseln und die dazu erforderlichen Prozeduren allein veranlassen können. Das bei der Einrichtung einer Berechtigung erstmals zu vergebende password muß dann nicht mehr und nicht weniger erlauben, als ein eigenes password für die weitere Arbeit zu bestimmen. Abgesehen vom Sicherheitswert ist ein solches Verfahren besonders geeignet, den berechtigten Benutzer auf seine Verantwortung für die Sicherheit hinzuweisen.

— Höchstfristen für die Geltungsdauer

  Damit passwords in angemessenen kurzen Zeitabständen geändert werden, sollte die Geltungsdauer jedes passwords überwacht werden. Das kann soweit gehen, daß ein password nach Ablauf der Frist nicht mehr als gültig anerkannt wird. Die Frist sollte sich an den Besonderheiten der Anwendung orientieren und im Regelfall sechs Monate nicht übersteigen.

— Besondere Anlässe für einen Wechsel des passwords

  Es muß festgelegt und bekanntgemacht werden, welche Ereignisse Anlaß für einen unverzüglichen Wechsel des passwords sind. Dazu gehören Personalwechsel und jeder Verdacht, daß ein password ganz oder zum Teil einem Dritten bekannt ist. Auch wenn der Inhalt oder die Bedeutung der zu schützenden Daten sich so ändern, daß ein höherer Schutz erforderlich ist, sollten die passwords der Zugriffsberechtigten dem angepaßt werden.

— Speicherung der passwords

  Weil vom System stets zu prüfen ist, ob das vom Benutzer eingegebene password das richtige ist, muß zumindest für diesen Vergleich auf das gespeicherte password zugegriffen werden. Die sichere Speicherung von passwords wird deswegen schwierig, weil der Zugriff auf die password-Datei erfolgen muß, bevor die Berechtigung nachgewiesen ist. Eine Lösung bieten Verfahren der Einweg-Verschlüsselung. Dabei wird das vergebene oder gewählte password so verschlüsselt, daß aus dem zu speichernden Kryptogramm das password praktisch nicht rekonstruiert werden kann. Das vom Benutzer eingegebene password wird auf gleiche Weise verschlüsselt und die Kryptogramme werden verglichen. Dieses Kryptogramm braucht dabei nicht mehr gegen unberechtigtes Lesen geschützt zu werden.

— Verdeckte Eingabe des passwords

Viele Betriebssysteme bieten heute die Möglichkeit, das vom Benutzer einzugebende password nicht am Bildschirm anzuzeigen. Dies sollte stets genutzt und je nach Anwendung selbst programmiert werden, wenn die Hersteller keine Hilfen anbieten. Denn über die unmittelbare Sicherheitswirkung hinaus erinnert es den Berechtigten bei jeder Eingabe seines passwords an seine Mitverantwortung.

— Trennung von Identifikation und password

Jeder Zugriffsberechtigte sollte eine Benutzeridentifikation (z. B. USER-ID und/oder Abrechnungsnummer) haben, die er eingibt, um dem System mitzuteilen, wer er ist, und ein davon getrenntes password, durch dessen Eingabe er glaubhaft macht, daß er diese Identifikation berechtigt verwendet. Damit werden sowohl die Geheimhaltung des passwords als auch sein Wechsel erleichtert.

— Angemessene Reaktion auf Fehlversuche

Es ist nicht unmöglich, durch Probieren ein gültiges password herauszufinden, besonders wenn die Art des passwords oder Teile davon richtig vermutet werden. Andererseits ist ein Probieren schwer von einem Tippfehler des Berechtigten zu unterscheiden. Deshalb sollten alle Fehlversuche protokolliert und dem Berechtigten mitgeteilt werden. Nach einer an der Anwendung zu orientierenden Zahl von Fehlversuchen sollte der Benutzer und/oder das dazu benutzte Terminal gesperrt, zumindest aber die aufgebaute Verbindung abgebrochen werden. Das Probieren kann auch dadurch erschwert werden, daß die Zeit für die Prüfung des passwords nach jedem Fehlversuch verlängert wird.

— Regeln für kurzfristige Unterbrechungen

Auch im Prinzip kontinuierliche Arbeiten am Terminal werden gelegentlich unterbrochen. Solche Unterbrechungen enthalten die Gefahr, daß die Arbeit von Nicht-Berechtigten „fortgesetzt" wird. Diese Gefahr kann dadurch vermindert werden, daß nach einer je nach Art der Anwendung zu bemessenden Zeitspanne ohne Aktivität das password erneut einzugeben ist. Es kann auch sinnvoll sein, dem Berechtigten eine Möglichkeit zur kurzfristigen Abmeldung anzubieten, nach der er nur durch Eingabe des passwords sich wieder anmelden kann.

Wichtig ist auch, daß nach systembedingten Unterbrechungen die Eingabe des passwords verlangt wird, weil nicht davon ausgegangen werden kann, daß alle Berechtigten den Wiederanlauf am Terminal abwarten.

— Abstimmung mit der Arbeitszeit

Ein wichtiges Hilfsmittel zur Erhöhung der Zugriffssicherheit kann darin liegen, daß die Berechtigung jeweils nur für die möglichen Arbeitszeiten gelten. Besonders für längere Abwesenheiten (z. B. Urlaub) sollte der Berechtigte die Möglichkeit haben und nutzen, seine Berechtigung für diese Zeiten zu sperren.

— Anzeigen der letzten Nutzung

Das Erkennen unberechtigter Nutzungen und Nutzungsversuche wird wesentlich erleichtert, wenn jeweils nach der Eingabe des richtigen passwords — gleichsam als Quittung — die letzte Nutzung der Berechtigung und die seitdem erfolgten Fehlversuche angezeigt werden. Auch diese Maßnahme weist den Benutzer auf seine Verantwortung für eine sichere Datenverarbeitung hin.

— Transparente Organisation der Sicherungen

Es erhöht keineswegs die Sicherheit, wenn die Beteiligten und Zugriffsberechtigten nur wenig über die Wirkung und Bedeutung des Schutzes durch passwords wissen. Mit der Verteilung von Zugriffsmöglichkeiten muß die Verteilung von Verantwortung für die Sicherheit verbunden sein. Dazu gehört, daß die Berechtigten wissen, welcher Schutz durch passwords erreicht werden soll, wann passwords zu ändern sind und wie man dies veranlaßt. Die je nach Art der Anwendung angemessenen zentralen Kontrollen können die Mitwirkung der Berechtigten ergänzen und auch sichern, aber nicht ersetzen.

Einige der hier genannten Maßnahmen lassen sich schon deswegen nicht in jeder Anwendung realisieren, weil die erforderliche Unterstützung im Betriebssystem, im Datenfernverarbeitungssystem oder in der Datensicherungssoftware nicht vorgesehen ist. Andere Maßnahmen verlangen möglicherweise Änderungen in der Programmierung oder in der Organisation, die nicht ohne weiteres zu verwirklichen sind. Bei der Einführung neuer und durch die Pflege bestehender Verfahren muß aber ein Maß an Sicherheit erreicht werden, das auch Schutz vor intelligenten Freizeitspielereien von Computerfans mit Systemkenntnissen bietet. Deshalb werde ich auch zukünftig im Rahmen von Kontrollen und Beratung auf diese Probleme besonders achten.

26. Novellierung des BDSG

Im Fünften Tätigkeitsbericht (S. 110ff.) habe ich meine Auffassung zum Referentenentwurf 1982 des Bundesministeriums des Innern zur Novellierung des BDSG dargelegt und Ergänzungsvorschläge unterbreitet. Nach Bildung der neuen Bundesregierung wurde der Entwurf überarbeitet und mit Sachstand vom 23. Juni 1983 u. a. den obersten Bundesbehörden und mir zu Stellungnahme zugeleitet. Ich habe mit Bedauern festgestellt, daß darin nur wenige meiner Vorschläge berücksichtigt wurden,

während der Entwurf Forderungen übernommen hat, die in anderen Stellungnahmen vorgebracht worden sind und eine Reduzierung des Datenschutzes bewirken würden.

Ich habe mich zu dem Entwurf 83 eingehend schriftlich gegenüber dem Bundesminister des Innern geäußert, dabei meine Kritik deutlich gemacht und eine Reihe meiner früheren Vorschläge wiederholt. An den Besprechungen über den Entwurf mit den beteiligten Stellen habe ich mitgewirkt und dabei den Eindruck gewonnen, daß der Entwurf bis zur Kabinettreife nochmals gründlich überarbeitet wird, was mir auch im Hinblick auf die grundlegenden Ausführungen des Bundesverfassungsgerichts im Volkszählungsurteil vom 15. Dezember 1983 zum „informationellen Selbstbestimmungsrecht" und zu dessen Konsequenzen unerläßlich erscheint.

Mit Rücksicht auf diesen Sachstand verzichte ich hier auf die inhaltliche Wiedergabe meiner Stellungnahme, zumal sie zu einem erheblichen Teil mit meinen Darlegungen im Fünften Tätigkeitsbericht übereinstimmt. Meine Auffassung zum Referentenentwurf 83 ist auch in eine gemeinsame Erklärung der Datenschutzbeauftragten des Bundes und der Länder vom 4. November 1983 eingegangen, die als Anlage 2 zu diesem Bericht abgedruckt ist.

27. Ausland und Internationales

27.1 Die Datenschutzgesetzgebung im Ausland

Die Gesetzgebung des Auslandes zum Datenschutz hat im abgelaufenen Jahr stagniert. In mehreren Ländern haben sich Entwürfe für nationale Datenschutzgesetze oder Novellierungsentwürfe mit dem Ablauf der parlamentarischen Legislaturperiode erledigt. An der Zielsetzung ändert sich in diesen Ländern aber nichts. Man versucht, die Problematik durch ein bereichsübergreifendes, als Querschnittsmaterie angelegtes, nationales Datenschutzgesetz zu bewältigen. Unbestritten bleibt dabei das Ziel, die von der Datenschutzkonvention des Europarates definierten Forderungen zu erfüllen.

Bei der Novellierung geltender Datenschutzgesetze sind insbesondere drei Tendenzen sichtbar. Zum ersten geht es um eine Vereinfachung von Verwaltungs- und Kontrollroutinen. Dies betrifft vor allem Länder mit ausgeprägtem Lizenzierungs- oder Registrierungssystem. Nachdem dieses System in mehrjähriger Praxis einen sehr detaillierten Überblick über die Verarbeitung personenbezogener Daten erbracht hat, geht man nun eine Stufe zurück und nimmt alle Anwendungsfälle, die sich im Bereich des Typischen und Gebräuchlichen halten, von der Lizenzierungs- bzw. Registrierungspflicht aus oder begnügt sich insoweit mit stark vereinfachten Verfahrensweisen. Weiterhin gibt es Bemühungen, die gesetzlichen Regelungen dort auszubauen, zu präzisieren und den praktischen Bedürfnissen beser anzupassen, wo sich in den letzten Jahren besondere Brennpunkte gezeigt haben. Dies gilt etwa für den Bereich Forschung und Statistik. Schließlich gibt es die verschiedensten Bemühungen, erkannte Unzulänglichkeiten auszugleichen und die Rechte der Betroffenen zu verbessern.

27.2 Inter- und supranationale Datenschutzbestrebungen

Die Mitarbeit im Expertenkomitee für Datenschutz des Europarates wurde fortgesetzt. Das Komitee arbeitet an Empfehlungen für den Bereich der Sozialen Sicherung und für den Bereich des Direktmarketing einschließlich des Adressenhandels; zu diesem stehen die Beratungen vor dem Abschluß. Die im Vorjahr erarbeitete Empfehlung über den Datenschutz im Bereich der wissenschaftlichen Forschung und der Statistik ist im September vom Ministerrat verabschiedet worden (abgedruckt als Anlage 3).

Die Einigung zwischen den Mitgliedsländern auf einen gemeinsamen Text ist bei den bisherigen Beratungen von Empfehlungsentwürfen recht schwierig gewesen. Nicht selten haben Länder, deren geltendes Recht mit einzelnen Punkten der Entwurfstexte nicht übereinstimmte, dies zum Anlaß genommen, nachhaltig auf eine Änderung der Empfehlung zu dringen, und zwar insbesondere wenn diese im Anwendungsbereich oder hinsichtlich der Schutzwirkung über das nationale Recht hinausging. Bei der Abstimmung der Empfehlung zu Wissenschaft und Forschung zeigte sich ein derartiger Widerstand auch in der Bundesrepublik. Er hatte zur Folge, daß die Bundesregierung der Empfehlung nur unter Vorbehalten zustimmte.

Ich versuche, einer solchen Betrachtungsweise entgegenzutreten. Gemeinsame Empfehlungen auf der Ebene des Europarats sind ein wertvolles Instrument zur Harmonisierung des Datenschutzes. Da die nationalen Rechtsordnungen Unterschiede aufweisen, bedeutet der Standpunkt eines Landes, die Empfehlung dürfe von seinem Recht nicht abweichen, nichts anderes, als daß entweder alle anderen Länder sich anpassen müßten oder daß gemeinsame Empfehlungen unmöglich sind.

Die Empfehlungen sind natürlich darauf gerichtet, praktische Folgen herbeizuführen, sie unterscheiden sich aber von einer Konvention doch ganz grundlegend darin, daß sie weder gegenüber den Teilnehmer-Staaten noch gegenüber den Rechtssubjekten innerhalb dieser Staaten rechtliche Bindungswirkung haben. Vielmehr bleibt es den Ländern wie auch den einzelnen datenverarbeitenden

Stellen überlassen, in welchem Umfang und in welcher Weise im einzelnen den Empfehlungen gefolgt werden soll. Die Bereitschaft zur europäischen Integration sollte aber doch jedenfalls so weit gehen, daß man Empfehlungen auch dann akzeptiert, wenn abzusehen ist, daß man sich mit ihrem Inhalt später argumentativ auseinandersetzen müssen wird.

Das Expertenkomitee betrachtet als künftige Arbeitsschwerpunkte die aus der Dezentralisierung der Datenverarbeitungssysteme resultierenden Probleme, die polizeiliche Informationsverarbeitung und den Arbeitnehmerdatenschutz. Im Hinblick auf die Bedeutung seiner Aufgaben und seine bisherigen Erfolge hat das Generalsekretariat des Europarats die Mittel des Expertenkomitees für Datenschutz beträchtlich erhöht und damit die Voraussetzungen für die gleichzeitige Bearbeitung mehrerer Problembereiche geschaffen.

Die OECD hat im Dezember ein internationales Symposium über den grenzüberschreitenden Datenverkehr veranstaltet, auf dem sowohl praktische Erfahrungen ausgetauscht als auch über Grundsätze der Steuerung und Kontrolle solcher Datenflüsse beraten wurde. Diese Konferenz wäre für mich von großem Interesse gewesen. Auch der (federführende) Bundesminister für Wirtschaft hatte auf meine Teilnahme Wert gelegt. Die zu gering bemessenen Haushaltsmittel für Auslandsdienstreisen ließen dies aber leider nicht zu. Die wachsende Bedeutung der internationalen Probleme des Datenschutzes, die den Europarat zu einer Verdoppelung seiner Anstrengungen bewogen haben, sollten auch bei der Aufstellung des Haushalts meiner Dienststelle beachtet werden, zumal die Bundesrepublik Deutschland zu den Ländern gehört, die am besten in der Lage sind, auf der Grundlage langjähriger und breiter Erfahrungen zur Entwicklung eines gemeinsamen europäischen Datenschutzes beizutragen, andererseits aber aufgrund dieses Ausbaustandes und der engen internationalen Verflechtungen daran auch besonders interessiert sein muß.

27.3 Rechtsetzung der Europäischen Gemeinschaft

In zunehmenden Umfang werden in der Bundesrepublik Deutschland die Verarbeitung personenbezogener Daten und der Datenschutz von internationalen und supranationalen Regelungen mitgeformt. Bereits bei der Volkszählung war von Regierungsseite immer wieder darauf hingewiesen worden, daß ein zehnjähriger Erhebungsturnus bei Volkszählungen der internationalen Norm und der vorgesehene Termin einer Empfehlung der Vereinten Nationen (Resolution Nr. 1947 L VIII vom 5. Mai 1975) entspreche. In der Öffentlichkeit weniger beachtet wurde die EG-Stichprobenerhebung über Arbeitskräfte, die die Statistischen Landesämter im Juni 1983 durchführten. Die Durchführung der Erhebung, einschließlich der Auskunftspflicht für die betroffenen Bürger, wurde unmittelbar durch einen Rechtsetzungsakt der Europäischen Gemeinschaft angeordnet (EWG-Verordnung Nr. 603/83 des Rates vom 14. März 1983, Amtbl. der EG Nr. L 72 S. 1).

Ich habe den Bundesminister des Innern darauf hingewiesen, daß mehrere in den Erhebungsformularen vorgesehene Fragen durch den Wortlaut der EG-Verordnung nicht gedeckt sind. Er hat jedoch die Rechtsgrundlage für ausreichend angesehen, da die Fragen auf dem gemeinsamen Schlüsselverzeichnis beruhten, welches die EG-Kommission gemäß der Verordnung den Statistischen Ämtern der Mitgliedstaaten vorgegeben habe. Ich konnte mich dieser Argumentation nicht anschließen, da zwar Rechtsetzungsakte der Gemeinschaft in der Form der Verordnung unmittelbar Pflichten für die Bürger der Bundesrepublik begründen können, der Kommission aber nicht die Befugnis zusteht, solche Verpflichtungen inhaltlich auszuweiten. Da ich bei der Vorbereitung der Statistik nicht beteiligt worden war und die Erhebung bereits lief, als ich damit befaßt wurde, habe ich mich darauf beschränkt, den Bundesminister des Innern im Hinblick auf künftige EG-Statistiken auf die Problematik hinzuweisen. Gerade bei der sensiblen Materie der Statistik halte ich eine peinlich genaue Beachtung des Grundsatzes für geboten, daß der Bürger nur im gesetzlich vorgesehenen Umfang mit Auskünften in Anspruch genommen wird.

27.4 Zusammenarbeit der Datenschutz-Kontrollinstanzen

Die engen und regelmäßigen Kontakte mit den Datenschutz-Kontrollinstanzen anderer Länder haben sich auch in diesem Jahr für alle Beteiligten als nützlich erwiesen. Dem außerordentlichen Interesse des Auslands an den Vorgängen um die geplante Volkszählung 1983 entspricht ein deutsches Interesse zu erfahren, wie in anderen Ländern die öffentliche Meinung, die Presse und die politisch Verantwortlichen zu Volkszählungen, aber auch wie sie zu Alternativen zur klassischen Volkszählung stehen. Als Alternative zum Interview-Zensus wird die gemeinsame und abgestimmte Auswertung einer Vielzahl von Verwaltungsdateien angesehen. Bei der Beratung zeigte sich, daß die Datenschutzbeauftragten gegen eine statistische Auswertung der einzelnen, dem Verwaltungsvollzug dienenden Dateien zwar keine grundsätzlichen Bedenken haben, wohl aber gegen eine zusammenfassende, auf der Verknüpfung von Einzeldaten aus ganz verschiedenen Verwaltungsbereichen beruhende Auswertung. Die erheblichen Vorbehalte gegen derartige Lösungen richten sich nicht gegen die bezweckte statistische Auswertung, sondern dagegen, daß eine Infrastruktur geschaffen würde, die es, was die technischen und organisatorischen Möglichkeiten betrifft, außerordentlich erleichtert, Verknüpfungen der verschiedenen Dateien auch zu ganz anderen Zwecken vorzunehmen. Auch wenn das Statistikgeheimnis jede nicht-statistische Verwendung verbietet — dies ist in den skandinavischen Ländern, die einschlägige Erfahrungen haben, der Fall —, wird das durch die technische Struktur bedingte Mißbrauchsrisiko als zu hoch angesehen.

In der praktischen Entwicklung des Datenschutzes in den einzelnen Ländern sind nach wie vor erhebliche Entwicklungsunterschiede zu beobachten. Gegenstand gemeinsamer Sorge war jedoch die Beobachtung, daß die ungünstige wirtschaftliche Entwicklung in mehreren Ländern zum Anlaß für Versuche genommen wurde, datenschutzrechtliche Regelungen und datenschutzorientierte Verfahrensweisen in Frage zu stellen. Die Datenschutzbeauftragten verkennen keineswegs die Notwendigkeit, alle Möglichkeiten der Einsparung öffentlicher Mittel zu überprüfen und dabei auch darauf zu achten, daß die Tätigkeiten verschiedener staatlicher Leistungsbereiche sachgerecht aufeinander abgestimmt werden. Dies kann beispielsweise bedeuten, daß die verschiedenen Stellen, die mit der Durchführung von Leistungsprogrammen befaßt sind, wissen müssen, welche sonstigen Leistungen ein Bürger erhält. Auf der anderen Seite gehört der Datenschutz heute zu den grundlegenden Menschen- und Bürgerrechten. Damit verträgt es sich nicht, den Datenschutz je nach wirtschaftlicher Wetterlage vor- oder zurückzudrehen. Die Glaubwürdigkeit des staatlichen Bekenntnisses zum Datenschutz würde dadurch untergraben.

Zu den wichtigsten fachspezifischen Beratungsthemen der diesjährigen Internationalen Konferenz der Datenschutz-Instanzen gehörten die Neuen Medien und die international wirkenden Organisationen mit humanitärer oder den Menschenrechten verpflichteter Zielsetzung. Der meines Erachtens besonders wichtige Beschluß zum Thema Neue Medien ist als Anlage 4 zu diesem Bericht abgedruckt.

28. Bilanz

In meinem Fünften Tätigkeitsbericht habe ich auf zahlreiche offengebliebene Fragen und Probleme hingewiesen. Wie die nachfolgende Aufstellung zeigt, konnten viele davon im Berichtsjahr gelöst werden. Zu anderen Punkten wurden die Bemühungen um eine Lösung fortgesetzt, was sich zum Teil deswegen als langwierig erwies, weil unterschiedliche Interessen mehrerer beteiligter Stellen berücksichtigt werden mußten. Bei einigen Fragen stehen sich aber auch die gegensätzlichen Rechtspositionen im wesentlichen unverändert gegenüber.

1. Die Datenverarbeitung des Ausländerzentralregisters gab zu datenschutzrechtlichen Bedenken Anlaß (5. TB S. 15f.). Zur Beratung über eine grundlegende Neuordnung hat der Bundesminister des Innern eine Arbeitsgruppe gebildet, an der ich beteiligt bin.

2. Über Vorschläge für eine Novellierung des Bundeszentralregistergesetzes habe ich berichtet (5. TB S. 18). Diese Vorschläge sind in das Gesetzgebungsverfahren bislang nicht einbezogen worden. Ich bin mit dem Bundesminister der Justiz darüber im Gespräch, wie diese Vorschläge in einer neuen Novelle realisiert werden können.

3. Gegen das bisherige Verfahren bei Mitteilungen in Strafsachen habe ich Bedenken vorgebracht (5. TB S. 19). Seit kurzem liegt mir ein Entwurf einer Arbeitsgruppe der Justizministerkonferenz vor, zu dem ich eine Stellungnahme abgeben werde.

4. Auf die Notwendigkeit einer datenschutzgerechten Überarbeitung der Richtlinien für das Strafverfahren und das Bußgeldverfahren habe ich hingewiesen (5. TB S. 19f.). Der Bundesminister der Justiz hat auf meine Anregungen in einer Reihe von Punkten positiv reagiert, siehe dazu Nr. 3.5 in diesem Bericht.

5. Für problematische Mitteilungspflichten im Personenstandwesen (z. B. Aufgebot) habe ich Änderungen angeregt (5. TB S. 21). Zu einer Reihe wichtiger Punkte hat die Bundesregierung meine Anregungen aufgegriffen, siehe dazu Nr. 3.2 in diesem Bericht.

6. Für die Kontrollmitteilungen an die Finanzämter habe ich eine klare Rechtsgrundlage und mehr Transparenz für den Betroffenen gefordert (5. TB S. 24f.). Der derzeitige Entwurf zur Änderung der Abgabenordnung sieht zwar eine Verbesserung der Rechtsgrundlage vor, schafft aber für den Betroffenen nicht die erwünschte Transparenz, s. dazu Nr. 4.1 in diesem Bericht.

7. Einer beabsichtigten Änderung der Abgabenordnung, nach der Finanzbehörden in Steuersachen im Verhältnis zueinander nicht mehr als Dritte im Sinne des BDSG anzusehen sind, bin ich entgegengetreten (5. TB S. 25). Der Bundesminister der Finanzen ist diesen Bedenken gefolgt, s. dazu Nr. 4.1 in diesem Bericht.

8. Die Angaben über die Arten der Steuerschulden in Pfändungsverfügungen habe ich kritisiert (5. TB S. 26). Inzwischen hat der Bundesminister der Finanzen meine Vorschläge in den Entwurf zur Änderung der Abgabenordnung übernommen, siehe dazu Nr. 4.1 in diesem Bericht.

9. Über die Frage, aus welchen Anlässen die Post Nachweise über einzelne Telefonverbindungen speichern und die Angaben dem Teilnehmer oder einem Dritten mitteilen sollte, habe ich berichtet (5. TB S. 32f.). Einem Auftrag des Postausschusses des Deutschen Bundestages folgend habe ich in enger Abstimmung mit dem Bundesminister für das Post- und Fernmeldewesen einen Vorschlag für eine sachgerechte Lösung entworfen, der im Januar dem Ausschuß vorgelegt wird.

10. Die aufgrund meiner im Jahre 1981 ausgesprochenen Beanstandung eingeleiteten Bemühungen des Bundesministers für Verkehr, die Be-

rufs- und Gewerbeangaben der Halter bei der zentralen Fahrzeugerfassung (5. TB S. 39) den Anforderungen des Bundesleistungsgesetzes und des Verkehrssicherstellungsgesetzes anzupassen, sind immer noch nicht abgeschlossen. Die Ursache dafür liegt in unterschiedlichen Auffassungen der beteiligten Verwaltungen über die Klassifikation dieser Angaben.

11. Gegen die unterschiedslose Mitteilung aller Entziehungen von Sonderfahrererlaubnissen an das Verkehrszentralregister habe ich Bedenken geäußert (5. TB S. 41). Untersuchungen des Bundesministers der Verteidigung haben bestätigt, daß eine Unterscheidung der Entziehungsgründe bei der Sonderfahrerlaubnis (5. TB S. 41) in solche, die von allgemeiner verkehrsrechtlicher Bedeutung sind, und solche, die nur bereichsinterne Bedeutung (bei der Post oder Bundeswehr usw.) haben, möglich ist. Dementsprechend habe ich gegenüber dem Bundesminister für Verkehr eine differenziertere Ausgestaltung der Übermittlungsbestimmungen (Mitteilung der Entscheidung über die Entziehung einer Fahrerlaubnis an das Verkehrszentralregister) in der StVZO gefordert.

12. Über unzulässige Verzögerungen bei der Entfernung tilgungsreifer Vorgänge aus dem Verkehrszentralregister habe ich berichtet (5. TB S. 41). Auf meine Anregung hin hat das Kraftfahrt-Bundesamt im Rahmen der Tilgungsaktion aufgrund der Anhebung der Eintragungsgrenze für Bußgeldentscheidungen von 40 DM auf 80 DM Erhebungen durchgeführt, die Aussagen über den möglichen Mehraufwand geben sollen, den eine zeitnahe Tilgung erbringen würde. Das Untersuchungsergebnis liegt mir seit kurzem vor; auf eine sachgerechte Lösung werde ich hinwirken.

13. Auf die Notwendigkeit gesetzlicher Regelungen für das Zentrale Verkehrsinformationssystem (ZEVIS) habe ich hingewiesen (5. TB S. 41 ff.). Nachdem gleichwohl der Übergang zum Regelbetrieb vollzogen wurde, habe ich diese Datenverarbeitung beanstandet, s. dazu Nr. 7 in diesem Bericht.

14. Über datenschutzrechtliche Probleme des Auswahlverfahrens für den gehobenen Flugverkehrskontrolldienst habe ich berichtet (5. TB S. 45). Ich habe die Bundesanstalt für Flugsicherung inzwischen gebeten, den Bewerbern anläßlich der Teilnahme an der Eignungsuntersuchung eine Einverständniserklärung zu der damit verbundenen Verarbeitung der Daten auch für wissenschaftliche Zwecke nicht erst unmittelbar vor Testbeginn, sondern bereits anläßlich der Übersendung des Fragebogens „Biographische Daten" vorzulegen. Dadurch steht den Bewerbern ausreichend Zeit zur Verfügung, ihre Entscheidung über die Teilnahme in Ruhe zu treffen.

15. Auf ein Forschungsvorhaben der Gesellschaft für Mathematik und Datenverarbeitung, mit dem bessere Anonymisierungsmethoden entwickelt werden sollen, hatte ich hingewiesen (5. TB S. 48). Das Forscherteam hat zunächst versucht, den Personenbezug für Daten wiederherzustellen, die zuvor durch (graduell zunehmendes) Verändern einzelner Werte „anonymisiert" worden waren. Die Ergebnisse deuten darauf hin, daß — außer bei Stichproben — das Re-Identifikationsrisiko selbst dann noch unvertretbar hoch ist, wenn die Daten wegen des Grades der Verfälschungen für Forschungszwecke nicht mehr geeignet sind. Nach diesem klärenden, für die Forschung allerdings sehr ungünstigen Zwischenergebnis wird nun untersucht, ob mit einer Kombination aus Datenänderungen, Aggregatbildungen und Mischtechniken ein Weg gefunden werden kann, die Anonymität zu sichern und zugleich die Datenqualität für Forschungszwecke besser zu erhalten.

16. Beim Forschungsprojekt „Örtliche Unfallforschung" bestanden datenschutzrechtliche Unklarheiten (5. TB S. 45). Inzwischen hat die Bundesanstalt für Straßenwesen von dem Forschungsteam die Zusage erhalten, daß Datenerhebungen nur dann durchgeführt werden, wenn eine schriftliche Einwilligung des Betroffenen vorliegt oder die Einwilligung offenkundig ist.

17. Auf das Fehlen von Tilgungsregelungen für Ordnungswidrigkeiten, die der Wasser- und Schiffahrtsverwaltung des Bundes mitgeteilt werden, habe ich hingewiesen (5. TB S. 45). Der Bundesminister für Verkehr hat nunmehr die Aufbewahrungsdauer für diese Mitteilungen auf fünf Jahre nach Abschluß des Verfahrens beschränkt.

18. Zum Referentenentwurf für ein Bundesarchivgesetz hatte ich Stellung genommen (vgl. 5 TB S. 48 f.) und gegen einige der vorgesehenen Regelungen Einwendungen erhoben. Nur eine meiner Empfehlungen wurde in der Zwischenzeit berücksichtigt. Ich bin bemüht, weitere Verbesserungen zu erreichen.

19. Für die Aufbewahrung statistischen Materials hatte ich gefordert, die von den Statistischen Ämtern festgelegten Mindestaufbewahrungsfristen künftig zugleich als Höchstfristen anzusehen (5. TB S. 50). Das Statistische Bundesamt hat dies zugesagt; es ist darüber hinaus bemüht, diese Fristen im Zusammenwirken mit den Landesämtern zu verkürzen.

20. Auf eine unangemessene Abgrenzung des Personenkreises bei der Bundesversicherungsanstalt für Angestellte, der einer Sicherheitsüberprüfung unterzogen werden sollte, habe ich hingewiesen (5. TB S. 60). Eine akzeptable Lösung zeichnet sich ab, siehe dazu Nr. 12.2 in diesem Bericht.

21. Die Entwicklungsphase des Projekts „Datenerfassung, Verarbeitung, Dokumentation und Information in den sozialärztlichen Diensten mit Hilfe der elektronischen Datenverarbeitung

(DVDIS)", über die ich berichtet habe (5. TB S. 66), ist abgeschlossen und das erwartete Gutachten liegt mir inzwischen vor. Danach habe ich gegen die beschriebene Konzeption keine konkreten Bedenken mehr. Die Erprobung und Durchführung des Projekts, bei der datenschutzrechtliche Probleme auftreten können, wird außerhalb meines Zuständigkeitsbereiches stattfinden. Es besteht Einvernehmen mit den jeweils zuständigen Landesbeauftragten für den Datenschutz, daß von diesen das weitere Verfahren beobachtet wird.

22. Über Datensicherungsmängel beim Informations- und Datenverarbeitungssystem für die Ortskrankenkassen (IDVS II) habe ich berichtet (5. TB S. 66). Der Bundesverband der Ortskrankenkassen hat mir inzwischen mitgeteilt, daß entsprechende Sicherheitspakete fertiggestellt sind und die Landesverbände ihre Mitgliedskassen veranlassen werden, die damit angebotenen Möglichkeiten auch zu nutzen.

23. Meine Bedenken gegen die Verwendung der Rentenversicherungsnummer außerhalb der Rentenversicherung und ohne besondere gesetzliche Ermächtigung habe ich dargelegt (5. TB S. 68f.). Der Bundesminister für Arbeit und Sozialordnung hat meine Bedenken aufgegriffen und sich in seiner Stellungnahme an den Bundestagsausschuß für Arbeit und Sozialordnung für eine gesetzliche Beschränkung wenigstens auf den Bereich der sozialen Sicherung ausgesprochen.

24. Auf die datenschutzrechtlichen Bedenken bei der Erteilung von Bankauskünften habe ich hingewiesen (5. TB S. 75). Der Bundesgerichtshof hat nunmehr in seinem Urteil vom 7. 7. 1983 — III ZR 159/82 — meinen datenschutzrechtlichen Ansatzpunkt bestätigt. Er hat klargestellt, daß eine Datenübermittlung nur dann im Rahmen der Zweckbestimmung eines Vertrages (§ 24 Abs. 1, 1. Alternative BDSG) liegt, wenn sie zur Erfüllung der Pflichten oder zur Wahrnehmung der Rechte aus einem mit dem Betroffenen geschlossenen Vertrag vorgenommen wird. Die Zweckbestimmung einer laufenden Geschäftsbeziehung erfordere jedoch nicht die Unterrichtung anderer über die persönlichen und wirtschaftlichen Verhältnisse des Kunden. Die Landesbeauftragten sowie die Landesaufsichtsbehörden sind mit mir der Auffassung, daß die Praxis der Erteilung von Bankauskünften geändert werden muß. Die geplanten Verhandlungen mit der Kreditwirtschaft, mit denen mehr Transparenz der Datenverarbeitung und eine Reduzierung des Datenkatalogs bei Bankauskünften erreicht werden sollen, sind noch nicht in Gang gekommen.

25. Über eine Auseinandersetzung um mein Einsichtsrecht in Akten des Bundesamtes für Verfassungsschutz habe ich berichtet (5. TB S. 77f.). Im Berichtsjahr wurden die Kontrollen nicht behindert, die gegensätzlichen Rechtsansichten bestehen aber fort, s. dazu Nr. 17.2.1 in diesem Bericht.

26. Auf mögliche Beeinträchtigungen schutzwürdiger Belange, die dadurch entstehen, daß den Meldungen über die Einleitung eines Ermittlungsverfahrens sehr oft nicht auch die Meldung über das Ergebnis folgt, habe ich hingewiesen (5. TB S. 80). Diese Situation hat sich nicht gebessert, s. dazu Nrn. 17.2.2, 18.1 und 18.3.2 in diesem Bericht.

27. Die Notwendigkeit, die umfangreichen Bereinigungsaktionen in den Datenbeständen der Sicherheitsbehörden fortzusetzen, habe ich begründet (5. TB S. 80f.). Die Bereinigungen werden fortgesetzt und sind noch nicht abgeschlossen, s. dazu Nrn. 18.4, 20.2 und 22 in diesem Bericht.

28. Auf die unterschiedliche und in einigen Bereichen sehr unbefriedigende Auskunftspraxis der Sicherheits- und der Finanzbehörden habe ich hingewiesen (5. TB S. 82f.). Diese Praxis ist im wesentlichen gleich geblieben, hinsichtlich des Bundesamtes für Verfassungsschutz ist neuerdings eine restriktive Handhabung festzustellen, s. dazu Nrn. 17.2.2 und 23 in diesem Bericht.

29. Auf die Schwierigkeiten, die Berechtigung von an das Bundesamt für Verfassungsschutz gerichteten Dateianfragen zu kontrollieren, habe ich hingewiesen (5. TB S. 84). Wegen der weiterhin gegensätzlichen Rechtsansichten war eine pragmatische Lösung schwer zu finden; ich hoffe jedoch, die zur Kontrolle notwendigen Akteneinsichten im kommenden Jahr vornehmen zu können, s. dazu Nr. 17.3 in diesem Bericht.

30. Über eine Kontrolle, die Mängel in der Datenverarbeitung der Abteilung Staatsschutz des Bundeskriminalamtes aufgedeckt hat, habe ich berichtet (5. TB S. 89f.). Meine Beanstandungen wurden im wesentlichen anerkannt, s. dazu Nr. 18.3.1 in diesem Bericht.

31. Die erheblichen datenschutzrechtlichen Probleme bei der Zusammenarbeit des Bundeskriminalamtes mit Interpol habe ich dargestellt (5. TB S. 91f.). Eine weitere Kontrolle hat keine Verbesserungen in der Auskunftspraxis erkennen lassen. Änderungen wurden jedoch zugesagt, s. dazu Nr. 18.1.1 in diesem Bericht.

32. Auf Differenzen in der Frage, in welchem Umfang Informationen über Mitglieder extremistischer Organisationen beim Bundesamt für Verfassungsschutz gespeichert werden dürfen, habe ich hingewiesen (5. TB S. 93f.). Diese Meinungsverschiedenheiten bestehen fort, s. dazu Nr. 20.1.1 in diesem Bericht.

33. Für eine Einschränkung der Übermittlungspraxis aus den Datenbeständen des Bundesnach-

richtendienstes habe ich mich eingesetzt (5. TB S. 98 f.). Es konnte ein vertretbarer Kompromiß erreicht werden, s. dazu Nr. 21.2 in diesem Bericht.

34. Über Anhaltspunkte dafür, daß durch die Datenverarbeitung beim Zollkriminalinstitut u. a. auch das Steuergeheimnis verletzt wird, habe ich berichtet (5. TB S. 100 f.). Da meine Kontrollkompetenz — außer bei Bürgereingaben — mit dem Hinweis auf das Steuergeheimnis bestritten wird, war mir eine Klärung nach wie vor nicht möglich, s. dazu Nr. 23 in diesem Bericht.

Bonn, den 13. Januar 1984

Dr. Baumann

Anlage 1 (zu Nr. 9.1)

Stellungnahme des Bundesbeauftragten für den Datenschutz, Dr. Reinhold Baumann, zu den Verfassungsbeschwerden gegen das Volkszählungsgesetz in der mündlichen Verhandlung vor dem Bundesverfassungsgericht am 18. und 19. Oktober 1983

1. Verfassungsrechtlicher Prüfungsmaßstab für Maßnahmen der Datenerhebung und automatischen Datenverarbeitung mit Eingriffs- und Gefährdungscharakter ist der Artikel 2 Abs. 1 i. V. m. Artikel 1 Abs. 1 des Grundgesetzes. Das Bundesverfassungsgericht hat hierzu in verschiedenen Entscheidungen Grundsätze aufgestellt, die in diesem Verfahren oft zitiert wurden und die ich deshalb nicht zu wiederholen brauche.

   Man könnte sich deshalb auf den Standpunkt stellen, daß diese Grundsätze im vorliegenden Verfahren — jeweils mit den Besonderheiten bei statistischen Erhebungen und Verarbeitungen — einfach nur fortzuschreiben sind.

   Eine solche Betrachtungs- und Verfahrensweise läuft jedoch Gefahr, zwischenzeitliche Entwicklungen nicht zu berücksichtigen und dem Phänomen der Volkszählung 1983, wie es sich uns heute darstellt, nicht gerecht zu werden. Einem Phänomen, das sich vor allem darin zeigt, daß noch vor zwölf Monaten in unserem Land Volkszählungen als Routine galten — lästig vielleicht, aber unverzichtbar. Der Datenschutz war kein Hauptproblem, und man glaubte, einem gewachsenen Datenschutzbewußtsein in der Bevölkerung durch weniger Fragen und durch bessere Geheimhaltungsvorschriften Rechnung getragen zu haben. Die Heftigkeit, mit der dann der Streit zur Jahreswende — einem Naturereignis gleich — einsetzte, alle Bereiche der Gesellschaft ergriff und bald die Züge eines Glaubenskrieges annahm, mußte daher überraschen, ja beängstigen. Denn das Mißverhältnis zwischen dem konkreten Anlaß und der Schärfe und Grundsätzlichkeit der Auseinandersetzungen erschien so evident, daß mancher die Kritik als hysterische Reaktion abtun oder in ihr nur ein gezieltes Manöver politischer Systemgegner sehen wollte. Solche Erklärungen würden indes zu kurz greifen. Gewiß, auch die Eigengesetzlichkeiten des Wahlkampfes dürften zu den Emotionen beigetragen haben. Bestimmte Einstellungen müssen indes in der Bevölkerung bereits latent vorhanden gewesen sein und brauchten dann nur noch geweckt zu werden.

   Die Ursachen dafür sind allerdings nicht nur in Mängeln des Volkszählungsgesetzes oder der Vorbereitung der Zählung zu sehen, sie liegen tiefer. Immer mehr Menschen haben heute ihre ganz persönlichen Erfahrungen mit der modernen Informationstechnik gemacht. Es sind nur zu oft Erfahrungen, bei denen man leicht nachvollziehen kann, daß sie zu Skepsis und Mißtrauen führen. Ich nenne nur wenige Beispiele.

   — So ist Datenverarbeitung oft das Gegenteil von bürgerfreundlich. Trotz fortgeschrittener Technik wird dem Bürger noch immer eine Computersprache zugemutet, die für viele unverständlich ist.

   — Bei vielen Befragungen für Zwecke der Verwaltung, der Planung oder der Wissenschaft wird der Bürger nur als Informationsquelle betrachtet, die es optimal auszubeuten gilt. Die Forderung des Bundesdatenschutzgesetzes, ihn auf die Freiwilligkeit seiner Auskünfte bzw. auf die gesetzliche Grundlage seiner Auskunftspflicht hinzuweisen, wird meistens ungenügend oder überhaupt nicht erfüllt.

   — Die Direktwerbung mit Hilfe ausgesuchter Adressensammlungen betrifft heute fast jedermann. Das Unbehagen kommt von der Ungewißheit des Empfängers, warum gerade er auf dieses Produkt oder jene Dienstleistung angesprochen wird.

   — Millionen von Bürgern werden von Kreditauskunfteien davon benachrichtigt, daß man Daten über sie speichert. Aber die Chance, den Bürger wirklich aufzuklären und auf seine Datenschutzrechte hinzuweisen, wird nicht genutzt.

   — Der Einzug der Mikroelektronik in die Arbeitswelt führt zu veränderten Anforderungen an die Arbeitnehmer und zum Wegfall von Arbeitsplätzen; massive Ängste vor Überforderung, Herabstufung und Arbeitslosigkeit sind die Folge; ebenso einschneidend kann die verschärfte Überwachung sein, die oft mit dem Einzug der Informationstechnik einhergeht.

   Alles in allem — der Bürger erlebt die automatische Datenverarbeitung als etwas, das ihm feindlich gesonnen ist. Die strukturbedingten negativen Züge einer Verwaltung — das Fehlen menschlicher Wärme, der distanziert-förmliche Umgang, der Vorrang quantitativer vor qualitativen Bewertungskriterien — sieht er durch die automatische Datenverarbeitung geradezu verkörpert. Wenn die gesamte Bevölkerung nunmehr mit computerlesbaren Belegen erfaßt werden soll, so sind vor diesem Hintergrund Mißtrauen und Ablehnung verständliche Reaktionen. Sie können bei einer zeitgemäßen Interpretation des Grundgesetzes, die den Technologiesprung des vergangenen Jahrzehnts mit einbezieht, nicht unberücksichtigt bleiben, wenn die Problematik in ihrer Gesamtheit erfaßt werden soll.

2. Dies führt zunächst zu der Frage, inwieweit das überkommene Verständnis dieses Prüfungs-

maßstabes der Datenverarbeitung im Jahre 1983 noch gerecht wird.

In der gegenwärtigen rechtlichen Betrachtungsweise steht die Informationsverarbeitung vielfach noch ganz im Schatten der zu erlassenden Entscheidung. Die hoheitliche Entscheidung, und ihre Ausführung — Verwaltungsakt und Maßnahme, Willenserklärung und Realakt — sind nach gegenwärtiger Rechtslage die wesentlichen Anknüpfungspunkte rechtlicher Regelung. Informationsaktivitäten, also das Sammeln, Speichern, Auswerten, Weitergeben und Löschen von Informationen, werden der Sphäre der Entscheidungsvorbereitung zugewiesen. Unser Grundgesetz ist im Kern auf die Entscheidung angelegt, nicht auf die Phase der Entscheidungsvorbereitung, wie insbesondere der Artikel 19 Abs. 4 GG zeigt, der die einfachgesetzlichen Regelungen — wie etwa das Verwaltungsverfahrensgesetz — entsprechend geprägt hat.

Man kann diese Einengung zur Tugend erklären. Der Verzicht auf den steuernden Eingriff des Rechts erscheint dann als Gebot der Freiheit, das Platz greifen muß, weil der Informationsverarbeitungsprozeß als Internum verstanden wird.

Die Gegenposition — vor vielen Jahren schon im Datenschutzschrifttum entwickelt — betrachtet jede Verarbeitung einer Information, die eine bestimmte Person betrifft, als dieser gegenüber rechtlich relevant, im Bereich des öffentlichen Rechts sieht sie darin einen Eingriff, der einer gesetzlichen Ermächtigung bedarf.

3. Ich halte beide Positionen nicht für überzeugend und tragfähig. Die Lösung muß in der Mitte liegen und sie dürfte auch für die verfassungsrechtliche Beurteilung der Volkszählung die Prüfungsmaßstäbe liefern:

   Die Tiefe des Eindringens in den Persönlichkeitsbereich — Stichwort: „Sphärentheorie" — und die Nachhaltigkeit der Einwirkung auf den Betroffenen sind dafür wesentliche Beurteilungskriterien; aber es müssen weitere Gesichtspunkte berücksichtigt werden.

   Wir dürfen uns nicht damit begnügen, den konkreten Vorgang der Datenspeicherung oder Übermittlung isoliert zu betrachten, sondern müssen die Konsequenzen sehen, die sich aus der vermehrten Mobilität der Daten ergeben: Die denkbare weitere Verwendung der Daten — sei es für andere Zwecke der gleichen Stelle, sei es nach Übermittlungen in ganz neue Sachzusammenhänge, wie beispielsweise in § 9 des Volkszählungsgesetzes vorgesehen — muß bei der ersten Maßnahme mit einkalkuliert werden, wenn ihre Bedeutung für den Betroffenen zutreffend beurteilt werden soll.

   Es ist ferner der Aspekt der Transparenz zu berücksichtigen. Wenn Art und Umfang der Datenverarbeitung und ihre Konsequenzen nicht erkennbar sind, kann die Verarbeitung personenbezogener Daten den Betroffenen sogar stärker in der Entfaltung seiner Persönlichkeit beeinträchtigen, als freiheitsbeschränkende Maßnahmen. Denn dann gibt die Datenverarbeitung zu Befürchtungen Anlaß, die das Verhalten des einzelnen maßgeblich beeinflussen können.

4. Der Übergang von der manuellen zur automatischen Datenverarbeitung ist vor allem in diesem Zusammenhang nicht nur von methodischer und organisatorischer Bedeutung; gravierende Auswirkungen auf den Grundrechtsschutz sind unverkennbar:

   Die isolierte Automation einzelner Verwaltungsaufgaben, die massenhaft anfallen — etwa in der Sozial- und Steuerverwaltung —, bereitet noch die geringsten Schwierigkeiten. Die Übertragung von Routineaufgaben auf Maschinen ändert meist wenig an der Beziehung zwischen Bürger und Behörde. Die Probleme der Verständlichkeit von Bescheiden und der Durchschaubarkeit des Verfahrens lassen sich mit klassischen verfassungs- und verwaltungsrechtlichen Grundsätzen lösen.

   Qualitative Veränderungen bewirkt dagegen die integrierte Datenverarbeitung, d. h. die zusammengefaßte Verarbeitung von Daten aus verschiedenen Verwaltungsaufgaben. Sie steht unter der Zielvorstellung, gleiche Daten, die in unterschiedlichen Zusammenhängen benötigt werden, nur einmal zu erheben und zu speichern und dadurch Bürger und Verwaltung zu entlasten. Die integrierte Datenverarbeitung war vor 15 Jahren das erklärte Ziel der Verwaltungsautomation, wurde aber nur in Ansätzen realisiert. Entsprechende Tendenzen könnten aber bald wieder aufleben, wie etwa das in Schweden vom Statistischen Zentralamt geplante System FOBALT zeigt. So einleuchtend das Prinzip der Einmalspeicherung und Vielfachverwendung von Daten auch erscheint, so wenig dürfen seine Auswirkungen übersehen werden. Sie bestehen einmal darin, daß eine wechselseitige Abhängigkeit staatlicher Aufgabenerledigung eintritt, die die Zuständigkeitsregelung gesetzlicher Aufgabenverteilung in Frage stellt. Zum anderen führt eine konsequent durchgeführte integrierte Datenverarbeitung zu einem Höchstmaß von organisatorisch-technischer Gleichschaltung — etwa in der Form übergreifender Nummernsysteme und streng normierter Formen der Datenspeicherung —, die auf eine umfassende technische Verfügbarkeit aller vom Staat verarbeiteten personenbezogenen Daten hinausläuft. Damit wird aber auch die faktisch als Freiheitssicherung wirkende Vielfalt durch die integrierte Datenverarbeitung aufgehoben.

   Die Automatisierung fördert die Tendenz zur zentralen, umfassenden Speicherung und zur massenhaften Verarbeitung personenbezogener Daten. Dadurch werden Wirkungen nicht nur quantitativ gesteigert, sondern sie können auch eine neue Qualität erhalten. So macht es

für den einzelnen, der für eine Statistik Auskünfte geben oder seine Personalien überprüfen lassen muß, zunächst keinen Unterschied, wie viele andere Bürger in gleicher Weise in Anspruch genommen werden. Der Unterschied wird aber bei der anschließenden Verwertung der Daten deutlich: Je größer und vollständiger eine Datensammlung, um so stärker das Interesse Dritter; ein wachsendes Datenangebot erzeugt und vermehrt auch die Datennachfrage.

Und schließlich erwähne ich das besondere Risiko der mißbräuchlichen und fehlerhaften Verarbeitung von Daten welches im automatisierten Verfahren ganz andere Dimensionen erlangt — mit oft irreversiblen Folgen für die Rechte des einzelnen.

Es kann nicht zweifelhaft sein, daß sich Risiken und Gefahren für den Grundrechtsschutz des Betroffenen bei statistischen Erhebungen und Verarbeitungen erheblich vermindern, wenn die Anonymisierung sichergestellt ist, die Daten nicht für Zwecke des Verwaltungsvollzugs und vor allem nicht zum Nachteil der Betroffenen verwendet werden. Genau diese Voraussetzungen sind aber bei der Volkszählung nicht erfüllt, wie ich im einzelnen in meinem Schriftsatz ausgeführt habe. Daraus folgt, daß ein verfassungsrechtlicher Prüfungsmaßstab hier ebenso unverzichtbar ist und daß er kein milderer sein kann als bei der automatisierten Verarbeitung personenbezogener Daten in anderen Fällen.

5. Soweit man danach das Vorliegen eines Eingriffs im Einzelfall bejaht, ist für die Verarbeitung von Informationen eine gesetzliche Ermächtigung erforderlich; diese muß sich ihrerseits an der Verfassung messen lassen. Die vermehrten Folgen der Informationsverarbeitung müssen auch bei der Anwendung des rechtsstaatlichen Grundsatzes der Normenklarheit, der für das Verhältnis zwischen dem einzelnen und dem Staat von fundamentaler Bedeutung ist, beachtet werden. Es ist nämlich die Frage, ob Befugnisnormen, die früher als hinreichend bestimmt betrachtet werden konnten, diese Anforderungen heute noch erfüllen.

   Dazu sind Zweifel anzumelden. Für große und die Grundrechtsgewährleistung wesentliche Bereiche der Informationsverarbeitung gibt es nur generalklauselartige Regelungen, deren konkrete Tragweite vom Bürger schwerlich nachzuvollziehen ist. Ich denke hier an Polizei und Verfassungsschutz. Das maßgebliche Kriterium der Erforderlichkeit für die Aufgabenerfüllung ist hier weit entfernt von einem exakten Maßstab, der in jedem Einzelfall ein eindeutiges Ergebnis liefert. Durch die Zukunftsbezogenheit der Aufgabe werden die Behörden zu Prognosen gezwungen, in die zwangsläufig Unwägbarkeiten mit eingehen. Die Unsicherheit wächst, wenn — wie gerade im Sicherheitsbereich — die Aufgabe vom Gesetz nur mit sehr unbestimmten und in hohem Grade wertausfüllungsbedürftigen Begriffen umschrieben ist. Und die Unsicherheit wirkt auf den Betroffenen um so bedrückender, wenn seine Daten im geheimen verarbeitet werden.

   Ich nenne dieses nur scheinbar den Bezug zur Volkszählung entbehrende Beispiel, weil es deutlich macht, daß eine nicht durch klare Normen vorhersehbare und eingrenzbare Nutzung von Daten zurückwirkt auf das Maß der Beeinträchtigung, die der Bürger durch die zwangsweise Abfrage seiner Daten erleidet.

6. Aus dieser Analyse des Standes der Informationsverarbeitung und ihrer Auswirkungen auf Staat und Gesellschaft möchte ich — mehr als ein Jahrzehnt nach der Mikrozensusentscheidung des Bundesverfassungsgerichts — folgendes Fazit ziehen:

6.1 Bei der Volkszählung ergeben sich Auswirkungen auf das Recht auf freie Entfaltung der Persönlichkeit unzweifelhaft schon aus der Verpflichtung des einzelnen, die vorgesehenen Angaben zu machen. Die Bewertung dieser Auswirkungen hängt maßgeblich von den speziellen Angaben ab, die zu machen sind, von der Art der Erhebung, von der vorgesehenen Verwendung der Daten und von ihrer Sicherung gegen eine mißbräuchliche Verwendung.

   Die Volkszählung bedurfte deshalb auch nach der herkömmlichen Eingriffstheorie eines Gesetzes, das zumindest die Auskunftsverpflichtung des Betroffenen, die Grundzüge der Datenerhebung, die vorgesehene Verwendung der Daten und die zu treffenden Sicherungsmaßnahmen regelt. Ich habe in diesem Zusammenhang meine Zweifel, ob beispielsweise für die Frage nach der Zugehörigkeit des Betroffenen zu einem Haushalt im Volkszählungsgesetz 1983 eine Grundlage gegeben ist, schriftlich dargelegt.

6.2 Die Anforderungen, die nach dem rechtsstaatlichen Grundsatz der Normenklarheit an die Verständlichkeit eines Gesetzes zu stellen sind, müssen sich wegen der fundamentalen Bedeutung dieses Grundsatzes für das Verhältnis zwischen dem einzelnen und dem Staat auch nach den geschilderten Auswirkungen der fortgeschrittenen Informationstechnik richten. Die Statistikgesetze umschreiben regelmäßig nur die zu erhebenden Lebenssachverhalte, nicht aber die konkreten Fragen, die der Bürger zu beantworten hat. Mir scheint eine Überprüfung dieser Praxis erforderlich. Wenn die konkreten Fragen im Gesetz genannt würden, ließen sich Zweifel an der Intensität des in der Auskunftspflicht liegenden Grundrechtseingriffs eher vermeiden. Solche Zweifel sind um so weniger hinnehmbar, wenn es sich um die Erhebung von Daten handelt, deren weitere Verwendung nur pauschal bzw. generalklauselartig umschrieben werden kann.

6.3 Im Hinblick auf den Grundsatz der Normenklarheit erscheinen aber auch die Vorschriften über die Verwendung der Volkszählungsdaten,

also die Übermittlungsvorschriften des § 9 VZG verbesserungsbedürftig.

Im Bereich staatlicher Tätigkeit mit unmittelbarer Auswirkung auf die Rechte und Pflichten des Bürgers gehört es zu den selbstverständlichen Grundsätzen der Rechtsstaatlichkeit, daß der betroffene Bürger zu keinem Zeitpunkt im unklaren darüber gelassen wird, welchen grundsätzlichen Charakter die staatliche Tätigkeit hat. Diese Berechenbarkeit des staatlichen Handelns muß auch im Bereich der Informationsverarbeitung gewährleistet sein. Die Übermittlungsvorschriften müssen deshalb zweifelsfrei klarstellen, daß eine Verwendung der Daten nur für planerische, statistische und wissenschaftliche Zwecke zulässig ist und daß die Übermittlung nur in dem Umfang erfolgen darf, wie der konkrete zugelassene Zweck diese erfordert. Deshalb sollte z. B. in § 9 Abs. 2 darauf hingewiesen werden, daß die obersten Bundes- und Landesbehörden als zugelassene Datenempfänger die Angaben an andere Stellen nicht für deren Aufgabenerfüllung weiterleiten dürfen, und bei der Datenübermittlung an Gemeinden zu statistischen Zwecken sollte die Übermittlung des Namens in keinem Fall zugelassen werden.

6.4 Bei dem den Melderegisterabgleich regelnden § 9 Abs. 1 VZG stellt sich zusätzlich die Frage, ob es verfassungsrechtlich zulässig ist, in einem einzigen Erhebungsverfahren dem Bürger personenbezogene Daten abzufordern, die der Staat für grundlegend verschiedene Verwendungszwecke benötigt. Beim Melderegister handelt es sich um eine Funktion der Ordnungsverwaltung, bei der der Eingriffs- und Kontrollaspekt ganz im Vordergrund steht. Daten des Meldewesens können uneingeschränkt auch gegen den Betroffenen verwendet werden, etwa durch Finanz- und Polizeibehörden. Zu den Wesensmerkmalen statistischer Erhebungen gehört es dagegen, daß sich die staatlichen Organe nicht für die Verhältnisse des einzelnen interessieren, sondern seine Angaben lediglich als statistisches Zählmaterial verwenden. Mit anderen Worten: dem Begriff der Statistik ist es inhärent, daß dem Bürger aus seiner Auskunft keinerlei Nachteile erwachsen können. Man könnte pointiert sagen, saß hier Vertrauen, dort aber die Erwartung staatlicher Eingriffe und Überprüfungen die Geschäftsgrundlage bilden. Die Frage, die hier zu stellen und zu beantworten ist, lautet daher, ob nicht aus Gründen der Berechenbarkeit und der Klarheit staatlichen Handelns eine Verbindung zweier Erhebungswege dann ausgeschlossen sein muß, wenn diese diametral entgegengesetzte Orientierungen des Bürgers voraussetzen und bedingen. Ich neige dazu, einen solchen Ausschluß zu bejahen, weil nur er dem Gebot der Rechtsklarheit und der Voraussehbarkeit staatlichen Handelns entspricht.

6.5 Zu der weiteren Frage des Gerichts, inwieweit Organisation und Verfahren durch Gesetz oder Rechtsverordnung geregelt werden sollten, habe ich in meinem Schriftsatz detailliert dargelegt, welche Bereiche nach meinen Vorstellungen gesetzlich geregelt werden sollen. Ich darf — um Wiederholungen zu vermeiden — hierauf Bezug nehmen, wobei ich nur noch einmal darauf hinweisen möchte, daß diese Forderung nach gesetzlicher Regelung m. E. nicht nur nach der vom Bundesverfassungsgericht entwickelten Wesentlichkeitstheorie zu beurteilen, sondern schon aus dem rechtsstaatlichen Grundsatz der Rechtsklarheit und Voraussehbarkeit abzuleiten ist.

7. Lassen Sie mich zum Abschluß auf ein zusätzliches Erfordernis des Grundrechtsschutzes hinweisen, das bisher kaum in der Diskussion stand.

Die Kontrolle durch besondere staatliche Organe — den Bundes- und die Landesbeauftragten — ist ein Kernstück der deutschen Datenschutzgesetzgebung. Sie hat sich in der Staatspraxis schnell einen festen Platz erobert. Anders als beim Wehrbeauftragten fehlt aber, wenn man von Nordrhein-Westfalen absieht, ihre Verankerung im Verfassungstext. Ich bin indes der Ansicht, daß der enorme Machtzuwachs, den die stetig fortschreitende Informationstechnik den staatlichen Organen dadurch beschert, daß sie ihre Befugnisse zu Eingriffs- und Kontrollmaßnahmen immer umfassender ausüben können, auf erhebliche verfassungsrechtliche Bedenken stoßen würde, wenn nicht die fortlaufende Beobachtung, Kontrolle und Kritik dieser Vorgänge durch besondere Instanzen gewährleistet wäre. Dies gilt in besonderem Maße für diejenigen Zonen staatlicher Tätigkeit, die dem Blick der Öffentlichkeit und der Kontrolle durch den einzelnen Betroffenen entzogen bleiben. Auch in den anderen Bereichen, z. B. denen der Steuerverwaltung, der Sozialverwaltung und der amtlichen Statistik, ist eine wirksame Kontrolle unverzichtbar. Erachtet man die Datenschutzkontrolle als Voraussetzung verfassungsrechtlich unbedenklicher Verwendung der Informationstechnik durch den Staat, so ergeben sich für die nähere Ausformung dieser Kontrolle die folgenden unverzichtbaren Positionen:

- ausreichende Untersuchungsbefugnisse, damit die grundrechtsrelevanten Auswirkungen der Informationstechnik in allen Bereichen staatlicher Tätigkeit beurteilt werden können,
- unmittelbarer Bericht an das Parlament und
- Unabhängigkeit der Kontrollinstanzen von den zu kontrollierenden Einrichtungen der Exekutive.

Ich meine, daß diese Gesichtspunkte für die Einschätzung der Risiken, die von jeder Informationsverarbeitung auf die Grundrechte des einzelnen ausgehen, von erheblicher Bedeutung sind.

Anlage 2 (zu Nr. 26)

Erklärung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz zur Novellierung des Bundesdatenschutzgesetzs vom 4. November 1983

I. Die öffentliche Diskussion zu den Themen Volkszählung, maschinenlesbarer Personalausweis, Personalinformationssysteme wie auch Bildschirmtext und andere Neue Medien zeigt eine zunehmende Sensibilisierung zu Fragen des Datenschutzes. Vor diesem Hintergrund ist in der Öffentlichkeit die Erwartung entstanden, daß eine Novellierung des Bundesdatenschutzgesetzes

— die bisher gewonnenen Erfahrungen sowie die neu aufgetretenen Probleme aufgegreift und regelt und

— den Datenschutzinstanzen wirksamere Kontrollinstrumente an die Hand gibt.

Die Datenschutzbeauftragten haben sich mehrfach für eine Novellierung ausgesprochen und sind nach wie vor der Meinung, daß das Bundesdatenschutzgesetz novellierungsbedürftig ist. Sie sehen jedoch im vorliegenden Referentenentwurf keinen geeigneten Beitrag zur Fortentwicklung des Datenschutzes, weil er

1. das geltende Datenschutzrecht teilweise verschlechtert,
2. hinter den bisherigen Entwürfen (CDU-Entwurf von 1980, SPD/FDP-Entwurf von 1980, Referentenentwurf von 1982) zurückbleibt,
3. wesentliche Forderungen der Datenschutzbeauftragten (Beschluß der Konferenz vom 21. 6. 1982) unberücksichtigt läßt und
4. den Anforderungen nicht gerecht wird, die sich aus der technischen Entwicklung ergeben.

II. Die Datenschutzbeauftragten fordern zu folgenden Punkten:

1. Aufgabe des Datenschutzes

Die Umschreibung der Aufgabe des Datenschutzes im Bundesdatenschutzgesetz als Schutz vor Mißbrauch ist irreführend, widerspricht dem Regelungsgehalt des Gesetzes und verkürzt den Schutz des Betroffenen. Im Gesetz ist deshalb klarzustellen: Aufgabe des Datenschutzes ist die Regelung des rechtmäßigen Umgangs mit personenbezogenen Daten und nicht nur die Verhinderung vorwerfbaren Fehlverhaltens. Neben der Speicherung, Veränderung, Löschung und Übermittlung sind deshalb auch die Erhebung und sonstige Nutzung Gegenstand des Datenschutzes.

2. Dateibegriff

Die Entscheidung des Gesetzgebers, bei der Anwendung des Bundesdatenschutzgesetzes von der Verarbeitung personenbezogener Daten in Dateien auszugehen, ist für den Bürger kaum verständlich, führt in der Praxis zu Unzuträglichkeiten und mindert die Wirksamkeit des Datenschutzes. Solange diese Anknüpfung besteht, muß der Dateibegriff wenigstens so definiert werden, daß ein Höchstmaß an Schutz für den Betroffenen erreicht wird. Dazu gehört, daß alle automatisierten Verfahren und alle Akten und Aktensammlungen einbezogen werden, die mit Hilfe automatisierter Verfahren erschlossen werden können.

3. Interne Dateien

Ausnahmeregelungen für interne Dateien sind mit einem konsequenten Schutz der Betroffenen unvereinbar. Deshalb muß das Bundesdatenschutzgesetz grundsätzlich auch auf interne Dateien anwendbar sein.

4. Einwilligung

Da das Gesetz jede Datenverarbeitung zuläßt, wenn die Einwilligung des Betroffenen vorliegt, muß der Gesetzgeber durch besondere Regelungen den Betroffenen davor schützen, daß er durch soziale, wirtschaftliche und psychische Zwänge (etwa als Mieter, Patient oder Arbeitsuchender) in seiner Entscheidungsfreiheit unangemessen eingeschränkt wird.

5. Unterrichtung des Betroffenen

Transparenz der Datenverarbeitung ist eine notwendige Voraussetzung des Datenschutzes. Der Betroffene ist deshalb in jedem Fall über die Tragweite seiner Einwilligung in die Datenverarbeitung sowie über die Rechtsgrundlage der Datenerhebung zu unterrichten, und zwar auch dann, wenn er dies nicht ausdrücklich verlangt. Die Unterrichtung bei der Datenerhebung muß ohne Rücksicht darauf erfolgen, ob die Daten in einer Datei, in Akten oder sonstigen Unterlagen festgehalten werden.

6. Verschuldensunabhängiger Schadensersatzanspruch und Folgenbeseitigungsanspruch

Bei unzulässiger oder unrichtiger Datenverarbeitung muß der Betroffene einen verschuldensunabhängigen Schadensersatzanspruch (auch für Nichtvermögensschäden) sowie einen Folgenbeseitigungsanspruch haben.

7. On-line-Anschlüsse

Der direkte Zugriff auf automatisierte Dateien über On-line-Anschlüsse ist für den Bürger mit besonderen Risiken verbunden. Dies gilt vor allem dort, wo Daten aus dem Medizin-, Sozial- und Sicherheitsbereich oder über strafbare Handlungen, Ordnungswidrigkeiten, religiöse und politische Anschauungen zum Abruf bereitgehalten werden. Diesen Risiken trägt der Entwurf nicht hinreichend Rechnung. Die Anforderungen an die Zulässigkeit von On-line-An-

schlüssen sind zu erhöhen und präziser zu fassen.

8. Zweckbindung

Die Zweckbindung der Daten ist eine der wichtigsten Voraussetzungen für den Schutz des Bürgers. Sie muß insbesondere in folgenden Bereichen verstärkt werden:

- Die Datenweitergabe innerhalb derselben Behörde muß grundsätzlich den gleichen Einschränkungen unterworfen werden wie die Datenübermittlung an andere öffentliche Stellen.
- Bei der Datenübermittlung an andere öffentliche Stellen muß die Verantwortung der übermittelnden Stelle ungeschmälert bleiben.
- Werden Daten an Stellen außerhalb des öffentlichen Bereichs übermittelt, so darf der Empfänger die Daten nur für den Zweck verwenden, zu dessen Erfüllung sie ihm übermittelt wurden.

9. Auskunftsanspruch

Das Recht des Bürgers auf Auskunft über seine Daten ist ein grundlegendes Datenschutzrecht. Es darf nicht eingeschränkt, sondern muß verstärkt werden. Dieses Auskunftsrecht muß gegenüber allen Behörden bestehen, grundsätzlich auch gegenüber den Sicherheits- und Finanzbehörden. Eine generelle Befreiung von der Begründungspflicht ist abzulehnen. Sie stände weder mit der Verfassung noch mit der Rechtsprechung in Einklang. Die Verweigerung einer Auskunft in Ausnahmefällen muß nachprüfbar sein. Die Erteilung der Auskunft muß stets kostenfrei sein.

10. Kontrolle

Im Interesse des Bürgers ist eine unabhängige und umfassende Datenschutzkontrolle unerläßlich. Die Datenschutzbeauftragten stellen dazu fest:

- Ihre Kontrollbefugnis umfaßt die Einhaltung der Datenschutzgesetze und aller anderen Datenschutzvorschriften, unabhängig davon, ob Daten in Dateien, in Akten oder in sonstiger Form festgehalten werden.
- Sie haben das Recht, uneingeschränkt alle Akten einzusehen, die mit der Verarbeitung personenbezogener Daten in Zusammenhang stehen.
- Besondere Geheimhaltungsvorschriften können ihnen bei ihrer Tätigkeit nicht entgegengehalten werden.

III. Eine Novellierung des Bundesdatenschutzgesetzes kann notwendige bereichsspezifische Regelungen nicht ersetzen. Die Datenschutzbeauftragten erinnern an ihre frühere Forderung nach Sonderregelungen insbesondere für den Sicherheitsbereich und für den Arbeitnehmerdatenschutz.

IV. Unabhängig von den verschiedenen Vorstellungen zur Novellierung des Bundesdatenschutzgesetzes können und dürfen die sich aus der technologischen Entwicklung ergebenden Konsequenzen nicht übersehen werden. Das Vordringen mittlerer und kleinerer Datenverarbeitungssysteme, die automatisierte Textverarbeitung sowie die Einführung bundesweiter Kommunikationssysteme stellen die Eignung des jetzigen Datenschutzkonzeptes in Frage. Der Gesetzgeber wird daher nicht umhin können, in naher Zukunft erneut und umfassend zum Datenschutz Stellung zu beziehen.

Anlage 3 (zu Nr. 27.2)

EUROPARAT

Empfehlung No. R(83)10 des Ministerkomitees an die Mitgliedstaaten zum Schutz personenbezogener Daten für Zwecke der wissenschaftlichen Forschung und Statistik

Das Ministerkomitee, kraft Artikel 15 (b) der Satzung des Europarates,

in der Erwägung, daß das Ziel des Europarats darin besteht, eine größere Einheit unter seinen Mitgliedern herzustellen,

in dem Bewußtsein, daß es notwendig ist, den Persönlichkeitsbereich des einzelnen gegenüber der zunehmenden Anwendung der Datenverarbeitung in dem Bereich der wissenschaftlichen Forschung und der Statistik zu schützen,

in der Überzeugung, daß die Verwendung personenbezogener Daten oft eine notwendige Bedingung für den Fortschritt der Wissenschaft darstellt,

in Anbetracht der Bedeutung, die der wissenschaftlichen Forschung sowohl als Wert für sich wie als unerläßlicher Faktor für den Fortschritt in der Gesellschaft zukommt,

eingedenk der Ausnahmen, die zugunsten der Tätigkeiten auf dem Gebiet der wissenschaftlichen Forschung und der Statistik in dem Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten zugelassen sind,

in der Feststellung, daß Ausnahmen in diesem Sinn auch von mehreren Mitgliedstaaten in den bestehenden oder in Ausarbeitung befindlichen Datenschutzgesetzen vorgesehen sind,

unter Berücksichtigung der Erklärung der European Science Foundation über den Schutz des Persönlichkeitsbereichs und die Verwendung personenbezogener Daten für Forschungszwecke,

eingedenk der Erfordernisse des Forschungsbereichs,

in der Erwägung, daß ein Ausgleich zwischen den Erfordernissen der Forschung und Statistik einerseits und dem unerläßlichen Schutz des einzelnen andererseits, besonders bei der automatisierten Datenverarbeitung geschaffen werden muß,

in dem Bewußtsein, daß es notwendig ist, geeignete Verfahren festzulegen, um die Interessen der verschiedenen betroffenen Parteien in Einklang zu bringen,

EMPFIEHLT den Regierungen der Mitgliedstaaten,

— ihr innerstaatliches Recht und ihre innerstaatlichen Praktiken hinsichtlich der Verwendung personenbezogener Daten zu Zwecken der wissenschaftlichen Forschung und der Statistik an den Grundsätzen und Leitlinien zu orientieren, die in dem Anhang zu dieser Empfehlung aufgeführt sind;

— dafür zu sorgen, daß diese Empfehlung in den mit wissenschaftlicher Forschung und Statistik befaßten öffentlichen und privaten Kreisen weite Verbreitung findet.

Anhang zur Empfehlung Nr. R (83) 10

1. Anwendungsbereich und Begriffsbestimmungen

1.1 Die in diesem Anhang enthaltenen Grundsätze und Leitlinien gelten für die Verwendung personenbezogener Daten für Zwecke der wissenschaftlichen Forschung und der Statistik sowohl im öffentlichen als auch im privaten Bereich, unabhängig davon, ob diese Daten automatisch oder nach manuellen Methoden verarbeitet werden.

1.2 Im Sinne dieser Empfehlung:

bedeutet „personenbezogene Daten" jede Information über eine bestimmte oder bestimmbare natürliche Person. Eine natürliche Person gilt nicht als „bestimmbar", wenn die Feststellung der Identität einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft erfordert;

umfaßt „Forschung" auch die Sammlung Verarbeitung personenbezogener Daten zu statistischen Zwecken;

1.3 Die Mitgliedstaaten können diese Grundsätze und Richtlinien auf Informationen über Personengruppen, Vereinigungen, Stiftungen, Gesellschaften, Körperschaften oder andere Stelle anwenden, die unmittelbar oder mittelbar aus natürlichen Personen bestehen, unabhängig davon, ob diese Stellen Rechtspersönlichkeit besitzen oder nicht.

2. Achtung des Persönlichkeitsbereichs

2.1 Die Achtung des Persönlichkeitsbereichs ist im Rahmen jedes Forschungsprojekts zu gewährleisten, das die Verwendung personenbezogener Daten erfordert.

2.2 Forschung soll soweit wie möglich anonymisierte Daten verwenden. Die wissenschaftlichen und fachlichen Organisationen sowie die öffentlichen Behörden sollen die Entwicklung von Techniken und Verfahren zur Wahrung der Anonymität fördern.

3. Einwilligung des Betroffenen

3.1 Jede Person, die Daten über sich mitteilt, soll ausreichend über die Art des Projekts, seine Ziele sowie über den Namen der Person oder der Stelle unterrichtet werden, für die die Forschungsarbeit durchgeführt wird.

3.2 Falls für den Betroffenen keine Verpflichtung besteht, die erbetenen Daten zur Verfügung zu stellen, soll er darüber unterrichtet werden, daß es ihm freisteht, mitzuarbeiten oder seine Mitwirkung abzulehnen. Der Betroffene soll das Recht haben, jederzeit seine Mitwirkung ohne Darlegung von Gründen abzubrechen.

3.3 Wenn in Anbetracht des verfolgten Ziels die in Absatz 3.1 erwähnte Information nicht ganz oder teilweise offenbart werden kann, bevor die Daten erfaßt sind, soll der Betroffene unmittelbar nach der Datenerfassung über diesen Inhalt vollständig unterrichtet werden, und es soll ihm freistehen, seine Mitwirkung fortzusetzen oder abzubrechen, und im letzteren Fall soll er die Löschung der erfaßten Daten verlangen können.

3.4 Besondere Schutzmaßnahmen sollen im Hinblick auf die Personen getroffen werden, deren Daten erfaßt werden und die unfähig sind, ihre eigenen Interessen zu wahren, oder die nicht in der Lage sind, ihre Einwilligung frei zu erteilen.

4. Verwendung der Daten

4.1 Die für Forschungszwecke beschafften personenbezogenen Daten dürfen für keinen anderen Zweck als die Forschung verwendet werden.

Insbesondere dürfen sie nicht verwendet werden, um Entscheidungen oder Maßnahmen zu treffen, die den einzelnen unmittelbar angehen, außer im Rahmen der Forschung oder mit ausdrücklicher Einwilligung des Betroffenen.

4.2 Die personenbezogenen Daten, die im Rahmen eines bestimmten Forschungsprojekts und mit Einwilligung der Betroffenen erhoben wurden, dürfen nur mit Einwilligung des Betroffenen für ein anderes Forschungsprojekt benutzt werden, daß sich in seiner Art und seinem Ziel wesentlich von diesem unterscheidet. Wenn es jedoch nicht möglich ist, diese Einwilligung wegen der inzwischen verstrichenen Zeit oder der großen Anzahl von Betroffenen zu erlangen, können die früher erhobenen Daten im Einklang mit Sicherheitsbestimmungen des innerstaatlichen Rechts verwendet werden.

4.3 Die öffentlichen und privaten Stellen sollen berechtigt sein, die personenbezogenen Daten, die sie für Verwaltungszwecke haben, für eigene Forschungszwecke zu verwenden. Wenn im Verlauf derartiger Forschungsarbeiten personenbezogene Daten in Dateien eingefügt werden, die bei dem betreffenden Verwaltungsorgan bereits geführt werden, oder wenn dessen Dateien verändert werden, sollen diese neuen Dateien nicht dem Verwaltungspersonal zur Verfügung gestellt werden, das mit Einzelfällen beschäftigt ist, es sei denn, mit Einwilligung des Betroffenen.

4.4 Die Bekanntgabe personenbezogener Daten durch öffentliche oder private Stellen zu Forschungszwecken darf nur mit Einwilligung des Betroffenen oder gemäß sonstigen Sicherheitsbestimmungen des innerstaatlichen Rechts erfolgen.

5. Erstellung von Stichproben

Der Zugang zu Einwohnermelderegistern sollte Forschern erleichtert werden, damit sie für die Erhebungen erforderlichen Stichproben zusammenstellen können. Vorbehaltlich der von den nationalen Behörden in bestimmten Fällen vorgesehenen Einschränkungen können die Stichproben über Namen, Anschrift, Geburtsdatum, Geschlecht und Beruf Aufschluß geben.

6. Zugang des Betroffenen zu den Daten

6.1 Das Recht des einzelnen auf Zugang und Berichtigung der ihn betreffenden Daten darf eingeschränkt werden, wenn die Daten zu rein statistischen Zwecken oder anderen Forschungszwecken erhoben und gespeichert werden und die erstellten Statistiken oder Forschungsergebnisse den einzelnen nicht leicht identifizieren, und wenn es angemessene Sicherheitsmaßnahmen gibt, um seinen Persönlichkeitsbereich in jedem Stadium des Forschungsprojekts zu schützen, einschließlich der Speicherung der Daten für eine spätere Verwendung.

6.2 Diese Bestimmung findet keine Anwendung, wenn in Anbetracht der Art der Forschung die natürliche Person ein besonders schutzwürdiges Interesse nachweisen kann.

7. Sicherung der Daten

7.1 Die Forschungsprojekte sollen ausdrücklich technische und organisatorische Maßnahmen vorsehen, um die Sicherung und Vertraulichkeit der Daten zu gewährleisten.

8. Veröffentlichung der Daten

8.1 Die für Forschungszwecke verwendeten personenbezogenen Daten dürfen nur dann in personenbezogener Form veröffentlicht werden, wenn die Betroffenen ihre Einwilligung gegeben haben, und in Einklang mit sonstigen Sicherheitsbestimmungen des innerstaatlichen Rechts.

9. Aufbewahrung der Daten

Bei jedem Forschungsprojekt soll, soweit wie möglich, angegeben werden, ob die erfaßten personenbezogenen Daten nach Beendigung des Projekts gelöscht, anonymisiert oder aufbewahrt werden, und im letzteren Fall unter welchen Bedingungen.

9.2 Wenn die Einwilligung des Betroffenen für die Durchführung eines Forschungsprojekts erforderlich ist, sollte sie auch die Frage der eventuellen Aufbewahrung der erfaßten personenbezogenen Daten nach Beendigung des Programms umfassen. War es nicht möglich, um die Einwilligung zur Aufbewahrung der Daten zu bitten, dürfen die Daten unter der Bedingung aufgehoben werden, daß die Aufbewahrung entsprechend den Sicherheitsbestimmungen des innerstaatlichen Rechts erfolgt.

9.3 Bevor über die Löschung personenbezogener Daten entschieden wird, die von öffentlichen Behörden in Besitz gehalten werden, sollte die mögliche zukünftige Verwendung solcher Daten für Forschungszwecke in Betracht gezogen werden, vorzugsweise nach Beratung mit für die Aufbewahrung öffentlicher Unterlagen zuständigen Institutionen.

9.4 Wenn nach Abschluß eines Projekts die verwendeten personenbezogenen Daten nicht gelöscht oder anonymisiert werden, wäre es angebracht, ihre Aufbewahrung in Institutionen zu fördern, die mit dieser Aufgabe betraut sind und in denen geeignete Sicherungsmaßnahmen ergriffen wurden.

10. Einrichtung von Kontrollgremien innerhalb des Forschungsbereichs

10.1 Die Einrichtung von Kontrollgremien innerhalb des Forschungsbereichs soll gefördert werden, um zur Entwicklung der in dieser Empfehlung enthaltenen Grundsätze und Leitlinien beizutragen.

Anlage 4 (zu Nr. 27.4)

Internationale Konferenz der Datenschutzinstanzen vom 17. bis 19. Oktober 1983

Beschluß zum Thema „Neue Medien"

1. Die Internationale Konferenz der Datenschutzbeauftragten geht übereinstimmend davon aus, daß der Einsatz Neuer Medien, die über Kabelnetze verbreitet werden, eine erhebliche Gefährdung für die Persönlichkeitsrechte mit sich bringen kann.

   Soweit bei den Neuen Medien die Kommunikation zwischen Informationsanbietern und Teilnehmern durch elektronische Datenverarbeitungsanlagen gesteuert wird, ist — im Gegensatz zu herkömmlichen Medien — die Speicherung personenbezogener Daten in einem gewissen Umfang erforderlich.

   So werden beim Medium „Bildschirmtext" (Videotex) Verbindungs- und Abrechnungsdaten gespeichert. Bei manchen Diensten werden die vom Teilnehmer abgerufenen Sendungen registriert. Das Recht der Unverletzlichkeit der Wohnung wird berührt, wenn mit neuen Diensten von außen in den Wohnungen Wirkungen ausgelöst und Messungen vorgenommen werden.

   Über die auf diese Weise an zentralen Stellen automatisiert entstehenden Sammlungen personenbezogener Daten könnten Persönlichkeitsprofile aller Benutzer erstellt werden. Deren soziale Beziehungen und Verhaltensweisen können damit zum Gegenstand von Maßnahmen gemacht werden.

   Darüber hinaus können mit Hilfe der Neuen Medien personenbezogene Daten jeglicher Art mit geringem Aufwand und in großem Umfang verbreitet werden. Erfahrungen mit Bildschirmtext haben gezeigt, daß Anbieter und Benutzer mißbräuchlich sensible Daten über die Neuen Medien veröffentlichen.

2. Um die Rechte der Bürger beim Einsatz Neuer Medien zu wahren, erachtet die Konferenz folgendes für erforderlich:

   Durch geeignete Maßnahmen, insbesondere der Gesetzgebung, sollten in jedem Land die Betriebsbedingungen so gestaltet werden, daß durch den Einsatz der Neuen Medien Persönlichkeitsrechte nicht beeinträchtigt werden.

   Hierzu müssen Erhebung, Speicherung und Übermittlung personenbezogener Daten bei der Nutzung auf das unumgängliche Maß eingeschränkt werden. Die Erstellung von Nutzungsprofilen muß untersagt werden.

   Der Inhalt der Informationsangebote darf Persönlichkeitsrechte nicht verletzen.

   Technische und organisatorische Maßnahmen, die dem jeweiligen Stand der Technik entsprechen, müssen die Durchsetzung dieser rechtlichen Forderungen unterstützen.

   Die Staaten sollten dabei die Auswirkungen bei der grenzüberschreitenden Nutzung beachten; insbesondere sollte verhindert werden, daß durch die Verarbeitung personenbezogener Daten sowie die Gestattung des Zugriffs auf diese Daten in einem Land bestehende gesetzliche Bestimmungen in einem zweiten Land umgangen werden können. Der Mindeststandard der Richtlinien über den Datenschutz und den grenzüberschreitenden Verkehr mit personenbezogenen Daten der OECD vom 23. September 1980 sowie der Datenschutzkonvention des Europarates vom 28. Januar 1981 sollte auch bei der Nutzung Neuer Medien gewährleistet sein, und zwar auch dann, wenn das nationale Recht Ausnahmebestimmungen vom Datenschutz für Presse und Rundfunk vorsieht.

3. Die Konferenz hält eine internationale Zusammenarbeit der Kontrollinstitutionen für den Datenschutz bei der Überwachung Neuer Medien für geboten.

Sachregister

Abkürzungsverzeichnis

ADV	Automatisierte Datenverarbeitung
AO	Abgabenordnung
APIS	Arbeitsdatei PIOS-Innere-Sicherheit
AWV	Arbeitsgemeinschaft für wirtschaftliche Verwaltung e. V.
AZR	Ausländerzentralregister
BAT	Bundes-Angestelltentarifvertrag (Bund, Länder, Gemeinden)
BBG	Bundesbeamtengesetz
BDSG	Bundesdatenschutzgesetz
BfA	Bundesversicherungsanstalt für Angestellte
BfD	Bundesbeauftragter für den Datenschutz
BfV	Bundesamt für Verfassungsschutz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGS	Bundesgrenzschutz
BKA	Bundeskriminalamt
BKGG	Bundeskindergeldgesetz
BMA	Bundesminister für Arbeit und Sozialordnung
BMI	Bundesminister des Innern
BMJFG	Bundesminister für Jugend, Familie und Gesundheit
BMP	Bundesminister für das Post- und Fernmeldewesen
BMV	Bundesminister für Verkehr
BND	Bundesnachrichtendienst
BPersVG	Bundespersonalvertretungsgesetz
BStatG	Bundesstatistikgesetz
BT	Bundestag
Btx	Bildschirmtext
BVerfGE	Bundesverfassungsgerichtsentscheidung
BZR	Bundeszentralregister
BZRG	Bundeszentralregistergesetz
DA	Dienstanweisung für die Standesbeamten und ihre Aufsichtsbehörden
DATEX-P	Paketvermittelnde Datenübermittlung (DATa EXchange)
DAV	Allgemeine Verwaltungsvorschrift für die Einrichtung und Benutzung dienstlicher Fernmeldeanlagen für die Amtsverwaltung (Dienstanschlußvorschriften)
EDV	Elektronische Datenverarbeitung
EWS	Elektronisches Wählsystem
G 10	Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses
GABl	Gemeinsames Amtsblatt von Baden-Württemberg
GAN	Grenzaktennachweis
GG	Grundgesetz
IDVS II	Informations- und Datenverarbeitungssystem für die Ortskrankenkassen
INPOL	Informationssystem der Polizei
IRG	Gesetz über die Internationale Rechtshilfe in Strafsachen
ISD	Internationaler Suchdienst
KAN	Kriminalaktennachweis
KBA	Kraftfahrt-Bundesamt
KpS-Richtl.	Richtlinien über die Errichtung und Führung kriminalpolizeilicher personenbezogener Sammlungen
LKA	Landeskriminalamt
MAD	Militärischer Abschirmdienst
MinBlFin	Ministerialblatt des Bundesministers der Finanzen und des Bundesministers für Wirtschaft

MiStra	Mitteilungen in Strafsachen
MiZi	Mitteilungen in Zivilsachen
MTB II	Manteltarifvertrag für Arbeiter des Bundes vom 27. Februar 1964
NADIS	Nachrichtendienstliches Informationssystem
NJW	Neue Juristische Wochenschrift
NVwZ	Neue Zeitschrift für Verwaltungsrecht
OVG	Oberverwaltungsgericht
PIOS	Auskunftssystem über Personen, Institutionen, Objekte und Sachen
PIOS-TE	PIOS-Terrorismus
RiStBV	Richtlinien für das Strafverfahren und das Bußgeldverfahren
RVO	Reichsversicherungsordnung
SCHUFA	Schutzgemeinschaft für allgemeine Kreditsicherung GmbH
SGB	Sozialgesetzbuch
SGB X	Sozialgesetzbuch Zehntes Buch
SPUDOK	Spurendokumentationssystem
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
STS	Schalterterminalsystem
StVG	Straßenverkehrsgesetz
StVZO	Straßenverkehrs-Zulassungs-Ordnung
TB	Tätigkeitsbericht *)
VG	Verwaltungsgericht
VwVfG	Verwaltungsverfahrensgesetz
VZG	Volkszählungsgesetz
VZR	Verkehrszentralregister
ZEVIS	Zentrales Verkehrsinformationssystem

*) Erster Tätigkeitsbericht ist erschienen als Bundestags-Drucksache 8/2460
Zweiter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache 8/3570
Dritter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache 9/93
Vierter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache 9/1243
Fünfter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache 9/2386

Druck: Bonner Universitäts-Buchdruckerei, 5300 Bonn
Alleinvertrieb: Verlag Dr. Hans Heger, Postfach 20 08 21, Herderstraße 56, 5300 Bonn 2, Telefon (02 28) 36 35 51
ISSN 0722-8333