Deutscher Bundestag
13. Wahlperiode

Drucksache 13/7500

16. 04. 97

Sachgebiet 204

Unterrichtung

durch den Bundesbeauftragten für den Datenschutz

Tätigkeitsbericht 1995 und 1996 des Bundesbeauftragten für den Datenschutz – 16. Tätigkeitsbericht –

Gliederung

Zugeleitet mit Schreiben des Bundesbeauftragten für den Datenschutz vom 16. April 1997 – L – 111/18 – gemäß § 26 Abs. 1 des Bundesdatenschutzgesetzes.

1 Einführung

Mit dem 16. Tätigkeitsbericht, den ich dem Deutschen Bundestag vorlege, gebe ich einen Überblick über die Schwerpunkte meiner Arbeit in den Jahren 1995 und 1996 und einen Ausblick auf anstehende wichtige Fragen. Dieser Tätigkeitsbericht ist zugleich der zweite in meiner Amtszeit als Bundesbeauftragter für den Datenschutz. Vor allem den Mitgliedern des Deutschen Bundestages danke ich für vielfache Unterstützung und Aufgeschlossenheit. Den Mitarbeiterinnen und Mitarbeitern meiner Dienststelle danke ich besonders für zuverlässige und engagierte Zusammenarbeit.

Datenschutz muß dem Schutz des allgemeinen Persönlichkeitsrechts ebenso genügen wie dem Anspruch der Allgemeinheit auf erforderliche Informationen. Richtiges Augenmaß ist hier die Richtschnur. Kontroversen in diesem Zusammenhang sehe ich deshalb nicht nur als unausweichlich, sachliche Kontroversen als ausgesprochen nützlich.

1.1 Einstieg in das Informationszeitalter – Der Kunde im Glashaus?

Vor 20 Jahren hatte das Bundesdatenschutzgesetz – mit ihm auch der Bundesbeauftragte für den Datenschutz – seine Geburtsstunde. Entsprechend unserer Grundrechtstradition geht das Gesetz auch nach einzelnen Änderungen vor allem von dem Gedanken eines informationellen Abwehrrechts des selbstbestimmten Bürgers gegenüber einem mächtigen Staat aus. In der Tat waren manche staatliche Behörden für manchen Bürger informationshungrig. Nach 20 Jahren hat der Datenschutz im Verhältnis Staat – Bürger aber ein insgesamt hohes Maß an Akzeptanz und Normalität gewonnen, in Recht und Gesetz ist er weitgehend und sicher verankert.

Demgegenüber kennzeichnen Multimedia, weltweite Kommunikation im Internet und die Verbreitung der Datenverarbeitung im privaten Bereich die Situation für den Datenschutz im ausgehenden 20. Jahrhundert. Längst hat die neue Wirklichkeit begonnen. „Surfen im Internet" verspricht nicht nur einen Freizeitspaß, sondern weite informationelle Räume. Immer mehr private Rechner sind vernetzt und können untereinander Informationen austauschen. Hierbei fallen Informationen gleichsam nebenbei an. Smartcards sind bald in jedem Lebensbereich zu finden – nicht nur bei Banken und beim Einkauf, auch im Gesundheitssektor. Anbieter haben ein großes wirtschaftliches Interesse an dieser Entwicklung, und bei vielen Kunden stößt diese auf Zustimmung. Auch der Datenschutz steht dieser Entwicklung nicht im Wege. Dennoch machen sich bereits bei vielen Kunden Skepsis und Sorge breit. Längst ist für bestimmte Unternehmen von „Geldwert", das Konsumverhalten der Kunden im einzelnen zu studieren. Zu einer guten Kundenbetreuung gehört es mittlerweile, außer vom Kunden den Namen, die Anschrift, das Alter und den Beruf auch zu wissen, was und wieviel er gekauft hat und in welchem Zeitraum, ob er ein guter oder ein säumiger Kunde ist oder ob er mit Reklamationen eher Schwierigkeiten macht. Sein Interesse kann mit Preisausschreiben und Werbegeschenken getestet werden, am Ende will man Risikokunden frühzeitig erkennen, um deren Abwanderung zu verhindern. Das Szenario läßt sich beliebig fortsetzen, denn es ist bereits Realität. Dennoch muß festgestellt werden: Dem legitimen Interesse von Handel und Wirtschaft auf Verkauf steht das Interesse des Bürgers gegenüber auf Durchsichtigkeit und Beherrschbarkeit der privaten Datenverarbeitung. Den Kunden im Glashaus will unsere Verfassung nicht haben.

In einer Umfrage konnte man jüngst nachlesen, daß auf einer Skala von Bedrohungen, vor denen sich die Bürger am meisten fürchten, an erster Stelle und mit deutlichem Abstand die Befürchtung steht, die eigenen Daten würden zu Werbezwecken mißbraucht. Erst danach kamen Ängste wie Opfer einer Straftat zu werden oder im Straßenverkehr zu verunglücken.

1.2 Datenschutz im Umbruch

Die bereits vorhandenen und weiter steigenden Informationssammlungen und -verarbeitungen in privater Hand führen zu veränderten Datenschutzproblemen, deren Gefährlichkeit angesichts ihrer Vorteile nicht für jedermann auf den ersten Blick erkennbar ist. Gemeinsam ist den neuen Technologien, daß sie zu mehr Datenspuren, Datensammlungen und Datenabgleichen imstande sind. Wer zur unbegrenzten Preisgabe seiner Daten verlockt wird, muß wissen, daß am Ende umfassende Profile über ihn erstellt werden können, was in der Regel ungeahnte Einsichten in seine Persönlichkeit erlaubt.

Damit ist auf längere Sicht das Konzept eines Datenschutzes in Frage zu stellen, das sich bislang auf den Staat als Informationsverarbeiter konzentriert und die private Datenverarbeitung eher am Rande wahrnimmt. Für den Datenschutz ist dies eine Herausforderung, an die zur Zeit des Volkszählungsurteils in 1983 niemand denken konnte. Auch zukünftig wird nach unserer Verfassung zwischen staatlichem Verhalten einerseits und privatem, wirtschaftlichem Verkehr andererseits zu trennen sein. Für den Grundrechtsschutz im Hinblick auf die informationelle Selbstbestimmung des Bürgers wird aber die Unterscheidung nach öffentlicher und nicht-öffentlicher Ursächlichkeit zunehmend an Bedeutung verlieren.

1.3 EG-Datenschutzrichtlinie – Chance für modernes Datenschutzrecht

Nach der Unterzeichnung der EG-Datenschutzrichtlinie im Oktober 1995 müssen alle EU-Mitgliedsstaaten ihr Datenschutzrecht bis Oktober 1998 harmonisieren. Dies ist ein bedeutsamer Schritt in Richtung internationaler Verbindlichkeit auf dem Gebiet des Datenschutzes. Manche der deutschen Datenschutzvorschriften sind zu wesentlichen Teilen in die europäische Datenschutzrichtlinie eingeflossen. Sie haben damit Vorbildcharakter und sind zu einem Exportmodell geworden. Dies kann nicht hoch genug gewürdigt werden, insbesondere nachdem Datenschutz in Deutschland in früheren Jahren eher häufig auf Kritik und auch Ablehnung gestoßen ist. Zu

Recht stellt die Richtlinie fest, daß Datenverarbeitungssysteme im Dienste des Menschen stehen.

Mit der Umsetzung der EG-Datenschutzrichtlinie in nationales Recht sind die Vorschriften für den öffentlichen und den privaten Bereich weitgehend zu vereinheitlichen. Unter anderem werden die Rechte der Betroffenen auf Information durch die datenverarbeitenden Stellen über die Verwendung ihrer Daten ebenso erweitert wie die Rechte auf Auskunft und Widerspruch und hinsichtlich der Einwilligung. Bei der Vorbereitung von Regelungen mit Auswirkungen auf den Datenschutz werden Risikoanalyse, Vorabkontrolle, Technikfolgenabschätzung sowie Verpflichtung zur Beteiligung der Datenschutzbeauftragten verpflichtend vorgeschrieben. Über die allgemeinen Datenschutzgesetze von Bund und Ländern hinaus sind zahlreiche bereichsspezifische datenschutzrechtliche Regelungen zu überprüfen. Bedenkt man, daß die Vorarbeiten zur letzten Reform des Bundesdatenschutzgesetzes in 1990 mehr als 4 Jahre gedauert haben, dann zeigt sich die Eilbedürftigkeit dieses Vorhabens.

Wie meine Kollegen in den Ländern appelliere ich an den Gesetzgeber, die Umsetzung der Richtlinie nicht nur als Beitrag zur europäischen Integration zu verstehen, sondern auch als Aufforderung und Chance, den Datenschutz fortzuentwickeln. Angesichts der sich rapide verändernden Welt der Datenverarbeitung, der Medien und der Telekommunikation ist eine Modernisierung des deutschen Datenschutzrechts notwendig, damit der einzelne auch künftig über die Verwendung seiner persönlichen Daten so weit wie möglich selbst bestimmen kann. In diesem Rahmen habe ich der Bundesregierung ein detailliertes Positionspapier zur Umsetzung der Europäischen Datenschutzrichtlinie und zur Novellierung des Bundesdatenschutzgesetzes übergeben.

Den Datenschutzbeauftragten geht es dabei um mehr als durch Gemeinschaftsrecht erzwungene Minimalkorrekturen. Mit meinen Kollegen aus den Ländern bin ich der Auffassung, daß die Anpassung des deutschen Rechts an die EU-Richtlinie genutzt werden sollte, das Datenschutzrecht in Deutschland von überholten Konzepten zu befreien und zugleich den Regelungserfordernissen einer von Multimedia, Internet und Chipkarten geprägten Zukunft gerecht zu werden. Nur wenn diese Chance ergriffen wird, kann das Datenschutzrecht Ende des ausgehenden 20. Jahrhunderts seine Rolle für das informationelle Selbstbestimmungsrecht des Einzelnen erfüllen (s. Nr. 2.1).

1.4 Forderungen für den Datenschutz im privaten Sektor auf dem Weg ins Jahr 2000

Entwicklungen in den unterschiedlichsten privaten Bereichen machen deutlich, daß das Persönlichkeitsrecht der Bürger nicht hinter diesen zurückbleiben darf, sondern mit ihnen Schritt halten muß. Für eine Stärkung des Persönlichkeitsrechts sehe ich Handlungsbedarf besonders in folgenden Punkten:

- Zur Verhütung von Diebstählen oder Überfällen haben **Videoüberwachungen** im privaten Bereich rasant zugenommen. Sie erfolgen teils offen, teils aber auch verdeckt. Kaum noch ein Kaufhaus oder ein Verkehrsbetrieb kommen ohne den Einsatz von Videokameras aus. So sehr dieser Einsatz von Videoüberwachung beispielsweise zur Vorbeugung von Straftaten notwendig oder vertretbar ist, so dringend ist der datenschutzrechtliche Regelungsbedarf in Bezug auf die Erhebung und Verarbeitung der Daten von zumeist vielen Menschen. Hier fehlt es bisher völlig an Datenschutzvorschriften. Es muß daher Rechtsklarheit darüber hergestellt werden, unter welchen Voraussetzungen überhaupt eine Videoüberwachung zulässig ist. Notwendig ist insbesondere eine Vorschrift, wonach die Bürger in bestimmten Fällen ausdrücklich auf die Videoüberwachung hingewiesen werden müssen. Ferner ist zu regeln, für welche Zwecke die Aufnahmen benutzt werden dürfen (s. Nr. 31.1).
- Besondere Datenschutzvorschriften fordere ich auch für die Entwicklung und den Einsatz von **Chipkarten**. Insbesondere ist festzulegen, daß personenbezogene Daten auf der Chipkarte auf den unbedingt erforderlichen Umfang zu beschränken sind. Der Kartenherausgeber oder Systembetreiber ist zu verpflichten, durch technisch-organisatorische Maßnahmen zu gewährleisten, daß die Kartendaten nur entsprechend ihrer jeweiligen Zweckbindung verarbeitet werden können. Er sollte die Pflicht haben, dem Betroffenen die Möglichkeit zur kostenlosen, vertrauenswürdigen und ohne großen Aufwand realisierbaren Selbstinformation zu gewährleisten, wozu in bestimmten Fällen auch die Information gehört, wer wann auf welche Daten zugegriffen hat (s. Nr. 9).
- Für die **privaten Krankenversicherungen** gibt es bisher anders als bei den gesetzlichen Krankenversicherungen nur sehr allgemeine Regelungen zum Datenschutz. In umfassendem Maße werden aber auch bei den privaten Krankenversicherungen besonders sensible Gesundheitsdaten, wie Diagnose und Therapie, die in Arztpraxen oder Krankenhäusern dem strafbewehrten Arztgeheimnis unterliegen, verarbeitet. Für die Durchbrechung des Arztgeheimnisses ist hier bislang ausschließlich maßgeblich die Einwilligungserklärung des Versicherten. Wie mit dem strengen Sozialdatenschutz für die gesetzliche Krankenversicherung im Sozialgesetzbuch X geregelt, muß sorgfältig geprüft werden, welche speziellen Rechtsnormen für die private Krankenversicherung zum Schutz der Gesundheitsdaten der freiwillig Versicherten unabdingbar sind.
- Die starke Kriminalitätsentwicklung hat auch dazu geführt, daß **private Sicherheitsdienste** z. B. zum vorbeugenden Schutz vor Straftaten in besonderem Maße beauftragt werden. In das Visier der privaten „Hilfssheriffs" kommen aber nicht nur bescholtene, sondern auch unbescholtene Bürger. Dossiers über Personen oder Warndateien sowie verdeckte Ermittlungen und Observationen sind Stichworte, die ein Licht auf die Datenschutzproblematik der wachsenden Sicherheitsbranche werfen. Auch im Hinblick auf das staatliche Gewaltmonopol ist daher vor allem zu klären, welche

Daten private Sicherheitsdienste erheben dürfen, in welcher Form und zu welchem Zweck dies möglich sein soll, an wen die Daten weitergegeben werden dürfen und wann sie zu löschen sind (s. Nr. 31.1).

- Die stark zunehmende Werbepost zeigt, daß **Adreßhandel** und **Direkt-Marketing** wie nie zuvor boomen. Mehr als je zuvor wenden sich aber auch Bürger an mich, die bei Werbeaktionen einen Mißbrauch ihrer persönlichen Daten befürchten. In Umsetzung der EG-Datenschutzrichtlinie ist zu erwarten, daß im Bundesdatenschutzgesetz ein Recht auf Information über die Möglichkeit des Widerspruchs vor der ersten Weitergabe an Dritte eingeführt wird. Über diese Vorschrift hinaus fordere ich zur Verstärkung des Schutzes gegenüber Adresshandel und Direkt-Marketing, diese Informationen bereits bei Vertragsschluß zu geben, wenn die Nutzung oder Weitergabe der Daten für diese Zwecke von vornherein beabsichtigt ist. Eine Verwendung der Daten für Werbung oder Markt- und Meinungsforschung sollte nur nach vorheriger Information des Betroffenen über sein Widerspruchsrecht möglich sein. Ebenso muß das werbende Unternehmen verpflichtet werden, Auskunft über die Datenquellen zu geben.

1.5 Leitplankensystem an der Datenautobahn mit Löchern?

In dem Arbeitsprogramm der Enquete-Kommission „Zukunft der Medien" heißt es: *„In den Industriestaaten vollzieht sich gegenwärtig ein Wandel, der in seinen Wirkungen vergleichbar mit dem Übergang von der Agrar- zur Industriegesellschaft im letzten Jahrhundert ist."* Ein besonderes Wirtschaftswachstum wird bei den Netzen für multimediale Informations- und Kommunikationsdienste erwartet. Die Einzelheiten dieser neuen Märkte sind heute erst in Umrissen erkennbar. Die außerordentlichen Vorteile der informationstechnischen Revolution werden aber erst dann voll zur Geltung kommen, wenn wirksame Regeln zum Schutz der Privatsphäre und als Vertrauensbasis für geschäftliche Beziehungen geschaffen werden, d. h. die Informationsgesellschaft braucht die Akzeptanz der Menschen. Zur Zeit ist die Unsicherheit der Bürger gegenüber den neuen Informationstechnologien immer noch groß. Berichte über die „anarchischen" Zustände im Internet haben viele abgeschreckt. Wenn auch vereinzelt noch darauf spekuliert wird, neben den Entgelten von Kunden und den Einnahmen aus der Werbung in den Multimedianetzen mit den im Prinzip herstellbaren Kundenprofilen eine dritte Einnahmequelle zu haben, haben viele wirtschaftlich orientierte Anbieter längst erkannt, daß Datenschutz das Vertrauen des Nutzers in die Vertraulichkeit und Verläßlichkeit der neuen Dienste in großem Maße mitbestimmt. Neben Verbraucherschutz und IT-Sicherheit wird Datenschutz der gewünschte Begleiter sein, ohne den die Bürger den Weg in die Informationsgesellschaft nicht gehen werden. Oder anders ausgedrückt: Datenschutz ist einer der Erfolgsfaktoren für die neuen Informationstechnologien.

Der von der Bundesregierung im Dezember 1996 beschlossene Entwurf des Informations- und Kommunikationsdienstegesetzes trägt diesen Anforderungen in weiten Teilen Rechnung. Als besonders positiv ist hervorzuheben, daß sich die Gestaltung und Auswahl technischer Einrichtungen für Teledienste an dem Ziel auszurichten haben, keine oder so wenig wie möglich personenbezogene Daten zu erheben und zu verarbeiten. Damit fände ein Grundsatz, für den Datenschützer stets eingetreten sind, erstmals in dieser Deutlichkeit Eingang in ein Gesetz.

Zu meinem Bedauern enthält der Gesetzentwurf nicht mehr die ursprünglich vorgesehene Möglichkeit, ein „Datenschutzaudit" einzurichten. Damit könnten zur Verbesserung von Datenschutz und Datensicherheit Diensteanbieter ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten sowie das Ergebnis der Prüfung veröffentlichen lassen. Angesichts der technischen Entwicklungen im Bereich der neuen Informations- und Kommunikationsdienste wäre das Datenschutzaudit eine richtige Antwort auf das gestiegene Datenschutzbewußtsein bei der Verarbeitung personenbezogener Daten. Es wäre ein Instrument, im Wege der Selbstregulierung und der Schaffung marktgerechter Anreize ein hohes Datenschutzniveau sicherzustellen. Das Fehlen eines Qualitätssiegels wie des Audits verhindert oder erschwert demgegenüber die Orientierung, die für eine breite Akzeptanz notwendig ist und die den massenhaften Einstieg ins informationstechnische Zeitalter überhaupt erst ermöglicht.

Große Bedenken habe ich gegen die im Gesetzentwurf vorgesehene Verpflichtung der Diensteanbieter, der Polizei, den Nachrichtendiensten und Verwaltungsbehörden auf Verlangen die Bestandsdaten ihrer Kunden zu übermitteln. Eine derart weitreichende Zugriffsbefugnis auf personenbezogene Daten bei privaten Dienstleistern würde beispielsweise Anbieter von home-banking, tele-learning-Diensten oder von online-Zeitungen dazu verpflichten, der Polizei oder Verwaltungsbehörden ohne weitere Voraussetzungen Auskunft über die Nutzer ihrer Dienste zu geben. Derartige Eingriffe in das Recht auf informationelle Selbstbestimmung mit der Möglichkeit der Erstellung von Nutzerprofilen und der Gefahr einer Überwachung auch von Unverdächtigen sind nicht akzeptabel. Die Teledienste sollen als moderne Informations- und Kommunikationsdienste herkömmliche Angebote von Dienstleistungen und Gütern ergänzen und ersetzen. Es ist daher überhaupt nicht ersichtlich, warum Angebote in elektronischer Form anders als herkömmliche Angebote behandelt werden sollen, für deren Anbieter eine derartige Auskunftspflicht über Kunden nicht besteht. Sowohl das Strafprozeßrecht als auch die Polizeigesetze enthalten in diesem Bereich bereits ausreichende Eingriffsbefugnisse zur Strafverfolgung bzw. Gefahrenabwehr.

Ich hoffe daher sehr, daß im weiteren Gesetzgebungsverfahren hierzu noch Korrekturen erfolgen und den Nutzern der Teledienste ein solch weitreichender Eingriff in die Informations- und Meinungs-

freiheit erspart bleibt. Ebenso hoffe ich auf Nachbesserungen des Gesetzgebers beim Datenschutzaudit (s. Nr. 8.1).

1.6 Spannungsverhältnis „Großer Lauschangriff" – Datenschutz

Mein besonderes Plädoyer gilt einer Neuorientierung des Datenschutzes im privaten Bereich vor dem Hintergrund der rasanten Entwicklung neuer Medien. Aber auch die herkömmliche, „klassische" Thematik des Datenschutzes im Verhältnis Staat – Bürger hat an Bedeutung nicht verloren. Die aktuelle Diskussion ist besonders von dem Thema „Großer Lauschangriff" geprägt. Während führende Stimmen und auch Fachleute davor warnen, die akustische Wohnraumüberwachung als Allheilmittel zur Bekämpfung der organisierten Kriminalität zu sehen, wird in Teilen der politischen Diskussion schon gefordert, zugleich auch die Videoüberwachung in Privatwohnungen einzuführen. Vielfach vernachlässigt die Diskussion andere Problemfelder der ebenso bedrohlichen allgemeinen Kriminalitätssituation in Deutschland.

Während um die akustische Wohnraumüberwachung bei der Verbrechensbekämpfung politisch gerungen wird, ist der Lauschangriff im Bereich der Gefahrenabwehr seit z. T. längerer Zeit fester Bestandteil der Landespolizeigesetze. In 15 der 16 Bundesländer ist das Abhören und Aufzeichnen von Gesprächen und Wohnungen und sonstigen Räumen unter bestimmten Voraussetzungen erlaubt. Trotz dieser Befugnisse werden aber die technischen Mittel der Wohnraumüberwachung im Bereich Gefahrenabwehr offensichtlich wenig genutzt.

Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich mit dem Thema der akustischen Wohnraumüberwachung beschäftigt und dazu Empfehlungen vorgelegt.

Unabhängig davon, daß die meisten Landesdatenschutzbeauftragten der Einführung der akustischen Wohnraumüberwachung ablehnend gegenüberstehen, sehe ich in den Empfehlungen der Konferenz einen konstruktiven Beitrag für die weitere politische Beratung. Nach meinem Empfinden wird in der politischen Auseinandersetzung zu sehr auf Gangster und Verdächtige abgestellt. Daß aber auch zu einem wesentlichen Teil unverdächtige und unbescholtene Dritte von der akustischen Wohnraumüberwachung betroffen sein werden, kommt in der Diskussion zu kurz.

Angesichts des offenkundigen Spannungsverhältnisses zwischen dem Einsatz der akustischen Wohnraumüberwachung und dem Persönlichkeitsrecht der Betroffenen haben mich Äußerungen, Datenschutz habe mit der Thematik nichts zu tun, verwundert und überrascht. Insgesamt hoffe ich, daß die vom Gesetzgeber zu schaffende gesetzliche Regelung den datenschutzrechtlichen Kernanliegen Rechnung tragen wird, geht es doch hier nicht nur um „Gangsterwohnungen", sondern auch um einen Eingriff in das durch die Menschenwürde geschützte private Refugium anderer Betroffener (s. Nr. 6.1.1).

1.7 Fahndungspannen und Datenschutz – Vorwürfe ohne Sinn und Verstand

Im Herbst 1995 flüchtete der mehrfache Mörder Holst aus einer Hamburger Klinik, wo er nach seiner Verurteilung untergebracht war. Erst Ende 1995 stellte er sich der Polizei. Ebenfalls im Herbst 1995 entwichen 11 Häftlinge aus der JVA Lingen, wo sie als Untersuchungs- oder Strafhäftlinge einsaßen. Auch diese Häftlinge konnten nicht bzw. nicht kurzfristig wieder gefaßt werden.

Beide Fälle fanden ein außerordentlich lebhaftes Presseecho. Der Mißerfolg der Fahndungsmaßnahmen wurde anfangs in der Presse besonders dem Datenschutz angelastet. Wegen Datenschutzes sei ein aktuelles Fahndungsfoto von Holst zurückbehalten worden, nach den Ausbrechern aus der Lingener Haftanstalt habe man zunächst ohne Fotos gefahndet.

Im Zusammenhang mit dem Mordfall Kim Kerkow Anfang 1997 wurden Vorwürfe erhoben, die aus Datenschutzgründen erfolgte Vernichtung von Akten des bereits einmal straffällig gewordenen mutmaßlichen Täters habe die Ermittlungen der Polizei verzögert.

Wie sich schließlich gezeigt hat, hatten alle diese Fälle mit Datenschutz nichts zu tun. Derartige vorschnelle Schuldzuweisungen können jedoch einen Vertrauensschaden nach sich ziehen. Für die Bürgerinnen und Bürger führen diese unhaltbaren Unterstellungen zudem zu Verunsicherungen. Meist wird gerade die Polizei alleingelassen, wenn es gilt, möglicherweise unpopuläre Entscheidungen zu treffen. Da ist es sehr bequem, dem Datenschutz den „Schwarzen Peter" zuzuschieben.

Bisher habe ich in keinem einzigen Fall vom Bundeskriminalamt erfahren, daß eine konkrete datenschutzrechtliche Regelung sich aufgrund der gewonnenen Erfahrungen als wirkliches Hindernis für eine effektive Strafverfolgung erwiesen hat. Ich bin jederzeit zu Gesprächen und auch zur Mitverantwortung bereit, wenn es darum gehen sollte, datenschutzrechtliche Schranken für ein Tätigwerden der Strafverfolgungsbehörden bei der Kriminalitätsbekämpfung zu erörtern und – wenn möglich – zu beheben.

1.8 Datenschutzrechtliche Regelungen im Strafverfahren – Silberstreif am Horizont

Seit langem weise ich auf die längst überfällige Lücke des Persönlichkeitsschutzes im Strafverfahren in so wichtigen Bereichen wie der Aktenauskunft, Akteneinsicht und der Öffentlichkeitsfahndung hin. Auch hier geht es nicht nur um Daten von „Gangstern", sondern ebenso um Daten von Verbrechensopfern, Tatzeugen und Unbeteiligten – häufig ermittelt unter Zeugniszwang und unter Eingriff in die Privatsphäre.

Im Dezember 1996 hat die Bundesregierung einen Gesetzentwurf über bereichsspezifische Datenschutznormen im Strafverfahren verabschiedet. In wesentlichen Teilen schafft dieser Entwurf präzise und meinen Forderungen entsprechende Regelun-

gen, z. B. für die Öffentlichkeitsfahndung wie die Ausschreibung zur Aufenthaltsermittlung eines Zeugen. Dieser Entwurf stellt aus meiner Sicht ein tragfähiges Konzept für die erforderliche gesetzliche Regelung der Datenverarbeitung im Strafverfahren dar. Er könnte durchaus als Silberstreif am Horizont gesehen werden, wäre da nicht ein Bundesratsentwurf mit erheblichen, massiven Verschlechterungen. Meines Erachtens wird der Bundesrats-Entwurf den vom Bundesverfassungsgericht im Volkszählungsurteil aufgestellten Maßstäben der Verhältnismäßigkeit und Normenklarheit, an denen sich gesetzesförmige Eingriffe in das Grundrecht auf Datenschutz zu messen haben, nicht gerecht. Er fällt vielmehr hinter den Standard der allgemeinen Datenschutzgesetze zurück. Ich hoffe sehr, daß sich der Gesetzgeber hiervon nicht beeindrucken läßt, sondern die verfassungsrechtlich gebotenen, im Interesse der Rechtssicherheit und Rechtsklarheit notwendigen Rechtsgrundlagen schafft (s. Nr. 6.1.2).

1.9 Sozialdatenschutz: Datenabgleich und kein Ende?

Unser Sozialstaat hat ein umfassendes Netzwerk geknüpft. Insgesamt mehr als 90 Prozent unserer Bevölkerung gehören zu diesem sozialen Sicherungssystem. Gerade im Sozialbereich spielt die datenschutzrechtliche Problematik eine besondere Rolle, was sich auch zu einem großen Teil in den jährlich etwa 3 000 Anfragen oder Eingaben von Bürgern an mein Haus niederschlägt. Einerseits geht es darum, dem Bürger in einer Vielzahl von Bedarfssituationen vom Gesetz vorgesehene Sozialleistungen zukommen zu lassen. Andererseits geht damit eine hohe Datendurchlässigkeit zwischen verschiedenen Systemen einher. Wenn aber einerseits aus sozialstaatlichen Gesichtspunkten ein weitgehender Informationsfluß akzeptiert werden muß, so müssen damit andererseits Informationsrechte des Betroffenen verbunden sein. Auch im Berichtszeitraum bin ich für das aus meiner Sicht unerläßliche Korrektiv der Datentransparenz für den Betroffenen mehrfach eingetreten; so z. B. bei dem am 1. Januar dieses Jahres in Kraft getretenen SGB VII (Unfallversicherungsrecht), bei dem es mein vorrangiges Ziel war, den Versicherten soweit wie möglich in das Verfahren zur Feststellung der Berufskrankheit einzubeziehen und ihm die einzelnen Verfahrensschritte transparent zu gestalten (s. Nr. 23.1).

Die Forderung nach mehr Transparenz ist insbesondere dort von entscheidender Bedeutung, wo automatisierte und pauschalierte Datenübermittlungs- und Datenabgleichsverfahren zum Einsatz kommen. Deren Ziel ist es in aller Regel, einen rechtswidrigen Bezug von Sozialleistungen aufzudecken. Die Zahl derartiger Verfahren ist in jüngster Zeit weiter angestiegen. Forderungen nach weiteren Verfahren werden immer wieder von verschiedenen Seiten gestellt. Soweit das Ziel eines Datenabgleichs im einzelnen Fall auch unterstützenswert ist, so besteht andererseits aber die Gefahr, daß immer mehr pauschalierte Datenübermittlungs- und Datenabgleichsverfahren tatsächlich zum „gläsernen Beitragszahler oder Leistungsbezieher" im Sozialbereich führen. Daher kann die Einführung entsprechender Verfahren nur unter restriktiven Voraussetzungen zulässig sein. Der Deutsche Bundestag hat sich in seiner Entschließung zu meinem 14. TB zur Frage des Datenabgleichs geäußert. Er hat die Bundesregierung aufgefordert, jeweils zu prüfen, ob ein vorgesehenes Datenabgleichsverfahren im Interesse des Gemeinwohls zur Erreichung eines konkreten Zieles erforderlich und verhältnismäßig ist. Er hat hierzu gefordert, daß die Bürger auf Datenabgleiche zur Verhinderung von Leistungsmißbrauch durch Hinweise in Vordrucken und Merkblättern sowie in Veröffentlichungen aufmerksam gemacht werden sollen.

Datenabgleiche, insbesondere in derart massiver Weise, berühren das Persönlichkeitsrecht vieler Menschen und geben Anlaß zur Sorge, lediglich zum Objekt der Datensysteme zu werden. Aus meiner Sicht ist es daher höchste Zeit, die bestehenden Datenabgleichsverfahren in ihrer praktischen Bedeutung und Auswirkung auf den Verhältnismäßigkeits- und Erforderlichkeitsgrundsatz zu überprüfen.

1.10 Rechtstatsachenforschung: Kurz nach dem Start fehlt Beschleunigung

Wie auch Antworten der Bundesregierung auf parlamentarische Anfragen zeigen, ist das vorhandene Wissen über die Wirksamkeit besonders einschneidender strafprozessualer Ermittlungsbefugnisse, wie z. B. der Telefonüberwachung, eher lückenhaft und unzureichend. Vielfach mangelt es daran, daß Landesjustiz und Landesbehörden konkrete Erkenntnisse sammeln und den Bundesbehörden zur Verfügung stellen. Zugleich gilt aber für jede Forderung nach neuen staatlichen Eingriffsbefugnissen, daß diese auf sorgfältigen Tatsachenermittlungen und vertretbaren Einschätzungen beruhen. Nach der Rechtsprechung des Bundesverfassungsgerichtes bedarf es einer gründlichen Bestandsaufnahme und Evaluierung des strafprozessualen und polizeirechtlichen Instrumentariums, um sowohl mit Blick auf die gebotene Effizienz als auch mit Blick auf die Einschränkung von Grundrechten Verdächtiger und erst recht Unbeteiligter das richtige Maß zu finden. Deshalb müssen neue Eingriffsbefugnisse nach ihrer Einführung und Anwendung hinsichtlich ihrer Wirkungen bewertet werden können, um sowohl ein Unter- als auch ein Übermaß zu vermeiden.

1994 hat die Innenministerkonferenz die Einrichtung einer sogenannten Rechtstatsachensammlung beschlossen, die der Erhebung und Verarbeitung polizeilicher Ermittlungsmethoden und Eingriffsbefugnisse dienen soll. Dazu hat das Bundeskriminalamt von der Innenministerkonferenz den Auftrag erhalten, eine sogenannte Bund/Länder-Fallsammlung einzurichten. An der 1995 angelaufenen Informationserhebung haben sich allerdings bis Ende 1996 neben dem Bundeskriminalamt, dem Zollkriminalamt und der Grenzschutzdirektion bislang nur 6 Landeskriminalämter beteiligt. Aufgrund der z. Z. noch geringen Beteiligung der Polizeidienststellen habe ich erhebliche Zweifel, ob gegenwärtig eine hinreichend ausreichende Aufarbeitung von Rechtstatsachen möglich ist.

Ich hoffe daher sehr, daß die beschlossene Rechtstatsachensammlung nicht bereits kurz nach dem Startschuß zum Stehen kommt. Gesetzgeberische Aktivitäten in diesem Bereich kann es nur mit ausreichender Überprüfung der rechtstatsächlichen Auswertungen geben (s. Nr. 11.2).

1.11 Liberalisierung von Telekom und Post – vom Datenschutz begleitet

Telekommunikationsdienste

Mit dem am 1. August 1996 in Kraft getretenen Telekommunikationsgesetz wurde mir die Datenschutzkontrolle für alle Unternehmen übertragen, die für die geschäftsmäßige Erbringung von Telekommunikationsdiensten Daten von natürlichen und juristischen Personen erheben, verarbeiten oder nutzen. Hierdurch wurde meine Zuständigkeit auch auf die privaten Telekommunikationsunternehmen erweitert. Wichtigster Grund für den deutlich zunehmenden Umfang der Beratungs- und Kontrollaufgabe ist der nach wie vor starke Zuwachs an Unternehmen, die Telekommunikationsdienste erbringen. Mit Stand vom 22. Januar 1997 gehörten dazu 1 151 Unternehmen. Ebenso stark ist der Zuwachs bei den Kundenzahlen, insbesondere im Bereich der Mobilfunkdienste (Ende 1995: 3,8 Mio. Teilnehmer, Ende 1996: über 5,8 Mio. Teilnehmer). Für das Jahr 2000 werden ca. 14 Mio. Mobilfunkteilnehmer erwartet. Ab 1. Januar 1998 wird der Telekommunikationssektor in vollem Umfang privatisiert sein. Bis zu diesem Zeitpunkt und auch darüber hinaus wird ein völlig neuer Markt entstehen.

Bereits jetzt ist festzustellen, daß die Netzbetreiber sowie die größeren Serviceprovider und die Mobilfunkunternehmen mein Haus um umfassende Beratung bitten (s. Nr. 10.1).

Postdienstleistungen

Für die Liberalisierung der Postdienstleistungen enthält die sogenannte Postreform III die entscheidende Weichenstellung. Indem die Regulierungsbehörde Lizenzen an geeignete Unternehmen erteilt, erhalten auch andere private Beförderungsunternehmen Zugang zum Markt der Postdienstleistungen. Da die bisherigen öffentlichen Aufgaben der Post von Privaten wahrgenommen werden, ist die besondere Herausforderung für den Datenschutz, das bisherige Schutzniveau (Postgeheimnis) sowohl für Kunden als auch für Postempfänger beizubehalten. Dies ist weitgehend gelungen.

Bei den Überlegungen für den Entwurf eines neuen Postgesetzes habe ich Bedenken besonders insoweit, als eine Verpflichtung der Postdienstunternehmen zur Übermittlung von Vertragsdaten über Postdienstleistungen z. B. an Nachrichtendienste, Polizei- und Ordnungswidrigkeitsbehörden sowie an das Zollkriminalamt vorgesehen ist. Sie enthält auch keine Abstufung danach, ob es sich um Bagatellfälle oder Schwerkriminalität handelt. Grundsätzlich ist meines Erachtens zu klären, ob unter dem Gesichtspunkt der Privatisierung derart weitreichende Eingriffsbefugnisse, die im Widerspruch zu der angestrebten Liberalisierung des Marktes stehen, überhaupt gewünscht sein können (s. Nr. 29).

1.12 Beratungen und Kontrollen, insbesondere Beanstandungen

Ohne die Kenntnis der tatsächlichen Abläufe bei der Erfüllung von Aufgaben fiele mir die Beratung des Deutschen Bundestages und der Bundesregierung sehr viel schwerer. Diese Kenntnis erlange ich überwiegend durch Kontrollen und Informationsbesuche. Deshalb sind die mir gesetzlich zugewiesenen Aufgaben der Beratung und Kontrolle von öffentlichen Stellen des Bundes ausgesprochen wichtig. Im Berichtszeitraum habe ich nicht nur zu zahlreichen Gesetzesvorhaben und datenschutzrechtlichen Fragen Bundesbehörden und sonstige öffentliche Stellen des Bundes beraten, sondern ich habe auch viele Kontrollen und Informationsbesuche durchgeführt. Die von mir kontrollierten Stellen sind in **Anlage 2** aufgeführt.

Nach dem Bundesdatenschutzgesetz muß ich Verstöße gegen datenschutzrechtliche Vorschriften förmlich beanstanden (§ 25 BDSG). Von einer Beanstandung kann ich u. a. absehen, wenn die Verstöße oder Mängel von geringer Bedeutung sind, aber auch wenn ein aus meiner Sicht datenschutzrechtliches Fehlverhalten sofort geändert wird. Hierauf ist zurückzuführen, daß die Zahl der Beanstandungen im Berichtszeitraum deutlich gesunken ist. Zu den Beanstandungen im einzelnen siehe **Anlage 3**.

1.13 Hinweis für die Ausschüsse des Deutschen Bundestages

In der **Anlage 1** habe ich dargestellt, welche Kapitel dieses Berichts für welchen Ausschuß des Deutschen Bundestages von besonderem Interesse sein könnten.

2 Der informationelle Großraum Europa

2.1 Europäische Datenschutzrichtlinie

2.1.1 Eine verbindliche supranationale Datenschutzregelung als Antwort auf die Herausforderungen des informationellen Großraums Europa

Die EG-Datenschutzrichtlinie, über deren Entstehungsgeschichte und wichtigste Etappen auf dem Weg zu ihrer Verabschiedung ich in den zurückliegenden Tätigkeitsberichten (13. TB S. 87 ff., 14. TB S. 159 f., 15. TB Nr. 33.1) berichtet habe, wurde fünf Jahre nach der Vorlage des Entwurfs durch die Europäische Kommission am 24. Oktober 1995 verabschiedet. Die „Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr", so der exakte Wortlaut, war zuvor auf der Grundlage des sogenannten Gemeinsamen Standpunkts vom 20. Februar 1995 (s. 15. TB Nr. 33.1.1) mit einzelnen kleineren Korrekturen im Wortlaut und in den Erwägungsgründen aufgrund von Änderungswünschen aus der

2. Lesung im Europäischen Parlament vom 15. Juni 1995 im Europäischen Ministerrat am 24. Juli desselben Jahres angenommen worden. Mit Ausnahme des Vereinigten Königreichs, das sich der Stimme enthielt, haben alle Mitgliedstaaten der Union für die Richtlinie gestimmt, die damit einstimmig angenommen wurde. Als „veröffentlichungsbedürftiger Rechtsakt" nach Artikel 191 EG-Vertrag wurde die Richtlinie im Amtsblatt der Europäischen Gemeinschaften bekannt gemacht (ABl. Nr. L 281 vom 23. November 1995, S. 31 ff.).

Die Richtlinie bedeutet nach dem Europaratsübereinkommen zum Schutz des Menschens bei der automatischen Verarbeitung personenbezogener Daten aus dem Jahre 1981 (Konvention 108) einen weiteren wichtigen Schritt in Richtung internationaler Verbindlichkeit auf dem Gebiet des Datenschutzes. Mit der Richtlinie findet eine Erweiterung und Vertiefung des Persönlichkeitsschutzes auf europäischer Ebene statt. Für die Mitgliedstaaten der Europäischen Union schafft sie erstmals einen – rechtsverbindlichen – grenzüberschreitenden Rahmen, in dem mit personenbezogenen Daten nach weitgehend einheitlichen Regeln umgegangen werden muß. Unbestreitbar ist der gemeinschaftsrechtliche Zugang zum Datenschutz auch marktwirtschaftlicher Natur. Die Richtlinie stützt sich auf die Regelungskompetenz „Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten zur Erreichung des Binnenmarktes" gem. Artikel 100 a EG-Vertrag. Zugleich ist die Richtlinie ein wichtiger Beitrag zum „Europa der Bürger", das zu den vordringlichen Zielen der Gemeinschaftspolitik zählt. Aus deutscher Sicht – hier ist spätestens seit dem Volkszählungsurteil aus dem Jahre 1983 (BVerfGE 65, S. 1 ff.) an das verfassungsrechtlich abgesicherte und im BDSG und den Landesdatenschutzgesetzen konkretisierte Recht auf informationelle Selbstbestimmung zu denken – liegt es daher nahe, das europarechtliche Gegenstück nunmehr auf der Grundrechtsebene von Gemeinschaft und Union zu suchen. Insofern kommt dem Vertrag über die Europäische Union (Maastricht-Vertrag) eine besondere Bedeutung zu, der, anknüpfend an eine langjährige Rechtsprechung des EuGH, die Union – und damit auch deren Mitgliedstaaten – zur Achtung der Grundrechte verpflichtet (Artikel F Abs. 2). Durch diese doppelte Zuordnung zur marktwirtschaftlich-industriellen Entwicklung und zur rechtlich-kulturellen Entfaltung erhält die Richtlinie ihren ganz besonderen Stellenwert für das Europa an der Schwelle des Informationszeitalters.

2.1.2 Aufbau und wichtigste Merkmale der Richtlinie

Die Richtlinie, deren wesentliche Bestandteile auf den schon vorhandenen europäischen Datenschutzkonzepten beruhen (s. 15. TB Nr. 33.1.2), ist als Querschnittsregelung angelegt, die durch bereichsspezifische Gemeinschaftsvorschriften ergänzt werden kann und soll, wie z. B. durch die ISDN-Richtlinie (s. u. Nr. 10.3).

Sie zielt nicht auf einen gleichförmigen europäischen Einheitsdatenschutz, sondern auf harmonisierte nationale Datenschutzsysteme. Sie fordert von den Mitgliedstaaten ein Tätigwerden, überläßt ihnen aber in der konkreten Ausgestaltung die Wahl zwischen mehreren Möglichkeiten, wie z. B.

- zwischen verschiedenen Verfahrensweisen beim Widerspruchsrecht gegen Datennutzung für Marketingzwecke (Artikel 14),
- zwischen Dateienregistrierung bei der Kontrollstelle und einer internen Umsetzung durch betriebliche und behördliche Datenschutzbeauftragte (Artikel 18) und
- zwischen einem administrativen Typ der Kontrollstelle nach dem Modell der Aufsichtsbehörden und einem mehr politischen, auf die parlamentarische Verwaltungskontrolle bezogenen Modell nach dem Vorbild des Bundesbeauftragten für den Datenschutz (Artikel 28).

Dieses Konzept der Offenheit zeigt sich besonders an Artikel 5, der es den Mitgliedstaaten überläßt, die näheren Voraussetzungen zu bestimmen, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist. Die Erwägungsgründe stellen dazu fest, daß den Mitgliedstaaten ein Spielraum zusteht, in dem sie die Bedingungen rechtmäßiger Verarbeitung festlegen können, wobei eine Verbesserung des Schutzes anzustreben ist (Erwägungsgrund 9).

Für eine gewisse Offenheit sorgen auch die zahlreichen in der Richtlinie enthaltenen Generalklauseln. Mit ihnen entspricht die Richtlinie dem in Artikel 3 b des EG-Vertrages niedergelegten Subsidiaritätsprinzip und erlaubt den Mitgliedstaaten in einem gewissen Rahmen, bewährte nationale datenschutzrechtliche Regelungen beizubehalten und neue Lösungen zu finden, die ihren jeweiligen Rechtstraditionen entsprechen.

Die Richtlinie, die den Schutz der Grundrechte und Grundfreiheiten, insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten garantieren soll, will dies dadurch erreichen, daß von den Mitgliedstaaten verlangt wird,

- Regelungen zu den Voraussetzungen einer Datenverarbeitung und zur Zweckbestimmung zu treffen,
- Informations-, Auskunfts-, Berichtigungs-, Widerspruchs- und Löschungsrechte zugunsten der Betroffenen zu verankern,
- die Sicherheit der Datenverarbeitung zu garantieren,
- Pflichten zur Meldung und zur Kontrolle festzulegen,
- Haftungs- und Schadensersatzfragen zu lösen,
- unabhängige Datenschutzkontrollinstanzen einzurichten und
- den Datenverkehr mit Drittländern einheitlich zu handhaben.

Auch wenn in einigen Punkten Kompromisse nötig waren, kann als Ergebnis festgehalten werden, daß das gemeinsame Ziel der Harmonisierung des europäischen Datenschutzes auf hohem Niveau erreicht wurde (s. schon 15. TB Nr. 33.1.3).

Die in den Bestimmungen der Richtlinie getroffenen Kernaussagen wurden im 15. Tätigkeitsbericht (Nr. 33.1.4) dargestellt. Da sich nach der Verabschiedung des Gemeinsamen Standpunkts vom 20. Februar 1995 keine wesentlichen Änderungen ergeben haben, kann darauf verwiesen werden (zur Frage der Übermittlung in Drittländer s. u. Nr. 2.1.4).

2.1.3 Die Datenschutzgruppe nach Artikel 29

Für die laufende Zusammenarbeit der Kontrollstellen im Hinblick auf die Koordinierung der Kontrollpraxis und die Weiterentwicklung des Datenschutzes auf Gemeinschaftsebene sieht die Richtlinie eine „Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten" vor, welche die Richtlinie kurz als „Gruppe" bezeichnet (Artikel 29 Abs. 1). Die Gruppe berät die Kommission und trägt zur einheitlichen Anwendung der zur Umsetzung der Richtlinie erlassenen einzelstaatlichen Vorschriften bei. Bei der Wahrnehmung ihrer Aufgaben ist sie nach Erwägungsgrund 65 völlig unabhängig.

Die Gruppe hat sich am 17. Januar 1996 erstmals getroffen und sich in ihrer dritten Sitzung im September 1996 eine vorläufige Geschäftsordnung gegeben. In diesem Gremium sind alle Mitgliedstaaten mit unabhängigen Datenschutzkontrollbehörden vertreten, Beobachterstatus haben Norwegen und Island. Der föderalen Struktur der deutschen Datenschutzkontrolle wird dadurch Rechnung getragen, daß an den Sitzungen auch je ein Vertreter der Landesbeauftragten und der obersten Aufsichtsbehörden der Länder teilnimmt. Der Gruppe gehört auch ein Vertreter der Kommission sowie ein Vertreter der Stelle bzw. der Stellen an, die die Datenschutzkontrolle bei den Institutionen und Organen der Gemeinschaft wahrnehmen. Allerdings sind diese bisher nicht eingerichtet (zur defizitären Lage des Datenschutzes auf Gemeinschafts- und Unionsebene s. u. Nr. 2.2).

Die Arbeitsgruppe leistet Hilfestellung bei der Umsetzung der Richtlinie in innerstaatliches Recht der Mitgliedstaaten und schaltet sich bei Zweifelsfragen der Interpretation der Richtlinie ein. In den vier Sitzungen des Jahres 1996 wurden hierzu Arbeitsdokumente u. a. zur Behandlung der Medien und zur Regelung der Meldepflicht beraten. Von deutscher Seite wurde unter dem Titel „Der Datenschutzbeauftragte in Behörden und privaten Unternehmen (DSB)" das deutsche Modell der internen Datenschutzkontrolle erläutert und als von der Richtlinie zugelassene Alternative zu umfassenden Meldepflichten empfohlen. Die Kommission hat der Gruppe alle europäischen Regelungsprojekte mit Datenschutzbezug zur Stellungnahme vorzulegen. Zu den Aufgaben der Gruppe wird es auch gehören, in Zweifelsfällen das Datenschutzniveau in Staaten außerhalb der Gemeinschaft, in die personenbezogene Angaben übermittelt werden sollen, auf seine Angemessenheit im Vergleich mit dem nach der Richtlinie verbindlichen gemeinschaftsweiten Standard zu überprüfen. Hierzu läuft gegenwärtig eine methodische Studie (vgl. im folgenden).

2.1.4 Übermittlungen personenbezogener Daten in Drittländer

Einen der wichtigsten Teile der Richtlinie bildet das Kapitel IV mit seinen Bestimmungen über Datentransfers in Drittstaaten, also in einen der etwa 150 Staaten außerhalb der Europäischen Union. Während künftig innergemeinschaftliche Datenübermittlungen über die Grenzen des jeweiligen Mitgliedstaates hinweg den inländischen gleichzustellen sind, soll nach den Artikeln 25 und 26 bei Datenübermittlungen aus dem Gebiet der Gemeinschaft eine Harmonisierung erreicht werden. Danach muß das personenbezogene Daten empfangende Drittland mindestens ein „angemessenes Schutzniveau" gewährleisten. Ist dies nicht der Fall, so ist die Übermittlung personenbezogener Daten in dieses Land grundsätzlich unzulässig (Artikel 25 Abs. 1, Erwägungsgrund 57). Die Angemessenheit des Schutzniveaus, das ein Drittland bietet, ist unter Berücksichtigung aller Umstände im Hinblick auf eine Übermittlung oder eine Kategorie von Übermittlungen zu beurteilen (Artikel 25 Abs. 2). In bestimmten Fällen können die Mitgliedstaaten eine Übermittlung unabhängig vom Schutzniveau im Empfängerstaat zulassen, so z. B. bei Einwilligung der betroffenen Person, im Rahmen der Erfüllung eines Vertrages, zur Wahrung wichtiger öffentlicher Interessen oder im Rahmen eines Gerichtsverfahrens. Auch kann die Übermittlung zugelassen werden, wenn besondere Maßnahmen – die sich insbesondere aus entsprechenden Vertragsklauseln ergeben können – getroffen werden, die das unzureichende Schutzniveau in dem Drittstaat für den betreffenden Vorgang ausgleichen (zum Inhalt der Artikel 25 und 26 s. im einzelnen 15. TB Nr. 33.1.4.9).

In den Beratungen der Gruppe nach Artikel 29 stand bisher das Thema der Angemessenheit des Schutzniveaus in Drittstaaten im Vordergrund und insbesondere der Versuch, einen Kriterienkatalog zu ihrer Beurteilung zu erarbeiten. Die Europäische Kommission hat dazu einem belgischen Universitätsinstitut den Auftrag zur Erstellung einer „Methodologie" erteilt. Bereits beraten wurde eine Untersuchung zweier amerikanischer Professoren zur Beurteilung des Datenschutzniveaus in den Vereinigten Staaten (Paul Schwartz und Joel Reidenberg, Data Privacy Law – A Study of United States Data Protection, Charlottesville/Virginia, 1996). Die Thematik wird die Arbeit der Gruppe noch geraume Zeit bestimmen.

2.1.5 Umsetzung der Richtlinie – Novellierung der Datenschutzgesetze – Modernisierung des Datenschutzrechts

Die Richtlinie verpflichtet die Mitgliedstaaten, ihr Datenschutzrecht binnen dreier Jahre zu harmonisieren (Artikel 32 Abs. 1). Ausgehend von ihrer Unterzeichnung durch die Präsidenten von Europäischem Parlament und Ministerrat am 24. Oktober 1995 muß die Richtlinie damit spätestens zum 24. Oktober 1998 in nationales Recht umgesetzt sein.

Bei der Umsetzung der Richtlinie in das deutsche Recht ist der Bundesgesetzgeber nicht nur für den öffentlichen Bereich des Bundes zuständig, sondern aufgrund seiner Gesetzgebungsbefugnis nach Arti-

kel 74 GG auch für den nicht-öffentlichen Bereich, wo die meisten Änderungen zu erwarten sind. Die Federführung für die Umsetzung liegt für die Bundesregierung beim Bundesministerium des Innern. Da nicht nur das Bundesrecht, sondern – vorzugsweise im öffentlichen Bereich – auch die Landesdatenschutzgesetze mit den Vorgaben der Richtlinie in Einklang zu bringen sind, haben auch die Länder ihre jeweilige Datenschutzgesetzgebung anzupassen. Über die allgemeinen Datenschutzgesetze hinaus ist eine Vielzahl bereichsspezifischer datenschutzrechtlicher Regelungen des Bundes und der Länder zu überprüfen. Bedenkt man, daß die letzte Reform des BDSG (1990) mehr als vier Jahre dauerte, dann zeigt sich die Eilbedürftigkeit der Angelegenheit.

Zur Konzeption der Umsetzung hat die 51. Konferenz der Datenschutzbeauftragten des Bundes und der Länder im März 1996 mit einer Entschließung unter dem Titel „Modernisierung und europäische Harmonisierung des Datenschutzrechts" Posititon bezogen **(s. Anlage 15)**. Die Datenschutzbeauftragten appellieren an den Gesetzgeber in Bund und Ländern, die Umsetzung der Richtlinie nicht nur als Beitrag zur europäischen Integration zu verstehen, sondern auch als Aufforderung und Chance, den Datenschutz fortzuentwickeln. Angesichts der sich rapide verändernden Welt der Datenverarbeitung, der Medien und der Telekommunikation sprechen sie sich für eine Modernisierung des deutschen Datenschutzrechts aus, damit der einzelne auch künftig über den Umlauf und die Verwendung seiner persönlichen Daten soweit wie möglich selbst bestimmen kann.

Im Juni 1996 habe ich der Bundesregierung ein auf dieser Linie liegendes detailliertes Positionspapier zur Umsetzung der europäischen Datenschutzrichtlinie und zur Novellierung des Bundesdatenschutzgesetzes übermittelt.

Den Datenschutzbeauftragten geht es dabei um mehr als durch Gemeinschaftsrecht erzwungene Minimalkorrekturen. Mit meinen Kollegen aus den Ländern bin ich der Auffassung, daß das Gebot der Anpassung der deutschen Rechtslage an die EG-Richtlinie als Chance wahrgenommen werden muß, das Datenschutzrecht in Deutschland von überholten Konzepten zu befreien und den Regelungserfordernissen einer von Multimedia (s.u. Nr. 8.1), Internet (s.u. Nr. 8.2) und Chipkarten (s.u. Nr. 9) geprägten Zukunft gerecht zu werden. Nur in diesem Dreiklang

- Umsetzung der europäischen Datenschutzrichtlinie
- Novellierung des Bundesdatenschutzgesetzes, der Landesdatenschutzgesetze und Anpassung bzw. Schaffung bereichsspezifischer Regelungen
- Modernisierung des Datenschutzrechts

kann das Datenschutzrecht auch am Ende dieses Jahrtausends seine Rolle für das informationelle Selbstbestimmungsrecht des einzelnen erfüllen.

Demgegenüber vertrat die Bundesregierung bei den Beratungen meines 15. Tätigkeitsberichts im Deutschen Bundestag die Auffassung, daß die Richtlinie eine weitergehende „Modernisierung" des gesamten Datenschutzrechts nicht fordere. Die Umsetzung der Richtlinie zum Anlaß für eine Anpassung des geltenden Rechts an die veränderten rechtlichen, technischen und sozialen Entwicklungen zu nehmen, gehe daher über den Regelungsrahmen der Richtlinie hinaus. Zwar sei mein Anliegen angesichts der datenschutzrechtlichen Probleme, die die Fortentwicklung der sog. Informationsgesellschaft mit sich bringt, durchaus berechtigt. Meine Forderungen könnten jedoch nicht im Zusammenhang mit der Umsetzung der Richtlinie, die sich ausschließlich auf die Novellierung des allgemeinen Datenschutzrechts (BDSG und Landesdatenschutzgesetze) beziehe, erhoben werden. Neue Entwicklungen, die unter dem Stichwort „Multimedia" bereits zu bereichsspezifischen gesetzgeberischen Maßnahmen der Bundesregierung geführt hätten (Informations- und Kommunikationsdienstegesetz, IuKD-Gesetz), würden vom Geltungsbereich der Richtlinie nicht umfaßt, da diese ähnlich dem BDSG als Querschnittsmaterie konzipiert sei, der bereichsspezifische Richtlinien folgen sollen.

Auch mir ist bewußt, daß das primäre Regelungsziel der Richtlinie zunächst in der Schaffung allgemeiner Datenschutzgesetze in den Mitgliedstaaten der Union liegt, um das unterschiedliche Datenschutzniveau in Europa im Wege der Harmonisierung zu überwinden. Ich vermag aber keine überzeugenden Gründe dafür zu erkennen, die Novellierung des BDSG auf die unumgänglichen Anpassungen an die europäischen Vorgaben zu reduzieren. Sicher würde dies die Gesetzgebung kurzfristig entlasten und den in den Jahren 1998 bis 2001 zu leistenden Umstellungsaufwand (Artikel 32) begrenzen. Aber der Praxis wäre ein Bärendienst geleistet, wenn einer gerade abgeschlossenen Europäisierung die dann noch dringendere Modernisierung mit der Notwendigkeit einer erneuten Umstellung auf dem Fuße folgte.

Die Regelungen des geplanten IuKD-Gesetzes für den Bereich „Multimedia" decken zwar einen wichtigen Teilaspekt der geforderten rechtlichen Antworten auf die ungeheuren Möglichkeiten der Informations- und Kommunikationstechnik, aber eben nur einen Teilaspekt ab. Zugleich bedarf es umfassender Regelungskonzepte – und zwar entsprechend dem Subsidiaritätsprinzip und zur Förderung der praktischen Einführung neuer IuK-Anwendungen nicht erst aufgrund abzuwartender bereichsspezifischer Vorgaben aus Brüssel – wie etwa im Bereich der Chipkarten. In meinem der Bundesregierung im Juni 1996 übermittelten Positionspapier habe ich hierzu einen Katalog erstellt, der die folgenden Forderungen beinhaltet:

- Festlegung, daß auf der Chipkarte selbst ergänzend zum allgemeinen Erforderlichkeitsprinzip eine Beschränkung der personenbezogenen Daten auf den unbedingt erforderlichen Umfang erfolgt,
- betroffenenfreundliche Regelung der Rechtewahrnehmung (entspr. §§ 6 Abs. 2, 7 Abs. 4 BDSG),
- Verpflichtung des Kartenherausgebers oder Systembetreibers, durch technisch-organisatorische Maßnahmen zu gewährleisten, daß die Kartendaten nur entsprechend ihrer (jeweiligen) Zweckbin-

dung verarbeitet werden können (Multifunktionskarte),

- Einbeziehung des infrastrukturellen Umfelds in die technisch-organisatorischen Maßnahmen,
- gesetzliche oder (gesetzlich vorstrukturierte) vertragliche Verteilung der Verantwortung zwischen den am Verarbeitungsprozeß Beteiligten,
- Pflicht des Herausgebers bzw. Betreibers, dem Betroffenen die Möglichkeit zur kostenlosen, vertrauenswürdigen und ohne großen Aufwand realisierbaren Selbstinformation zu gewährleisten, wozu in bestimmten Fällen auch die Information gehört, wer wann auf welche Daten zugegriffen hat (z. B. realisierbar durch ein auf der Karte gespeichertes Logbuch),
- Transparentmachung des Verfahrens für den Betroffenen (unabhängig von der Möglichkeit zur umfassenden Selbstinformation).

Der Referentenentwurf der Bundesregierung (Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes) ist mir inzwischen am 20. Februar 1997 zugegangen.

2.2 Datenschutz bei den Organen und Einrichtungen von Europäischer Gemeinschaft und Union

Mit der Verabschiedung der EG-Datenschutzrichtlinie (s. o. Nr. 2.1.1) hat sich an der marginalen Rolle, die der Datenschutz bei den Organen und Einrichtungen von Europäischer Gemeinschaft und Union seit jeher spielt, nichts geändert. Da die Richtlinie allein für den europäischen Binnenmarkt konzipiert ist – ausgeschlossen hat sie ihren Anwendungsbereich nach Artikel 3 Abs. 2 etwa für die Bereiche der Gemeinsamen Außen- und Sicherheitspolitik und die Zusammenarbeit in den Bereichen Justiz und Inneres des Vertrages über die Europäische Union – und da sie nach Artikel 34 ausschließlich an die Mitgliedstaaten gerichtet ist, erstreckt sich ihr Geltungsanspruch nicht auf die Organe und Einrichtungen von Gemeinschaft und Union. Abgesehen von einzelnen sektoriellen Bestimmungen fehlt es für diese aber nach wie vor an den notwendigen datenschutzrechtlichen Regelungen, was bereits schwerwiegende Störungen beim Informationsaustausch zur Folge hatte (vgl. 12. TB S. 49, 13. TB S. 57 f., 15. TB Nr. 33.6).

Mit diesem unhaltbaren Zustand haben sich die Datenschutzbeauftragten der Mitgliedstaaten der Europäischen Union anläßlich der 17. Internationalen Konferenz am 8. September 1995 in Kopenhagen eingehend befaßt (s. u. Nr. 32.2.1). Mit Blick auf die 1996 begonnene Regierungskonferenz zur Überprüfung des Vertrages über die Europäische Union („Maastricht II") haben die europäischen Datenschutzbeauftragten eine von mir vorgelegte Erklärung verabschiedet, die als „Kopenhagener Resolution" **(s. Anlage 4)** die nachfolgend wiedergegebenen Forderungen enthält:

- Verankerung eines europäischen Grundrechts auf Datenschutz im Grundrechtskatalog einer geschriebenen EU-Verfassung
- Schaffung eines verbindlichen Datenschutzrechts für die Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen von Gemeinschaft und Union
- Einrichtung eines unabhängigen europäischen Datenschutzbeauftragten.

Im gleichem Sinne hat sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung vom 9./10. November 1995 zur „Weiterentwicklung des Datenschutzes in der Europäischen Union" **(s. Anlage 12)** ausgesprochen.

Der Beschluß von Kopenhagen wurde im Vorfeld der Regierungskonferenz zur Überprüfung des Vertrages über die Europäische Union den deutschen Mitgliedern der sog. Reflexionsgruppe zugeleitet. Der Vorsitzende der Reflexionsgruppe wurde durch den dänischen Konferenzvorsitzenden über die Forderungen der Kopenhagener Resolution unterrichtet. Ich habe den Chef des Bundeskanzleramtes, den Bundesminister des Auswärtigen, den Bundesminister des Innern, die Bundesministerin der Justiz und den Bundesminister für Wirtschaft hierüber informiert.

Leider habe ich, wie auch meine europäischen Kollegen, hierauf bisher lediglich abwartende Antworten erhalten.

Auch die Reaktionen aus Brüssel zu diesen seit langem bekannten Forderungen – diejenigen nach Schaffung verbindlicher Verarbeitungsgrundlagen und einer unabhängigen Kontrollinstanz stammen bereits aus der Zusatzerklärung der Datenschutzbeauftragten der EG-Länder zur Berliner Resolution der Internationalen Konferenz der Datenschutzbeauftragten vom 30. August 1989 – können nur als zögerlich und hinhaltend bezeichnet werden. Zwar haben sich Rat und Kommission aus Anlaß der Annahme des Gemeinsamen Standpunktes im Hinblick auf die Richtlinie verpflichtet, deren Schutzprinzipien auf sich anzuwenden (Ratsdok. 4730/95 ECO 20 vom 8. Februar 1995). Danach sollen im Hinblick auf eine zusammenhängende und einheitliche Anwendung der Schutzregeln in der Union für die Datenverarbeitungen, die von Institutionen und Organen der EU durchgeführt werden, dieselben Schutzprinzipien gelten wie für die von der Richtlinie erfaßten Verarbeitungen.

Europäische Kommission und Rat müssen sich jedoch darüber im klaren sein, daß interne Organisationsregelungen von der rechtlichen Qualität her nicht ausreichend sind. Die gemeinsame Erklärung von Rat und Kommission, in der die beiden Gemeinschaftsorgane die „Ansicht" vertreten, daß ihre Datenverarbeitungen und die der anderen Institutionen und Gremien der Union den gleichen wie den in der Richtlinie enthaltenen Schutzprinzipien unterliegen „sollten", führt nur die mangelnde Bindungswirkung der Richtlinie im Hinblick auf die Organe und Einrichtungen von Gemeinschaft und Union vor Augen. Die gewählten Formulierungen verdeutlichen, daß – angesichts des Umstandes, daß die Richtlinie sich nach Artikel 34 ausschließlich an die Mitgliedstaaten richtet – eine rechtliche Verpflichtung nicht einzulösen ist.

Unabdingbar sind daher die institutionelle Absicherung einer unabhängigen europäischen Datenschutzkontrollinstanz in den Verträgen über die Europäische Union sowie europarechtliche Rechtsgrundlagen für die Verarbeitung und insbesondere die Weitergabe personenbezogener Daten an und durch Dienststellen von Gemeinschaft und Union – und zwar unabhängig von einem Selbstbindungswillen der Gemeinschafts- und Unionsorgane. Solange die europäischen Gremien nicht über einen Datenschutzstandard verfügen, der dem in den Mitgliedstaaten gleichwertig ist, ist aus Sicht des Datenschutzes gegenüber der Einführung neuer Datenübermittlungen von den Mitgliedstaaten an Organe und Einrichtungen der Gemeinschaft besondere Zurückhaltung geboten. Aber auch lang praktizierte Formen des Datenaustausches werden spätestens dann überprüft werden müssen, wenn – mit dem Ablauf der Umsetzungsfrist für die Richtlinie – der gemeinschaftliche Datenschutz verbindlich wird. Der Datenschutz für die Organe und Einrichtungen der Gemeinschaft ist daher mit gleicher Dringlichkeit wie der in den Mitgliedstaaten voranzutreiben.

Zur sonstigen Entwicklung des Datenschutzes in und außerhalb Europas siehe unten Nr. 32.

3 Datenschutz beim Bundespräsidialamt – Ehrung von Alters- und Ehejubilaren –

Zu den hergebrachten Aufgaben des Bundespräsidenten gehört es, älteren Mitbürgern zu hohen Geburtstagen und anläßlich besonderer Hochzeitstage zu gratulieren.

Die für die Gratulation notwendigen Daten der Jubilare erhält der Bundespräsident von den Ländern. Das dabei zu beachtende Verfahren ist in den sog. Grundsätzen über die Ehrung von Alters- und Ehejubilaren durch den Bundespräsidenten geregelt. Neben Namen, Anschrift und Art des Jubiläums wird auch – „soweit bekannt" – eine im Glückwunschschreiben zu berücksichtigende Information über den Gesundheitszustand des Jubilars erbeten. Zusätzlich soll angegeben werden, ob eine bestimmte Einkommensgrenze „offenkundig" überschritten wird, was das im Regelfall vorgesehene Geldgeschenk unangebracht erscheinen läßt.

In bezug auf die erbetenen Angaben über Gesundheitszustand und Vermögenssituation der Jubilare bin ich aus dem Kreis der Landesbeauftragten für den Datenschutz darauf aufmerksam gemacht worden, daß trotz der vorgenannten Einschränkungen aufgrund mißverständlicher Formulierungen in den Grundsätzen der Eindruck entstehen könnte, das Bundespräsidialamt fordere in diesen sehr sensiblen Lebensbereichen umfangreiche Datenerhebungen. Gleichzeitig wurde geltend gemacht, hierfür und für die Datenübermittlungen an das Bundespräsidialamt bedürfe es einer bereichsspezifischen gesetzlichen Grundlage. Wegen der Gefahr, daß die Grundsätze in den Ländern falsch ausgelegt und dementsprechend doch Datenermittlungen durchgeführt werden könnten, habe ich die Bedenken meiner Kollegen in den Ländern aufgegriffen und die Angelegenheit mit dem Bundespräsidialamt besprochen.

Das Bundespräsidialamt hat zu der Frage, warum es für die Gratulation Informationen über die Einkommensverhältnisse des Jubilars benötige, auf haushaltsrechtlich zwingende Gründe verwiesen. Zu den gewünschten Angaben über den Gesundheitszustand legte es dar, in der Vergangenheit hätten sich immer wieder Angehörige von Jubilaren über den Text des Glückwunschschreibens beschwert, wenn die Wünsche für die Gesundheit des Jubilars nicht dem tatsächlichen Gesundheitszustand entsprochen hätten.

Trotz dieses vertretbaren Informationsbedürfnisses war seitens des Bundespräsidialamtes nie eine gesonderte Datenerhebung hierzu in den Heimatgemeinden der Jubilare verlangt worden. Das Bundespräsidialamt hat mir bestätigt, daß weder Ermittlungen zum Einkommen durchgeführt noch medizinische Befunde erhoben werden sollen. Nur wenn die vorgegebene Einkommensgrenze „offenkundig" überschritten werde, sei dies dem Bundespräsidialamt mitzuteilen; bei der Beantwortung dieser Frage solle großzügig verfahren werden. Die Angaben über den Gesundheitszustand sollten allgemeiner Art sein und nur mitgeteilt werden, soweit sie „bekannt" sind.

Auf meine Empfehlung hin hat das Bundespräsidialamt dies in einem Schreiben an die Staats- und Senatskanzleien der Länder klargestellt. Mögliche Mißverständnisse über den Regelungsinhalt der Grundsätze dürften damit ausgeräumt worden sein. Ebenso sehe ich bei dieser Sachlage nicht die Notwendigkeit einer bereichsspezifischen gesetzlichen Regelung.

4 Auswärtiger Dienst

4.1 Weltweiter Einsatz automatisierter Verfahren

In den letzten Jahren hat das Auswärtige Amt (AA) zunehmend automatisierte Verfahren in seinen Auslandsvertetungen eingesetzt, um die Arbeitsabläufe rationeller zu gestalten. Die Mitarbeiter des AA sollen in allen Auslandsvertretungen die gleichen ihnen bekannten Systeme und Programme vorfinden, damit zeitaufwendige und teure Fortbildungsmaßnahmen eingespart werden können.

Mit dem Einsatz von Informationstechnik kommen auf die Auslandsvertretungen jedoch neue Anforderungen zu, wie z. B. die Gewährleistung der Sicherheit von vernetzten oder Einzelplatz-Personalcomputern, die Sicherung personenbezogener Daten auf Disketten, Festplatten und Netzservern, die Abwehr von Computerviren oder die Umsetzung des erhöhten Schutzbedarfs in besonders sensiblen Arbeitsbereichen wie etwa bei den Militärattachés. Der ganz überwiegende Teil der von mir anläßlich meiner Beratungen und Kontrollen in den Auslandsvertretungen festgestellten Probleme konnte mit dem AA konstruktiv gelöst werden.

In einer mir wichtigen Frage hat sich das AA aber bislang nicht meiner Auffassung anschließen kön-

nen. Es handelt sich dabei um den Zugangsschutz für Arbeitsplatzcomputer im Einzelplatzbetrieb. Diese verfügen regelmäßig nur über ein sogenanntes BIOS-Paßwort, dessen Geheimhaltung nicht immer sichergestellt werden kann, wie z. B. bei Vertretung des Benutzers während Urlaub oder Krankheit. Dieser Zugangsschutz entspricht nicht den üblichen datenschutzrechtlichen Anforderungen, zumal das Paßwort-Änderungsverfahren sehr zeit- und arbeitsaufwendig ist und deshalb häufig unterbleibt. Hinzu kommt, daß keine differenzierten Rechte- und Zugriffsregelungen – insbesondere für Diskettenlaufwerke und die Betriebssystemebene – möglich sind. Die Kenntnis eines Paßwortes ermöglicht dem Benutzer daher zwangsläufig den Zugang zu allen auf der Festplatte gespeicherten Daten. Auch das Einspielen oder Kopieren von Programmen oder Daten über das Diskettenlaufwerk kann nicht verhindert werden. Zwar hat das AA auf seinen Arbeitsplatzcomputern eine Benutzeroberfläche installiert, die einige Funktionalitäten einer Sicherheitssoftware aufweist. Damit können die vorgenannten Probleme jedoch nur ansatzweise bewältigt werden. Vor diesem Hintergrund habe ich wiederholt den Einsatz einer Sicherheitssoftware – zumindest für Bereiche mit besonders sensibler Datenverarbeitung – angeregt. Das AA hat diese Empfehlung zu meinem Bedauern bislang nicht aufgegriffen.

Im Rahmen meiner Beratungen und Kontrollen habe ich mir regelmäßig auch den Betrieb spezieller automatisierter Verfahren vorführen lassen. Beispielhaft möchte ich hier nennen:

- die in fast allen Arbeitseinheiten der Auslandsvertretungen eingesetzten Kontaktpflegedateien,
- das in den Zahlstellen genutzte Zahlungs- und Anordnungsprogramm,
- das in den Visaabteilungen vorgehaltene „elektronische Fahndungsbuch" sowie
- das Message-Handling System Auslands-Vertretungen (MHSAV).

Beim MHSAV handelt es sich um ein vom AA entwickeltes Kommunikationssystem zwischen den Auslandsvertretungen und der Zentrale in Bonn. Dieses System ist an ein kryptographisches Verfahren gekoppelt, so daß die Kommunikation datenschutzgerecht nur in verschlüsselter Form erfolgen kann. Es hat sich gezeigt, daß die Mitarbeiter des AA verantwortungsbewußt und damit in der Regel auch datenschutzgerecht mit den neuen technischen Möglichkeiten umgehen, die ihnen durch die vorgenannten Programme eröffnet werden.

4.2 Visaverfahren

4.2.1 Bonität des Gastgebers

In den beiden letzten Jahren war ich wiederholt mit einem besonderen datenschutzrechtlichen Aspekt der Visaerteilung durch deutsche Auslandsvertretungen befaßt. Es handelte sich um Fälle, in denen dem Antrag auf Erteilung eines Besuchervisums für die Bundesrepublik Deutschland eine entsprechende Einladung eines in Deutschland lebenden Gastgebers zugrundelag.

Die für die Visaerteilung zuständigen deutschen Auslandsvertretungen haben jeweils im Einzelfall zu prüfen, ob die für die Erteilung eines beantragten Visums erforderlichen Voraussetzungen vorliegen und kein Versagungsgrund entgegensteht. Eine Aufenthaltsgenehmigung wird u. a. dann versagt, wenn der Ausländer seinen Lebensunterhalt während seines Aufenthaltes in der Bundesrepublik Deutschland nicht aus eigenen Mitteln bestreiten kann. Diesem Versagungsgrund kann in Fällen einer Einladung dadurch begegnet werden, daß der Gastgeber eine sog. Verpflichtungserklärung nach § 84 Ausländergesetz (AuslG) abgibt. Darin verpflichtet er sich der Ausländerbehörde in Deutschland oder der deutschen Auslandsvertretung gegenüber, die Kosten für den Lebensunterhalt des Eingeladenen während des Besuchsaufenthaltes zu tragen.

In den mir bekanntgewordenen Fällen haben sich die Auslandsvertretungen für die Bearbeitung von Visaanträgen diverse Unterlagen wie Reisepaß, Heiratsurkunde, Einkommensnachweis, Kontoauszug, Krankenversicherungsnachweis u. ä. vorlegen lassen. In einem Fall sollte der Gastgeber der Auslandsvertretung die geforderten Unterlagen sogar über den Antragsteller des Visums vorlegen. Auf diese Weise erhält der Eingeladene ohne sachlichen Grund Einblick in persönliche Verhältnisse des Gastgebers, die ihm möglicherweise sonst nicht bekannt sind oder bekannt würden. Sicherlich kann es im Einzelfall erforderlich sein, die Bonität eines Gastgebers bzw. dessen Identität zu überprüfen und die hierzu notwendigen Nachweise zu verlangen. Dies kann aber nur dann zulässig sein, wenn die Auslandsvertretung begründete Zweifel hieran hat.

Das AA teilt zwar grundsätzlich meine Auffassung. Es verweist jedoch darauf, daß bislang ein einheitlicher Maßstab für die Prüfung von Verpflichtungserklärungen fehlt, so daß allein eine vom Gastgeber gegenüber der Ausländerbehörde in Deutschland abgegebene Verpflichtungserklärung die Auslandsvertretung nicht von ihrer Prüfungspflicht entbinde. Wegen der unterschiedlichen Praxis bei den einzelnen Ausländerbehörden könnten sich die Auslandsvertretungen nicht ausreichend auf die dort gemachten Angaben des Einladenden verlassen. Wünschenswert wäre, wenn die Ausländerbehörden in Deutschland im Fall einer Verpflichtungserklärung grundsätzlich selbst die Bonität und – falls erforderlich – auch die Identität des Gastgebers zu prüfen hätten. Dann wäre eine entsprechende Prüftätigkeit der Auslandsvertretungen regelmäßig entbehrlich; deren Datenerhebungen könnten insoweit unterbleiben. Einen entsprechenden Vorschlag hat das AA dem BMI unterbreitet. Es bleibt abzuwarten, ob diese Anregung aufgegriffen wird.

Das BMI erarbeitet derzeit Verwaltungsvorschriften zu § 84 AuslG. Darin sollen jedenfalls im einzelnen die konkreten Anforderungen der Bonitätsprüfung festgelegt werden. Auch die Frage, welche Belege von dem Einladenden vorzulegen sind, soll dort geregelt werden, damit ein verbindlicher und einheit-

licher Maßstab bei den Ausländerbehörden sichergestellt werden kann. Ein einheitliches Formular für die Abgabe von Verpflichtungserklärungen liegt bereits vor. Dieses wird sowohl von den Ausländerbehörden als auch von den Auslandsvertretungen benutzt.

4.2.2 Unzulässige Spontanübermittlungen

Durch eine Eingabe bin ich darauf aufmerksam gemacht worden, daß eine deutsche Auslandsvertretung personenbezogene Daten von Visumantragstellern an das Bundesamt für die Anerkennung ausländischer Flüchtlinge (BAFl) in Nürnberg übermittelt hat, ohne von diesem dazu ersucht worden zu sein.

Die Auslandsvertretung hätte die ihr vorliegenden Informationen über die Visumantragsteller nach § 8 Abs. 1 Asylverfahrensgesetz (AsylVfG) aber nur auf Ersuchen an das BAFl übermitteln dürfen.

Nach der gesetzlichen Vorgabe hat das BAFl nach Stellung eines Asylantrages zu prüfen, ob es mit dem Auswärtigen Amt oder der jeweils zuständigen Auslandsvertretung Kontakt aufnehmen soll, um die Umstände der Beantragung und Erteilung eines Visums aufzuklären. Ich schließe nicht aus, daß das BAFl nicht nur zur Prüfung einzelner Asylanträge, sondern auch beispielhaft zum Zwecke der Verhütung vergleichbarer Fälle einzelne Antragsfälle, denen eine mißbräuchliche oder gar kriminelle Visumserschleichung vorausging, mit dem AA personenbezogen erörtert. Für einen diesbezüglichen Informationsaustausch muß die Initiative aber ausschließlich vom BAFl ausgehen (s. auch Nr. 5.2).

Im vorliegenden Fall hatte eine Botschaft dem BAFl gegenüber eine „Regelanfrage" für alle aus ihrem Amtsbezirk stammenden Asylbewerber angeregt, weil nach ihrer Auffassung mitteilungsbedürftige Sachverhalte nicht nur in den übermittelten Fällen, sondern regelmäßig vorlägen. Dieses Anliegen hätte die Auslandsvertretung jedoch auch ohne gleichzeitige Übermittlung personenbezogener Daten vorbringen können, um gegebenenfalls anschließend aufgrund einer entsprechenden Anfrage durch das BAFl und nach Prüfung der Voraussetzungen des § 8 Abs. 1 AsylVfG dem BAFl personenbezogene Daten der Visumantragsteller mitzuteilen.

Das AA hat die durch die Botschaft veranlaßte Datenübermittlung damit gerechtfertigt, daß in dem Bemühen des BMI um eine verbesserte Zusammenarbeit im Interesse einer wirksamen Bekämpfung des Asylmißbrauchs ein Ersuchen zur Datenübermittlung in allgemeiner Form gesehen werden könne. Dem kann nicht zugestimmt werden. Wegen der nach § 8 Abs. 1 AsylVfG gebotenen Abwägung, ob einer Übermittlung personenbezogener Daten überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen, wäre ein derartig pauschales Ersuchen in allgemeiner Form mit dem Schutzzweck der Vorschrift nicht vereinbar.

Obwohl ich mich dem Anliegen von AA und BMI, dem Asylmißbrauch wirksam zu begegnen, nicht verschließe, habe ich wegen des offenkundigen Verstoßes gegen § 8 Abs. 1 AsylVfG die Datenübermittlung förmlich beanstandet. Trotz gegenteiliger Auffassung in der Sache hat das AA seine Auslandsvertretungen angewiesen, künftig entsprechend meiner Rechtsauffassung zu verfahren.

5 Innere Verwaltung

5.1 Umsetzung des AZR-Gesetzes und der AZRG-Durchführungsverordnung

5.1.1 Allgemeine Verwaltungsvorschriften zum AZR-Gesetz und zur AZRG-Durchführungsverordnung

In meinem 15. TB (Nr. 3.1) habe ich über vorbereitende Arbeiten des BMI an der AZRG-Durchführungsverordnung berichtet, bei deren Gestaltung ich aufgrund der frühzeitigen und intensiven Beteiligung Verbesserungen erreichen konnte. Die inzwischen in Kraft getretene Durchführungsverordnung enthält zu einzelnen Vorschriften des Gesetzes nähere Regelungen und ermöglicht damit eine leichtere Handhabung des Gesetzes in der Praxis. Insbesondere enthält sie Einzelheiten zum Inhalt des Registers, zur Datenübermittlung an und durch die Registerbehörde, zur Auskunft an den Betroffenen sowie zu den Aufzeichnungen bei Datenübermittlungen und zur Sperrung und Löschung von Daten.

Eine weitere Hilfe für die Praxis sind die Allgemeinen Verwaltungsvorschriften zum Gesetz über das Ausländerzentralregister und zur AZRG-Durchführungsverordnung. Auch bei der Erarbeitung dieser Vorschriften bin ich durch das BMI in einem frühen Stadium beteiligt worden, so daß ich auch hier in zahlreichen Detailfragen Verbesserungen erreichen konnte. Die Allgemeinen Verwaltungsvorschriften sind in dem vom Bundesministerium des Innern herausgegeben Gemeinsamen Ministerialblatt Nr. 24 vom 24. Juni 1996 veröffentlicht worden.

Bereits kurz nach Inkrafttreten des das Ausländerzentralregister betreffenden Regelwerkes habe ich mir einen Eindruck von der Umsetzung der Vorschriften durch die Registerbehörde verschafft. Hierüber wird unter Nrn. 5.1.2 bis 5.1.5 sowie unter 5.3.1 berichtet.

5.1.2 Identitätsfindung

Ein Problem, das sich bei Registern stellt, die vielen Stellen zur Abfrage zur Verfügung stehen – sei es über Papierbelege, über Datenträger oder im Wege der Fernabfrage – ist die sichere Identitätsfeststellung. Ich habe mich beim Bundesverwaltungsamt als der Registerbehörde des AZR kurz nach Inkrafttreten des AZR-Gesetzes ausführlich darüber informiert, wie die Identität gefunden und festgestellt wird. Das Gesetz enthält hierfür in § 10 Abs. 2 und 3 Regeln. Danach muß das Ersuchen, das die anfragende Stelle an das AZR richtet – wenn möglich – die Grundpersonalien des Betroffenen und die AZR-Nummer enthalten. Fehlt die AZR-Nummer und stimmen die in dem Übermittlungsersuchen bezeichneten Personalien mit den gespeicherten Daten nicht überein, ist die Datenübermittlung unzulässig, es sei denn, Zweifel an der Identität bestehen nicht. Nur dann, wenn die Registerbehörde nicht selbst die Identität eindeutig feststellen kann, darf sie die Identitätsfeststellung

der ersuchenden Stelle überlassen. Hierzu hat sie ihr neben Hinweisen auf aktenführende Ausländerbehörden die Grundpersonalien und weitere Personalien **ähnlicher** Personen zu übermitteln (auch als „Ähnlichen-Service" bezeichnet).

Bei meiner Kontrolle habe ich bezüglich des automatisierten Abrufverfahrens festgestellt, daß die Registerbehörde eine Trefferliste dieses Inhalts schon immer dann übermittelte, wenn die Anfragedaten nicht exakt mit denen eines vorhandenen Datensatzes übereinstimmten. Wichtiger Punkt meiner Bemühungen war daher, hier eine Korrektur zu erwirken, nach der die Registerbehörde die Identitätsfindung in den Fällen selbst treffen muß, in denen – trotz gewisser Abweichungen in den Daten – Identitätszweifel nicht bestehen. Darüber hinaus konnte sich zum Zeitpunkt meiner Kontrolle eine ersuchende Behörde zu jedem der in der Trefferliste angezeigten Datensätze den vollen Datensatz des AZR (im Umfang der §§ 15 ff. AZR-Gesetz) anzeigen lassen. Das war ihr auch dann noch möglich, nachdem sie die Identitätsentscheidung getroffen hatte. Ich habe der Registerbehörde nachdrücklich empfohlen, auch dieses Verfahren umgehend zu ändern.

Sie ist meiner Empfehlung gefolgt und hat entsprechende Programmänderungen eingeleitet: So erhält die ersuchende Stelle den vollen Datensatz erst dann, wenn sie entschieden hat, welche Grundpersonalien in der Trefferliste zu dem Fall gehören, zu dem sie eine Anfrage gestellt hat. Und sie erhält den vollen Datensatz auch nur zu dem „Treffer", für den sie sich entschieden hat.

Ein anderes Problem stellt sich nach meinen Feststellungen im Zusammenhang mit Anfragen und Auskünften im Wege des Magnetband- und des Belegverfahrens. Das AZR-Gesetz sieht hier die Übermittlung der AZR-Nummer zum Zwecke der Identitätsfeststellung zu den in der Trefferliste aufgeführten Personen nicht vor. Dies bedeutet, daß einer Behörde, die auf der Basis der von der Registerbehörde übermittelten Personalien einen Datensatz als den des Betroffenen identifiziert hat, das eindeutige Identifizierungsmerkmal „AZR-Nummer" nicht zur Verfügung steht. Wenn diese Behörde sich – mit den Personalien der identifizierten Person – wieder an die Registerbehörde wendet, um von ihr den vollen Datensatz zu dieser Person zu erhalten, wird ihr bisher im Regelfall wiederum nur eine Trefferliste übermittelt. Diese nachteiligen Folgen für die Praxis sind im Rahmen des Gesetzgebungsverfahrens offensichtlich nicht erkannt worden.

Ich habe dem BMI empfohlen, das AZR-Gesetz bei nächster Gelegenheit dahingehend zu ergänzen, daß die Übermittlung der AZR-Nummer im Zusammenhang mit der Identitätsfindung stets zugelassen wird. Das BMI hat meine Empfehlung positiv aufgenommen.

5.1.3 „Kombi-Abfrage" und „Kombi-Anwort" im AZR und Schengener Informationssystem

Das BVA verwaltet neben dem AZR auch den nationalen Teil der im Schengener Informationssystem gespeicherten personenbezogenen Daten zur Einreiseverweigerung nach Artikel 96 des Schengener Durchführungsübereinkommens (nachfolgend als „SIS-Datenbestand" bezeichnet); hier ist es Auftragnehmer des BKA.

Im Einklang mit den geltenden Vorschriften werden diese Datenbestände im Bundesverwaltungamt getrennt geführt. Erhebliche datenschutzrechtliche Probleme bereitete dem BVA aber die Datenverarbeitung zur Beantwortung sogenannter kombinierter Abfragen der Ausländerbehörden, die Zugriff auf den SIS-Datenbestand haben und nach dem AZR-Gesetz zugleich befugt sind, Informationen aus dem Ausländerzentralregister zu erhalten. Das BVA hat das Abfrageverfahren bisher dergestalt eingerichtet, daß Ausländerbehörden die AZR-Abfrage zwingend „mit Personalien" vornehmen müssen, und das BVA hat programmtechnische Maßnahmen dahingehend getroffen, daß mit diesen Personalien auch der SIS-Datenbestand abgefragt wird. Gegenüber dem BVA habe ich deutlich gemacht, daß dies einen Verzicht auf die AZR-Nummer als eindeutiges Identifizierungsmittel bei der AZR-Abfrage auch in solchen Fällen bedeutet, in denen den Ausländerbehörden die AZR-Nummer zur Verfügung steht. Dies läuft jedoch dem Gebot zuwider, Identitätszweifel soweit möglich zu vermeiden. In Abstimmung mit dem BMI und dem BVA wurde ein neues Kombi-Verfahren konzipiert: Wenn die abfrageberechtigte Stelle über die AZR-Nummer verfügt, so hat die Abfrage beim AZR mit dieser AZR-Nummer zu erfolgen, um eine eindeutige Identifizierung im AZR-Datenbestand zu ermöglichen. Die im gefundenen Datensatz des Ausländerzentralregisters mit der AZR-Nummer verbundenen Grundpersonalien (im Sinne des § 3 Nr. 4 AZR-Gesetz) werden dann zur Abfrage des SIS-Datenbestandes verwandt. In Fällen, in denen die abfrageberechtigte Stelle nicht über die AZR-Nummer verfügt, bleibt es selbstverständlich bei der Kombi-Abfrage „mit Personalien". Nach wie vor darf es aber auch eine Kombi-Antwort geben: In der Bildschirmmaske sind auch Hinweise (etwa in der Fußleiste) auf den jeweils anderen Datenbestand zulässig.

5.1.4 Datensicherheit beim Ausländerzentralregister

Das BVA hat durch technische und organisatorische Maßnahmen für eine sichere Datenverarbeitung des Ausländerzentralregisters zu sorgen. Besonders wichtig in diesem Zusammenhang ist, durch welche Maßnahmen die Registerbehörde sicherstellt, daß die zur Kommunikation mit dem Register berechtigten öffentlichen Stellen auch nur den für sie gesetzlich vorgesehenen Datenumfang zur Verfügung gestellt bekommen. Hierzu hat die Registerbehörde die Erteilung eines sog. Behördenkennzeichens zur Voraussetzung für die Berechtigung gemacht, aus dem Register Auskünfte zu erhalten oder Informationen im Register zu speichern. Sie hat ein sorgfältiges Prüfverfahren entwickelt, um festzustellen, ob die beantragende Stelle auch tatsächlich eine berechtigte Stelle i. S. d. AZR-Gesetzes ist. Darüber hinaus hat sie durch programmtechnische Maßnahmen entsprechende Vorkehrungen dafür getroffen, daß die berechtigten Behörden auch nur den gesetzlich festgelegten Datenumfang speichern bzw. übermittelt bekommen können.

Vom BVA mit einem Behördenkennzeichen versehene Stellen haben die Möglichkeit, im sog. C-Belegverfahren (Papier), im Datenträgeraustauschverfahren (Magnetband) oder im Wege der Direkteingabe (s. auch Nr. 5.1.5) mit dem AZR zu kommunizieren. Die Kommunikationswege einschließlich der Anzahl der Datenanlieferungen (Auskunftsersuchen und Änderungen der Datensätze) für das Jahr 1995 sind in Abbildung 1 dargestellt. Meine Überprüfung der Maßnahmen der Registerbehörde zur Verhinderung von Manipulationen bei der Anlieferung, Verarbeitung und Auskunftserteilung hat ergeben, daß diese gut sind und den Anforderungen des Datenschutzrechts entsprechen.

5.1.5 Zulassung zum automatisierten Abruf

Schon bald nach Inkrafttreten des Gesetzes über das Ausländerzentralregister (AZR-Gesetz) und der Verordnung zur Durchführung dieses Gesetzes (AZRG-DV) haben mich das BMI und das BVA um Beratung zu folgendem gebeten: Im Rahmen des vorgeschriebenen Zulassungsverfahrens zum automatisierten Verfahren nach § 22 AZR-Gesetz i. V. m. § 10 AZRG-DV müssen die die Zulassung beantragenden Stellen u. a. „die zur Datensicherung erforderlichen technischen und organisatorischen Maßnahmen" treffen. In der Praxis hat sich gezeigt, daß die Beschreibung der nach § 9 BDSG getroffenen Maßnahmen, die von der Registerbehörde zu bewerten sind, uneinheitlich war. So haben einige Stellen detailliert erläutert, welche konkreten Datensicherungsmaßnahmen sie getroffen haben und entsprechende Unterlagen übersandt; andere Stellen erklärten lediglich, daß sie die notwendigen Maßnahmen nach § 9 BDSG oder nach den entsprechenden Vorschriften der Landesdatenschutzgesetze getroffen hätten. Der Registerbehörde war somit eine zuverlässige Beurteilung und Entscheidung über die Zulassung nach § 22 AZR-Gesetz nur mit erheblichem Zeitaufwand möglich.

Mit dem Ziel einer sicheren und auch rationellen Prüfung der Anträge auf Zulassung zum automatisierten Verfahren haben die Registerbehörde und das BMI eine sog. „Datenschutzrechtliche Checkliste für den Direktanschluß nach § 22 AZR-Gesetz" entworfen und mit mir abgestimmt. Die Checkliste enthält unter den Überschriften, die der Anlage zu § 9 Satz 1 BDSG entsprechen, eine Reihe von konkreten Maßnahmen zur Datensicherung. Die den automatisierten Abruf beantragenden Stellen haben die von ihnen getroffenen Maßnahmen anzukreuzen bzw. zu erläutern.

In der Erprobungsphase hat sich gezeigt, daß die Checkliste positiv von den betroffenen Stellen aufgenommen wurde. Das BMI hat im November 1995 diese Checkliste offiziell den Innenressorts der Länder zur Kenntnis gegeben und darauf hingewirkt, daß sie künftig einheitlich benutzt wird.

Dieses Verfahren ermöglicht es nunmehr der Registerbehörde, schnell und einheitlich zu beurteilen, ob die notwendigen technischen und organisatorischen Maßnahmen von den beantragenden Stellen getroffen worden sind und ob Rückfragen oder Ergänzungen erforderlich sind. Darüber hinaus nutzt die Registerbehörde die ausgefüllte Checkliste, um ihrer Verpflichtung nach § 22 Abs. 1 Satz 3 AZR-Gesetz nachzukommen, mich von der Zulassung zu unterrichten, und zwar in der Form, daß sie mir jeweils eine Ablichtung der Checkliste der von ihr zugelassenen Stelle zur Verfügung stellt.

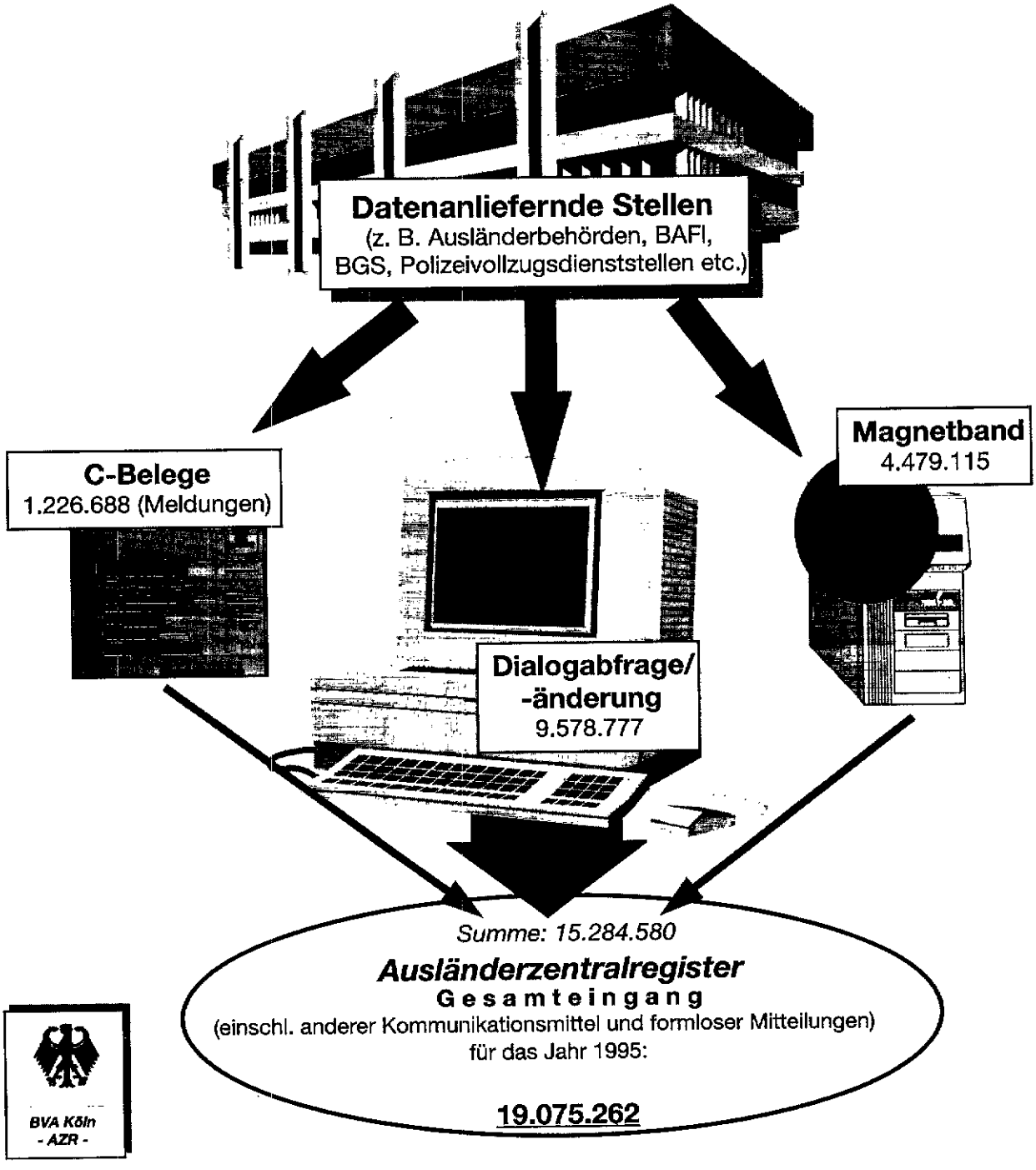
5.2 Mißbrauch von Visa zur Stellung von Asylanträgen

Sowohl das BMI als auch das AA versuchen Erkenntnisse darüber zu erlangen, in welchen Fällen Ausländer die ihnen von deutschen Auslandsvertretungen erteilten Visa in der Weise mißbrauchen, daß sie nach der Einreise in die Bundesrepublik Deutschland einen Asylantrag stellen. Ich habe in diesem Zusammenhang darauf hingewiesen, daß nach Inkrafttreten des Gesetzes über das Ausländerzentralregister (AZR-Gesetz) für die Registerbehörde die Möglichkeit besteht, statistische Auswertungen – d. h. Auswertungen ohne Personenbezug – zu erstellen. So könnten Hinweise darauf gewonnen werden, bei welchen Auslandsvertretungen in welchem Zeitraum und für wieviele Personen Visa beantragt wurden und wieviele dieser Personen zu einem späteren Zeitpunkt einen Asylantrag gestellt haben. Die für die Erstellung einer solchen Geschäftsstatistik erforderlichen programmtechnischen Vorbereitungen sind beim Ausländerzentralregister bislang aber noch nicht abgeschlossen. Vor diesem Hintergrund halte ich ausnahmsweise und für eine kurze Übergangszeit die Ersatzlösung für vertretbar, daß Visadaten an das Bundesamt für die Anerkennung ausländischer Flüchtlinge übermittelt werden und dort mit dem System ASYLON zur Gewinnung ausschließlich derartiger statistischer Informationen abgeglichen werden. Ein solcher Abgleich mit zufällig ausgewählten Visadaten bestimmter weniger Auslandsvertetungen wird derzeit realisiert.

Über diese statistischen Angaben hinaus hält das AA eine bessere Information der Auslandsvertetungen über diejenigen Ausländer für erforderlich, die mit einem Visum eingereist sind und dann einen Asylantrag gestellt haben. Es besteht allseits Einvernehmen, daß die vom Auswärtigen Amt gewünschte Unterrichtung der Auslandsvertretungen wichtige Hinweise auf mißbräuchliches Verhalten geben kann. Die Vorschriften der §§ 15, 21 und 32 Abs. 2 des AZR-Gesetzes lassen in ihrer derzeitigen Fassung solche Datenübermittlungen jedoch nicht zu. Schon jetzt kann das BAFl aber im Asylverfahren auf sein Ersuchen gemäß § 32 AZR-Gesetz aus der Visadatei des Ausländerzentralregisters erfahren, ob und ggf. wo ein Asylantragsteller ein Visum beantragt hat. Es kann dann im Zusammenhang mit der Notwendigkeit, für das Asylverfahren Informationen über die Art der Einreise zu erlangen, gem. § 8 Abs. 1 AsylVfG wiederum auf sein Ersuchen bei der Auslandsvertretung, bei der der Antragsteller das Visum beantragt hat, die näheren Umstände zu diesem Antrag erfahren. Auf diese Weise erhält auch die Auslandsvertretung davon Kenntnis, daß das von ihr erteilte Visum für eine Einreise in die Bundesrepublik zum Zweck der Stellung eines Asylantrags genutzt

Abbildung 1

Ausländerzentralregister
– Kommunikationswege –
(einschließlich Darstellung der Zahlen der Datenanlieferung im Jahre 1995)



worden ist. Gegen diese Verfahrensweise habe ich keine Bedenken.

5.3 Kontrolle und Beratung des Bundesamtes für die Anerkennung ausländischer Flüchtlinge und seiner Außenstellen

5.3.1 Kommunikation mit dem AZR

Beim BAFl habe ich mich über die Anwendung des Regelwerkes zum AZR nicht nur aus der Sicht der Aufgabenstellung der Registerbehörde, sondern auch aus der eines „Bedarfsträgers" informiert. Das Bundesamt ist nach § 6 Abs. 1 Nr. 4 i. V. m. § 2 Abs. 2 Nr. 1 AZR-Gesetz verpflichtet, der Registerbehörde Daten „im Falle" der Stellung eines Asylantrages zu übermitteln. Dieses Verfahren der Direkteingabe im Sinne des § 7 i. V. m. § 22 Abs. 1 AZR-Gesetz habe ich im Asylverfahrenssekretariat der Außenstelle Zirndorf kontrolliert. Dabei konnte ich eine erfreulich große Sorgfalt bei der Erhebung und Übermittlung der in § 3 Nrn. 4 und 5 AZR-Gesetz genannten Personalien feststellen: Die Mitarbeiter des BAFl prüfen die in der von der Zentralen Aufnahmeeinrichtung des Landes Bayern ausgestellten „Bescheinigung über die Meldung des Asylbewerbers" enthaltenen Angaben in Anwesenheit des Asylbewerbers und unter Einsatz eines Dolmetschers auf der Basis der verfügbaren Ausweise und Unterlagen des Betroffenen (im Sinne des § 15 Abs. 2 Nrn. 4 und 5 i. V. m. Abs. 3, insbesondere Nr. 1 AsylVfG). Dabei versuchen sie, sich etwa ergebende Unklarheiten und Widersprüche aufzuklären. Das elektronische Verfahren der Erstmeldung entspricht § 5 Abs. 1 Satz 1 AZRG-Durchführungsverordnung, vor der Direkteingabe „durch Abruf im automatisierten Verfahren festzustellen, ob im allgemeinen Datenbestand des Registers zu dem Betroffenen bereits ein Datensatz besteht". Zu begrüßen ist hierzu der in der Eingabeanweisung des Bundesamtes enthaltene Hinweis: *„Im AZR sind alle bekannten Daten für einen Suchlauf einzugeben, um ein qualifiziertes Ergebnis zu erhalten. Unzureichende Angaben können zu Doppelerfassungen führen."*

Unbeschadet der guten Eindrücke in der BAFl-Außenstelle Zirndorf muß ich nach zwischenzeitlichen Hinweisen der Registerbehörde aber davon ausgehen, daß weiterer Bedarf der Mitarbeiterschulung in den Außenstellen des BAFl besteht. Ich habe empfohlen, durch Stichproben der hausinternen Datenschutzbeauftragten sowohl das Direktabrufverfahren mit dem AZR als auch das Verfahren der Direkteingabe verstärkt zu kontrollieren, um bei allen Außenstellen die nötige Sorgfalt bei Anwendung dieses Verfahrens sicherzustellen.

5.3.2 Einsatz von Dolmetschern und Übersetzern beim Bundesamt für die Anerkennung ausländischer Flüchtlinge

Beim BAFl habe ich mich auch über die Verarbeitung personenbezogener Daten von beim BAFl eingesetzten Dolmetschern informiert. Vor seinem ersten Einsatz als Dolmetscher wird der Betroffene zur Überprüfung seiner Eignung und Zuverlässigkeit aufgefordert, ein Behördenführungszeugnis gem. § 30 Abs. 5 BZRG beizubringen und einen mehrseitigen Erklärungsvordruck auszufüllen. Dieser enthält eine Vielzahl von teilweise sehr sensiblen Fragen, wie z. B. über im In- und Ausland anhängige oder bereits abgeschlossene Strafverfahren. Ich habe kritisiert, daß die verwendete Fragestellung dem Betroffenen nicht deutlich macht, daß Taten im Ausland, die in der Bundesrepublik einen Straftatbestand erfüllen oder Auslandsstraftaten, die auch in der Bundesrepublik sanktioniert werden, bei der Beantwortung der Frage relevant sind; Taten, die diese Voraussetzungen nicht erfüllen, hingegen nicht. Inzwischen hat das BAFl den Erklärungsvordruck unter Berücksichtigung meiner Empfehlungen überarbeitet.

Zur Feststellung der Eignung eines Dolmetschers wird neben der Auswertung der Angaben des Erklärungsvordruckes und des Führungszeugnisses auch das BfV um dessen Überprüfung gebeten. Dies geschieht mangels gesetzlicher Ermächtigung mit Einwilligung (per Vordruck) des Bewerbers. Ich teile die Auffassung des BMI nicht, daß diese Überprüfung nach §§ 17 Abs. 1 und 19 Abs. 1 BVerfSchG zulässig sei, weil diese Vorschriften lediglich die Datenübermittlung durch das BfV an andere Behörde regeln, nicht aber eine Grundlage für die Anfrage beim Verfassungsschutz bilden. Auch eine Einwilligung halte ich nicht für die angemessene Lösung: Solche Art von Routineüberprüfungen sollten nur aufgrund gesetzlicher Regelung erfolgen (s. hierzu 15. TB Nr. 26.4).

Ferner habe ich geprüft, wie im Zusammenhang mit dem Einsatz von Dolmetschern in den Außenstellen des BAFl deren Daten verarbeitet werden. Für Zwecke der Beauftragung sowie der Abrechnung von Honoraren werden eine Vielzahl von personenbezogenen Daten der Dolmetscher erhoben und gespeichert. Daher habe ich angeregt, in einer Dienstanweisung zu regeln, welche Daten erhoben und wie lange diese Informationen – auch zum Zwecke der Rechnungsprüfung – aufgehoben werden sollen. Inzwischen hat das BAFl eine umfangreiche Dienstanweisung in Kraft gesetzt, die meinen Anforderungen Rechnung trägt.

In der BAFl-Außenstelle Zirndorf werden außerdem bundesweit Übersetzungsaufträge koordiniert, die im Zusammenhang mit konkreten Asylverfahren stehen. Zu übersetzende Texte, Schreiben von Asylbewerbern und Dokumente werden zunächst per Telefax von den anderen Außenstellen an die Außenstelle Zirndorf übermittelt. Der von dieser beauftragte Übersetzer erhält die zu übersetzenden Unterlagen in der Regel ebenfalls per Telefax mit der Aufforderung, dieses Fax zusammen mit seiner Übersetzung der Außenstelle Zirndorf wieder zurückzusenden. In meinen Empfehlungen an das BAFl habe ich deutlich gemacht, daß verbindliche Regelungen getroffen werden müssen, die sicherstellen, daß der mit dem Übersetzungsauftrag Betraute keine Kopien der zu übersetzenden Texte und seiner Übersetzungen (auch nicht in elektronischer Form) erstellt, aufbewahrt oder weitergibt. Das BAFl hat daraufhin einen solchen Passus in die mit den Übersetzern zu schließenden Vereinbarungen aufgenommen.

5.3.3 Kommunikation mit Vertragsstaaten des Schengener und des Dubliner Übereinkommens

Nach Artikel 31 des Schengener Durchführungsübereinkommens (SDÜ) sind die Vertragsparteien bestrebt, möglichst schnell zu klären, welcher Mitgliedstaat für die Behandlung eines Asylbegehrens zuständig ist. Zu diesem Zweck können die in Artikel 38 Abs. 2 SDÜ abschließend genannten Daten zwischen den Vertragsparteien ausgetauscht werden. Das Übereinkommen sieht vor, daß ein derartiger Datenaustausch nur auf Antrag eines Mitgliedstaates und nur zwischen solchen Behörden stattfinden kann, die dem aufgrund des Übereinkommens von den Vertragsparteien eingerichteten Exekutivausschuß mitgeteilt worden sind. Für die Bundesrepublik Deutschland ist dies das BAFl. Das BAFl hat zur Durchführung dieser Aufgaben eine eigene Organisationseinheit, die „Koordinierungstelle Schengen/Dublin – Internationale Aufgaben (KSD/IA)", eingerichtet. Somit wird vermieden, daß jede Außenstelle des BAFl mit den Schengener Vertragsstaaten unmittelbar in Kontakt tritt.

Über die Datenübermittlungen auf Ersuchen von Vertragsstaaten nach Artikel 38 SDÜ sowie über Entscheidungen über und die Durchführung von Übernahmeersuchen aus und an Vertragsstaaten nach Artikel 31 SDÜ habe ich mich beim BAFl – KSD/IA – informiert. Die Erhebung, Speicherung und Übermittlung personenbezogener Daten von Asylbewerbern durch die KSD/IA, die sich zum Zeitpunkt meiner Kontrolle noch in der Aufbauphase befand, geht in einzelnen Arbeitsschritten über das erforderliche Maß hinaus. Schon während meines Besuches in der KSD/IA hat das BAFl von mir festgestellte Mängel abgestellt bzw. zugesagt, diese so schnell wie möglich zu beseitigen.

Bei stichprobenartigen Kontrollen ist mir zudem aufgefallen, daß die in dem beim BAFl geführten DV-System ASYLON dokumentierten Verfahrenssachstände nicht immer mit denen des Ausländerzentralregisters übereinstimmten. Nach Aussagen des BAFl sei dies darauf zurückzuführen, daß nach dem SDÜ vom BAFl wahrzunehmende neue Aufgaben in beiden DV-Systemen programmtechnisch noch nicht so umgesetzt seien, um alle Verfahrensschritte vollständig zu dokumentieren und nachzuvollziehen. Das BMI hat mir inzwischen bestätigend mitgeteilt, daß die Programmierung der ASYLON-Anpassung und somit die Einführung der Sachstände noch nicht abgeschlossen ist. Dabei hat mir das BMI zugesagt, nach Abschluß dieser Programmierarbeiten von der KSD/IA veranlaßte Meldungen sowohl im System ASYLON als auch im Ausländerzentralregister auf Richtigkeit zu kontrollieren und erforderlichenfalls zu korrigieren.

5.4 Austausch von Asylbewerberdaten mit der Schweiz

5.4.1 Absprache über den einmaligen Abgleich von Fingerabdruckblättern von Asylbewerbern zu statistischen Zwecken

Das BMI hat wiederholt die Bedeutung einer entschlossenen Bekämpfung des Asylmißbrauchs und des Schlepperunwesens hervorgehoben und verdeutlicht, daß es für eine erfolgreiche Asylpolitik unerläßlich ist, über nationale Grenzen hinweg Erkenntnisse über Mehrfachanträge sowie vor allem über die Verwendung von Mehrfachidentitäten zu gewinnen. Mit Blick auf das bisherige Niveau der Normsetzung für grenzüberschreitende Übermittlungen von Asylbewerberdaten kann die gebotene Entscheidungsfindung aber nicht allein der Verwaltung überlassen bleiben, sondern es müssen für die notwendigen Maßnahmen präzise rechtliche Vorgaben geschaffen werden. Auch habe ich empfohlen, auf der Basis von Verwaltungsvereinbarungen zeitlich befristete, u. U. auch für eine Übergangszeit, Ausnahmen lediglich zur Gewinnung statistischer Erkenntnisse zuzulassen. Dies könnte auch als „Vorgriff" auf zwischenstaatliche, von der Bundesrepublik durch Ratifizierungsgesetz umzusetzende, Übereinkommen geschehen.

Zu diesen Empfehlungen hat das BMI Einvernehmen signalisiert: Schon im Vorfeld der Vorbereitung einer Absprache mit der Schweiz über den Abgleich von Fingerabdrücken von Asylbewerbern hat das BMI im Juli 1994 entschieden, den Innenausschuß des Deutschen Bundestages zu beteiligen. Wesentliche Merkmale dieser Absprache sind, daß es sich um eine einmalige Aktion, bezogen auf einen begrenzten Zeitraum, und um die Verwendung der personenbezogenen Daten ausschließlich zu statistischen Zwecken handelt. Bei der Vorbereitung der Absprache bin ich frühzeitig beteiligt worden. Ich habe erreichen können, daß hinsichtlich des Umfangs der zu übermittelnden Daten, der Bestimmungen über ihren Transport und über ihre Auswertung deutliche Präzisierungen aufgenommen worden sind. Dem Innenausschuß des Deutschen Bundestages hat das BMI das Vorhaben am 25. Oktober 1995 vorgestellt. Der Innenausschuß hat zustimmend Kenntnis genommen. Die Absprache ist daraufhin Ende November 1995 in Bern unterzeichnet worden.

Beim Bundeskriminalamt habe ich mich davon überzeugt, daß nach Maßgabe der Absprache verfahren wird: Es wurden von nach einem Zufallsprinzip ausgesuchten Fingerabdruckblättern Kopien gefertigt und der Schweiz übergeben. Dort wurden sie dann ausgewertet. Mein schweizerischer Kollege hat mir Gelegenheit gegeben, ihn bei der Kontrolle der Stellen zu begleiten, die die Auswertung der Fingerabdruckblätter und die sich daran anschließende statistische Aufbereitung vornehmen. Als Ergebnis seiner Kontrolle, das auch meinem Eindruck entspricht, hat er festgestellt, daß die datenschutzrechtlichen Vorschriften der Absprache durch die Stellen in der Schweiz eingehalten werden.

5.4.2 Austausch personenbezogener Daten zum Zwecke der Verwendung im Asylverfahren

Aufgrund von Hinweisen auf – im Zeitpunkt der Hinweise aber bereits beendete – regelmäßige Übermittlungen personenbezogener Daten von Asylbewerbern an die Schweiz zwecks Verwendung in dort geführten Asylverfahren habe ich das BAFl hierzu Mitte November 1995 kontrolliert.

Nach meinen Feststellungen sind in der Zeit von 1986 bis zum 23. Oktober 1995 auf Anfragen des Schweizer Bundesamtes für Flüchtlinge in einer Vielzahl von Fällen personenbezogene Daten von Asylbewerbern an die Schweiz zur Verwendung in dort anhängigen Asylverfahren übermittelt worden. Den Anfragen waren unterschiedlich gestaltete „Ermächtigungen" des Asylbewerbers beigefügt: In einigen Fällen waren sie auf einem besonderen Formular entweder in deutscher oder in französischer Sprache, in anderen Fällen in beiden Sprachen ausgefertigt. Bisweilen bin ich auch darauf gestoßen, daß diese „Ermächtigung" des Asylbewerbers erst am Ende eines z. B. zwölfseitigen Anhörungsbogens erteilt wurde. In vielen Fällen wurde die Ermächtigung zur Auskunftseinholung in einem „europäischen Drittstaat" mit einer Ermächtigung gegenüber „sämtlichen eidgenössischen, kantonalen und kommunalen Behörden, dem Bundesamt für Flüchtlinge und den zuständigen Behörden" so verbunden, daß der Asylbewerber nur die Möglichkeit hatte, diese Ermächtigungen zusammen zu erteilen.

In einem von mir festgestellten Einzelfall einer Anfrage der Botschaft der Schweiz richtete sich das Ersuchen auf die „Zustellung einer Kopie der Daktyloskopie". Meine Kontrolle hat aber keine Anhaltspunkte dafür ergeben, daß auf solche Anfragen tatsächlich Fingerabdruckblätter oder Kopien hiervon an schweizerische Behörden übermittelt wurden. Wie mir erläutert wurde, sei dies schon deshalb nicht möglich gewesen, weil Fingerabdruckblätter nicht Bestandteil der Asylbewerberunterlagen des BAFl sind. In den Fällen, in denen das BAFl Unterlagen über die genannte Person fand, lautete die Antwort regelmäßig: „Beigefügt erhalten Sie die gewünschten Kopien aus der Asylakte". Aus dieser Formulierung läßt sich im nachhinein nicht erkennen, welche Unterlagen im Einzelfall übermittelt worden sind. Wenig hilfreich waren in diesem Zusammenhang auch die unter „Anlagen" gemachten Eintragungen in den Akten des BAFl, die standardmäßig „diverse Kopien" lauteten. Mir ist durch das BAFl erläutert worden, daß es sich hierbei um Kopien der Niederschrift, der Anhörung und des Bescheides des BAFl und in seltenen Fällen, da solche Unterlagen nur ausnahmsweise durch den Asylbewerber vorgelegt würden, auch um Kopien von Personaldokumenten (Paß, Personalausweis) gehandelt haben könnte.

Ich halte es für erforderlich, daß für derartige Datenübermittlungen eine klare normative Grundlage geschaffen wird. Das BMI habe ich darauf hingewiesen, daß für den Datenfluß in der umgekehrten Richtung, nämlich von ausländischen Behörden in die Bundesrepublik mit § 7 Abs. 2 AsylVfG bereits eine Rechtsvorschrift besteht.

Die Übermittlung personenbezogener Daten von Asylbewerbern an Behörden von Staaten, mit denen die Bundesrepublik innerhalb der Europäischen Union besonders eng verbunden ist, ist im Schengener Übereinkommen vom 19. Juni 1990 und im Dubliner Übereinkommen vom 15. Juni 1990 sowie in den zu diesen Übereinkommen beschlossenen Ratifizierungsgesetzen vom 15. Juli 1993 und vom 27. Juni 1994 geregelt. Die wichtigsten Elemente der damit geschaffenen gesetzlichen Grundlagen sind:

- die Präzisierung zulässiger Übermittlungsinhalte (Artikel 15 Abs. 2 des Dubliner Übereinkommens, Artikel 38 Abs. 2 des Schengener Übereinkommens),
- die Verpflichtung zu Richtigkeit und Aktualität (Artikel 15 Abs. 6 des Dubliner Übereinkommens, Artikel 38 Abs. 6 des Schengener Übereinkommens),
- das absolute Verbot der Verwendung der übermittelten Informationen für asylverfahrensfremde Zwecke (Artikel 15 Abs. 5 des Dubliner Übereinkommens, Artikel 38 Abs. 5 des Schengener Übereinkommens),
- die Verpflichtung zu präziser Dokumentation des Datenaustausches (Artikel 15 Abs. 8 des Dubliner Übereinkommens, Artikel 38 Abs. 8 des Schengener Übereinkommens),
- Informationsrechte des Betroffenen bezüglich der ausgetauschten Informationen (Artikel 15 Abs. 7 des Dubliner Übereinkommens, Artikel 38 Abs. 7 des Schengener Übereinkommens).

Das BMI teilt meine Auffassung bislang nicht. In einem Ende Oktober 1996 mit dem zuständigen Staatssekretär geführten Gespräch konnte aber ein Kompromiß erreicht werden, der darauf zielt, in der Praxis entsprechende Gewährleistungen durchzusetzen:

- Eine gesonderte Einwilligungserklärung des Asylbewerbers zur Übermittlung seiner personenbezogenen Daten in seiner jeweiligen Sprache;
- eine präzise und abschließende Beschreibung der Unterlagen, die weitergegeben werden dürfen;
- Transparenz bezüglich der Folgewirkung der Einwilligung: Soweit davon Gebrauch gemacht wird, wird der Asylbewerber von den zuständigen Behörden in Kenntnis gesetzt;
- Transparenz auch für den Fall der Nicht-Einwilligung: Dem Asylbewerber wird deutlich gemacht, daß im Falle der Unterschriftsverweigerung das Asylverfahren unter Zugrundelegung der gegenwärtigen Aktenlage bearbeitet werden kann;
- Zweckbindung: Die übermittelten Daten werden nur für die Bearbeitung des Asylantrages genutzt.

Mit dem BMI habe ich abgesprochen, daß eine Ausdehnung dieses Einwilligungsverfahrens auf weitere Staaten nicht ohne meine vorherige Konsultation erfolgt.

5.5 Europäisches daktyloskopisches Fingerabdrucksystem zur Identifizierung von Asylbewerbern – EURODAC –

In meinem 15. Tätigkeitsbericht (Nr. 3.2.2) berichtete ich bereits über europäische Überlegungen, ein dem nationalen AFIS-System entsprechendes elektronisches System zur Speicherung und zum Abgleich aller Fingerabdrücke europäischer Asylsuchender einzurichten. Grundlage für die Einrichtung dieses

Systems ist Artikel 15 des im Juni 1990 unterzeichneten Dubliner Übereinkommens über die Bestimmung des zuständigen Staates für die Prüfung eines in einem Mitgliedstaat der Europäischen Union gestellten Asylantrages. Nach diesem Übereinkommen übermittelt jeder Mitgliedstaat dem beantragenden Mitgliedstaat die personenbezogenen Informationen, die erforderlich sind, um den für die Prüfung des gestellten Asylantrages zuständigen Mitgliedstaat zu bestimmen. Nach Artikel 15 Abs. 2 des Dubliner Übereinkommens handelt es sich bei diesen personenbezogenen Informationen insbesondere um die zur Identifizierung des Antragstellers erforderlichen Merkmale. Fingerabdrücke sind hierbei ein wichtiges Indiz zur zweifelsfreien Identifizierung des Antragstellers.

Während der italienischen EU-Ratspräsidentschaft im ersten Halbjahr 1996 wurde erstmals ein Konventionsentwurf zur Einrichtung von EURODAC vorgelegt. Dieser Entwurf wurde in der Folgezeit intensiv auf internationaler und der jeweiligen nationalen Ebene diskutiert und weiter überarbeitet. Das BMI hat mich frühzeitig beteiligt und mir so auch die Möglichkeit gegeben, an Sitzungen der Arbeitsgruppe EURODAC beim Rat der Europäischen Union teilzunehmen, um mich über den jeweiligen Diskussionstand zu informieren.

Inzwischen zeichnet sich ab, daß in einem noch festzulegenden Mitgliedstaat der EU eine Stelle eingerichtet werden soll, bei der alle Fingerabdruckbilder von jedem Asylbewerber, der in einem EU-Mitgliedstaat einen Antrag gestellt hat, elektronisch gespeichert und abgeglichen werden. In diese zentrale Datenbank sollen keine Personalien des Asylantragstellers aufgenommen werden; die Reidentifizierung soll nur anhand einer von dem einspeichernden Mitgliedstaat zu vergebenen Kennummer ermöglicht werden. Näheres über die Struktur und Organisation der Vergabe der Kennummer ist noch nicht bestimmt. Gleichwohl billige ich diesen Ansatz, weil dieses Verfahren ein hohes Maß an Gewähr für die Verhinderung etwaiger Mißbräuche und für die Durchsetzung der vorgesehenen Zweckbindungsregel bietet, wonach eine Nutzung für andere als in Artikel 15 Abs. 1 des Dubliner Übereinkommens genannten Zwecke nicht zulässig ist.

Beim BMI und BMJ setze ich mich darüberhinaus dafür ein, daß in den in der Konvention vorgesehenen Regelungen über Auskunfts-, Berichtigungs- und Löschungsansprüche des Betroffenen, in den Regelungen in bezug auf die Verantwortung der einspeichernden Mitgliedstaaten für die Richtigkeit der Daten sowie in den Regelungen über organisatorische und technische Maßnahmen zur Datensicherheit sowie bezüglich der Kontrollrechte ein hoher Datenschutzstandard verankert wird.

5.6 Rückübernahmeabkommen

5.6.1 Vietnam

Zwischen der Bundesregierung und der Regierung der Sozialistischen Republik Vietnam ist im Juli 1995 ein Abkommen über die Rückübernahme von vietnamesischen Staatsangehörigen geschlossen worden, die keinen gültigen Aufenthaltstitel für die Bundesrepublik Deutschland haben.

Der Vertrag enthält aus datenschutzrechtlicher Sicht positiv zu bewertende Zweckbindungsregelungen und Auskunftsrechte der Betroffenen. Der „Selbstangabe"-Fragebogen, der Anlage zum Durchführungsprotokoll ist und mit dem Angaben über Reisewege und ausgeübte Tätigkeiten, über den Grund der Einreise sowie die Aufenthaltsorte in Deutschland erhoben werden, schien mir dagegen unverhältnismäßig (s. auch 15. TB Nr. 3.2.2).

Das BMI hat mir hierzu erläutert, das Selbstangabeformular sei auf Wunsch der vietnamesischen Seite in das Protokoll aufgenommen worden, da ein entsprechendes Formular auch bei der Rückführung von Vietnamesen aus anderen Staaten verwendet werde. Der Fragebogen solle von den Rückkehrern freiwillig ausgefüllt werden. Sofern der Fragebogen nicht oder nicht vollständig ausgefüllt werde, seien von der die Rückführung betreibenden Behörde die Angaben des Antragsformulars auf Ausstellung eines Paßersatzes und, falls diese Angaben nicht zu erlangen seien, die im Durchführungsprotokoll bezeichneten Mindestangaben – bestimmte Personalien, Staatsangehörigkeit, letzter Wohnort in Vietnam, sowie – soweit möglich – Angaben über nahe Verwandte in Vietnam – zu machen (Artikel 1 Abs. 2 Satz 5 des Durchführungsprotokolls).

Meine Bedenken waren mit diesem ausdrücklichen Hinweis auf die Freiwilligkeit im Zusammenhang mit der Ausfüllung des Fragebogens ausgeräumt. Dem BMI habe ich empfohlen, sein Verständnis des Artikel 1 Abs. 2 des Durchführungsprotokolls den Innenministerien der Länder mitzuteilen, damit die zuständigen Behörden das Übereinkommen auch richtig ausführen können. Das BMI hat meiner Bitte entsprochen. Gegenüber den Landesbeauftragten für den Datenschutz habe ich angeregt, sich unter Berücksichtigung der Interpretation des BMI für eine praktische Anleitung zur Umsetzung des Übereinkommens und des Durchführungsprotokolls einzusetzen und die Handhabung in der Praxis zu überwachen. Dies ist meines Wissens geschehen.

Es ist bedauerlich, daß das BMI mich nicht frühzeitiger beteiligte. Das wäre in dieser empfindlichen Angelegenheit sicher auch mit Blick auf die Öffentlichkeit angebracht gewesen.

5.6.2 Jugoslawien

Ähnlich war es bei dem mit der Bundesrepublik Jugoslawien im Oktober 1996 geschlossenen Rückführungs- und Rückübernahmeabkommen. Auch hier bin ich nicht schon bei der Vorbereitung des Vertrages beteiligt worden. Ungereimtheiten gab es hier insofern, als, abweichend von dem Text des Abkommens (Artikel 6), der eine abschließende Aufzählung der zu übermittelnden personenbezogenen Daten enthält, das Durchführungsprotokoll (in Artikel 1 unter Abs. 2 A.b und in Artikel 4 Abs. 2 sowie in den Anlagen 1 und 3) Angaben auch „zum Gesundheitszustand und lateinischer Name einer eventuellen ansteckenden Krankheit" und „Hinweise auf even-

tuelle Abhängigkeit der Person von fremder Hilfe, Pflege und Fürsorge wegen Krankheit oder Alter" vorsieht.

Es mag Fälle geben, in denen zur Abwehr und Bekämpfung von Seuchengefahren eine Übermittlung von Krankheitsdaten auf der Basis internationaler Vereinbarungen – ggf. auch gegen den Willen des Betroffenen – zwingend geboten ist. Insoweit hat der aufnehmende Staat sicherlich Anspruch auf die notwendigen Informationen, um seine Bevölkerung vor der Einschleppung ansteckender Krankheiten zu bewahren. Die Formulierungen des Protokolls und seiner Anlagen gehen hierüber aber weit hinaus.

Nachdem Nachbesserungen des Übereinkommens nicht mehr zu erreichen waren, habe ich dem BMI umso dringender empfohlen, bei der Unterrichtung der Länder, die das Abkommen auszuführen haben, mit aller Deutlichkeit auf die Beachtung notwendiger Differenzierungen hinzuwirken und darauf hinzuweisen, daß die Gesundheitsdaten in dem vorgesehenen Umfang nur mit Einwilligung des Betroffenen erhoben und übermittelt werden dürfen. Das BMI ist meinen Empfehlungen gefolgt: In seinem Schreiben an die Innenminister und -senatoren der Länder hat es darum gebeten, sicherzustellen, daß Gesundheitsdaten, soweit sie nicht ansteckende Krankheiten nach dem Bundesseuchengesetz betreffen, nur mit Einwilligung des Betroffenen erhoben und übermittelt werden dürfen. Auch hier habe ich die Landesbeauftragten für den Datenschutz gebeten, sich für eine entsprechende Handhabung einzusetzen.

5.7 Staatsangehörigkeitsdatei im Bundesverwaltungsamt

Beim Bundesverwaltungsamt wird seit 1982 automatisiert die Staatsangehörigkeitsdatei – Stada – geführt. Im Oktober 1996 umfaßte die Stada 2,8 Millionen Datensätze, wovon 893 000 aus dem AZR stammten. Der Datensatz ist in der Regel wie folgt aufgebaut:

- Personalien (z. B. Familienname, Vorname, Geburtsdatum)
- Fundstellen (z. B. Behörde, die über die Einbürgerung entschieden hat).

Die Daten wurden u. a. aus folgenden Unterlagen in die Stada übernommen:

- Unterlagen des ehemaligen Reichs- und Preußischen Ministeriums des Innern zur Einbürgerung
- Unterlagen über Sammeleinbürgerungen 1939 bis 1945, z. B. Danzig-Land oder Gotenhafen
- Unterlagen über Rußlandumsiedler
- Unterlagen „Südwestafrika/Südafrika"
- Karteikarten „Donauschwaben" 1940 bis 1945 (Personen, die im Zweiten Weltkrieg als gefangen gemeldet wurden oder als vermißt galten)
- Unterlagen deutscher Auslandsvertretungen (z. B. 1845 bis 1938 Matrikelbände der deutschen Botschaft in Buenos Aires/Argentinien)
- Unterlagen über den Verlust der deutschen Staatsangehörigkeit (z. B. 1933 bis 1945 Aberkennung und Widerruf der deutschen Staatsangehörigkeit oder 1920 bis 1950 Verlust durch Entlassung aus der deutschen Staatsangehörigkeit Landratsamt Unterallgäu in Mindelheim oder 1922 bis 1924 Verlust durch Option für Polen)
- Einbürgerungsmitteilungen der USA ab 1956
- Daten eingebürgerter Ausländer (die Datensätze werden aus dem Ausländerzentralregister übernommen).

Das BMI will für die Stada mit der Neuregelung des Staatsangehörigkeitsrechts die erforderliche Rechtsgrundlage schaffen. Diese fehlt bislang völlig für die Gruppe der Deutschen, deren Daten bis zu ihrer Einbürgerung im AZR waren oder die die deutsche Staatsangehörigkeit abgegeben haben. Für die historischen Datensätze (überwiegend Artikel 116 GG – Deutsche) läßt sich eine Aufbewahrung der Daten beim Bundesverwaltungsamt nach dem BDSG rechtfertigen, weil es die Behörden nicht mehr gibt, die die Unterlagen führen durften; das Bundesverwaltungsamt ist insofern Rechtsnachfolger. Bisher konnte mir das BMI aber keine zwingenden Gründe darlegen, warum die anderen Daten zentral automatisiert gespeichert sein müssen. Umso dringlicher ist eine Entscheidung des Gesetzgebers.

Bis zu dieser Entscheidung des Gesetzgebers hat sich das BMI mit mir auf folgende Feststellungen verständigt:

a) Die Staatsangehörigkeitsdatei bedarf einer umfassenden gesetzlichen Grundlage; die bisherigen rechtlichen Regelungen genügen nicht den sich aus dem Recht auf informationelle Selbstbestimmung ergebenden Anforderungen.

b) Hinsichtlich der „historischen" Datenbestände in der Staatsangehörigkeitsdatei ist die Speicherung und Nutzung der Daten sinnvoll und liegt im Interesse der Betroffenen. Ferner ist es sachlich geboten, daß diese Aufgabe von einer Behörde des Bundes wahrgenommen wird.

c) Die aus dem AZR überführten Daten über ehemalige Ausländer, die durch Einbürgerung die deutsche Staatsangehörigkeit erworben haben, werden heute kaum genutzt. Inwieweit sie künftig benötigt werden, läßt sich erst abschließend beurteilen, wenn feststeht, wie die Regelungen über Erwerb, Verlust und Nachweis der deutschen Staatsangehörigkeit im Rahmen der Neuregelung des deutschen Staatsangehörigkeitsrechts gestaltet werden. Eine zentrale Speicherung auf Bundesebene wird dabei nicht notwendig sein, wenn den Beweisinteressen der Betroffenen durch Maßnahmen auf Landesebene (z. B. hinreichende Aufbewahrungsfristen für Einbürgerungsvorgänge oder für Durchschriften der Einbürgerungsurkunden) genügt werden kann.

d) Bis zur Entscheidung des Gesetzgebers über die Neuregelung des deutschen Staatsangehörigkeitsrechts sollen keine Maßnahmen getroffen werden, die in seine Gestaltungsfreiheit eingrei-

fen. Insbesondere kommt eine Löschung von Daten nicht in Betracht, weil sonst kein Entscheidungsspielraum verbliebe. Die Daten über eingebürgerte Personen sollen vorläufig weiter aus dem AZR an die Staatsangehörigkeitsdatei übermittelt werden.

e) Die aus dem AZR stammenden Daten in der Staatsangehörigkeitsdatei (im November 1996 ca. 904 000 Personen), werden bis zu einer gesetzlichen Neuregelung eingefroren. Auskünfte aus diesem Datenbestand dürfen nur an die Betroffenen selbst oder mit deren ausdrücklicher Einwilligung erfolgen.

5.8 Datenübermittlung von Aussiedleraufnahmedaten des Bundesverwaltungsamtes an den Suchdienst des Deutschen Roten Kreuzes in Hamburg

Das BMI hat mich erneut im Zusammenhang mit der Übermittlung von personenbezogenen Daten aus dem Aussiedleraufnahmeverfahren des Bundesverwaltungsamtes an den Suchdienst des Deutschen Roten Kreuzes (DRK) um Beratung gebeten (siehe auch 14. TB Nr. 4.8). Dabei bin ich davon ausgegangen, daß der DRK-Suchdienst Hamburg insoweit als im Aufnahmeverfahren mitwirkende Behörde i. S. d. § 29 Abs. 1 Bundesvertriebenengesetz (BVFG) angesehen werden und Daten aus diesem Verfahren erhalten kann, als er Aufgaben des Aussiedleraufnahmeverfahrens wahrnimmt. Eine der Aufgaben des DRK-Suchdienstes bestand in der Abrechnung der Fahr- und Paßkosten der in Deutschland eintreffenden Spätaussiedler. Diese Aufgabe wird aber seit 1995 vom BVA selbst wahrgenommen.

In den mit BMI, BVA und DRK-Suchdienst Hamburg geführten Gesprächen wurde deutlich, daß die derzeitige Aufgabenerledigung des DRK-Suchdienstes Hamburg durch die Suchdienstvereinbarung vom 28. Mai 1958 nicht mehr getragen wird. So liegt heute der Schwerpunkt der Aufgaben des DRK-Suchdienstes Hamburg weniger in der Suchdiensttätigkeit, sondern mehr in der Familienzusammenführung und Unterstützung von noch in den Aussiedlungsgebieten lebenden Deutschen.

Zu den Aufgaben, die der DRK-Suchdienst Hamburg im Zusammenhang mit dem Aussiedleraufnahmeverfahren wahrnimmt, zählt die Suche nach einem im Bundesgebiet lebenden Bevollmächtigten als Verwaltungsverfahrenshelfer zur Durchführung des Aufnahmeverfahrens beim BVA. Darüber hinaus berät der DRK-Suchdienst Hamburg Ausreisewillige über die jeweiligen Ausreisebestimmungen des Landes und bearbeitet einen Großteil der sog. Wysows (Anforderungen). Hierbei handelt es sich um eine vom Ausreisewilligen nach wie vor in den meisten der heutigen Staaten der ehemaligen Sowjetunion vorzulegende Bestätigung, daß die Aufnahmevoraussetzungen in der Bundesrepublik vorliegen. Nur bei Vorlage eines Wysows wird dem Antragsteller ein Reisepaß ausgestellt. Allerdings ist nicht zwingend vorgeschrieben, daß alle Wysow-Anträge über den DRK-Suchdienst gestellt werden. Vielmehr können sie auch den Ausreisewilligen nach Übersetzung durch ein privates Übersetzerbüro und nach amtlicher Bestätigung der Richtigkeit (Vorliegen eines Aufnahmebescheides) durch die zuständige kommunale Behörde direkt zugesandt werden. Weitere Aufgaben des DRK-Suchdienstes Hamburg sind allgemeine Beratungen von Ausreisewilligen zur Durchführung des Aussiedleraufnahmeverfahrens, Amtshilfe in anderen Verwaltungsverfahren auf konkretes Ersuchen der diese Verfahren durchführenden Stellen, wie z. B. Staatsangehörigkeitsfeststellungsverfahren oder Rentenangelegenheiten, und klassische Suchdiensttätigkeiten zum Zwecke der Familienzusammenführung von Spätaussiedlerfamilien.

Zur Aufgabenerledigung greift der DRK-Suchdienst auf einen eigenen Datenpool zurück, den er aus Informationen von beim DRK gestellten Wysow-Anträgen, vom BVA bislang übermittelten Daten von Übernahmeanträgen, Aufnahmebescheid- sowie Registrierdaten und vom DRK selbst erhobenen Daten von ratsuchenden Aussiedlern gebildet hat. Der DRK-Suchdienst stellt anhand dieser Daten familiäre Verknüpfungen ("Familienverbände") dar, mit denen das Auffinden gesuchter Personen erleichtert wird.

Einvernehmlich mit dem BMI habe ich festgestellt, daß diese Aufgaben zwar eng mit dem Aussiedleraufnahmeverfahren verbunden sind, sie aber nicht mehr die permanente Übermittlung von Spätaussiedlerdaten durch das BVA an den DRK-Suchdienst Hamburg **auf Vorrat** rechtfertigen. Das BVFG (§ 29 Abs. 2) erlaubt die Datenübermittlung vom BVA an den DRK-Suchdienst auf Ersuchen **im Einzelfall** für Zwecke der Datenverwendung in einem bestimmten Aufnahmeverfahren; die Vorschrift ist aber keine Basis für einen ständigen Datenfluß zur Stützung von DRK-Aufgaben in ihrer gegenwärtigen Breite.

Ich habe dem BMI deshalb empfohlen, eine konkrete Absichtserklärung dergestalt abzugeben, daß die Bundesregierung in absehbarer Zeit eine gesetzliche Regelung anstrebt, die im einzelnen bestimmt, welche personenbezogenen Daten der DRK-Suchdienst Hamburg für seine Suchdienstaufgaben aus dem Aussiedleraufnahmeverfahren des BVA und gegebenenfalls anderen näher zu bezeichnenden Quellen erhält. Eine notwendige Übergangsregelung muß vor allem Aussagen über die konkreten Aufgaben, die Zweckbindung der Daten und die vom DRK zu treffenden technischen und organisatorischen Maßnahmen zur Datensicherheit (§ 9 BDSG) enthalten.

5.9 Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR

5.9.1 Verwendung von Stasi-Unterlagen für Zwecke parlamentarischer Untersuchungsausschüsse

Zu den Entscheidungen des Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (BStU), die ein hohes Maß an öffentlicher Aufmerksamkeit gefunden haben, zählt die Anfang März 1995 erfolgte Übermittlung von Stasi-Unterlagen an den 1. Untersuchungsausschuß der 13. Wahlperiode im Schleswig-Holsteinischen Landtag, den sog.

Schubladen-Ausschuß, in Antwort auf dessen Ersuchen vom Juni 1994.

Der an den BStU gerichteten „Beweismittelanforderung" lag der Auftrag des Untersuchungsausschusses zugrunde, der als Untersuchungsgegenstand insbesondere „weitere Kontakte jeglicher Art" zwischen bestimmten namentlich genannten Personen und „anderen Personen aus dem Kreis der SPD, der SPD-geführten Landesregierung und ihren jeweiligen Mitarbeitern sowie weiteren Personen vor und nach der Landtagswahl 1987 sowie deren Anlaß, Inhalt und weitere Umstände" nannte. Die Anforderung gab den Beschluß des Ausschusses wieder, „Akten des ehemaligen Ministeriums für Staatssicherheit in der DDR zum Zwecke der Beweisverwertung beizuziehen, die zu folgenden Personen existieren oder Bezüge zu ihnen aufweisen: . . .". Bei den vom BStU übermittelten Unterlagen handelt es sich um Informationen aus Ferngesprächen. Sie sind Produkte der als „Funkaufklärung" beschriebenen Tätigkeit der Abteilung III des Staatssicherheitsdienstes in Rostock, die teils aus sogenannten „Mitschriftprotokollen", teils aus ausschnittsweisen Wiedergaben der Gespräche unter Nennung der Gesprächspartner bestehen.

Ich habe erhebliche rechtliche Bedenken, auf der Grundlage des geltenden § 22 StUG Stasi-Unterlagen an einen Untersuchungsausschuß zu übermitteln, wenn seine Beweiserhebung ersichtlich in keinem Zusammenhang mit den Zielen steht,

- die Einflußnahme des Staatssicherheitsdienstes auf das „persönliche Schicksal" einer Person zu klären,
- den einzelnen vor einer Beeinträchtigung seines Persönlichkeitsrechts durch den Umgang mit Stasi-Unterlagen zu schützen,
- die Tätigkeit des Staatssicherheitsdienstes historisch, politisch oder juristisch aufzuklären.

Mit Blick auf die Normqualität des § 22 StUG bin ich allerdings zu der Überzeugung gelangt, daß die bestehenden Unsicherheiten über Inhalt und Tragweite des Zugriffsrechts parlamentarischer Untersuchungsausschüsse auf Unterlagen des MfS nicht im Verantwortungsbereich des BStU liegen.

Ich habe daher der Bundesregierung empfohlen, im Rahmen ihrer Rechtsaufsicht nach § 35 Abs. 5 Satz 3 StUG unter Berücksichtigung auch jüngerer Rechtsprechung des Bundesverfassungsgerichts ein Rechtsverständnis der maßgeblichen Vorschriften des Stasi-Unterlagen-Gesetzes sicherzustellen, das Zweifel an einer verfassungskonformen Rechtsanwendung ausschließt. In solchen Hinweisen der Bundesregierung sehe ich keinen Widerspruch zu der in § 35 Abs. 5 Satz 2 StUG verbürgten Unabhängigkeit des BStU in Ausübung seines Amtes.

Meiner dringlichen Empfehlung, die Unterlagen zurückzuverlangen, ist das BMI nicht gefolgt. Dieses Problem hat sich zwischenzeitlich insofern erledigt, als die Unterlagen vom Untersuchungsausschuß an den BStU zurückgegeben sind, nachdem das Amtsgericht und das Landgericht Kiel entschieden hatten, daß die Einsichtnahme in die vom BStU zur Verfügung gestellten Unterlagen unzulässig ist. Da die Stellungnahme der Bundesregierung noch aussteht, ist weiterhin nicht gelöst, wie in Zukunft mit Abhörprotokollen der Stasi zu verfahren ist, wenn erneut von einem Untersuchungsausschuß des Bundes- oder eines Landesparlaments Unterlagen vom BStU angefordert werden für Recherchen zu Fragen, die mit den Zielvorstellungen des Stasi-Unterlagen-Gesetzes nichts zu tun haben.

5.9.2 Weitere Kontrollen und Beratungen des BStU und seiner Außenstellen

Meine Kontrollen sowohl in der Zentrale des BStU in Berlin als auch in zwei seiner Außenstellen haben folgendes ergeben:

Der Aufbau der Datei „Elektronisches Personenregister" (EPR) ist mittlerweile weit vorangeschritten. In das EPR wurden bisher im wesentlichen rd. 180 dezentrale Karteien aus den Diensteinheiten des ehemaligen MfS, rd. 350 000 Personendatensätze, die bei der Erschließung der in den MfS-Diensteinheiten aufgefundenen Aktenbestände ermittelt wurden, Disziplinarunterlagen des ehemaligen MfS und verschiedene Sonderkarteien eingegeben. Unterlagen, die vormals aufgrund ihrer Vielzahl und Größe kaum für Recherchen genutzt werden konnten, stehen hierfür nunmehr zur Verfügung.

Zugleich stellt sich die Frage, ob und welche Wirkungen hiermit in bezug auf in zurückliegender Zeit erteilte Auskünfte des BStU verbunden sind. § 4 Abs. 3 StUG verpflichtet den BStU, personenbezogene Informationen, die aufgrund eines Ersuchens nach den §§ 20 bis 25 StUG übermittelt wurden und die sich hinsichtlich der Person, auf die sich das Ersuchen bezog, nach ihrer Übermittlung als unrichtig erweisen, „gegenüber dem Empfänger zu berichtigen, es sei denn, daß dies für die Beurteilung eines Sachverhaltes ohne Bedeutung ist" (s. auch 15. TB Nr. 3.6.2). Bisher wurden rd. 2 Millionen Auskünfte gegeben. Ein Abgleich aller dieser Auskünfte mit dem EPR ist nach Ansicht des BStU ein nicht leistbarer Arbeitsaufwand. Insofern werden die Auskünfte stets und ausdrücklich unter dem Vorbehalt des aktuellen Erschließungsstandes gegeben und dem Empfänger eine an der jeweiligen Bedarfs- und Interessenlage orientierte Zweit- bzw. Neuanfrage empfohlen. Die unter ausdrücklichem Bezug auf den aktuellen Erschließungsstand gegebenen Auskünfte würden nicht dadurch unrichtig, daß sich durch spätere Erschließung weiterer Unterlagen zusätzliche Erkenntnisse ergäben. Auch bestehe nach § 4 Abs. 3 StUG eine Verpflichtung zur Nachberichtigung gegenüber dem Empfänger der früheren Auskunft nur dann, wenn sich die Unrichtigkeit der Unterlagen als Folge eines Bearbeitungsfehlers des MfS (z. B. bei einer Personenverwechselung durch das MfS) erweise.

Ich habe Verständnis für die Hinweise des BStU auf den hohen Aufwand, zumal es mit dem Abgleich von EPR-Daten mit den Datensätzen von Personen, zu denen eine Auskunft erteilt wurde, nicht getan wäre. Vielmehr kommt es auf einen Vergleich zwischen Auskunfts- und Akteninhalten an. Dem kommt ent-

gegen, daß nicht schon die Erschließung neuer Unterlagen und die Erstellung neuer Datensätze allein im EPR eine Verpflichtung auslöst, Maßnahmen nach § 4 Abs. 3 StUG zu prüfen. Die Schlüsselrolle kommt hier dem Begriff „erweisen" zu: Erweisen sich – im Sinne deutlicher Erkenntnisse – durch den BStU früher erteilte Auskünfte im Vergleich zu neu erschlossenen Stasi-Unterlagen als inhaltlich unrichtig, sei es durch Feststellung von Gerichten, durch Hinweise der betroffenen Personen selbst, von dritter Seite oder sei es durch Erkenntnisse des BStU bei Gelegenheit der Bearbeitung eines neuen Ersuchens, so löst dies m. E. eine Nachberichtspflicht gemäß § 4 Abs. 3 StUG aus. Aus Sicht des Datenschutzes, dessen Aufgabe es ist, den einzelnen davor zu schützen, daß er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird, ist dies mindestens dann zu fordern, wenn es sich bei den neuen Informationen um entlastende Informationen handelt, die ein deutlich anderes Bild der „Beurteilung des Sachverhaltes" ergeben, als früher übermittelte Informationen. Die Diskussion mit dem BStU zu dieser Frage ist noch nicht abgeschlossen. Ich hoffe, auch hier eine einvernehmliche Lösung zu erzielen.

5.9.3 Vorgesehene Änderungen des Stasi-Unterlagen-Gesetzes

Dem am 29. Januar 1991 in Kraft getretenen Stasi-Unterlagen-Gesetz (StUG) kommt aus datenschutzrechtlicher Sicht eine herausragende Bedeutung zu. Das StUG verfolgt die Befriedung und den Ausgleich von zum Teil erheblich widerstreitenden Interessen in einem besonders sensiblen und konfliktträchtigen Bereich politischen wie juristischen Neulandes. Wenngleich dem StUG dies grundsätzlich gelungen ist, steht es – wohl unausweichlich – in besonderer Weise unter einem ständigen Prüfvorbehalt der in der Praxis, das heißt insbesondere durch die Arbeit des BStU gewonnenen Erfahrungen. Das StUG wurde bereits zweimal novelliert (vgl. 15. TB Nr. 3.6.1). 1996 wurde das Dritte Gesetz zur Änderung des Stasi-Unterlagen-Gesetzes (3. StUÄndG, BT-Drucksache 13/4356) als gemeinsamer Entwurf der Fraktionen der Koalition und der SPD in zweiter und dritter Lesung verabschiedet. Der Regelungsgehalt der Novellierung ist aus datenschutzrechtlicher Sicht zu begrüßen.

Die von mir bereits in meinem 14. TB (Nr. 4.4.1) dringend gegebene Empfehlung, das – auch vom BStU als novellierungsbedürftig bezeichnete (vgl. den 2. Tätigkeitsbericht des BStU Nr. 2.3.1, S. 14) – Recht auf Auskunft, Einsicht und Herausgabe bezüglich der dem Staatssicherheitsdienst der ehemaligen DDR überlassenen Justizakten zu erweitern, wurde auch im vorliegenden Gesetzentwurf nicht aufgegriffen. Das StUG verweist im hier einschlägigen § 18 auf die „jeweiligen gesetzlichen Verfahrensordnungen", ohne zu berücksichtigen, daß es sich durchweg um Unterlagen aus Strafverfahren handelt, in denen der Staatssicherheitsdienst die Untersuchungen geführt hat, und die daher mit gewöhnlichen Justizakten nicht vergleichbar sind. Der für das Strafverfahren einschlägige § 147 StPO ist auf das Informationsinteresse **vor** der Urteilsfindung zugeschnitten, da in einem rechtsstaatlichen Verfahren **nach** dessen rechtskräftigem Abschluß in der Regel kein weiterer Informationsbedarf besteht. Bei den Justizakten handelt es sich jedoch überwiegend um solche aus abgeschlossenen Verfahren. Dem Betroffenen wurde seinerzeit durch die Stasi Einblick in diese Akten verwehrt. Im Ergebnis erfahren Betroffene daher bei „Justizakten" im Vergleich mit anderen Stasi-Unterlagen eine deutliche Einschränkung ihrer Rechte. Die Problematik würde jedoch wesentlich entschärft, wenn sich die Überlegungen realisierten, im Rahmen des angestrebten Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts – Strafverfahrensänderungsgesetz 1996 (vgl. hierzu Nr. 6.1.2) – in § 147 StPO ausdrücklich auch Informationsrechte des Beschuldigten „nach rechtskräftigem Abschluß des Verfahrens" aufzunehmen. Ich werde daher eine Änderung oder Ergänzung des Strafverfahrensrechts auch unter diesem Gesichtspunkt aufmerksam verfolgen.

Bereits 1991, bei der Vorbereitung des StUG, habe ich mit Blick auf das Bundeszentralregistergesetz vorgeschlagen, angemessene Resozialisierungselemente vorzusehen und eine Regelung über eine „Zugangsverjährung" zu schaffen, die dem Zeitablauf seit Beendigung der Stasi-Mitarbeit Rechnung trägt (s. 14. TB Nr. 4.4.1). Die nunmehr vorgesehene Gesetzesregelung kommt diesen Überlegungen deutlich entgegen: Danach unterbleiben Mitteilung, Einsichtgewährung oder Herausgabe, wenn keine Hinweise für eine über den 31. Dezember 1975 hinausgehende Tätigkeit für den Staatssicherheitsdienst oder einen ausländischen Nachrichtendienst vorliegen. Ich verschließe mich dem Postulat nicht, daß hierbei für bestimmte politische Ämter Ausnahmen gelten sollen.

Im Verlauf der nunmehrigen Beratungen habe ich meinen Vorschlag wiederholt, die Vorschriften der §§ 20, 21 – jeweils Abs. 1 Nr. 6 und 7 – sowie § 13 Abs. 6 StUG, die die Mitteilung einer Stasi-Tätigkeit von Personen bis zum Alter von 18 Jahren ausschließen, auf Heranwachsende (18 bis 21jährige) auszuweiten. Der Gesetzentwurf ist ein Schritt in diese Richtung, indem er eine Erweiterung der „Jugendsündenregelung" der vorbezeichneten Vorschriften mit Ausnahme des § 13 Abs. 6 StUG insoweit vorsieht, als eine Verwendung von Informationen über geringfügige Tätigkeiten während des Wehrdienstes oder Wehrersatzdienstes bzw. dann unterbleibt, wenn nach dem Inhalt der erschlossenen Unterlagen feststeht, daß trotz einer Verpflichtung zur Mitarbeit keine Informationen geliefert worden sind. Diese Regelung ist eine wesentliche datenschutzrechtliche Verbesserung. Es sollte aber auch für die Zukunft im Auge behalten werden, ob nicht in der Entlastung von Verfehlungen in jungem Lebensalter ein weiterer Schritt gegangen werden kann.

Im Zusammenhang mit dem sog. Schubladen-Ausschuß (s. o. Nr. 5.9.1) ist deutlich geworden, daß es Unsicherheiten in der Handhabung des in § 5 StUG verankerten sogenannten Nachteilverbotes bereits mit Blick auf den Normadressaten dieser Vorschrift

gibt. Nach meiner Ansicht ist Adressat dieses grundsätzlichen Verbotes, personenbezogene Informationen über Betroffene zum Nachteil dieser Personen zu verwenden, nicht erst der Untersuchungsausschuß oder ein sonstiger Übermittlungsempfänger, sondern bereits der BStU als übermittelnde Stelle selbst. Ich gehe insoweit von einer gestuften Verantwortung im Rahmen der im jeweiligen Verfahrensstadium gegebenen Beurteilungsmöglichkeiten des BStU als übermittelnder Stelle wie auch des jeweiligen Übermittlungsempfängers aus. Meine Anregung, dies unmißverständlich zu regeln, hat der vorliegende Gesetzentwurf leider nicht aufgegriffen.

5.10 Melderecht – Wahlwerbung der politischen Parteien – Adreßbücher auf CD-ROM

Die Meldebehörden haben zum einen die Aufgabe, die in der jeweiligen Gemeinde wohnhaften Bürger zu registrieren, um deren Identität und Wohnungen feststellen und nachweisen zu können. Zum anderen sollen sie Daten an andere Behörden und sonstige öffentliche Stellen sowie an Personen und Stellen außerhalb des öffentlichen Bereichs übermitteln. Grundlage für das Meldewesen sind das Melderechtsrahmengesetz, die Landesmeldegesetze und die nach diesen Gesetzen erlassenen Rechtsverordnungen. Obwohl der Bund hier nur eine Rahmenkompetenz hat, wenden sich immer wieder Bürger an mich, weil sie Probleme mit den Meldebehörden oder Fragen zum Meldewesen haben. Ich gebe diese Eingaben in der Regel an die dafür zuständigen Landesbeauftragten für den Datenschutz ab. Gelegentlich wird mir jedoch dadurch ein Problem bekannt, bei dem es notwendig ist, sich an den Deutschen Bundestag oder an das BMI zu wenden.

Im Berichtszeitraum gab es zwei derartige Probleme, einen Brief im Zusammenhang mit Wahlwerbung und die Adreßbücher auf CD-ROM. Ende 1996 gab es darüberhinaus erste Überlegungen, die Melderegister für künftige Zensen, konkret für die „Volkszählung 2001", zu nutzen (s. hierzu Nr. 30.8).

- **Zur Wahlwerbung:**

  Im Zusammenhang mit den Wahlen in Rheinland-Pfalz und Baden-Württemberg beschwerten sich schriftlich und telefonisch bei mir und bei den Landesbeauftragten für den Datenschutz viele, insbesondere ältere Bürger darüber, daß sie Wahlwerbung von der CDU direkt adressiert erhalten hatten. Die Wahlwerbung war ein Schreiben des Bundeskanzlers und Parteivorsitzenden Dr. Helmut Kohl. Auch die Presse griff dieses Problem auf. Unabhängig von der Zuständigkeit habe ich gerade auch wegen des öffentlichen Drucks die CDU-Parteizentrale in Bonn gebeten, mir mitzuteilen, ob nach ihrer Kenntnis die Adressen der Angeschriebenen auf der Grundlage der nach den Landesmeldegesetzen zulässigen Auskünfte im Zusammenhang mit Wahlen erhoben worden seien. Dies wurde mir bestätigt.

  Für die Zukunft halte ich es für hilfreich und dies würde sicher auch die Anzahl der Protestschreiben verringern, daß auf derartigen Schreiben ein Hinweis auf die Quelle für die Adresse, wie z. B. „Ihre Anschrift habe ich gem. § 35 Meldegesetz Rheinland-Pfalz von der für Sie zuständigen Meldebehörde erhalten." gegeben wird.

- **Zu Adreßbüchern auf CD-ROM**

  Im Sommer 1996 machte eine CD-ROM Furore, mit der ein Verzeichnis von Fernsprechteilnehmern verbreitet wurde und die zudem Indikatoren zu der Adresse enthielt, wie z. B. „Villengegend". Die dazu geführte öffentliche Diskussion griff auch die 1995 begonnenen Überlegungen zu gesetzgeberischen Maßnahmen auf, den Bürgern andere Möglichkeiten des Einflusses auf die Weitergabe ihrer Adressen durch die Meldebehörden an Adreßbuchverlage zu geben, als sie bisher in den Landesmeldegesetzen vorgesehen sind. In diesem Zusammenhang ging man davon aus, daß auch Adreßbuchverlage dazu übergehen würden, ihre Erzeugnisse nicht nur in Buchform, sondern auch als CD-ROM anzubieten. Dies hat sich inzwischen bestätigt.

  Nach den Landesmeldegesetzen darf die Meldebehörde Adreßbuchverlagen eine einfache Melderegisterauskunft über sämtliche Einwohner erteilen, die das 18. Lebensjahr vollendet haben. Die einfache Melderegisterauskunft umfaßt Vor- und Familienname, akademischer Grad sowie Anschriften. Der Betroffene hat das Recht, der Weitergabe seiner Daten zu widersprechen. Hierauf ist er in der Regel bei der Anmeldung sowie mindestens einmal jährlich durch öffentliche Bekanntmachung hinzuweisen. Eine Unterscheidung nach Art der Verbreitung – Buch oder elektronisches Verzeichnis – ist bisher nicht vorgesehen. Zum Schutz der informationellen Selbstbestimmung ist es jedoch geboten, dem Betroffenen hier differenziertere Entscheidungsmöglichkeiten gesetzlich zu garantieren. So sollte der Betroffene Einfluß auf den Umfang des Eintrages in das Adreßbuch haben (z. B. kein Vorname), er sollte wählen können, ob seine Daten nur in Druckwerken (aber nicht in elektronische Verzeichnisse) aufgenommen werden, und es muß sichergestellt werden, daß nicht nur die Adreßbuchverlage, die die Daten von der Meldebehörde beziehen, sondern auch etwaige weitere Verwerter der Daten diese Entscheidung des Betroffenen beachten. Auch muß in diesem Zusammenhang diskutiert werden, ob das einfache Widerspruchsrecht hier noch ausreicht oder ob nicht vielmehr die Einwilligung des Betroffenen geboten ist.

  Das BMI hat sich zwar mit meinen Anregungen wohlwollend auseinandergesetzt, sieht sich jedoch nicht in der Lage, hierzu im Melderechtsrahmengesetz eine Vorschrift zu schaffen. Bislang besteht Einigkeit mit den Bundesländern darin, daß der Bund keine Rahmenkompetenz für eine Regelung zur Datenübermittlung an Adreßbuchverlage hat. Insofern können nur die Länder Regelungen in ihren Landesmeldegesetzen schaffen. Gleichwohl sieht das BMI im Zusammenhang mit der Novellie-

rung des BDSG eine Chance, die informationelle Selbstbestimmung des Betroffenen hier auf ähnliche Weise wie im Telekommunikationsrecht zu gewährleisten (s. Nrn. 2.1.5 und 10.1.4 i. V. m. 33.3).

Der Unterausschuß „Melde-, Paß- und Personalausweiswesen" des Arbeitskreises I der Ständigen Konferenz der Innenminister der Länder hat zu diesem Problem im Mai 1996 beschlossen:

„Im Unterausschuß bestand Einvernehmen, daß die Zulässigkeit von Melderegisterauskünften an Adreßbuchverlage ausschließlich nach dem jeweiligen Landesmelderecht zu beurteilen ist. Im Hinblick darauf, daß keine eindeutige rechtliche Möglichkeit besteht, Dritte zu hindern, die Daten der veröffentlichten Adreßbücher einzulesen und danach in elektronischen Verzeichnissen herauszugeben, wird eine Präzisierung im Bundesdatenschutzgesetz (§ 28) für erforderlich gehalten."

Neben dieser Initiative gibt es mittlerweile in mehreren Bundesländern Überlegungen, im Landesmelderecht die Selbstbestimmung des einzelnen im Zusammenhang mit der Herausgabe von Adressen an Adreßbuchverlage zu verbessern. Hier wird jedoch den Vertretern der Innenministerien, aber auch den Landesbeauftragten gelegentlich entgegengehalten, daß die Veränderung der Vorschriften über die Weitergabe von Daten an Adreßbuchverlage, insbesondere die Änderung von der Widerspruchs- zur Einwilligungslösung, schwerwiegende Folgen für die Arbeitsplätze bei den Adreßbuchverlagen nach sich zöge. Diese Argumente scheinen mir aber ungeeignet – auch unter dem Aspekt der Gleichbehandlung mit den Herausgebern von elektronischen Fernsprechverzeichnissen – die aus der Sicht des Datenschutzes notwendige Verbesserung des Rechtes auf informationelle Selbstbestimmung abzulehnen.

In der Praxis sind einige Innenministerien dazu übergegangen, den Meldebehörden zu empfehlen, Daten nur noch an Adreßbuchverlage weiterzugeben, wenn diese zusichern, daß sie die Adreßbücher nur als Druckwerke und nicht als CD-ROM herausgeben. In einzelnen Ländern ist sogar empfohlen worden, mit den Adreßbuchverlagen zu vereinbaren, daß die Teile der Adreßbücher, die nicht nach Namen, sondern nach Straßen sortiert sind, nicht mehr erstellt werden sollen.

Diese Maßnahmen helfen sicher nur wenig, das Unbehagen vieler Bürger abzubauen, denen die neuen Möglichkeiten im Zusammenhang mit Netzen, Chipkarten oder CD-ROM's fremd sind, und weil sie nicht wissen, wie sie hierauf Einfluß nehmen sollen. Insofern wäre es wünschenswert, wenn wenigstens durch die Novellierung des BDSG in diesem Bereich ein weiteres Stück Selbstbestimmung für den einzelnen gewonnen werden könnte.

5.11 Ordensangelegenheiten

In meinem 15. TB (Nr. 3.7) habe ich die Datenerhebung im Zusammenhang mit Ordensverleihungen erstmals problematisiert und dem BMI empfohlen, eine bereichsspezifische Rechtsgrundlage zu schaffen. Zunächst sah das BMI hierfür kein Erfordernis. Nach Besprechungen mit BPräsA, BMI und BMJ habe ich inzwischen den Eindruck, daß die Überzeugung wächst, das Verfahren der Ordensverleihung in Zukunft unter Berücksichtigung datenschutzrechtlicher Belange zu gestalten. Die Gespräche haben gezeigt, daß die Praxis zur Vorbereitung einer Ordensverleihung weit komplizierter und auch uneinheitlicher ist, als von mir zunächst angenommen. Als nicht richtig stellte sich die mir früher zugegangene Information heraus, auch der BND und der MAD würden bei der Prüfung der Ordenswürdigkeit des Betroffenen beteiligt.

Die Prüfung der Voraussetzungen für eine Ordensverleihung, nämlich, ob die Verdienste des Betroffenen eine Ordensverleihung rechtfertigen und ob der Betroffene auch würdig ist, eine solche Auszeichnung zu tragen, wird in der Regel von den Ländern in eigener Zuständigkeit durchgeführt. Anregungen für eine Ordensverleihung kann jedermann an die Vorschlagsberechtigten richten. Vorschlagsberechtigt sind die Ministerpräsidenten der Länder und die Leiter der obersten Bundesbehörden. Die Verdienste und die Ordenswürdigkeit werden in der Regel von den Ordenskanzleien (Staats- und Senatskanzleien) selbst geprüft, teilweise delegieren Länder aber auch Aufgaben auf die Ebene der Regierungspräsidien oder Kommunen.

Üblich ist, daß alle vorschlagsberechtigten Stellen Auskunftsersuchen an das Bundeszentralregister und in vielen Fällen an den Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR richten. Darüber hinaus weichen die Verfahrensweisen in den Ländern allerdings stark voneinander ab, insbesondere soweit es um die Beteiligung der Polizei, der Staatsanwaltschaft und des jeweiligen Landesamtes für Verfassungsschutz sowie um die zeitliche Abfolge der Prüfung von Verdiensten einerseits und der Prüfung der Ordenswürdigkeit andererseits geht. So werden diese Prüfungen in neun Bundesländern parallel vorgenommen, in zwei Ländern wird vor der Prüfung der Verdienste zunächst die Ordenswürdigkeit festgestellt, und in fünf Bundesländern wird die Prüfung der Ordenswürdigkeit erst nach abgeschlossener Prüfung der Verdienste eingeleitet. Letztere Verfahrensweise halte ich nach dem Stand der bisherigen Diskussion für die datenschutzrechtlich vertretbare; die beiden anderen Verfahren, wonach Daten mit potentiell belastendem Inhalt (Ausschließungsgründe für eine Ordensverleihung) parallel oder sogar vor der Prüfung der Verdienste erhoben werden, sind mir bislang nicht plausibel.

Eine Erhebung potentiell belastender Daten ist aus meiner Sicht solange nicht erforderlich, als sie möglicherweise entbehrlich ist. Ihr Inhalt ist für die zu treffende Entscheidung überflüssig, wenn die Verdienste nicht zumindest glaubhaft dargelegt sind oder die Verdienste nicht von solcher Qualität sind, daß der Betroffene für einen Vorschlag zur Verleihung des Verdienstordens ernsthaft in Betracht zu ziehen ist.

Die Informationsgewinnung, insbesondere beim BZR aber auch beim BStU, stelle ich nicht in Frage, halte hierfür aber eine konkrete Erhebungsnorm für erforderlich. In diesem Zusammenhang ist an den Grundsatz des § 13 BDSG bzw. der entsprechenden Vorschriften der Landesdatenschutzgesetze zu erinnern, wonach personenbezogene Daten beim Betroffenen oder zumindest mit seiner Mitwirkung zu erheben sind. Eine Erhebung ist im übrigen auch dann nicht erforderlich, wenn der Betroffene den Orden ablehnt oder signalisiert, für einen Ordensvorschlag nicht in Betracht kommen zu wollen.

Vor diesem Hintergrund trete ich für ein zweistufiges Verfahren ein, wonach zunächst die Verdienste des Betroffenen zu prüfen sind und in einem zweiten Schritt die Prüfung der Ordenswürdigkeit einzuleiten wäre. Von einer Unterrichtung des Betroffenen in der ersten Phase läßt sich aus meiner Sicht absehen, soweit es darum geht, daß sich die vorschlagsberechtigte Stelle von der Richtigkeit der vorgetragenen Verdienste überzeugen möchte. Insoweit halte ich auch die Befragung Dritter ohne Unterrichtung des Betroffenen für vertretbar.

Die Prüfung der Ordenswürdigkeit und die dafür erforderlichen Datenerhebungen dürfen jedoch nicht ohne Einwilligung des Betroffenen erfolgen. Der Betroffene muß Gelegenheit haben zu erfahren, daß und welche Daten über seine Person bei welchen Stellen erhoben werden. Den Betroffenen zusätzlich darüber in Kenntnis zu setzen, daß es nicht nur auf die autonome Entscheidung des Bundespräsidenten, sondern zuvor schon auf das Ergebnis einer Prüfung seiner Ordenswürdigkeit ankommt, ist ansatzweise schon jetzt aus den Ordensvorschriften ersichtlich und sollte künftig noch mehr verdeutlicht werden. Erteilt der Betroffene seine Einwilligung nicht, ist das Verfahren abgeschlossen; es kommt zu keinen weiteren Datenerhebungen und -verarbeitungen, aber auch nicht zu einer Ordensverleihung. Durch diese umfassende Information könnte die „Erwartungshaltung" des Betroffenen – vom BMI und dem Bundespräsidialamt bislang angeführte Begründung für eine Nichtbeteiligung – minimiert werden.

Der gegenwärtige Diskussionsstand bestärkt mich in meiner Empfehlung, im Ordensgesetz eine bereichsspezifische Regelung zur Erhebung und Verarbeitung personenbezogener Daten zu schaffen, die für eine Würdigkeitsprüfung erforderlich sind.

5.12 Neufassung des Personenstandsgesetzes

Über notwendige Verbesserungen des Personenstandsrechts habe ich schon vor Jahren berichtet (s. 10. TB S. 17 f.). Nachdem die Arbeiten an der geplanten Änderung des Personenstandsgesetzes – PStG – nach Herstellung der deutschen Einheit zunächst geruht hatten und dann unter Beteiligung der neuen Bundesländer wieder aufgenommen worden waren, hat das BMI im März 1996 einen neuen Vorentwurf vorgelegt, zu dem ich Stellung genommen habe.

Der Entwurf des BMI berücksichtigt bereits die voraussichtlichen Änderungen des PStG durch den Entwurf eines Gesetzes zur Neuordnung des Eheschließungsrechts (EheSchlRG). Die für mich bedeutsamste und schon seit langem geforderte Bestimmung in diesem Entwurf ist die Abschaffung des öffentlichen Aufgebotes; eine Änderung, die von der Bundesregierung bereits 1983 angekündigt wurde.

Auch wird den jahrelangen Forderungen der Datenschutzbeauftragten, die in die Personenstandsbücher einzutragenden Angaben auf die Daten zu beschränken, die für den Beurkundungszweck von Bedeutung sind, Rechnung getragen. So soll u. a. künftig im Heiratsbuch auf die Angaben über den Beruf und die Religionszugehörigkeit der Ehegatten sowie über den Beruf und das Alter der Zeugen verzichtet werden. Positiv bewerte ich auch die Absicht, die Nutzung der Personenstandsbücher in der Art zu erleichtern, daß hierzu allgemein das Vorliegen eines **berechtigten** Interesses ausreicht, wenn seit dem Tod des Betroffenen mindestens 30 Jahre oder, falls der Todestag nicht bekannt ist, seit seiner Geburt mindestens 120 Jahre vergangen sind. Diese Neuregelung wird insbesondere den Ahnenforschern zugute kommen, die sich häufig bei mir darüber beklagen, daß ihnen der Zugang zu Informationen über Vorfahren in den Seitenlinien dadurch unmöglich ist, daß bis dato ein **rechtliches** Interesse daran nachgewiesen werden muß.

In meinem 10. Tätigkeitsbericht bin ich auch auf das Vorhaben eingegangen, die Gewährung von Informationen zum Zwecke wissenschaftlicher Forschung gesetzlich zu regeln. Der neue Vorentwurf sieht zwar eine derartige Regel (§ 61 d) vor, ich habe jedoch empfohlen, deutlicher zu formulieren, daß die Gewährung von Auskunft aus einem oder Einsicht in einen Personenstandseintrag grundsätzlich nur mit Einwilligung des Betroffenen erfolgen darf.

Erhebliche datenschutzrechtliche Bedenken habe ich – in Übereinstimmung mit einer Reihe von Landesbeauftragten für den Datenschutz – gegen die in § 66 PStÄndG vorgesehene Generalklausel zur Datenübermittlung. Diese genügt nicht den Anforderungen, die das Bundesverfassungsgericht im Volkszählungsurteil (BVerfGE 65, S. 1 ff.) als Voraussetzung für eine normenklare bereichsspezifische Datenverarbeitungsregel bezeichnet hat. Bereits im Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14. März 1988 wurde ausgeführt, daß es für die Mitteilungspflichten des Standesbeamten präziser Rechtsgrundlagen bedarf. Im Gesetz sollten daher – wie bereits im Vorentwurf vom März 1989 vorgesehen – die als Mitteilungsempfänger vorgesehenen Behörden und Stellen genannt, der Umfang der Mitteilungsinhalte beschrieben und dargestellt werden, zu welchem Verwendungszweck die Mitteilung erfolgen darf.

Wie bereits 1983 (vgl. 6. TB S. 12) und 1988 (vgl. 10. TB S. 18) habe ich nochmals empfohlen, vor allem Sterbeurkunden so zu fassen, daß bei Angaben über Ort und Zeitpunkt des Todes Peinlichkeiten für die Hinterbliebenen vermieden werden und Dritten kein Anlaß zu Spekulationen über die näheren Umstände des Todes gegeben wird.

§ 5 PStÄndG regelt erstmalig den Einsatz der automatisierten Datenverarbeitung in den Standesämtern. Neben dem Personenstandsbuch in Papierform, das im Hinblick auf das Erfordernis der dauernden Aufbewahrung der Personenstandsbücher als unverzichtbar gilt, soll der Standesbeamte künftig den für die Beurkundung erhobenen Datenbestand weiter für spätere Ausdrucke von Personenstandsurkunden bereithalten dürfen. Eine Kopie des fortgeschriebenen Datenbestandes kann mit festgesetzten Löschungsfristen als Zweitbuch geführt werden. § 44 Abs. 2 PStÄndG sieht vor, das Zweitbuch in einem anderen als in dem Gebäude aufzubewahren, in dem sich das Standesamt mit den Erstbüchern befindet. Das reicht als Maßnahme zur Datensicherung nicht aus. Unter Berücksichtigung der Schutzwürdigkeit der Personenstandsdaten sollten zusätzlich die erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherung gemäß § 9 BDSG (z. B. Zugangskontrolle, Speicherkontrolle, Datenträgerkontrolle) zumindest im Grundsatz im PStG selbst geregelt werden. Einzelheiten könnten dann in der Dienstanweisung für die Standesbeamten bestimmt werden.

5.13 Geplante Änderung des Bundeswahlgesetzes

Bereits in meinem 2. Tätigkeitsbericht für das Jahr 1979 habe ich darauf hingewiesen, daß die öffentliche Auslegung des Wählerverzeichnisses in der heutigen Zeit keine Berechtigung mehr hat, da von dem Einsichtsrecht nur noch sehr vereinzelt Gebrauch gemacht wird. Schon damals habe ich die Abschaffung der Auslegung gefordert. Auch in den darauf folgenden 17 Jahren bin ich wiederholt mit dieser Forderung an das BMI herangetreten. Sie wurde jedoch stets mit dem Hinweis auf die Notwendigkeit der Öffentlichkeit der Wahlhandlung zurückgewiesen **(s. auch Anlage 5)**. Umso erfreulicher ist es, daß in einem vom BMI erstellten Referentenentwurf zur Änderung des Bundeswahlgesetzes nunmehr die Abschaffung der Auslegung des Wählerverzeichnisses vorgesehen ist und durch ein an bestimmte Voraussetzungen gebundenes Einsichtsrecht ersetzt werden soll. Ich hoffe, daß dieser Passus des Entwurfes noch in dieser Legislaturperiode von allen zuständigen Gremien gebilligt wird

Der Entwurf enthält für die Wahlstatistik, deren Durchführung der Deutsche Bundestag für die Bundestagswahl am 16. Oktober 1994 wegen erheblicher Bedenken ausgesetzt hatte (s. 15. TB Nr. 22.6), nunmehr angemessene Regelungen zur Gewährleistung des Wahlgeheimnisses auch in den Wahllokalen, in denen die Wahlstatistik durchgeführt werden soll.

6 Rechtswesen

6.1 Strafverfahrensänderungsgesetz 1996

6.1.1 Akustische Wohnraumüberwachung

Das Thema „Lauschangriff" ist unter den Vorzeichen notwendiger Maßnahmen für die Strafverfolgung wie auch des Schutzes des Persönlichkeitsrechts nach wie vor ein herausragendes Thema politischer und öffentlicher Diskussion. Der Begriff „Lauschangriff" bezeichnet die akustische Wohnraumüberwachung für Strafverfolgungszwecke. Die besondere Schattenseite hierbei ist, daß die Wohnraumüberwachung nicht nur Tatverdächtige, sondern auch unbescholtene Bürger treffen kann.

BMJ und BMI haben am 13. Juni 1996 „Eckpunkte der Wohnraumüberwachung zur Beweismittelgewinnung" veröffentlicht. Zur Vorbereitung der Kabinettvorlagen hat das BMJ den obersten Bundesbehörden und mir im August 1996 den Entwurf eines Gesetzes zur Änderung des Grundgesetzes (Artikel 13 GG) sowie den Entwurf eines Strafverfahrensänderungsgesetzes 1996 zugesandt. Auf der Basis der vorgesehenen Verfassungsänderung ist die Schaffung einer gesetzlichen Grundlage für die akustische Wohnraumüberwachung ein wichtiges Regelungsziel des letztgenannten Entwurfs.

Die aktuelle Diskussion um eine Verfassungsänderung zur akustischen Überwachung von Wohn- und Geschäftsräumen war auch für die Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 22./23. Oktober 1996 in Hamburg erneut Anlaß, sich mit diesem Thema intensiv zu beschäftigen. Unabhängig davon, daß eine Mehrheit der Datenschutzbeauftragten dieser Maßnahme nach wie vor ablehnend gegenübersteht, sehe ich in den Empfehlungen der Konferenz, die nach langen, intensiven Diskussionen gegeben wurden, im Vorfeld endgültiger Entscheidungsfindung auf Bundes- und Länderebene einen konstruktiven Beitrag für die weiteren parlamentarischen Beratungen. Dies habe ich dem BMI, dem BMJ, den Fraktions- bzw. Gruppenvorsitzenden im Deutschen Bundestag, den Vorsitzenden des Innen- und des Rechtsausschusses des Deutschen Bundestages sowie den Berichterstattern und den für den Datenschutz zuständigen Abgeordneten in diesen Ausschüssen übermittelt.

Die Empfehlungen lauten wie folgt:

„1. Im Grundgesetz selbst ist festzulegen,
   - daß der Einsatz technischer Mittel zur Wohnraumüberwachung nur zur Verfolgung schwerster Straftaten, die im Hinblick auf ihre Begehungsform oder Folgen die Rechtsordnung nachhaltig gefährden und die im Gesetz einzeln bestimmt sind,
   - und nur auf Anordnung eines Kollegialgerichts

   erfolgen darf.
2. Die Maßnahme darf sich nur gegen den Beschuldigten richten. Erfolgt ein Lauschangriff in der Wohnung eines Dritten, müssen konkrete Anhaltspunkte die Annahme rechtfertigen, daß sich der Beschuldigte in der Wohnung aufhält. In allen Fällen muß die durch Tatsachen begründete Erwartung vorliegen, daß in der überwachten Wohnung zur Strafverfolgung relevante Gespräche geführt werden.
3. Das Mittel der Wohnungsüberwachung darf nur dann angewandt werden, wenn andere Methoden zur Erforschung des Sachverhalts erschöpft

oder untauglich sind. Bei einem Lauschangriff in Wohnungen dritter Personen bedeutet dies auch, daß die Maßnahme nur durchgeführt werden darf, wenn aufgrund bestimmter Tatsachen anzunehmen ist, daß ihre Durchführung in der Wohnung des Beschuldigten allein nicht zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsorts des Täters führen wird.

4. Das Zeugnisverweigerungsrecht von Berufsgeheimnisträgern und Personen, die aus persönlichen Gründen zur Verweigerung des Zeugnisses berechtigt sind, muß gewahrt werden.

5. Die Dauer der Maßnahme ist zeitlich eng zu begrenzen. Auch die Möglichkeit der Verlängerung der Maßnahme ist zu befristen.

6. Eine anderweitige Verwendung der erhobenen Daten (Zweckänderung) ist weder zu Beweiszwecken noch als Ermittlungsansatz für andere als Katalogtaten zulässig.

   Personenbezogene Erkenntnisse aus einem Lauschangriff dürfen zur Abwehr von konkreten Gefahren für gewichtige Rechtsgüter verwendet werden.

7. Wenn sich der ursprüngliche Verdacht nicht bestätigt, sind die durch den Lauschangriff erhobenen Daten unverzüglich zu löschen.

8. Die Betroffenen müssen unverzüglich und vollständig über die Durchführung der Maßnahme informiert werden, sobald dies ohne Gefährdung des Ermittlungsverfahrens möglich ist.

9. Eine Verfahrenssicherung durch den Zwang zur eingehenden Begründung und durch detaillierte jährliche Berichtspflichten der Staatsanwaltschaft für die Öffentlichkeit ähnlich den gerichtlichen Wire-Tap-Reports in den USA einschließlich einer Erfolgskontrolle ist vorzusehen. Anhand der Berichte ist jeweils – wegen der Schwere des Eingriffs – in entsprechenden Fristen zu überprüfen, ob die gesetzliche Regelung weiterhin erforderlich ist.

10. Die effektive Kontrolle der Abhörmaßnahme und der Verarbeitung und Nutzung der durch sie gewonnenen Erkenntnisse durch Gerichte und Datenschutzbeauftragte ist sicherzustellen."

6.1.2 Regierungsentwurf StVÄG 1996

Meinen Appell, endlich die längst überfälligen Lücken des Persönlichkeitsschutzes im Strafverfahren in so wichtigen Bereichen wie der Aktenauskunft und der Akteneinsicht sowie der Öffentlichkeitsfahndung durch geeignete Regelungen zu beseitigen, habe ich inzwischen mehrfach wiederholt (14. TB, 5.1.4; 15. TB, 4.2.1). Dabei möchte ich auch bewußt machen, daß es nicht um die personenbezogenen Daten von „Gangstern" oder nur von Verdächtigen, sondern ebenso um Daten von Verbrechensopfern, Tatzeugen und Unbeteiligten geht. Die Bundesregierung hat in ihrer Stellungnahme zu dem im Oktober 1994 vom Bundesrat beschlossenen Entwurf eines StVÄG 1994 (BR-Drucksache 620/94 Beschluß; BT-Drucksache 13/194) erklärt, es stehe *„außer Frage, daß die zu schaffenden Regelungen in jeder Beziehung verfassungsrechtlichen und datenschutzrechtlichen Anforderungen genügen müssen"*; von einer Stellungnahme im einzelnen wolle sie daher absehen und *„alsbald einen Regierungsentwurf"* vorlegen. Die Vorlage erfolgte im Dezember 1996. Ich begrüße, daß mit dem vom Bundeskabinett beschlossenen Entwurf eines StVÄG 1996 Regelungen zur Wohnraumüberwachung von dem im August 1996 verteilten Referentenentwurf gleichen Namens (s. o. Nr. 6.1.1) getrennt wurden, um die Verabschiedung der sonstigen dringend regelungsbedürftigen Inhalte dieses Entwurfes nicht weiter zu verzögern. Zu diesen habe ich gegenüber BMI und BMJ im August 1996 detailliert Stellung genommen; hier möchte ich nur einige Anmerkungen machen:

- Der Entwurf schafft für die Öffentlichkeitsfahndung, insbesondere für die Ausschreibung zur Aufenthaltsermittlung eines Zeugen unter dem Gesichtspunkt der Verhältnismäßigkeit präzise Regelungen. Dies entspricht meinen Forderungen. Regelungen über die Öffentlichkeitsfahndung sind um so wichtiger, je breiter die Öffentlichkeit ist, die man mit Hilfe auch neuer Kommunikationsmittel erreicht. Gerade die Fahndung im Internet zeigt, wie sehr es auf geeignete Abstufungen ankommt **(vgl. Anlage 16)**.

- Mit den vorgesehenen Regelungen über die längerfristige Observation – dies sind planmäßig angelegte Beobachtungen, die länger als 24 Stunden dauern oder an mehr als zwei Tagen stattfinden – wird anerkannt, daß es sich hierbei um einen Eingriff von einer Tiefe handelt, der über eine allgemeine Ermittlungsmaßnahme hinausgeht. Es kommt deshalb, wie in vergleichbaren Fällen, besonders auf Transparenz und die Bildung von Vertrauen an, sobald dies ohne Gefährdung des Untersuchungszwecks geschehen kann. Ich habe daher eine frühestmögliche Benachrichtigung der Personen empfohlen, gegen die sich die Maßnahme gerichtet hat. Dies gilt vor allem für unbescholtene Kontaktpersonen.

- Zur Erteilung von Auskünften und zur Akteneinsicht habe ich mit Unterstützung der Landesbeauftragten für den Datenschutz schon gegenüber dem Entwurf des Bundesrats gefordert, ein **rechtliches** – und nicht nur ein berechtigtes – Interesse zur Voraussetzung einer Übermittlung personenbezogener Daten aus Ermittlungsakten an private Personen oder nicht-öffentliche Stellen zu machen. Leider ist man meinem Vorschlag bislang nicht gefolgt.

- Ein zentrales datenschutzrechtliches Anliegen sind Zweckbindungs- und Verwendungsregelungen. Eine der Fragen ist, wie Regelungen in bereichsspezifischen Vorschriften – ohne Bezug zu Strafverfahren – zur Verwendung von Daten und ihrer Zweckbindung wirken, wenn diese Daten gleichwohl für Strafverfahren genutzt werden sollen. Die beabsichtigte Unzulässigkeit der Informationserhebung bei entgegenstehenden Verwendungsregelungen ist in diesem Zusammenhang eine gute Lösung. Ich hoffe sehr, daß hiermit dem Vorschlag des Bundesratsentwurfs eine endgültige Absage erteilt ist, der die Informationserhebung

nur dann gehindert sehen will, wenn eine gesetzliche Vorschrift die Verwendung für Strafverfahren ausdrücklich ausschließt.

6.2 Genomanalyse im Strafverfahren

Die Genomanalyse als verfeinerte kriminalistische Untersuchungsmethode gewinnt bei der Verfolgung und Ahndung von Straftaten zunehmende Bedeutung. So hat das Bundesverfassungsgericht (BVG) jüngst bestätigt, daß grundsätzlich keine verfassungsrechtlichen Bedenken bestehen, auch eine große Zahl von Personen genanalytisch zu untersuchen, die ein gemeinsames – auch nur potentiell – tatrelevantes Merkmal verbindet, das einen Tatverdacht begründet (BVG, Beschluß vom 2. August 1996 – 2 BvR 1511/96). Wegen der Eingriffstiefe und der nicht abschätzbaren Entwicklung der Möglichkeiten der Gentechnologie habe ich bereits in meinem 15. Tätigkeitsbericht (s. 15. TB Nr. 4.2.2) dem Gesetzgeber geraten, die unerläßlichen Regelungen über den Einsatz gentechnischer Methoden im Strafverfahren zu schaffen, nachdem dies in der zurückliegenden Legislaturperiode nicht gelungen war. Inzwischen wurden in den Beratungen des Rechtsausschusses des Deutschen Bundestages der Gesetzentwurf der Bundesregierung vom März 1995 (BT-Drucksache 13/667) und der Entwurf der Fraktion der SPD vom November 1995 (BT-Drucksache 13/3116) einander angenähert. Dieser Kompromiß wurde im Dezember 1996 vom Bundestag angenommen (BT-Drucksache 13/6420). Damit ist noch in dieser Legislaturperiode rechtliche Klarheit in dieser Frage zu erwarten.

Ich habe im Vorfeld und im bisherigen Verlauf der Beratungen, u. a. in einer Anhörung im Rechtsausschuß des Deutschen Bundestages im Juni 1996, Empfehlungen zu den Entwürfen vorgetragen. Erfreulicherweise besteht Einvernehmen darüber, daß sich die Genomanalyse im Strafverfahren nicht auf die Bereiche des menschlichen Genoms erstrecken darf, die Informationen über erbliche Eigenschaften enthalten. Zulässiger Zielbefund des Einsatzes der Genomanalyse im Strafverfahren ist ausschließlich die durch den Vergleich zweier Proben gefundene und in einem Ja-/Nein-Befund bestehende Antwort auf die Frage nach dem Bestehen oder Nichtbestehen einer Abstammung bzw. der Erzeugung oder Nichterzeugung des Spurenmaterials durch den Beschuldigten oder den Verletzten.

Zu bedauern sind hingegen die weiterhin fehlenden präzisen Grenzziehungen in der Frage, ob bzw. inwieweit im Laufe der molekulargenetischen Untersuchung anfallende Ergebnisse (Test-, Zwischen-, Teil- und Endergebnis) in anderen Strafverfahren bzw. anderen als Strafverfahren verwendet werden dürfen. Denn das Ergebnis einer – regelmäßig in einem Gutachten niedergelegten – genetischen Untersuchung, die Gegenstand der mündlichen Verhandlung und als solche Grundlage der Entscheidung und notwendiger Bestandteil der Verfahrensakte wird, erschöpft sich nicht in dem beschriebenen Ja-/Nein-Befund, sondern umschließt auch die dem konkreten Untersuchungsbefund zugrundeliegenden Gendaten bzw. das im Laufe der Untersuchung erstellte DNA-Profil. Damit liegt ein **Identifizierungsmerkmal** vor, das insbesondere wegen der Möglichkeit der Digitalisierung von Untersuchungsergebnissen auch den computergesteuerten Abgleich mit außerhalb des jeweiligen Strafverfahrens gewonnenen DNA-Profilen erlaubt. Leider wurde meine Empfehlung zu den Gesetzentwürfen der Bundesregierung und der SPD, eine möglichst restriktive Befugnis zur zweckändernden Verwendung des DNA-Profils vorzusehen, in der vom Bundestag nunmehr angenommenen Fassung nicht aufgegriffen. Die Erhebung und Verarbeitung der DNA-Profile in Datenbanken ermöglicht die Abgleichung mit anderen automatisiert gespeicherten DNA-Profilen. Dabei stellt sich auch die Frage einer Speicherung in dem durch das Verbrechensbekämpfungsgesetz geschaffenen Zentralen Staatsanwaltschaftlichen Verfahrensregister (ZStV), in das neben den Personendaten des Beschuldigten – soweit erforderlich – andere zur Identifizierung geeignete Merkmale einzutragen sind (§ 474 Abs. 2 Satz 1 Nr. 1 StPO). Auch zu dieser Frage gibt der angenommene Entwurf keine Antwort. Angesichts der Neuartigkeit des Einsatzes der Genomanalyse im Strafverfahren sollten erst einmal Erfahrungen gesammelt werden. Diese könnten dann Grundlage für eine gesetzgeberische Entscheidung zu dem Problem der digitalisierten und automatisiert gespeicherten sogenannten genetischen Fingerabdrücke in Datenbanken sein.

DNA-Analysen sind empfindliche Eingriffe in die Privatsphäre des einzelnen. Ich begrüße, daß sich – entgegen den Vorschlägen des Bundesrates – durchgesetzt hat, die Anordnung der Untersuchung mit molekulargenetischen Methoden einem ausschließlichen Richtervorbehalt zu unterstellen, d. h. eine staatsanwaltschaftliche Eilzuständigkeit hierfür nicht zuzulassen. Eilfällen ist durch die Möglichkeit der Anordnung der Entnahme des Untersuchungsmaterials durch die Staatsanwaltschaft bzw. deren Hilfsbeamten hinreichend Rechnung getragen.

Eingehend diskutiert wurde die Frage, ob bzw. inwieweit die genomanalytische Untersuchung anonymisiert, z. B. unter einem Code durchgeführt werden sollte. Der Kompromiß vom Dezember 1996 sieht vor, dem Sachverständigen das Untersuchungsmaterial ohne Mitteilung des Namens, der Anschrift und des Geburtstages und -monats des Betroffenen zu übergeben. Damit ist der datenschutzrechtlichen Notwendigkeit zur Anonymisierung des Untersuchungsverfahrens in hohem Maße Rechnung getragen.

Das Recht des Betroffenen auf Auskunft und Information ist eines der zentralen Mitwirkungs- und Kontrollrechte des Bürgers, das ihn erst in die Lage versetzt, seine eigenen Rechte frühzeitig und effektiv wahrzunehmen. Daher ist es besonders erfreulich, daß in den Beratungen des Rechtsausschusses des Deutschen Bundestages diese wichtige datenschutzrechtliche Garantie aufgegriffen und im nunmehr angenommenen Gesetzentwurf durch Aufnahme des neuen § 81e StPO in den Katalog des § 101 Abs. 1 StPO, der bestimmte Benachrichtigungspflichten regelt, realisiert wurde.

6.3 Vernehmung unter Einsatz von Videotechnik zum Opfer- und Zeugenschutz

Die Überlegungen zur Verbesserung des Opfer- und Zeugenschutzes, die aus der polizeilichen, staatsanwaltschaftlichen oder richterlichen Vernehmung erwachsenden Belastungen besonders schutzbedürftiger Zeugen durch Einsatz der Videotechnik in Grenzen zu halten, verfolge ich sehr aufmerksam. Ein Gesetzentwurf des Bundesrates (BR-Drucksache 175/96 Beschluß, BT-Drucksache 13/4983), der Vorschläge zur Vernehmung kindlicher Zeugen in der Hauptverhandlung enthält, gibt mir Anlaß zu folgenden Bemerkungen:

a) Auch andere Personen können besonders schutzbedürftig sein, wie z. B. Opfer von Gewalttaten sowie alte, kranke, gebrechliche oder extrem gefährdete Zeugen. Insofern hoffe ich auf ergänzende Initiativen der Bundesregierung.

b) Inhaltlich geht es um zwei Maßnahmen, die getrennt zu bewerten sind, nämlich um

   - die Bild-Ton-Aufzeichnung zur Vermeidung immer wieder neuer Vernehmungen und
   - die Bild-Ton-Direktübertragung der Vernehmung aus einem anderen Raum in den Verhandlungssaal.

   Nach meinen Beobachtungen ist die Problematik der Vielzahl der Vernehmungen und damit der Bedarf, die Wiederholung der Vernehmung im Vorfeld des Hauptverfahrens zu vermeiden, deutlich größer als im Hauptverfahren selbst. Die Bundesregierung hat daher zu Recht angemerkt, daß die Zulässigkeit der Erstellung von Bild-Ton-Aufzeichnungen bei polizeilichen und staatsanwaltschaftlichen Zeugenvernehmungen der gesetzlichen Klarstellung bedürfe. Ich empfehle, alsbald gesetzgeberische Aussagen zu treffen, in welchen Fällen und unter welchen Voraussetzungen solche Maßnahmen der Strafverfolgungsbehörden geboten sind.

c) Was die Möglichkeiten eines gleichzeitigen Einsatzes beider Maßnahmen in der Hauptverhandlung anbelangt, nämlich der Direktübertragung und der Aufzeichnung, so erachte ich es als wesentlich, daß über diese beiden Maßnahmen – zunächst durch den Gesetzgeber wie dann im jeweiligen Einzelfall aufgrund richterlicher Entscheidung – getrennt entschieden wird. Mit anderen Worten: Direktübertragung und Aufzeichnung müssen nicht zwangsläufig miteinander gekoppelt werden.

d) Dies gilt um so mehr, als die Video-Aufzeichnung nicht nur den Vorteil der Vermeidung der Wiederholung bietet, sondern potentiell auch die Gefahr der im herkömmlichen Verfahren unzulässigen Fixierung des naturgemäß flüchtigen Erscheinungsbildes eines Zeugen, seines Gesichtsausdrucks, seiner Körpersprache, seiner Emotionen etc. schafft. Dieser potentielle Nachteil führt dann zu einer Verletzung des Persönlichkeitsrechts des Zeugen, wenn die Video-Aufzeichnung nicht erst anstelle einer erneuten Zeugenvernehmung genutzt wird, sondern schon an die Stelle eines Einblicks in das Protokoll bzw. einer Protokollverlesung oder eines Vorhalts aus dem Protokoll treten soll. Zum genannten Entwurf sind sich Bundesrat und Bundesregierung darin einig, daß die Video-Aufzeichnung das Protokoll nicht ersetzt – wenn auch offen ist, ob eine entsprechende Klarstellung verzichtbar ist. Um so weniger verständlich ist mir, daß die Bundesregierung beim Vorhalt gegenüber einem Zeugen anstelle der üblichen Protokollverlesung zur Gedächtnisunterstützung nach § 253 StPO dem Bundesrat in der Regelungsabsicht folgt, das Abspielen der Bild-Ton-Aufzeichnung zuzulassen. Ich empfehle, dies nur ausnahmsweise dann geschehen zu lassen, wenn der Zeuge ausdrücklich beantragt, statt mit dem Protokoll mit der Video-Aufzeichnung seiner früheren Vernehmung konfrontiert zu werden.

6.4 Novellierung des Geldwäschegesetzes

Das Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz – GwG) ist im November 1993 in Kraft getreten. Nach weniger als drei Jahren zeichnet sich mit dem Entwurf eines Gesetzes zur Verbesserung der Geldwäschebekämpfung (BT-Drucksache 13/6620 vom 19. Dezember 96) bereits eine erste, nicht nur marginale Änderung ab. Der Gesetzentwurf sieht vor,

- den Anwendungsbereich der Strafvorschrift gegen Geldwäsche zu erweitern,
- das strafprozessuale Ermittlungsinstrumentarium zu verbessern,
- Unsicherheiten bei der Handhabung des Geldwäschegesetzes zu beseitigen und
- die Aufsicht des Bundesaufsichtsamtes für das Kreditwesen auch auf Wechselstuben zu erstrekken.

Die aus datenschutzrechtlicher Sicht besonders sensible Verpflichtung der Geldinstitute, als quasistaatliche Ermittlungshelfer Verdachtsfälle der Geldwäsche anzuzeigen (§ 11 Abs. 1 Satz 1 GwG), soll nach dem Entwurf unverändert bleiben.

Wegen der verfassungsrechtlich ungewöhnlichen und nicht unproblematischen Verpflichtung der Kreditinstitute als quasipolizeilicher verlängerter Arm der Staatsanwaltschaft hielte ich es für wichtig, wenn die hohe Zahl der im Ergebnis nicht zu einer strafrechtlichen Verfolgung bzw. Ahndung führenden Verdachtsanzeigen (Gesamtzahlen 1995: 2 935 Ersthinweise, 1. Halbjahr 1996: 1 420 Ersthinweise) wesentlich reduziert werden könnte. Mit jeder Verdachtsanzeige werden Wirtschaftsdaten von Privatpersonen und/oder Unternehmen offenbart und damit ein besonders sensibler Bereich privater, grundsätzlich staatsfreier Lebensführung offengelegt. Dies ist mit Blick auf das verfassungsrechtliche Gebot der Verhältnismäßigkeit staatlicher Eingriffsmaßnahmen bedenklich und kann auf Dauer nur dann hingenommen werden, wenn die Effektivität („Trefferquote") der Verdachtsanzeigen – bei gleichzeitig deutlicher Reduzierung ihrer Anzahl – erheblich zunimmt.

Eine effektive Information („Feedback") der Kreditinstitute durch die Strafverfolgungsbehörden mit dem Ziel einer noch besseren Sensibilisierung für bekannte und typische, aber auch für neue Formen der Geldwäsche scheint mir hierfür unerläßlich. Ob dabei über ein einzelfallunabhängiges, „generalisiertes" Feedback hinaus eine detaillierte Information der Kreditinstitute über die Folgen jeder einzelnen Verdachtsanzeige geboten ist, halte ich für äußerst zweifelhaft. Ausweislich der Begründung der geplanten Novellierung des Geldwäschegesetzes strebt die Bundesregierung an, *„im Zusammenhang mit dem Strafverfahrensänderungsgesetz eine gesetzliche Regelung der Möglichkeit einer Rückmeldung herbeizuführen."* Diese Absicht sehe ich jedoch in dem Entwurf eines Strafverfahrensänderungsgesetzes 1996 (s. o. Nr. 6.1) nicht realisiert. Die dort in § 475 Abs. 4 i. V. m. Abs. 1 StPO vorgesehene Ermächtigung zur Erteilung von Auskünften auf Antrag im Einzelfall deckt eine „automatische" Information der Kreditinstitute ohne besonderen Antrag nach jeder einzelnen Verdachtsanzeige sicherlich nicht ab. Sofern ein Feedback in jedem Einzelfall eingeführt werden soll, wird die gebotene Regelung auch Antwort auf die Fragen geben müssen,

- ob die Kreditinstitute anders oder zu einem früheren Zeitpunkt als der – unmittelbar betroffene – Beschuldigte von der Einleitung eines Ermittlungsverfahrens in Kenntnis gesetzt werden sollen und
- ob es – mit Blick auf § 170 Abs. 2 StPO – Fälle geben soll, in denen dem Kreditinstitut die Einstellung des Verfahrens mitgeteilt wird, ohne daß der Betroffene von der Staatsanwaltschaft auch nur erfahren hat, daß gegen ihn Ermittlungen eingeleitet worden waren.

Schon bei der Vorbereitung des Entwurfs eines Geldwäschegesetzes habe ich darauf gedrungen, daß alle Informationsbeziehungen im Dreiecksverhältnis zwischen Kreditinstituten, Kunden und Strafverfolgungsbehörden in die Betrachtung einzubeziehen und dabei insbesondere auch die oben skizzierten Fragen sorgfältig zu prüfen sind.

Der Vorschlag des Bundesrates, zur Ermittlung in Geldwäscheverdachtsfällen die Telefonüberwachung zuzulassen (BR-Drucksache 554/96 Beschluß vom 18. Oktober 1996), sollte von einer eingehenden Überprüfung der Verfahren, der Wirksamkeit und Verhältnismäßigkeit der Telefonüberwachung abhängig gemacht werden (zuletzt im 15. TB Nr. 4.1.1).

6.5 Maßnahmen zur Korruptionsbekämpfung

Selbstverständlich unterstütze ich das Ziel von Gesetzgebung und Verwaltung, der Korruption entschieden entgegenzutreten. Gerade hier kommt es auf die Eignung und Effizienz der vorzusehenden Maßnahmen besonders an. Unter diesen Vorzeichen verfolge ich mit großer Aufmerksamkeit gemeinsam mit meinen Kollegen in den Ländern die Planungen für ein Korruptionsbekämpfungsgesetz. Der Gesetzentwurf des Bundesrates vom 3. November 1995 (BR-Drucksache 298/95 Beschluß, BT-Drucksache 13/3353) sieht vor, Bestechlichkeit und Bestechung in den Kreis derjenigen Tatbestände aufzunehmen, bei deren Verdacht die Überwachung des Fernmeldeverkehrs angeordnet werden darf. Zu diesem hat sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder besonders kritisch geäußert **(s. Anlage 13)**. Die Bundesregierung hatte, ebenso wie die Fraktionen von CDU/CSU und FDP in textgleichen Entwürfen (BT-Drucksache 13/5584) Maßnahmen der Prävention deutlicher in den Vordergrund gestellt und auf die Telefonüberwachung als Mittel der Strafverfolgung verzichtet. Vor dem Hintergrund der Stellungnahme des Bundesrates hat nunmehr die Bundesregierung das Anliegen der Telefonüberwachung als berechtigt bezeichnet (BT-Drucksache 13/6424). Ich hoffe, daß die Empfehlungen der Datenschutzbeauftragten in den weiteren Beratungen nochmals bedacht werden.

6.6 Schutz der Vertraulichkeit des Wortes – nur noch eine private Angelegenheit?

Der Bundesrat hat in seiner Sitzung am 1. März 1996 den Entwurf eines Zweiten Gesetzes zur Entlastung der Rechtspflege – Strafrechtlicher Bereich (BR-Drucksache 633/95) beschlossen, der als Zielsetzung die „Straffung des Prozeßablaufs unter Wahrung rechtsstaatlicher Erfordernisse" verfolgt. Artikel 2 Nr. 40 a dieses Gesetzentwurfes sieht vor, die Vergehen nach § 201 Abs. 1 und 2 StGB, also die strafrechtliche Sanktionierung einer Verletzung der Vertraulichkeit des Wortes, in den Katalog der Privatklagedelikte gemäß § 374 Abs. 1 StPO aufzunehmen. Zur Begründung führt der Entwurf aus, die unter Strafe gestellte Verletzung der Privatsphäre (§ 201 StGB) sei typischerweise eine Handlung, deren Bestrafung nicht im unmittelbaren öffentlichen Interesse liege. Es sei dem Verletzten auch zuzumuten, die Bestrafung des Täters dieser sich üblicherweise im privaten Bereich abspielenden strafbaren Handlung erforderlichenfalls im Wege der Privatklage durchzusetzen.

Mit Blick auf die Stellungnahme der Bundesregierung habe ich gegenüber dem BMJ dieser Auffassung widersprochen und darauf hingewiesen, daß das Privatklageverfahren bei bestimmten leichten Vergehen angemessen ist, die die Allgemeinheit in der Regel wenig berühren. Dies ist jedoch beim Straftatbestand des § 201 Abs. 1 und 2 StGB entgegen der Auffassung des Bundesrates nicht der Fall. Das Rechtsgut des § 201 StGB, nämlich die Privatsphäre des Menschen unter dem Aspekt, die Unbefangenheit seiner mündlichen Äußerungen zu wahren, spiegelt nicht nur das Interesse des im Einzelfall Betroffenen wider, sondern ebenso das Interesse der Allgemeinheit an einer Gewährleistung der Voraussetzungen einer ungehinderten mündlichen Kommunikation. Der Schutz der Unbefangenheit der menschlichen Kommunikation ist ein so bedeutsames Rechtsgut, daß die mit der Ausgestaltung als Privatklagedelikt einhergehende Verringerung des strafrechtlichen Schutzes (z. B. durch Fehlen eines Ermittlungsverfahrens gemäß §§ 158 ff. StPO) nicht hingenommen werden kann. Es gilt daher, hier bereits früh einer Entwicklung Einhalt zu gebieten, die den strafrechtlichen Schutz des Persönlichkeitsrechts – als oft-

mals einzig wirksamen – entscheidend relativiert, indem sie ihn der Privatinitiative des einzelnen überantwortet.

Ich bedauere, daß die Bundesregierung den Überlegungen des Bundesrates nicht eine deutliche Absage erteilt, sondern sich auf die Bewertung beschränkt hat, die vorgeschlagene Regelung „erscheine" dadurch, daß durch die Verletzung der Vertraulichkeit des Wortes im Einzelfall ein schwerwiegender Schaden eintreten könne, „nicht unproblematisch".

Ich hoffe, daß der Bundestag diesen weitgehenden Abbau des strafrechtlichen Schutzes der vertraulichen Kommunikation nicht zulassen wird.

6.7 Novellierung des Strafvollzugsgesetzes

Seit 1991 diskutiere ich mit dem BMJ über notwendige Änderungen des Strafvollzugsgesetzes (s. auch 14. TB Nr. 5.5). Im Sommer 1995 und im April 1996 wurden neue Referentenentwürfe erstellt. Der jüngste Entwurf enthält in einem gesonderten Titel Vorschriften über den Datenschutz. Diese berücksichtigen in erfreulichem Umfang meine Empfehlungen. So ist eine früher vorgesehene Ausnahmeregelung von der Unterrichtung eines Betroffenen über eine ohne seine Kenntnis erfolgte Erhebung personenbezogener Daten gestrichen worden. Mein Vorschlag zur Formulierung einer Regelung, für welche Zwecke personenbezogene Daten aus den Akten auch nach Ablauf eines Jahres seit der Entlassung des Gefangenen noch übermittelt oder genutzt werden dürfen, ist übernommen worden (§ 128 d Abs. 2 in der Fassung von 1995 bzw. § 184 Abs. 2 in der Fassung von 1996).

Besonders erwähnenswert ist auch die Regelung über erkennungsdienstliche Unterlagen, die zur Sicherung des Strafvollzuges angelegt werden: In der Neufassung des § 86 Abs. 3 Satz 2 soll zwingend vorgesehen werden, den Gefangenen nicht nur bei seiner erkennungsdienstlichen Behandlung, sondern auch bei der Entlassungsverhandlung darüber aufzuklären, daß er die Vernichtung dieser Unterlagen verlangen kann, sobald die Vollstreckung der richterlichen Entscheidung, die dem Vollzug zugrundegelegen hat, abgeschlossen ist (z. B. nach Ablauf der zur Bewährung ausgesetzten Reststrafe). Hierin liegt eine deutliche datenschutzrechtliche Verbesserung, wenngleich sie hinter meiner Empfehlung zurückbleibt, § 86 Abs. 3 dahingehend zu ändern, daß die erkennungsdienstlichen Unterlagen nach Ablauf der vorbezeichneten Frist in jedem Fall zu vernichten sind.

Daneben enthält der jüngste Entwurf aber auch Regelungen, die ich gegenüber dem BMJ kritisiert habe. Dazu folgendes Beispiel: § 180 Abs. 5 sieht unter näher bezeichneten Voraussetzungen vor, daß die Vollzugsbehörde auf schriftlichen Antrag öffentlichen und nicht-öffentlichen Stellen mitteilen darf, ob sich eine Person in Haft befindet oder ob ihre Entlassung voraussichtlich innerhalb eines Jahres bevorsteht. Meine Bedenken richten sich dagegen, daß nach § 180 Abs. 7 mit dieser Mitteilung weitere personenbezogene Daten des Betroffenen oder eines Dritten in Akten übermittelt werden dürfen, wenn diese mit den nach Abs. 5 übermittelten Daten „so verbunden (sind), daß eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, . . . soweit nicht berechtigte Interessen des Betroffenen oder eines Dritten an deren Geheimhaltung offensichtlich überwiegen". Einen Fall, daß derartige Informationen in der beschriebenen Weise miteinander verbunden sind, kann ich mir kaum vorstellen. Ich habe daher um klärende Hinweise gebeten, andernfalls die Streichung des Verweises auf Abs. 5 in Abs. 7 empfohlen. Leider wurde diese Empfehlung, wie auch andere meiner Änderungsvorschläge zu dem Entwurf von 1995, in dem Entwurf von 1996 nicht berücksichtigt.

Bei Anerkennung der datenschutzrechtlichen Verbesserungen, die der Referentenentwurf von 1996 gegenüber der Fassung des Jahres 1991 erfahren hat, bleibt zu hoffen, daß die von mir und den Landesbeauftragten für den Datenschutz gegenüber den Justizministerien gegebenen Empfehlungen im Strafvollzugsgesetz möglichst weitgehend berücksichtigt werden.

6.8 Eingriffsbefugnisse zur Strafverfolgung im Informations- und Telekommunikationsbereich

Die Entwicklung der modernen Informationstechnik und Telekommunikation beeinflußt zunehmend das Privat- und Berufsleben sowie das Kommunikations- und Konsumverhalten des einzelnen. Damit einher gehen aber auch die Möglichkeiten ihrer mißbräuchlichen Nutzung zu kriminellen Zwecken. Das hat wiederum die Gefahr zur Folge, daß die bestehenden Instrumentarien der Strafverfolgung zum Teil ihre Wirkkraft einbüßen. Dem muß der Gesetzgeber mit neuen Regelungen entgegentreten können, wobei die bestehenden Grenzen für die Eingriffsbefugnisse der Strafverfolgungsbehörden erhalten bleiben müssen. Die Datenschutzbeauftragten des Bundes und der Länder haben sich im Rahmen ihrer 52. Konferenz mit dieser Thematik befaßt (s. Entschließung vom 22./23. Oktober 1996, Anlage 19). Sollte es hierzu in absehbarer Zeit gesetzliche Initiativen geben, sind diese an den Anforderungen der Entschließung zu messen.

6.9 Länderübergreifendes staatsanwaltschaftliches Verfahrensregister

Auch in den zurückliegenden zwei Jahren habe ich mit Empfehlungen die notwendigen Arbeiten für das durch das Verbrechensbekämpfungsgesetz vorgesehene länderübergreifende staatsanwaltschaftliche Verfahrensregister (§§ 474 ff. StPO) begleitet.

Das Ergebnis ist nicht zufriedenstellend: Die am 7. August 1995 vom BMJ mit Zustimmung des Bundesrates erlassene „Allgemeine Verwaltungsvorschrift über eine Errichtungsanordnung für das länderübergreifende staatsanwaltschaftliche Verfahrensregister" enthält u. a. folgende Aussage:

„Die Übermittlung der . . . genannten Daten erfolgt an die Staatsanwaltschaft bzw. an die in steuer-

strafrechtlichen Angelegenheiten ihr gleichgestellte Finanzbehörde, von der eine Mitteilung über ein neues Ermittlungsverfahren eingeht. Ferner darf eine Übermittlung dieser Daten auf Ersuchen der Strafverfolgungsbehörden erfolgen."

Dabei macht das Wort „ferner" deutlich, daß es im zitierten ersten Satz um etwas anderes geht als um die Übermittlung „auf Ersuchen". Meine schon im 15. Tätigkeitsbericht (Nr. 4.1.2) gegebenen Hinweise, daß der Begriff der „Auskunft" in § 474 Abs. 3 Satz 2 StPO ein Ersuchen voraussetzt, waren ebenso vergeblich wie meine an das BMJ gerichteten Hinweise auf die herkömmliche Verwendung des Begriffes der „Auskunft" zum Beispiel im Bundeszentralregistergesetz (BZRG).

Zweifel an ihrem Einklang mit der gesetzlichen Vorgabe läßt auch ein weiterer Satz der genannten Verwaltungsvorschrift aufkommen:

„Kann die Registerbehörde ... eine Mitteilung oder ein Ersuchen einem Datensatz nur teilweise zuordnen, darf sie zur Identitätsprüfung auch die Angaben derjenigen Ermittlungsverfahren übermitteln, die im staatsanwaltschaftlichen Verfahrensregister unter abweichenden, aber ähnlichen Personendaten gespeichert sind."

Der Inhalt dieser Regelung bedeutet ein grundlegendes Abrücken von einem wichtigen Prinzip personenbezogener Auskunftserteilung aus Großregistern, wie z. B. aus dem Bundeszentralregister, wonach die Registerbehörde einen Datensatz nur dann weitergibt, wenn sie ein gewisses Maß an Überzeugung davon gewonnen hat, daß dieser Datensatz sich auf die im Auskunftsersuchen beschriebene Person bezieht. Dabei ist nicht ausschlaggebend, ob die Daten „gleich" oder nur „ähnlich" sind, sondern daß die Registerbehörde die Verantwortung für diese Identitätsfindung trägt. Da hiervon – unter bestimmten Voraussetzungen und nach bestimmten Maßgaben – abzuweichen in bezug auf ein staatsanwaltschaftliches Register durchaus sinnvoll erscheinen kann, habe ich das BMJ schon im Vorfeld der Bemühungen um gesetzliche Regelungen für dieses Register auf das Ausländerzentralregistergesetz (§ 10 Abs. 2 und 3) hingewiesen. Die Vorschriften nennen bestimmte Voraussetzungen, unter denen die Identitätsfindung dem Datenempfänger überlassen werden darf, und gebieten ihm, „alle Daten, die nicht zum Betroffenen gehören, unverzüglich zu löschen" (auch als „Ähnlichen-Service" bezeichnet).

Ich habe der Behandlung auch dieser Fragen besondere Aufmerksamkeit geschenkt bei der datenschutzrechtlichen Bewertung der gemäß Nr. 10 der Errichtungsanordnung erstellten „Leitlinien zur Regelung organisatorischer und technischer Einzelheiten", insbesondere zur Kommunikation zwischen den anliefernden Behörden und der Registerbehörde und zum Datenschutz und zur Datensicherheit. Leider wurde mein Hinweis nicht aufgegriffen, daß die Öffnung des Registers für einen „Ähnlichen-Service" nicht durch Verwaltungsvorschriften (Nr. 4.1 der Leitlinien), sondern nur auf der Grundlage eines formellen Gesetzes erfolgen kann.

Erfreulich ist demgegenüber, daß die ursprünglich in den Leitlinien enthaltene rechtliche Fiktion, wonach jede Mitteilung über die Einleitung eines Ermittlungsverfahrens zugleich auch ein Ersuchen um Auskunft aus dem Verfahrensregister sei, nicht aufrechterhalten wurde. Statt dessen wurde die Kompromißlösung aufgegriffen, wonach mit der Mitteilung über die Einleitung eines Ermittlungsverfahrens in aller Regel ein Ersuchen um Auskunft aus dem Verfahrensregister zu verbinden sei. Die Praxis wird zeigen, ob damit den Bedürfnissen des Datenschutzes hinreichend Rechnung getragen werden kann.

Erfolgreich war mein Hinweis, daß das BZRG es nicht zuläßt, eine Auskunft aus diesem Register an Bedingungen zu knüpfen, wie z. B. einer künftigen Mitteilung zum Zentralen Staatsanwaltschaftlichen Verfahrensregister: Diese in der ursprünglichen Fassung der Leitlinien (08 und 09 unter Nr. 3.2.1) enthaltene Möglichkeit ist in der jüngsten Fassung nicht mehr vorgesehen.

Besondere Bedeutung habe ich von Beginn an der Verschlüsselung der Daten auf dem Transportweg (Nr. 10 der Errichtungsanordnung) beigemessen. Obwohl die Errichtungsanordnung in Nr. 9 Satz 1 die in das Verfahrensregister aufzunehmenden Daten als „besonders sensibel" einstuft, stellen die Leitlinien (Nr. 8) lediglich die Prüfung der **eventuellen** Erforderlichkeit einer Verschlüsselung der Daten auf dem Übertragungsweg in Aussicht. Der zur Begründung angeführten Feststellung („Zur Funktionsfähigkeit von Verschlüsselungsverfahren und deren Akzeptanz in größeren, heterogenen Benutzergruppen liegen noch keine ausreichend belastbaren Erkenntnisse vor.") habe ich gegenüber dem BMJ wiederholt widersprochen – u. a. auch unter Hinweis auf die Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 9. Mai 1996 zu Forderungen zur sicheren Übertragung elektronisch gespeicherter personenbezogener Daten **(s. Anlage 18)**. Die Leitlinien (Nr. 8) weisen ausdrücklich auf das Erfordernis hin, „im fachlichen und dv-technischen Feinkonzept die notwendigen Voraussetzungen für eine Erweiterungsfähigkeit des Systems hinsichtlich einer Verschlüsselung der Daten auf dem Übertragungsweg zu berücksichtigen." Ich hoffe, daß in der weiteren Realisierung des Registers eine tragfähige Lösung dieses aus datenschutzrechtlicher Sicht wesentlichen Problems gefunden werden kann.

6.10 Bundeszentralregister – Novellierung des Bundeszentralregistergesetzes –

Bereits 1986 hat der Deutsche Bundestag die Bundesregierung aufgefordert, das Bundeszentralregistergesetz (BZRG) zu novellieren (s. auch 15. TB Nr. 4.4.2). Nachdem das BMJ einen ersten Referentenentwurf vorgelegt hatte, liegt nunmehr ein überarbeiteter Entwurf vom November 1996 vor. Durch meine frühzeitige Beteiligung konnten präzisierende Anregungen und Verbesserungsvorschläge in die Diskussion eingebracht werden.

So weist die Begründung auch zu dem jetzigen Entwurf die Berücksichtigung vieler meiner Verbesserungsvorschläge auf. Auch soll die praktisch lebens-

lange Eintragung einmal festgestellter Schuldunfähigkeit im Bundeszentralregister (§ 11 BZRG) entfallen und eine Regelung geschaffen werden, die dem Votum des Gutachters sowohl bei der Eintragung als auch – in Kombination mit einer Fristenregelung – bei einer Entfernung aus dem Register maßgebliche Bedeutung zuweist.

Darüber hinaus ist die Überarbeitung des Gesetzes in datenschutzrechtlich so bedeutsamen Bereichen vorgesehen wie der Auskunftserteilung für wissenschaftliche Forschungsvorhaben und der Protokollierungspflicht bezüglich aller erteilten Auskünfte und Hinweise durch die Registerbehörde.

6.11 Keine Resozialisierung bei der Verfahrenseinstellung unter Auflagen und Weisungen ?

Ohne Frage bedeutet § 153a StPO, der in bestimmten Fällen einer strafrechtlichen Schuld die „Einstellung des Verfahrens bei Erfüllung von Auflagen und Weisungen" zuläßt, nicht nur eine Entlastung der Rechtspflege; auch und gerade mit Blick auf die Interessen der Betroffenen verdient die Regelung eine positive Bewertung.

Eine andere Frage ist, welches Recht auf Resozialisierung ein Betroffener hat. Einer Eingabe habe ich entnommen, daß es der Praxis entspricht, in Strafsachen die Akten von nach § 153 a StPO eingestellten Verfahren auch dann noch beizuziehen, wenn die Tat sehr lange zurückliegt, um daraus Rückschlüsse zu ziehen und sie zur Überzeugungsbildung und Beweisführung zu verwenden. Dies geschieht sogar noch zu einem Zeitpunkt, zu dem – unterstellt, es wäre nicht zur Einstellung des Verfahrens nach § 153a StPO, sondern zu einer Verurteilung und somit zu einer Eintragung im Bundeszentralregister gekommen – die Informationen dem Verwertungsverbot des § 51 Abs. 1 BZRG unterlägen.

Ich habe daher dem BMJ empfohlen, darauf hinzuwirken, daß § 51 Abs. 1 BZRG entsprechend angewendet wird mit der Folge, den Betroffenen nach Zeitablauf nicht mehr das Geschehene vorzuhalten. Das Ministerium hat dem mit dem Argument widersprochen, das Vorhaltungs- und Verwertungsverbot für tilgungsreife Verurteilungen sei eingeführt worden, um den Verurteilten schließlich vom Strafmakel zu befreien. Damit habe der Gesetzgeber die gerichtliche Aufklärungspflicht allein im Hinblick auf das Resozialisierungsbedürfnis des Betroffenen eingeschränkt. Diese Voraussetzungen seien bei Einstellungen nach §§ 153 ff. StPO deshalb nicht gegeben, weil insoweit ein sicherer Schuldnachweis nicht erfolge bzw. nicht vorausgesetzt werde.

Diese Rechtsauffassung teile ich nicht, soweit es um § 153 a StPO geht: Informationen aus Verfahren, die nach dieser Vorschrift gegen Auflagen eingestellt wurden, müssen nach meiner Überzeugung dem Vorhaltungs- und Verwertungsverbot des § 51 BZRG oder zumindest einem vergleichbaren eingeschränkten Zugriff unterliegen, weil die Einstellung gegen Auflagen gemäß § 153 a StPO einen Schuldvorwurf voraussetzt. Den „Makel", von dem das BMJ spricht, und damit ein Resozialisierungsbedürfnis des Betroffenen sehe ich durchaus auch dann, wenn es um die Tatsache geht, Beschuldigter in einem nach § 153a StPO eingestellten Verfahren gewesen zu sein, das mit Auflagen und Weisungen abgeschlossen wurde. Ich vermag auch nicht einzusehen, daß bei gleichem Zeitablauf ein Geschehen, das zu einer Einstellung nach § 153a StPO geführt hat, noch herangezogen werden müßte, während hierauf dann verzichtet wird, wenn es zu einer Verurteilung gekommen ist. Ich habe das BMJ gebeten, seine Rechtsauffassung unter diesen Gesichtspunkten nochmals zu überdenken.

6.12 Bundesverfassungsgericht

Das Bundesministerium der Justiz hat einen Referentenentwurf für ein Sechstes Gesetz zur Änderung des Bundesverfassungsgerichtsgesetzes vorgelegt. Dieser enthält eine Reihe von datenschutzrechtlich bedeutsamen Bestimmungen.

6.12.1 Hörfunk- und Fernsehaufnahmen

Das Verbot von „Ton- und Fernseh-Rundfunkaufnahmen sowie Ton- und Filmaufnahmen zum Zwecke der öffentlichen Vorführung oder Veröffentlichung ihres Inhalts" nach § 169 Satz 2 GVG ist nach § 17 Bundesverfassungsgerichtsgesetz für das Bundesverfassungsgericht „entsprechend" anzuwenden. Zweck des unmittelbar an die Straf- und Zivilgerichtsbarkeit gerichteten Verbots im GVG ist der Schutz der Persönlichkeitsrechte aller Verfahrensbeteiligten und die Sicherung der Wahrheitsfindung im Prozeß. Den Prozeßparteien, den Zeugen und Sachverständigen sollen über die – bereits durch den Grundsatz der Öffentlichkeit geprägte – Prozeßsituation hinausgehende Belastungen erspart werden. Auch sollen die Prozeßbeteiligten während ihrer Aussagen nicht abgelenkt werden oder sich in Verhalten und Aussagen auf die Anwesenheit von Hörfunk und Fernsehen einstellen müssen. Dem Schutz des allgemeinen Persönlichkeitsrechts dient auch die Erstreckung des Verbots des § 169 Satz 2 GVG auf die Verkündung des Urteils.

In Verfahren vor dem Bundesverfassungsgericht sind die Prozeßbeteiligten jedoch, anders als in Zivil- und Strafverfahren weitgehend nicht in ihrer Privatsphäre betroffen, da sie vielfach als Prozeßvertreter, Organwalter oder als Personen des öffentlichen Lebens auftreten. Dies gilt jedenfalls für die klassischen Verfassungsstreitigkeiten wie z. B. für Verfahren zur abstrakten Normenkontrolle oder für Organstreitigkeiten, die – regelmäßig ohne Bezug zu einer Einzelperson – verfassungsrechtliche Rechtsfragen zum Gegenstand haben. Aber auch soweit Verfassungsbeschwerdeverfahren, die dem Rechtsschutz des einzelnen Bürgers dienen, mündlich verhandelt werden, ist dies grundsätzlich nicht anders. Auch in diesen Fällen stehen in der Regel allgemeine verfassungsrechtliche Fragen im Vordergrund.

Verfahren, die vor dem Bundesverfassungsgericht mündlich verhandelt werden, betreffen in aller Regel gerade Verfassungsfragen von erheblicher politischer Bedeutung, die zuvor nicht selten in der Öffentlichkeit mit großem Engagement ausführlich

diskutiert worden sind. Dem entspricht ein erhebliches Interesse der Öffentlichkeit an diesen Verfahren und den darin ergehenden Entscheidungen.

Diesen Überlegungen trägt der vorgenannte Gesetzentwurf Rechnung, der vorsieht, daß Hörfunk-, Fernseh- und Filmaufnahmen beim Bundesverfassungsgericht abweichend von § 169 Satz 2 Gerichtsverfassungsgesetz (GVG) in der mündlichen Verhandlung so lange zulässig sind, bis das Gericht die Anwesenheit der Beteiligten festgestellt hat. Außerdem sollen Aufnahmen bei der öffentlichen Verkündung von Entscheidungen zulässig sein. Zur Wahrung schutzwürdiger Interessen der Beteiligten oder Dritter sowie zur Sicherstellung eines ordnungsgemäßen Ablaufs des Verfahrens soll das Bundesverfassungsgericht die Aufnahmen oder deren Übertragung ganz oder teilweise ausschließen oder von der Einhaltung von Auflagen abhängig machen können.

Bei den Beratungen des Referentenentwurfs habe ich die Notwendigkeit des Schutzes des allgemeinen Persönlichkeitsrechts der an Verfahren beteiligten Privatpersonen deutlich hervorgehoben. Ein ausdrücklicher Hinweis auf das Persönlichkeitsrecht als zu schützendes Rechtsgut wurde daraufhin in die Begründung der entsprechenden Vorschrift des Entwurfs aufgenommen.

Da das Bundesverfassungsgericht nach dem Gesetzentwurf zur Wahrung der schutzwürdigen Interessen der Beteiligten oder Dritter die hierzu notwendigen Maßnahmen treffen kann, sind die ausreichenden Möglichkeiten vorgesehen, Beeinträchtigungen datenschutzrechtlicher Belange durch Hörfunk-, Fernseh- und Filmaufnahmen zu verhindern.

6.12.2 „Vorstücklisten" bei Verfahren über Verfassungsbeschwerden

Der Gesetzentwurf enthält u. a. auch bereichsspezifische Regelungen zur Aktenauskunft und Akteneinsicht. In diesem Zusammenhang ist eine dort vorgesehene Vorschrift zu erwähnen, wonach das Bundesverfassungsgericht in einem verfassungsgerichtlichen Verfahren zu den Akten gelangte personenbezogene Daten für ein anderes verfassungsgerichtliches Verfahren nutzen darf. Diese Regelung betrifft die Praxis des Gerichts, den in Verfassungsbeschwerdeverfahren geführten Akten eine sog. „Vorstückliste", d. h. eine Aufstellung aller von einem bestimmten Beschwerdeführer beim Bundesverfassungsgericht anhängig gemachten Verfahren vorzuheften. Sie soll im Hinblick auf die datenschutzrechtliche Zweckänderung durch die Verwendung von Daten aus einem Verfahren in einem anderen Verfahren auf eine gesetzliche Grundlage gestellt werden.

Aufgrund von Eingaben hatte ich mich bereits vor dem Gesetzentwurf mit den Vorstücklisten zu befassen. Im Rahmen meiner Erörterung dieser Frage mit dem Bundesverfassungsgericht vertrat dieses die Auffassung, daß es sich hierbei um eine Maßnahme der richterlichen Tätigkeit handelt, die daher nach § 24 Abs. 3 BDSG meiner Kontrolle und Bewertung entzogen ist. Dieser Auffassung habe ich mich angeschlossen. Im Zuge der Klärung dieser Frage wurde mir die Notwendigkeit dieser Liste erläutert. Das Erfordernis von Vorstücklisten ergibt sich aus der Besonderheit, daß in zahlreichen Eingaben an das Bundesverfassungsgericht von dem jeweiligen Antragsteller häufig nicht lediglich eine Beschwerde gegen einen konkreten Hoheitsakt erhoben wird. Vielmehr wird oft ein komplexer Lebenssachverhalt vorgetragen mit dem Ziel, sämtliche diesen Lebenssachverhalt betreffenden Handlungen der öffentlichen Gewalt (Gerichte, Behörden, Körperschaften u. a.) in ihrer Gesamtheit durch das Bundesverfassungsgericht überprüfen zu lassen. In diesen Fällen muß allein schon im Hinblick auf die Zuständigkeit innerhalb des Gerichts und seiner Senate festgestellt werden, ob bezüglich des vorgetragenen Sachverhalts bereits Verfahren desselben Beschwerdeführers anhängig sind oder waren. Diese Kennntnis ermöglicht dem Gericht, die Verfahren zu koordinieren und entsprechende sachleitende Verfügungen wie z. B. die Beiziehung von Akten früherer Verfahren zu treffen.

In einer Besprechung mit dem Bundesverfassungsgericht über die Vorstücklisten teilte mir dieses mit, es sei beabsichtigt, die Listen nicht mehr wie bisher bei den Verfahrensakten vorgeheftet zu lassen, die von anderen Verfahrensbeteiligten eingesehen werden können. Sie würden vielmehr in einem nicht der Akteneinsicht unterliegenden Sonderheft aufbewahrt. Ich begrüße dieses inzwischen bereits praktizierte Verfahren.

6.13 Justizmitteilungen aus gerichtlichen und staatsanwaltlichen Verfahren an andere Stellen

In meinem 15. Tätigkeitsbericht (Nr. 4.10) habe ich zum wiederholten Male auf die dringende Notwendigkeit einer gesetzlichen Grundlage für Spontanmitteilungen der ordentlichen Gerichtsbarkeit und der Staatsanwaltschaften aus den dortigen Verfahren an Gerichte, Behörden und sonstige öffentliche Stellen für andere Zwecke als die des Verfahrens hingewiesen. Nachdem das Gesetzgebungsverfahren für den damals vorliegenden Regierungsentwurf eines entsprechenden Justizmitteilungsgesetzes (JuMiG, BT-Drucksache 12/3199) in der abgelaufenen Wahlperiode nicht mehr abgeschlossen worden war, hat die Bundesregierung in dieser Legislaturperiode erneut einen Entwurf erstellt (BT-Drucksache 13/4709). Er berücksichtigt insbesondere auch die Einwendungen des Bundesrates gegenüber dem vorangegangenen Entwurf und liegt inzwischen dem Deutschen Bundestag vor.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat noch während der Vorbereitung des jetzigen Gesetzentwurfs vor allem zwei Punkte kritisiert und dies der Vorsitzenden der Konferenz der Justizministerinnen und Justizminister mitgeteilt.

Der Entwurf sieht zum einen nicht mehr vor, daß der Betroffene gleichzeitig mit einer Mitteilung an eine öffentliche Stelle des Bundes oder eines Landes grundsätzlich über deren Inhalt und den Adressaten dieser Mitteilung unterrichtet wird. Stattdessen soll der Betroffene – von einigen Ausnahmen abgesehen – nur auf Antrag hierüber Auskunft erhalten. Die Be-

denken der Datenschutzbeauftragten richten sich dagegen, daß das vorgesehene Gesetz nicht klar genug für den Einzelfall erkennen läßt, wann welche Daten an wen zu welchem Zweck übermittelt werden dürfen. Denn es sollen erst weitere Verwaltungsvorschriften erlassen werden, in denen die Gruppen der zulässigen Datenübermittlungen konkret festgelegt werden. Da das JuMiG noch ausfüllungsbedürftige Regelungen enthalten soll, würde die Festlegung der Verpflichtung, alle Betroffenen grundsätzlich jeweils von Amts wegen über den Inhalt und den Empfänger der Mitteilung zu unterrichten, eine verfassungsrechtlich gebotene Ergänzung der bisher vorgesehenen Bestimmungen bilden.

Der Regierungsentwurf sieht andererseits – abweichend vom Vorentwurf – nicht mehr vor, daß in bestimmten Fällen schwieriger Abwägungsfragen der Richter, der Staatsanwalt oder der Beamte des gehobenen Justizdienstes die Mitteilungen im Einzelfall anordnet. Entsprechende Regelungen sollen erst in die Verwaltungsvorschriften für die Durchführung des JuMiG aufgenommen werden. Da Justizmitteilungen erhebliche Auswirkungen für die Betroffenen haben können, sollte die Entscheidung über die Mitteilung – wenn im Einzelfall schwierige Abwägungsvorgänge nötig sind – besonders qualifizierten Bediensteten übertragen werden. Dies ergibt sich aus der Rechtsprechung des Bundesverfassungsgerichts im Volkszählungsurteil, wonach dem Recht auf informationelle Selbstbestimmung auch durch organisatorische Maßnahmen Rechnung zu tragen ist. Das Fehlen einer entsprechenden Regelung im derzeitigen Regierungsentwurf und die Regelung der Anordnungskompetenz lediglich in Verwaltungsvorschriften bedeuten einen deutlichen datenschutzrechtlichen Rückschritt gegenüber dem vorangegangenen Entwurf.

Ich habe diese Kritik im Rahmen weiterer Empfehlungen dem Rechtsausschuß des Deutschen Bundestages mitgeteilt, der inzwischen seine Beratungen zu dem Regierungsentwurf aufgenommen hat. Dort hoffe ich auf Unterstützung meines Anliegens.

6.14 Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich

Die Aufbewahrung von Akten und die Speicherung personenbezogener Daten in Dateien der Justiz über einen langen Zeitraum bedeuten für die Betroffenen im allgemeinen einen erheblichen Eingriff in ihr informationelles Selbstbestimmungsrecht. Als Beispiele sind Strafurteile und Strafbefehle, psychologische Gutachten – auch in Zivilsachen – sowie Ehescheidungsakten zu nennen.

Da es bislang an einer gesetzlichen Grundlage für die Aufbewahrung von Akten und die Speicherung personenbezogener Daten in Dateien der Justiz fehlt, hat sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder schon vor geraumer Zeit mit diesem Thema befaßt. Auf ihrer 49. Sitzung im Frühjahr 1995 verabschiedete sie eine Entschließung zu „Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich" **(s. Anlage 6)**. Darin wird auf die Notwendigkeit hingewiesen, die Aufbewahrung, Aussonderung und Vernichtung von Akten und die Speicherung personenbezogener Daten in Dateien in diesem Bereich nach den vom Bundesverfassungsgericht im Volkszählungsurteil (BVerfGE 65, S. 1 ff.) aufgestellten Grundsätzen für die Gerichte, Staatsanwaltschaften und Strafvollzugsbehörden gesetzlich zu regeln, wobei sich die Aufbewahrungsdauer am Recht auf informationelle Selbstbestimmung im allgemeinen und am Zweck der Speicherung im besonderen zu orientieren hat. Die Entschließung stellt außerdem fest, daß die Aufbewahrungsfristen zu vereinfachen und zu verkürzen sind. Ferner werden Einzelfragen wie der Beginn des Ablaufs der Aufbewahrungsfristen und die Behandlung von Akten und Datenträgern angesprochen, die Daten mehrerer beteiligter Personen enthalten.

Das BMJ hat zu der Entschließung mitgeteilt, es prüfe die Erforderlichkeit bereichsspezifischer Regelungen für die Aufbewahrung von Akten im Justizbereich. Diese Prüfung werde längere Zeit in Anspruch nehmen, da andere Vorhaben vorrangig betrieben werden müßten.

Ich bedauere diese Entscheidung des BMJ. Denn es sollte nicht übersehen werden, daß es sich im Hinblick auf die Sensibilität und die Vielzahl der in Rede stehenden Daten um eine vorrangige Aufgabe handelt, die grundsätzlich nicht zurückgestellt werden darf.

Dies habe ich in meiner Antwort an das BMJ dargelegt. Darüber hinaus habe ich ausgeführt, daß entsprechend den Vorgaben des Bundesverfassungsgerichts – neben dem zu beachtenden Erfordernis der Normenklarheit – um so weniger auf das nur allgemein gefaßte Bundesdatenschutzgesetz und die entsprechenden Datenschutzgesetze der Länder zurückgegriffen werden kann, je intensiver der Eingriff in das Persönlichkeitsrecht der Betroffenen ist. Somit bedarf es bereichsspezifischer gesetzlicher Grundlagen, während eine bereichsspezifische Interpretation der allgemeinen Datenschutzgesetze die erforderlichen eigene Regelung nicht ersetzen kann. Die allgemeinen Datenschutzgesetze kommen als ausreichende gesetzliche Grundlagen nur in Betracht, wenn es sich gewissermaßen um alltägliche Verarbeitungsvorgänge handelt, die üblicherweise keine besonderen Belastungen für die Betroffenen bringen, wie etwa die Verarbeitung von Daten im Rahmen der allgemeinen Verwaltung. Da es sich bei der Aufbewahrung von Daten im Justizbereich über lange Jahre jedoch um intensive Eingriffe in das Persönlichkeitrecht der Betroffenen handelt, kann die Notwendigkeit derartiger gesetzlicher Regelungen hier nicht in Frage stehen.

Auch habe ich gegenüber dem BMJ hervorgehoben, daß die Prüfung der Notwendigkeit bereichsspezifischer gesetzlicher Regelungen nicht daran hindern sollte, gleichzeitig die für die datenschutzrechtliche Praxis unmittelbar wichtige Frage der Dauer der derzeitigen Aufbewahrungsfristen anzugehen und diese Fristen unter Beachtung des Persönlichkeitsrechts der Betroffenen und des Zwecks der Speicherung kritisch zu überprüfen. Möglicherweise könnten viele Fristen – gegebenenfalls im Vorgriff auf spe-

zielle Regelungen – bei Berücksichtigung datenschutzrechtlicher Erfordernisse verkürzt werden.

Dabei ist mir bewußt, daß die Schaffung solcher Regelungen für Aufbewahrungsfristen und Dateiregelungen im Justizbereich einschließlich der Überprüfung der bisherigen Fristen eine umfangreiche Aufgabe bedeutet. Gerade deshalb sollte sie aber mit möglichst großem Nachdruck vorangebracht werden.

6.15 Bereichsspezifischer Datenschutz bei Notaren

Die Bundesregierung hat im März 1996 den Entwurf eines Dritten Gesetzes zur Änderung der Bundesnotarordnung und anderer Gesetze vorgelegt (BT-Drucksache 13/4184), um – neben anderen Zielen – im Anschluß an die Wiedervereinigung auch auf dem Gebiet des Berufsrechts der Notare die Rechtseinheit in Deutschland wiederherzustellen.

Bei der Vorbereitung des Regierungsentwurfs habe ich zu den datenschutzrechtlichen Bestimmungen gegenüber dem BMJ Stellung genommen. Dabei konnte ich erreichen, daß sich die Prüfung und Überwachung der Amtsführung der Notare durch die Aufsichtsbehörde nach § 93 Bundesnotarordnung auch auf die ordnungsgemäße Verarbeitung personenbezogener Daten in den Notariaten erstreckt. Demgegenüber war es mir nicht möglich, das BMJ für eine datenschutzgerechte Formulierung der beabsichtigten Änderung von § 1 Abs. 5 Rechtsberatungsgesetz zu gewinnen. Nach dem Regierungsentwurf dürfen Gerichte und Behörden grundsätzlich personenbezogene Daten, die für die Rücknahme oder den Widerruf der Erlaubnis oder zur Einleitung eines Rügeverfahrens „von Bedeutung sein können", der für die Entscheidung zuständigen Behörde übermitteln. Damit dürfen personenbezogene Daten auch dann übermittelt werden, wenn dies nicht für die Aufgabenerfüllung der die Daten empfangenden Behörde erforderlich ist. Der insoweit vorgesehene niedrigere Prüfungsmaßstab kann somit dazu führen, daß personenbezogene Daten in vielen Fällen unzulässig übermittelt werden. Ich werde den Punkt im weiteren Gesetzgebungsverfahren gegenüber dem Rechtsausschuß des Deutschen Bundestages aufgreifen.

7 Finanzwesen

7.1 Abgabenordnung immer noch ohne ausreichenden Datenschutz

Im 15. TB (Nr. 5.1) hatte ich über meine seit langem gegenüber dem BMF erhobenen Forderung berichtet, den bereichsspezifischen Datenschutz in der Abgabenordnung (AO) zu verbessern. Die darin in Abstimmung mit den Landesbeauftragten für den Datenschutz (LfD) angekündigten Vorschläge liegen inzwischen vor.

Dazu fand eine Besprechung mit Vertretern der obersten Finanzbehörden des Bundes und der Länder statt, an der neben Mitarbeitern meiner Dienststelle Vertreter des BMJ und der LfD Nordrhein-Westfalen teilnahmen, die den Vorsitz im Arbeitskreis „Steuerverwaltung" der Datenschutzbeauftragten des Bundes und der Länder innehat. Auf Wunsch des BMF wurde eingehend die Grundsatzfrage erörtert, ob die AO überhaupt aus datenschutzrechtlicher Sicht zu ändern oder zu ergänzen ist.

Für eine Änderung der AO spricht, daß

- die im wesentlichen am 1. Januar 1977 in Kraft getretene AO damals noch nicht unter Datenschutzgesichtspunkten formuliert worden ist, wie beispielsweise bereits die Verwendung des Wortes „dient" in § 30 Abs. 4 Nrn. 1 und 4 sowie in Abs. 6 Nr. 1 anstelle der datenschutzrechtlich zutreffenden Formulierung „erforderlich ist" zeigt;
- die AO bisher noch nicht gezielt unter Datenschutzgesichtspunkten überarbeitet worden ist, das BMF aber durch zwei frühere eigene Entwürfe eine Notwendigkeit hierfür bereits anerkannt hat;
- Korrekturbedarf bei verschiedenen Vorschriften, z. B. wegen Abweichungen von der üblichen Terminologie des Datenschutzes oder wegen zu wenig präziser Formulierung besteht;
- die AO der Ergänzung, z. B. um Regelungen über die Verarbeitung von Steuerdaten durch private Dritte, zum Auskunftsanspruch und zur Frage der Berichtigung oder Löschung von Daten bedarf, soweit nicht die Bestimmungen der allgemeinen Datenschutzgesetze gelten sollen.

In der sehr kontrovers verlaufenen Sitzung äußerten die Vertreter der obersten Finanzbehörden nahezu ausschließlich nachdrückliche Ablehnung gegenüber einer Änderung oder Ergänzung der AO und meinen hierzu vorgelegten Vorschlägen. Sie äußerten wiederholt die Befürchtung, hierdurch würden Eingriffsmöglichkeiten und für die Besteuerung erforderliche Verfahren beeinträchtigt. Der Hinweis, bei einer Änderung oder Ergänzung der AO sei stets ein Ausgleich zwischen den berechtigten Belangen der Steuerverwaltung und dem Persönlichkeitsrecht der Betroffenen zu finden und im überwiegenden öffentlichen Interesse erforderliche Eingriffsmöglichkeiten der Steuerverwaltung würden hierbei nicht eingeschränkt, blieb dagegen unbeachtet.

Eine Stellungnahme des BMF zu meinen Empfehlungen wird noch im Kreis der obersten Finanzbehörden des Bundes und der Länder abgestimmt. Im Interesse der Steuerpflichtigen wäre es sehr zu begrüßen, wenn trotz der bislang ablehnenden Haltung der Finanzverwaltung letztlich doch noch Einvernehmen über die Notwendigkeit datenschutzrechtlicher Verbesserungen in der AO erzielt werden könnte.

7.2 Automatisiertes Abrufverfahren für Steuerdaten

Der Bundesrat hatte das BMF wegen Bedenken der kommunalen Spitzenverbände gegen Regelungen der vorgesehenen Steuerdaten-Abruf-Verordnung gebeten, den hierfür vorgelegten Entwurf nochmals mit diesen zu erörtern (s. auch 15. TB Nr. 35 unter 4.). Die kommunalen Spitzenverbände hatten geltend gemacht, in der Verordnung würden die Bedürfnisse und technischen Möglichkeiten der Gemeinden nicht

ausreichend berücksichtigt. Nachdem eine vom BMF zur Vorbereitung der Gespräche mit den kommunalen Spitzenverbänden versuchte Abstimmung mit den obersten Finanzbehörden der Länder über eine mögliche Regelung für die Gemeinden ohne Erfolg geblieben ist, beabsichtigt das BMF nunmehr, gemeinsam mit den obersten Finanzbehörden der Länder eine einvernehmliche bundeseinheitliche „Steuerdaten-Abruf-Verwaltungsregelung" zu erreichen. Diese soll dann durch Erlaß des Bundes gegenüber dem Bundesamt für Finanzen und durch entsprechende Regelungen der Länder für die Landesfinanzbehörden umgesetzt werden. Hierfür wird der bisherige Text des Entwurfs für die Rechtsverordnung überarbeitet und vor allem der aktuellen technischen Entwicklung angepaßt. Die geplante Verwaltungsregelung bezieht sich allerdings nicht auf die Gemeinden.

Mit der Verwaltungsregelung wird aber zunächst wenigstens für den Bereich des Bundes und der Länder, in dem der Schwerpunkt der automatisierten Abrufe von Steuerdaten liegt, eine zwischen diesen unter Beteiligung der Datenschutzseite abgestimmte Regelung für die Praxis getroffen.

Abgesehen von der Frage der Rechtsform einer Verwaltungsregelung sehe ich darin eine gute und notwendige Maßnahme. Dieser Weg wurde im Hinblick auf die Rechtsauffassung des BMF und der obersten Finanzbehörden der Länder gewählt, wonach § 30 Abs. 6 Satz 1 Abgabenordnung (AO) bereits unmittelbar als Rechtsgrundlage für automatisierte Abrufe von Steuerdaten ausreiche. Gegen diese Ansicht habe ich – ebenso wie auch Landesbeauftragte für den Datenschutz – erhebliche Bedenken. Denn § 30 Abs. 6 Satz 1 AO reicht nicht als Rechtsgrundlage für den automatisierten Abruf von Steuerdaten aus. Diese Vorschrift entspricht für sich allein nicht dem Gebot der Normenklarheit, wonach der Bürger die Voraussetzungen und den Umfang der Beschränkungen seines Persönlichkeitsrechts durch den Umgang mit seinen Daten klar aus einer gesetzlichen Regelung erkennen können soll. Weitere gesetzliche Regelungen in Form der Rechtsverordnung nach § 30 Abs. 6 AO müssen hinzutreten.

Neben diesen Erwägungen ist für mich ebenso wesentlich, daß der erforderliche Schutz der Steuerdaten nicht davon abhängen kann, welche Stelle sie im Einzelfall abruft: Der datenschutzrechtliche Schutz muß bei allen Stellen, denen die Befugnis zum automatisierten Abruf eingeräumt wird, derselbe sein, d. h. beim Bundesamt für Finanzen, bei den Landesfinanzverwaltungen und ebenso bei den Gemeinden, soweit sie mit Steuerdaten umgehen. Dies bedeutet, daß die Gemeinden ebenfalls den für die Bundes- und Landesfinanzverwaltungen geltenden Standard einhalten müssen, wenn sie Steuerdaten automatisiert abrufen möchten.

Hierzu hat mir das BMF mitgeteilt, wenn der überarbeitete Text für eine Steuerdaten-Abruf-Verwaltungsregelung vorliege, beabsichtige es, an die kommunalen Spitzenverbände heranzutreten, um so zu versuchen, dem Anliegen des Bundesrates zu entsprechen, die Gemeinden in Regelungen über den automatisierten Abruf von Steuerdaten einzubeziehen.

Ich unterstütze dieses Vorhaben des BMF nachdrücklich. Wenn es gelingt, das Einverständnis der kommunalen Spitzenverbände zu erreichen, stünde dem Erlaß einer Rechtsverordnung nichts mehr im Wege.

Im 15. Tätigkeitsbericht (Nr. 35, dort Nr. 4) hatte ich auch auf die Zusage des BMF hingewiesen, eine Änderung des § 30 Abs. 6 AO in dem Sinne vorzuschlagen, daß auch den Rechnungsprüfungsbehörden ausdrücklich die Möglichkeit eingeräumt ist, Steuerdaten automatisiert abzurufen. Die Abgabenordnung wurde inzwischen im Rahmen des Jahressteuergesetzes 1996 mit dieser Ergänzung geändert.

7.3 „Gläsernes" Fahrtenbuch für steuerliche Zwecke ?

Mit dem Jahressteuergesetz 1996 ist die ertragsteuerliche Behandlung der privaten Kfz-Nutzung vereinfacht worden. Danach wird der private Nutzungsanteil eines zum Betriebsvermögen des Steuerpflichtigen gehörenden oder eines dem Arbeitnehmer vom Arbeitgeber zur Verfügung gestellten Kraftfahrzeugs pauschal in Höhe von monatlich 1 v. H. des Anschaffungswerts (inländischer Listenpreis) berücksichtigt. Die Pauschalregelung kann allerdings zu einer deutlichen Steuermehrbelastung führen, wenn das Fahrzeug nicht oder nur in geringem Umfang privat genutzt wird. Deshalb wurde dem Steuerpflichtigen eingeräumt, anstelle der Pauschalierung die auf Privatfahrten tatsächlich anfallenden Kosten anzusetzen. Nimmt er diese Möglichkeit in Anspruch, so muß er die für das Fahrzeug insgesamt entstehenden Aufwendungen belegen. Für den Nachweis der privaten und betrieblichen Fahrten hat er ein Fahrtenbuch mit folgenden Angaben zu führen:

- Datum und Kilometerstand zu Beginn und Ende der Geschäftsfahrt,
- Reiseziel mit Reiseroute,
- Reisezweck mit Angabe des aufgesuchten Geschäftspartners,
- jeweilige Abfahrts- und Ankunftszeit, soweit Verpflegungsmehraufwendungen geltend gemacht werden,
- Aufzeichnung der Privatfahrten im einzelnen, jedoch ohne Angabe des Reisewegs,
- kurzer Vermerk im Fahrtenbuch für die arbeitstäglichen Fahrten zwischen Wohnung und Arbeits- oder Betriebsstätte.

Zum Umfang der geforderten Fahrtenbuchaufzeichnungen sind mir mehrere Anfragen besorgter Bürger zugegangen, die um eine datenschutzrechtliche Prüfung baten. Die Betroffenen mußte ich darauf hinweisen, daß eine Bewertung der Erhebung und Verarbeitung personenbezogener Daten durch die Finanzämter in die Zuständigkeit der Landesbeauftragten für den Datenschutz fällt. Daneben habe ich das BMF um eine Stellungnahme zu der allgemeinen Frage gebeten, ob und ggf. warum derart umfangrei-

che Fahrtenbuchaufzeichnungen für Zwecke der Besteuerung erforderlich seien. Insbesondere erschien mir bedenklich, in das Fahrtenbuch Angaben über die aufgesuchten Geschäftspartner, also Dritte, aufzunehmen und dem Finanzamt zu übermitteln, wobei dies regelmäßig ohne deren Kenntnis geschehen dürfte. Außerdem habe ich auf die besonderen Probleme bei Patientenbesuchen von Ärzten im Hinblick auf die Wahrung des Arzt- bzw. Patientengeheimnisses hingewiesen.

Das BMF hat mir mitgeteilt, mit den obersten Finanzbehörden der Länder bestehe Einvernehmen darüber, daß zum Umfang der Fahrtenbuchaufzeichnungen berufsspezifischen Belangen jeweils Rechnung zu tragen sei. Bei Ärzten, die typischerweise Hausbesuche machen, reiche der Vermerk „Patientenbesuch" und die Ortsangabe, ohne die Namen der aufgesuchten Patienten anzugeben. Ähnliche Erleichterungen seien z. B. für Handelsvertreter und Taxifahrer vorgesehen. Insoweit konnten die datenschutzrechtlichen Bedenken also ausgeräumt werden.

Grundsätzlich halte die Finanzverwaltung aber die Angabe des aufgesuchten Geschäftspartners für den Nachweis der betrieblichen oder beruflichen Veranlassung der Fahrt für unverzichtbar, weil das Fahrtenbuch ohne diese Angaben keine schlüssige Dokumentation darstelle und als Beweismittel ungeeignet sei. Zudem sei meine Annahme, die im Fahrtenbuch enthaltenen Angaben würden regelmäßig den Finanzämtern übermittelt, unzutreffend. Die Fahrtenbücher würden „in der Regel ... (nur)" bei Betriebsprüfungen eingesehen, wobei die Daten durch das Steuergeheimnis nach § 30 Abgabenordnung ausreichend geschützt seien.

Die Argumente des BMF haben mich noch nicht vollständig überzeugt, und zwar einerseits im Hinblick auf die Notwendigkeit dieser Angaben allgemein und bezüglich des Verfahrens der Vorlage an das Finanzamt sowie andererseits auch und gerade wegen der fehlenden Transparenz für die betroffenen Dritten, die Geschäftspartner.

7.4 Kontrollmitteilungen

7.4.1 Regelmäßige Kontrollmitteilungen von Hauptzollämtern an Finanzämter

Im 15. TB (Nr. 5.2) habe ich darüber berichtet, daß **regelmäßige Kontrollmitteilungen** von Hauptzollämtern an Finanzämter in einigen Fällen nicht auf eine hinreichende gesetzliche Ermächtigung gestützt werden konnten und deshalb nach § 25 Abs. 1 BDSG zu beanstanden waren.

Im Berichtszeitraum habe ich bei mehreren Kontrollen von Hauptzollämtern festgestellt, daß diese Dienststellen bei der Weitergabe regelmäßiger Kontrollmitteilungen an Finanzämter sehr unterschiedlich verfahren:

- Bei einigen Ämtern wurde mir erklärt, alle Zahlungen – gleich welcher Höhe und aus welchem Rechtsgrund – würden stets dem für den Zahlungsempfänger zuständigen Finanzamt mitgeteilt.
- In anderen Fällen waren solche Mitteilungen nur für bestimmte Verfahren, z. B. Erstattung von Einfuhrumsatzsteuer in Höhe von mindestens 50,– DM, vorgesehen.
- Andere Hauptzollämter erklärten, sie würden keine regelmäßigen Kontrollmitteilungen erstatten.

Das BMF hat mir in seinen Stellungnahmen mitgeteilt, regelmäßige Kontrollmitteilungen seien grundsätzlich erforderlich, um eine gleichmäßige Besteuerung nach § 85 Abgabenordnung (AO) sicherzustellen. Um bewerten zu können, ob und ggf. für welche Verfahren regelmäßige Kontrollmitteilungen zulässig sind, hatte ich das BMF gebeten, mir mitzuteilen, für welche Arten von Zahlungen und ggf. ab welcher Höhe solche Mitteilungen aus fachlicher Sicht unverzichtbar seien, und welche Rechtsgrundlage ihnen jeweils zugrunde liege. Hierauf habe ich vom BMF noch keine ausreichende Antwort bekommen, obwohl ich nochmals dargelegt habe, daß eine abschließende Bewertung der Praxis von Kontrollmitteilungen voraussetzt, daß der Sachverhalt insoweit vollständig aufgeklärt wird. Ich hoffe auf eine baldige zufriedenstellende Antwort, auf deren Grundlage ich zu einer Regelung beitragen kann, die sowohl den fachlichen Erfordernissen der Finanzverwaltung als auch den datenschutzrechtlichen Belangen der Betroffenen gerecht wird.

7.4.2 Entwurf einer Zweiten Änderungsverordnung zur Mitteilungsverordnung

In diesem Zusammenhang ist auch der Entwurf einer Zweiten Änderungsverordnung zur **Mitteilungsverordnung** – MV – (vgl. auch 15. TB Nr. 5.11) bedeutsam, den mir das BMF im März 1996 übersandt hat. Der Entwurf sieht u. a. vor, für regelmäßige Mitteilungen von Zollbehörden an Landesfinanzbehörden über gewährte Ausfuhrerstattungen eine Rechtsgrundlage zu schaffen (§ 4a des Entwurfs). Das BMF hat dies unter Hinweis auf § 85 AO damit begründet, die Mitteilungen seien sowohl im Veranlagungsverfahren als auch bei Außen- und Betriebsprüfungen erforderlich, um festzustellen, ob die Empfänger diese Zahlungen als Betriebseinnahmen vollständig erfaßt haben.

Auf seine Begründung hin habe ich dem BMF zu bedenken gegeben, daß der mit einer regelmäßigen, spontanen Übermittlung personenbezogener Daten verbundene Eingriff in das Persönlichkeitsrecht der Betroffenen nach der Rechtsprechung des Bundesverfassungsgerichts im Volkszählungsurteil (BVerfGE 65, 1 ff.) – neben weiteren Voraussetzungen – nur dann zulässig ist, wenn er „zum Schutz öffentlicher Interessen unerläßlich ist." Durch den allgemeinen Hinweis auf § 85 AO allein sei das Erfordernis regelmäßiger Übermittlungen noch nicht nachgewiesen. Außerdem würde die beabsichtigte Regelung dem in § 93 Abs. 1 AO normierten Grundsatz zuwiderlaufen, die für die Besteuerung erheblichen Sachverhalte zunächst bei den Steuerpflichtigen selbst zu erheben.

Das BMF hat mir im Oktober 1996 erneut einen Entwurf für eine Zweite Verordnung zur Änderung der Mitteilungsverordnung zur Kenntnisnahme zugelei-

tet, der hinsichtlich der vorgeschlagenen Vorschrift über die Mitteilung von Ausfuhrerstattungen und der Begründung hierzu inhaltlich unverändert geblieben ist. Zu den von mir erhobenen Bedenken hat sich das BMF leider nicht geäußert, so daß ich nicht erkennen kann, aus welchen Gründen sie nicht berücksichtigt worden sind. Ich verfolge die Sache weiter.

7.5 Automatisiertes Vollstreckungssystem bei den Hauptzollämtern

Die den Vollstreckungsstellen der Hauptzollämter übertragenen Aufgaben werden seit mehreren Jahren mit dem Automatisierten Vollstreckungssystem (AVS) abgewickelt. In diesem Verfahren werden u. a. folgende Angaben über Vollstreckungsschuldner und Drittschuldner verarbeitet: Name, Vorname, Anschrift, Geburtsdatum, Geburtsort, Beruf und auftraggebende Stelle. Daneben enthält das Programm ein Freitextfeld „Notizen".

7.5.1 Umfang der Speicherung personenbezogener Daten

Bei zahlreichen Kontrollen von Hauptzollämtern habe ich festgestellt, daß Angaben in den **Datenfeldern „Geburtsort" und „Beruf"** zur Erfüllung der den Vollstreckungsstellen obliegenden Aufgaben regelmäßig nicht erforderlich sind. Meine Einschätzung wurde von den Mitarbeitern der besuchten Vollstrekkungsstellen bestätigt. Da eine Verarbeitung nicht benötigter personenbezogener Daten nach §§ 4 Abs. 1, 14 Abs. 1 BDSG unzulässig ist, habe ich das BMF gebeten, diese Felder aus der Datensatzstruktur des Systems zu entfernen. Nachdem die Frage der Erforderlichkeit mit dem BMF über längere Zeit erörtert wurde, konnte schließlich eine Kompromißlösung gefunden werden, derzufolge Angaben zum Geburtsort und zum Beruf künftig nur erhoben und gespeichert werden, wenn hierfür im Einzelfall ein unmittelbares Nutzungsbedürfnis besteht. Für bereits vorhandene Speicherungen ist bei der Bearbeitung eines Vollstreckungsfalls jeweils zu prüfen, ob die Angaben (weiterhin) benötigt werden; ggf. ist der Datenbestand insoweit zu bereinigen. Das BMF hat die betroffenen Dienststellen inzwischen entsprechend angewiesen.

Sog. **Freitextfelder**, wie das Feld „Notizen" im AVS, sind datenschutzrechtlich problematisch, weil hier ohne programmseitige Einschränkung Einträge vorgenommen werden können, die geeignet sind, das Persönlichkeitsrecht der Betroffenen unzulässig zu beeinträchtigen. Erfreulicherweise habe ich bei meinen Kontrollen insoweit keine Datenschutzverstöße festgestellt, da das Feld „Notizen" entweder unbenutzt blieb oder lediglich unbedenkliche Bearbeitungsvermerke enthielt. Um dieses Verfahren bei den Vollstreckungsstellen aller Hauptzollämter zu gewährleisten, habe ich das BMF gebeten, die Dienststellen entsprechend anzuweisen und insbesondere zu untersagen, daß in dieses Feld diskriminierende Angaben über Betroffene aufgenommen werden. Das BMF war jedoch zunächst der Ansicht, auch Einträge wie „Alkoholismus", „Neigung zur Gewalttätigkeit" oder „kriminelles Umfeld" seien zum Schutz der Vollziehungsbeamten erforderlich und damit zulässig. Nach weiteren Gesprächen mit dem BMF wurde auch hierzu Einvernehmen über ein datenschutzgerechtes Verfahren erzielt. Das BMF hat die Vollstreckungsstellen nunmehr angewiesen, in das Freitextfeld „Notizen" keine Daten einzutragen, die eine diskriminierende Wertung beinhalten oder zu solchen Wertungen verleiten könnten. Soweit objektive Feststellungen etwa zum Schutz der Vollziehungsbeamten bedeutsam sind, kann in das Feld „Notizen" ein Hinweis auf die Akten aufgenommen werden.

7.5.2 Organisatorische Datenschutzmaßnahmen

Bereits im September 1992 hatte ich dem BMF anläßlich einer Kontrolle mitgeteilt, die seinerzeit für das AVS ergangene „Vorläufige Anweisung Datenschutz und Datensicherung" sei ergänzungs- und verbesserungsbedürftig und Anregungen für eine Neufassung gegeben. Das BMF sagte mir daraufhin im Dezember 1992 eine entsprechende Neufassung zu. Bei weiteren Kontrollen von Hauptzollämtern habe ich über längere Zeit festgestellt, daß entgegen dieser und weiterer Zusagen und ungeachtet meiner mehrfachen Erinnerungen bei den besuchten Vollstreckungsstellen ohne eine Dienstanweisung mit den erforderlichen Datenschutzregelungen gearbeitet wurde. Daraufhin habe ich die Verarbeitung personenbezogener Daten im AVS ohne ausreichende Datenschutzvorkehrungen wegen Verstoßes gegen § 18 Abs. 1 und Abs. 2 Satz 3 BDSG im März 1995 nach § 25 Abs. 1 BDSG beanstandet und weiterhin – zuletzt im Oktober 1996 – nachdrücklich das Fehlen dieser Regelungen angemahnt. Ende November 1996 hat mir das BMF den Entwurf einer „Vorläufigen Dienstanweisung für den Einsatz des IT-Verfahrens AVS-APC bei den Vollstreckungsstellen der Hauptzollämter" (Stand: Juni 1996) übersandt. Die Prüfung dieses Entwurfs war bis Redaktionsschluß noch nicht abgeschlossen.

7.5.3 Technische Maßnahmen zur Datensicherheit

Ferner hatte ich gegenüber dem BMF die programmseitigen Schutzmechanismen für den Zugang zum AVS bemängelt. Das BMF wies hierzu auf die anstehende hard- und softwaremäßige Neukonzeption des Systems hin, mit der die aufgezeigten Mängel behoben werden könnten. Ob die Sicherheitsmängel inzwischen bei allen eingesetzten Systemen tatsächlich beseitigt worden sind, habe ich noch nicht vollständig nachprüfen können.

7.6 Einsatz tragbarer PC in der Zollverwaltung

Der Einsatz tragbarer Rechner – wie Laptops und Notebooks – bei Oberfinanzdirektionen und Hauptzollämtern für Zwecke der Betriebs- und Außenprüfung genügt nicht immer den datenschutzrechtlichen Anforderungen. Das BMF hat den Einsatz tragbarer Rechner zwar nur unter der Bedingung zugelassen, daß personenbezogene Daten – unabhängig von Speichermedium und Speicherort – ausschließlich verschlüsselt verarbeitet werden (vgl. 15. TB Nr. 30.2). Die Umsetzung dieser Vorgabe ge-

staltet sich jedoch sehr schwierig. So stand zwar bei den meisten von mir kontrollierten Stellen eine Offline-Verschlüsselungssoftware zur Verfügung, ordnungsgemäß eingesetzt wurde diese aber nur in wenigen Fällen. Die unverschlüsselte Speicherung personenbezogener Daten auf tragbaren Rechnern ist gemäß §§ 9 (mit Anlage) und 18 BDSG unzulässig und wurde deshalb von mir mehrfach beanstandet.

Auf meine Bitte, geeignete Maßnahmen zu treffen, die die Sicherheitslücken beim Einsatz tragbarer Rechner künftig schließen, hat mir das BMF mitgeteilt, alle betroffenen Stellen seien auf die besondere Problematik der Speicherung personenbezogener Daten auf tragbaren Rechnern hingewiesen worden. Nachfolgende Kontrollen haben leider ergeben, daß bei einem Großteil der geprüften Geräte personenbezogene Daten nach wie vor unverschlüsselt verarbeitet wurden. Die Mitarbeiter führten hierfür im wesentlichen folgende Gründe an:

- Die Bedienung des bereitgestellten Verschlüsselungsprogrammes sei benutzerunfreundlich. Die Verschlüsselung einer Datei sei zu aufwendig, die Vorgaben für die einzugebenden Schlüssel seien zu komplex. Ein Austausch von Dateien mit anderen Mitarbeitern sei nicht möglich.
- Ein Teil der benutzten Rechner (Rechner mit 286er und 386SX-Prozessoren) sei zu langsam. Die Verschlüsselung einer Datei dauere bis zu 30 Minuten. Dadurch werde der weitere Arbeitsfortgang erheblich behindert.
- Fehlbedienungen des Programms führten dazu, daß Dateien nicht mehr entschlüsselt werden könnten.
- Die Schlüsselverwaltung sei zu aufwendig und nötige dazu, die Schlüssel an irgendeiner Stelle zu notieren.
- Eine Schulung in der Bedienung des Programms habe nicht oder nicht ausreichend stattgefunden.

Nachdem ich wiederholt auf die Beschwerden der Mitarbeiter hingewiesen habe, hat das BMF erfreulicherweise das Verfahren geändert. Nunmehr sollen alle neuen tragbaren Rechner mit einer geeigneten Online-Verschlüsselung ausgestattet werden, so daß der Aufwand der Bearbeiter für die Verschlüsselung und die Schlüsselverwaltung entfällt. Die älteren Geräte sollen sukzessive ersetzt werden. Bis alle Geräte ausgetauscht bzw. umkonfiguriert worden sind, werden die Dienststellen das bisherige Verschlüsselungsverfahren anwenden. Diese Verfahrensänderung entspricht meinen datenschutzrechtlichen Forderungen.

7.7 Sicherheitsmängel bei Zollzahlstellen

Bei den Zahlstellen der Hauptzollämter werden die Kassengeschäfte im Zahlstellen-DV-Verfahren automatisiert abgewickelt. Dabei werden auch besonders schutzbedürftige personenbezogene Daten verarbeitet (z. B. aus Straf- oder Bußgeldverfahren, aus Abgabenbescheiden oder aus Vollstreckungsaufträgen), die zudem überwiegend einem besonderen Amtsgeheimnis (Steuer- oder Sozialgeheimnis) unterliegen.

Bereits vor längerer Zeit hatte ich im Rahmen von Kontrollen den Zugangsschutz des Zahlstellen-DV-Verfahrens bemängelt. Für den Programmzugang ist zwar die Eingabe einer Benutzerkennung und eines Paßwortes erforderlich. Die Benutzerkennung ist aber für alle Mitarbeiter identisch, so daß eine eindeutige Zuordnung des Programmzugangs oder eines Zugangsversuchs hierdurch nicht möglich ist. Außerdem akzeptiert das Programm sehr einfach gestaltete Paßwörter und läßt beliebig viele Fehlversuche zu, ohne das Terminal zu sperren. Daher war es meinen Mitarbeitern möglich, auch ohne Kenntnis eines Paßworts bereits nach wenigen Versuchen in die Anwendung zu gelangen und auf die gespeicherten Daten zuzugreifen.

Das Bundesministerium der Finanzen (BMF) hatte mir bereits im Jahre 1992 angekündigt, bei den Zahlstellen werde ein neues DV-Verfahren ohne die aufgezeigten Mängel eingerichtet. Bei weiteren Kontrollen von Hauptzollämtern habe ich jedoch festgestellt, daß die Zahlstellen noch über mehrere Jahre mit dem alten Zahlstellen-DV-Verfahren arbeiteten. Die Sicherheitsmängel waren nicht beseitigt worden. Auch die angekündigte Umstellung auf das neue Verfahren war bei diesen Ämtern auf absehbare Zeit nicht vorgesehen. Daraufhin habe ich die Verarbeitung personenbezogener Daten im Zahlstellen-DV-Verfahren ohne wirksame Benutzerkontrolle und ohne ausreichenden Zugangsschutz beanstandet (Verstoß gegen die §§ 9 i.V. m. Nrn. 1 und 4 der Anlage und 18 Abs. 2 Satz 3 BDSG).

Das „Neue IT-unterstützte Zollzahlstellenverfahren (NIZZA)" ist mir nunmehr bei einem Hauptzollamt im Probebetrieb vorgestellt worden. Außerdem hat mir das BMF seine zeitliche Planung für den Einsatz des Verfahrens NIZZA schriftlich mitgeteilt. Danach sollen alle Zollzahlstellen bis Mitte 1998 den Echtbetrieb mit dem neuen Verfahren aufgenommen haben.

Unter Abwägung der Angemessenheit gebotener Schutzmaßnahmen nach § 9 Satz 2 BDSG und insbesondere im Hinblick darauf, daß die Räumlichkeiten der Zollzahlstellen schon aus Gründen der Kassensicherheit gegen unbefugten Zutritt besonders geschützt sind, habe ich Verständnis für den Zeitplan der Verfahrensumstellung. Dabei gehe ich davon aus, daß – soweit die Zahlstellen noch mit dem alten Verfahren arbeiten – alle übrigen Sicherheitsmaßnahmen strikt eingehalten werden.

7.8 Unzulässige Speicherung von Ferngesprächsdaten bei Hauptzollämtern

Bei mehreren Hauptzollämtern habe ich festgestellt, daß die Erfassung und Speicherung von Ferngesprächsdaten durch die eingesetzten Telekommunikationsanlagen (TK-Anlagen) nicht immer den datenschutzrechtlichen Vorgaben der Dienstanschlußvorschriften entsprach. So wurden z. B. bei einer TK-Anlage neben den erforderlichen und damit zulässigen Daten auch die Uhrzeit und die Dauer der Gespräche erfaßt. Darüber hinaus wurden auch bloße

Gesprächsversuche registriert, bei denen keine Verbindung zustande kam. Bereits nachdem die für Privatgespräche vorgesehene persönlichen Kennziffer eingegeben wurde, erzeugte die TK-Anlage einen Datensatz, obwohl anschließend kein Gespräch geführt wurde. Eine Erfassung und Speicherung solcher Daten ist weder für die Abrechnung privater noch für die Haushaltsmittelkontrolle dienstlicher Gespräche erforderlich. Sie stellt damit einen unzulässigen Eingriff in das Persönlichkeitsrecht der Mitarbeiter dar.

Die zuständige Oberfinanzdirektion hatte die datenschutzrechtlichen Mängel bei der Gesprächsdatenerfassung zwar bereits erkannt und sich um Abhilfe bemüht, konnte aber wegen der mit einer Änderung der TK-Anlage verbundenen Kosten keine datenschutzgerechte Lösung herbeiführen.

Ich habe das BMF gebeten, für diesen und ggf. vergleichbare Fälle geeignete Maßnahmen zu treffen, die eine rechtswidrige Erfassung und Speicherung von Gesprächsdaten künftig verhindern. Darauf hat mir das BMF mit dem Hinweis, die beanstandete TK-Anlage sei bereits vor Inkrafttreten der Datenschutzbestimmungen in den Dienstanschlußvorschriften in Betrieb genommen worden, zunächst mitgeteilt, von einer Umrüstung der TK-Anlage werde wegen der zu erwartenden Kosten aus Haushaltsgründen abgesehen. Hierzu habe ich gegenüber dem BMF folgende Einwände erhoben:

- Die unzulässig gespeicherten Daten sind aus Datenschutzsicht hochsensibel und unterliegen dem Schutz des Artikel 10 GG (Fernmeldegeheimnis).
- Eine Erhebung und Verarbeitung nicht erforderlicher personenbezogener Daten ist nach §§ 13 Abs. 1 bzw. 4 Abs. 1 i.V. mit 14 Abs. 1 BDSG unzulässig. Dabei ist es unerheblich, ob die technischen Voraussetzungen, die zu den rechtswidrigen Speicherungen führen, bei Inkrafttreten der geänderten Dienstanschlußvorschriften bereits vorlagen.
- Eine Abwägung im Hinblick auf die aufwandsbezogene Angemessenheit erforderlicher Maßnahmen nach § 9 Satz 2 BDSG kommt nur hinsichtlich der Sicherung **zulässiger** Speicherungen in Betracht. Die Behebung eines rechtswidrigen Zustands ist unabhängig davon in jedem Fall erforderlich.

Erfreulicherweise hat das BMF nunmehr die Dienststellen seines Geschäftsbereichs angewiesen, TK-Anlagen, mit denen Daten über private Gesprächsverbindungen aufgezeichnet werden, deren Erfassung nach den Dienstanschlußvorschriften jedoch unzulässig ist, entsprechend umzurüsten. Bis zur Umrüstung solcher Anlagen sind die betroffenen Dienststellen gehalten, die automatisierte Erfassung der privaten Verbindungsdaten außer Betrieb zu setzen und die für die Gebührenabrechnung benötigten Angaben manuell zu verarbeiten. Mit dieser Regelung hat das BMF einen Weg gefunden, meinen Empfehlungen trotz der schwierigen Haushaltslage weitgehend zu folgen.

7.9 Inter- und supranationale Zusammenarbeit

7.9.1 Datenschutzklausel für Doppelbesteuerungsabkommen

Nachdem mit dem BMF Einvernehmen darüber erzielt werden konnte, die vom BMI federführend erarbeitete Datenschutzklausel als Muster für Doppelbesteuerungsabkommen der Bundesrepublik Deutschland mit anderen Staaten zu verwenden (vgl. 15. TB Nr. 5.4), bin ich durch das Sekretariat des Finanzausschusses des Deutschen Bundestags darüber unterrichtet worden, daß bei Verhandlungen über solche Abkommen mit einigen Staaten Probleme im Hinblick auf die Datenschutzklausel aufgetreten sind. Unter Hinweis darauf, daß die Datenschutzklausel weitgehend mit dem deutschen (§ 30 AO) und internationalen Steuergeheimnis (Artikel 26 OECD-Muster-Doppelbesteuerungsabkommen) übereinstimmt, hat das BMF nach dem einzuschlagenden Verfahren gefragt, wenn die deutsche Datenschutzklausel vom jeweiligen Verhandlungspartner teilweise oder ingesamt nicht akzeptiert wird. Es hat in diesem Zusammenhang geltend gemacht, die „sachfremde Materie des Datenschutzes" sorge regelmäßig für Konflikte bei den Verhandlungen.

In einer Sitzung des Finanzausschusses im Oktober 1996 habe ich deutlich gemacht, das über 30 Jahre alte Musterabkommen der OECD werde heutigen datenschutzrechtlichen Anforderungen nicht mehr gerecht. Außerdem müsse künftig nach Artikel 25 der EG-Datenschutzrichtlinie beim Datenverkehr mit Drittländern ein angemessenes Schutzniveau sichergestellt werden. Dem für die Datenschutzklausel federführenden BMI habe ich darin zugestimmt, daß für den grenzüberschreitenden Austausch personenbezogener Informationen auf zusätzliche Datenschutzregeln (wie z. B. zum Auskunftsanspruch der Betroffenen) in einer Datenschutzklausel insoweit verzichtet werden könne, als sie im nationalen Recht des Vertragspartners bereits vorhanden seien. Bei Verhandlungen mit Staaten, deren innerstaatliches Recht keine oder nur unzureichende Datenschutzvorkehrungen vorsehe, müsse hingegen die Wahrung des Persönlichkeitsrechts der Betroffenen durch entsprechende Regelungen im Text des Abkommens sichergestellt werden. Die Datenschutzklausel solle als Rahmen verstanden werden, der eine sachgerechte, unterschiedliche Ausgestaltung des Abkommens mit dem jeweiligen Vertragspartner zulasse.

Nachdem der Finanzausschuß der Bundesregierung aufgegeben hatte, die strittigen Punkte mit den beteiligten Ressorts und mir zu klären, hat das BMF diesem nach Erörterung mit BMI, BMJ und mir mitgeteilt, zur Behebung der Schwierigkeiten bei der Umsetzung der Datenschutzklausel in Doppelbesteuerungsabkommen sei folgende praxisnahe Regelung gefunden worden:

- Auch bei künftigen Vertragsverhandlungen wird zunächst grundsätzlich an der Datenschutzklausel festgehalten.
- Die in der Klausel vorgesehenen Regelungen über die Zweckbindung und die weitere Übermittlung der Daten an andere Stellen wird in Artikel 26 des

OECD-Musterabkommens übernommen, soweit dort noch nicht enthalten.

- Nach Umsetzung der EG-Datenschutzrichtlinie können für den innergemeinschaftlichen Datenaustausch über den Richtlinienstandard hinausgehende Anforderungen nicht gestellt werden. Übermittlungen personenbezogener Daten in Drittländer sind grundsätzlich nur zulässig, wenn der Empfängerstaat ein angemessenes Schutzniveau gewährleistet. Hiervon darf nur abgewichen werden, wenn im Einzelfall ein besonders wichtiges öffentliches Interesse einen Datenaustausch gebietet.
- Im übrigen kann die Datenschutzklausel bereits jetzt unter Berücksichtigung des Datenschutzstandards des Verhandlungspartners und der Bedeutung des Abkommens hinsichtlich einzelner Regelungen abgeändert werden.

Da ich gegenüber dem BMF seit 1993 die Auffassung vertrete, daß für einzelne Abkommen differenzierte Datenschutzvorkehrungen sachgerecht sein können, habe ich gegen jeweils notwendige Anpassungen der Datenschutzklausel keine grundsätzlichen Bedenken. Ich würde es allerdings begrüßen, wenn das BMF mich bei auftretenden Problemen frühzeitig beteiligte.

7.9.2 Zollzusammenarbeit mit der Russischen Föderation

Bereits im 14. TB (Nr. 6.7.3) hatte ich über datenschutzrechtliche Mängel in Verträgen über die Zollzusammenarbeit mit Staaten außerhalb der EU (u. a. mit der Russischen Föderation) berichtet. Zu dem inzwischen ratifizierten Vertrag mit der Russischen Föderation über die Zusammenarbeit und die gegenseitige Unterstützung der Zollverwaltungen hatte das BMF angeboten, die vertraglich vorgesehenen Datenschutzregeln in den Durchführungsbestimmungen zu präzisieren (vgl. 15. TB Nr. 35, dort 7.). Für die Vorbereitung der deutsch-russischen Expertenbesprechungen zur Abstimmung dieser Durchführungsbestimmungen hatte mich das BMF um Formulierungsvorschläge gebeten. Dabei habe ich dem BMF u. a. empfohlen,

- den Begriff „personenbezogene Daten" zu definieren,
- die vertraglichen Voraussetzungen für eine Übermittlung personenbezogener Daten enger zu interpretieren,
- klarzustellen, von welchen Behörden Betroffene Auskunft über zu ihrer Person gespeicherte Daten erhalten können, und
- vorzusehen, daß übermittelte personenbezogene Daten gelöscht werden, wenn ihre weitere Speicherung zu dem Zweck, für den sie übermittelt worden sind, nicht mehr erforderlich ist.

Das BMF hat meine Anregungen aufgegriffen und mich an der Erörterung der Datenschutzfragen mit der russischen Delegation beteiligt. Diese legte einen Text vor, der u. a. vorsieht, die zentralen und regionalen Behörden festzulegen, die aufgrund des Vertrags Direktbeziehungen zueinander unterhalten. Damit würden die Adressaten für Auskunftsersuchen hinreichend bestimmt. Außerdem sollen die übermittelten Informationen nach dem russischen Vorschlag durch die nationale Gesetzgebung in den Partnerstaaten geschützt werden. Zu meinen weitergehenden Empfehlungen war die russische Seite damit einverstanden, daß die deutsche Delegation ihr für die weiteren Verhandlungen einen modifizierten und ergänzten Gegenvorschlag unterbreitet. Das BMF hat mir zugesagt, in seinem Textvorschlag

- eine Definition des Begriffs „personenbezogene Daten" vorzusehen,
- die von mir vorgeschlagene Löschungsregelung aufzunehmen, und
- klarzustellen, daß die Vertragspartner ein angemessenes Schutzniveau im Sinne des Artikels 25 Abs. 1 der EG-Datenschutzrichtlinie gewährleisten müssen.

Ich hoffe, daß die Bemühungen des BMF zu einer Nachbesserung der Datenschutzregelungen führen werden. Weitere Unterstützung habe ich angeboten.

7.9.3 Betrugsbekämpfung bei der EG

Angesichts der durch den Europäischen Rechnungshof festgestellten erheblichen finanziellen Verluste für den Gemeinschaftshaushalt infolge von Unregelmäßigkeiten und Betrug, insbesondere im Bereich der Subventionen, hatte der Europäische Rat bereits vor einigen Jahren eine Arbeitsgruppe „Verbesserung der Kontrollmittel" eingesetzt, um die rechtlichen Grundlagen für eine wirksame Betrugsbekämpfung zu erweitern.

Die Ergebnisse der Arbeitsgruppe führten u. a. zur Verabschiedung einer Verordnung (EG) Nr. 1469/95 des Rates vom 22. Juni 1995 über Vorkehrungen gegenüber bestimmten Begünstigten der vom EAGFL (Europäischer Ausrichtungs- und Garantiefonds für die Landwirtschaft), Abteilung Garantie, finanzierten Maßnahmen (ABl. EG Nr. L 145/1 vom 29. Juni 1995) – sog. „Schwarze Liste" –, zu deren Durchführung die Verordnung (EG) Nr. 745/96 der Kommission vom 24. April 1996 (ABl. EG Nr. L 102/15 vom 25. April 1996) ergangen ist. Die bereits vorhandenen Kontroll- und Sanktionsmechanismen sind dadurch um eine Regelung ergänzt worden, die gegenüber Marktbeteiligten, bei denen das Risiko der Unzuverlässigkeit besteht, verstärkte Kontrollen und ggf. zusätzliche Maßnahmen (Aussetzung der Zahlungen oder Ausschluß von bestimmten Geschäften) vorsieht. Nach der Verordnung sollen Marktbeteiligte, die vorsätzlich oder grob fahrlässig eine Unregelmäßigkeit begangen haben, oder gegen die aufgrund konkreter Tatsachen bereits amtliche oder gerichtliche Feststellungen getroffen worden sind, identifiziert und unverzüglich allen zuständigen Behörden der Mitgliedstaaten sowie der Kommission zur Kenntnis gebracht werden. Zu diesem Zweck wird in den Mitgliedstaaten und bei der Kommission ein Identifikations- und Mitteilungssystem („Schwarze Liste") eingerichtet.

Das BMF hat mich an den Arbeiten zu den Verordnungen bereits in einem frühen Stadium beteiligt.

Meine datenschutzrechtlichen Empfehlungen hat das BMF aufgegriffen und in die Verhandlungen eingebracht. Sie sind weitgehend in die Verordnungstexte aufgenommen worden. Artikel 4 der Verordnung 1469/95 sieht – neben dem Anhörungs- und Beschwerderecht des Marktbeteiligten – vor, daß

- die Vertraulichkeit der ausgetauschten Informationen gewährleistet und das Berufsgeheimnis gewahrt wird,
- die innerstaatlichen Rechtsvorschriften des empfangenden Mitgliedstaats und entsprechende für die Gemeinschaftsorgane geltende Bestimmungen anzuwenden sind,
- die Daten grundsätzlich nur den zuständigen Personen mitgeteilt und nur für die in der Verordnung vorgesehenen Zwecke verwendet werden dürfen und
- außerdem die Datenschutzbestimmungen der Regelung über die gegenseitige Amtshilfe in Zoll- und Agrarfragen, deren Entwurf für eine Neufassung umfassende Datenschutzvorkehrungen enthält (vgl. 15. TB Nr. 5.6), gelten.

Darüber hinaus bestimmt Artikel 11 der Durchführungsverordnung 745/96, daß

- neben den Bestimmungen des Artikels 4 der Verordnung 1469/95 die Gewährleistungen der EG-Datenschutzrichtlinie (s. o. Nr. 2.1) angewendet werden,
- die Mitgliedstaaten und die Kommission die erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherheit treffen, womit insbesondere ein Zugang Unbefugter zu den Daten verhindert werden soll,
- die Mitgliedstaaten oder die Kommission nach den einzelstaatlichen bzw. gemeinschaftsrechtlichen Regelungen für Schäden haften, die einer Person durch eine unrechtmäßige Verarbeitung personenbezogener Daten entstehen.

Damit konnte für die Verarbeitung der sensiblen personenbezogenen Daten nach den genannten Verordnungen ein erfreulich hohes Schutzniveau normiert werden.

Für die Praxis ergibt sich allerdings ein Problem daraus, daß nach Artikel 2 der Durchführungsverordnung Marktbeteiligte nur in die „Schwarze Liste" aufzunehmen sind, wenn die ihnen vorgeworfene Unregelmäßigkeit allein oder zusammen mit anderen innerhalb eines Jahres festgestellten Unregelmäßigkeiten einen Betrag von über 100 000 ECU betrifft oder betreffen könnte. Diese Regelung macht es erforderlich, Aufzeichnungen über betroffene Marktbeteiligte zu führen, um zu überwachen, ob der Schwellenwert innerhalb des Jahreszeitraums überschritten wird. Das BMF teilt zwar meine Auffassung, daß die Daten Marktbeteiligter, bei denen dies nicht der Fall ist, nach Ablauf des einjährigen Überwachungszeitraums grundsätzlich gelöscht werden müßten. Es hat aber dargelegt, daß eine sofortige Löschung nach Ablauf der Jahresfrist nicht in Betracht gezogen werden kann, weil sich auch später – innerhalb der gesetzlichen Verjährungsfrist – ergeben könnte, daß ein Marktbeteiligter mit einer (weiteren) Unregelmäßigkeit, die in den Überwachungszeitraum fällt, den Schwellenwert überschritten hat. Aufgrund meiner Gespräche mit dem BMF wird eine Lösung angestrebt, die programmtechnisch und organisatorisch sicherstellen soll, daß ein Zugriff auf Daten Marktbeteiligter solange ausgeschlossen bleibt, wie der Schwellenwert nicht erreicht ist.

Mit der ebenfalls von der Arbeitsgruppe „Verbesserung der Kontrollmittel" vorbereiteten Verordnung (EURATOM, EG) Nr. 2185/96 des Rates vom 11. November 1996 betreffend die Kontrollen und Überprüfungen vor Ort durch die Kommission zum Schutz der finanziellen Interessen der Europäischen Gemeinschaften vor Betrug und anderen Unregelmäßigkeiten (ABl. EG Nr. L 292/2 vom 15. November 1996) wird die Kommission ermächtigt, für alle Tätigkeitsbereiche der Gemeinschaften Kontrollen und Überprüfungen vor Ort durchzuführen, um Unregelmäßigkeiten aufzudecken. Auch insoweit hat mich das BMF frühzeitig beteiligt. Die im Verordnungstext (Artikel 8) enthaltenen Datenschutzvorkehrungen über die Wahrung des Amtsgeheimnisses, die Anwendung nationaler bzw. gemeinschaftsrechtlicher Datenschutzbestimmungen, die Zulässigkeit der Offenbarung und die Zweckbindung der Daten halte ich insbesondere auch wegen der Bezugnahme auf die EG-Datenschutzrichtlinie für ausreichend.

Nach dem mir vom BMF übersandten Entwurf für Durchführungsbestimmungen (Vademekum der Kommission) zu dieser Verordnung sollen die Überprüfungen und Kontrollen vor Ort von der **Betrugsbekämpfungseinheit der Europäischen Kommission (UCLAF)** durchgeführt werden. Ich habe zu diesem Entwurf bereits schriftlich Stellung genommen und angeregt, den Umgang mit den erhobenen Daten zu normieren und dabei z. B. die Verpflichtung zur Löschung von Daten zu regeln, die unter Verstoß gegen nationale oder gemeinschaftsrechtliche Vorschriften gewonnen worden sind. Das BMF hat zugesagt, mich weiter zu beteiligen.

Um eine risikoorientierte Betrugsbekämpfung nach den gemeinschaftsrechtlichen Vorgaben sicherzustellen, wurde beim Hauptzollamt Hamburg-Jonas eine **Zentralstelle Betrugsbekämpfung (ZEB)** eingerichtet. Sie nimmt ihre Aufgaben derzeit in folgenden Arbeitsgruppen wahr:

- „Allgemeine Betrugsbekämpfung", insbesondere zur IT-unterstützten Vorbeugung und zur Aufdeckung von Risiken,
- „Risikoanalyse" zur Entwicklung einer Risikostrategie für Warenkontrollen bei den Zollstellen aufgrund der Verordnungen (EWG) Nr. 386/90 (sog. Kontrollverordnung) und Nr. 3122/94 (sog. Kriterienverordnung) mit dem IT-Verfahren „ARGUS",
- „Betriebsprüfungen" zur Planung, Unterstützung und Koordinierung von Prüfungen nach der Verordnung (EWG) Nr. 4045/89 (sog. Buchprüfungsverordnung; Verfahren „PROFIT" bei den Prüfungsstellen),

– „Unregelmäßigkeiten" zur Durchführung des mit der Verordnung (EWG) Nr. 595/91 eingerichteten Informationssystems (Verfahren „IRENE").

Für die Durchführung der Verordnung (EG) Nr. 1469/95 („Schwarze Liste") und ggf. aufgrund weiterer Rechtsakte der Gemeinschaft zur Betrugsbekämpfung kann die Bildung weiterer Arbeitsgruppen bei der ZEB erforderlich werden. Die mit der Verarbeitung und Nutzung personenbezogener Daten durch die ZEB verbundenen datenschutzrechtlichen Fragen habe ich mit der ZEB und dem BMF erörtert. Grundsätzliche Bedenken zur Konzeption und zur Praxis haben sich bislang nicht ergeben.

7.9.4 EG-Amtshilfe-Gesetz und Verbrauchsteuer-Kontrollverfahren

Im 15. TB (Nr. 5.5) hatte ich über die beabsichtigte Ergänzung der Richtlinie 92/12/EWG über das allgemeine System der Verbrauchsteuern (sog. „System-Richtlinie") um eine Regelung für innergemeinschaftliche Stichprobenkontrollen im Verbrauchsteuerbereich berichtet. Meine Empfehlungen zu dem damit verbundenen Informationsaustausch hinsichtlich des Umfangs der Datenerhebung, der Zweckbindung ihrer Verarbeitung und der Anwendung der Datenschutzvorschriften der EG-Amtshilfe-Richtlinie sowie des EG-Amtshilfe-Gesetzes (EG-AH-G) sind mit der Richtlinie 94/74/EG des Rates vom 22. Dezember 1994 (ABl. EG Nr. L 365/46 vom 31. Dezember 1994) in den neu eingefügten Artikel 15b der System-Richtlinie aufgenommen worden. Damit haben die Bemühungen des BMF zu einem datenschutzgerechten Ergebnis geführt.

Darüber hinaus hat das BMF anläßlich einer Änderung der Übermittlungsregelung für Informationen aus der Datenbank über Steueraussetzungsverfahren nach § 2a EG-AH-G (vgl. hierzu 14. TB Nr. 6.6) meinem weiteren datenschutzrechtlichen Anliegen entsprochen und sichergestellt, daß in diesem Verfahren übermittelte Daten – falls erforderlich – unverzüglich berichtigt, gesperrt oder gelöscht werden müssen (vgl. Neufassung des § 4 Abs. 3 Satz 2 EG-AH-G durch Artikel 6 des Gesetzes zur Änderung von Verbrauchsteuergesetzen und des EG-Amtshilfe-Gesetzes vom 12. Juli 1996 – BGBl. I S. 962, 976).

Mit dem Jahressteuergesetz 1997 hat das EG-Amtshilfe-Gesetz eine weitere Änderung erfahren. Die Neufassung des § 2 Abs. 3, der zum regelmäßigen innergemeinschaftlichen Datenaustausch über steuerliche Sachverhalte ermächtigt, sah u. a. zunächst vor, daß hierunter auch Angaben über *„Einkünfte und Vermögen, die für die Besteuerung durch einen Mitgliedstaat* **von Interesse** *sein könnten", fallen. Mein Vorschlag, den Text dahingehend zu präzisieren, daß die Informationen nur ausgetauscht werden dürfen, wenn „deren Kenntnis für die Besteuerung durch einen Mitgliedstaat* **erforderlich** *sein könnte", wurde übernommen. Außerdem wurde auf Anregung des BMJ § 3 Abs. 1, der die Grenzen der Auskunftserteilung regelt, um eine Vorschrift ergänzt, wonach Auskünfte nicht erteilt werden dürfen, „wenn ein angemessener Datenschutz in dem Mitgliedstaat nicht gewährleistet ist".*

Von einer Änderung des Bestätigungsverfahrens nach § 2a Abs. 6 EG-AH-G, zu der mich das BMF um Stellungnahme gebeten hatte (vgl. 15. TB Nr. 5.5), ist nach Auskunft des BMF entsprechend meiner Empfehlung abgesehen worden. Es bleibt daher bei der datenschutzkonformen Regelung, die eine Offenbarung von Informationen über eine bloße Bestätigung der Richtigkeit bereits bekannter Daten hinaus ausschließt.

Inzwischen habe ich mich bei der **Zentralstelle Verbrauchsteuer-Auskunftsersuchen**, die mit bundesweiter Zuständigkeit beim Hauptzollamt Stuttgart eingerichtet ist, über die tatsächlichen Abläufe des Verbrauchsteuer-Kontrollverfahrens „SEED" (System for the Exchange of Excise Data) informieren können. Grundsätzliche datenschutzrechtliche Bedenken haben sich dabei nicht ergeben. Offen gebliebene Einzelfragen, insbesondere zu den erforderlichen technisch-organisatorischen Datenschutzmaßnahmen, sind jedoch noch zu klären.

7.9.5 EG-Drittlandsabkommen – Amtshilfe im Zollbereich –

In Protokollen über die Amtshilfe im Zollbereich wird u. a. der Austausch personenbezogener Informationen im Rahmen der von der EG mit Drittstaaten abgeschlossenen Zusammenarbeitsabkommen geregelt. Über damit verbundene Datenschutzfragen habe ich im 14. (Nr. 6.7.2) und 15. TB (Nr. 5.7) berichtet. Das BMF hat mich zwischenzeitlich an den Vorarbeiten zu den Amtshilfeprotokollen mehrerer Abkommen beteiligt, wobei in den neueren Texten (z. B. für die Abkommen mit der **Schweiz, Kanada und Mexiko**) folgende Datenschutzregelungen vorgesehen werden konnten:

– Der Begriff „personenbezogene Daten" wird definiert.

– Die übermittelten Informationen sind vertraulich und unterliegen dem Schutz, den das nationale Recht des Empfängerstaates hierfür vorsieht.

– Personenbezogene Daten dürfen nur ausgetauscht werden, wenn der empfangende Staat ein Schutzniveau gewährleistet, das dem des übermittelnden Staats mindestens gleichwertig ist.

– Die erhaltenen Informationen dürfen nur für die Zwecke des jeweiligen Abkommens verwendet werden. Eine Verwendung für andere Zwecke bedarf der vorherigen, schriftlichen Zustimmung des liefernden Staats und unterliegt ggf. dessen Auflagen.

Diese Bestimmungen sollen vor allem sicherstellen, daß die Regelungen über die Amtshilfe im Zollbereich den Voraussetzungen des Artikels 25 Abs. 1 der EG-Datenschutzrichtlinie entsprechen, wonach die Übermittlung personenbezogener Daten in ein Drittland im Regelfall nur zulässig ist, wenn dieses Drittland ein angemessenes Schutzniveau gewährleistet.

Ende 1996 hat mich das BMF darauf hingewiesen, daß bei dem Zollunterstützungsabkommen der EG mit den **USA** ein Problem mit der vorgesehenen Regelung über eine zweckändernde Verwendung übermittelter Informationen aufgetreten ist. Die USA

haben darauf bestanden, in den Text des Abkommens eine Klausel aufzunehmen, die sie ermächtigt, die empfangenen Daten zu offenbaren oder zu verwenden, soweit ihr innerstaatliches Recht hierzu verpflichtet. Mit dieser Ergänzung würde die im Abkommen vorgesehene datenschutzgerechte Regelung über eine zweckändernde Verwendung der Daten (siehe oben, letzter Anstrich) stark relativiert. In der zuständigen Arbeitsgruppe des Rates gab es daher zunächst auch einen breiten Konsens unter den Mitgliedstaaten, den Vorschlag der USA nicht zu übernehmen. In weiteren Verhandlungen haben die USA ihren Vorschlag dahingehend präzisiert, daß die Ausnahmevorschrift nur für Strafverfahren gelten soll und angeboten, dies in einer Erklärung zum Ratsprotokoll festzuhalten. In Abstimmung mit dem BMJ habe ich dem BMF u. a. vorgeschlagen, die von den USA erläuterte Einschränkung in den Text des Abkommens zu übernehmen. Das BMF hat diesen Vorschlag aufgegriffen und im Rat eingebracht. Mangels ausreichender Unterstützung durch andere Mitgliedstaaten hat der Rat nach Mitteilung des BMF der von den USA geforderten Klausel inzwischen zugestimmt. Die Protokollerklärung der USA soll mit dem Abkommenstext veröffentlicht werden. In dieser Erklärung wird festgelegt, daß

- die Ausnahmeklausel nur für Strafverfahren anzuwenden ist, und
- die übermittelnde Vertragspartei entsprechend dieser Vorschrift in angemessener Frist über die beabsichtigte Verwendung benachrichtigt wird und eine solche Verwendung ablehnen oder an Bedingungen knüpfen kann.

Außerdem ist zu dieser Ausnahmeregelung eine gemeinsame Protokollerklärung von Rat und Kommission vorgesehen, die ausdrücklich klarstellt, daß die den USA zugestandene Lösung *„unter keinen Umständen einen Präzedenzfall für die künftige Annahme ähnlicher Abkommen darstellt."*

Dieses Ergebnis kann aus datenschutzrechtlicher Sicht nicht befriedigen, zumal nicht ersichtlich ist, was die USA bewogen hat, sich einer Änderung des Abkommenstextes im Sinne ihrer Protokollerklärung zu verschließen. Gleichwohl ist dem BMF für seine intensiven Bemühungen um eine Verbesserung des Abkommenstextes zu danken. Aufgrund der unmißverständlichen Erklärung von Rat und Kommission erwarte ich, daß die akzeptierte Ausnahmevorschrift nicht zu einer Verschlechterung des Datenschutzstandards bei künftigen Regelungen über die Amtshilfe im Zollbereich im Rahmen von EG-Drittlandsabkommen führen wird.

7.10 Datenabgleich mit Freistellungsaufträgen soll Mißbrauch von Arbeitslosenhilfe aufdecken helfen

Im 14. TB (Nr. 6.2) hatte ich über das mit dem Zinsabschlaggesetz eingeführte Kontrollverfahren zur Zinsbesteuerung und insbesondere über die bei dieser Regelung erreichte strikte Zweckbindung für die Verwendung der Daten aus Freistellungsaufträgen berichtet. Bisher durfte das Bundesamt für Finanzen diese Angaben nur verwenden, um die rechtmäßige Inanspruchnahme des Sparer-Freibetrags und des Pauschbetrags für Werbungskosten zu überprüfen (§ 45 d Abs. 2 EStG; vgl. 14. TB Nr. 6.2).

Mit dem Jahressteuergesetz 1997 wurde das Einkommensteuergesetz um eine Regelung für einen Datenabgleich zur Bekämpfung von Leistungsmißbrauch ergänzt (§ 45d Abs. 3 EStG). Danach darf das Bundesamt für Finanzen nunmehr der Bundesanstalt für Arbeit auf deren Ersuchen die Anzahl der von einem Leistungsbezieher erteilten Freistellungsaufträge zur Überprüfung des bei der Arbeitslosenhilfe zu berücksichtigenden Vermögens mitteilen. In Verbindung mit der Auskunftspflicht des Empfängers von Arbeitslosenhilfe nach § 60 SGB I und der mit dem Jahressteuergesetz 1997 neu begründeten Auskunftspflicht von Banken und gleichartigen Instituten, die Guthaben führen oder Vermögensgegenstände aufbewahren (§ 144 Abs. 2 und 5 Arbeitsförderungsgesetz), sollen Vermögen des Betroffenen, die beim Bezug von Arbeitslosenhilfe anzurechnen sind, wirkungsvoller ermittelt werden.

In seiner Entschließung zu meinem 14. Tätigkeitsbericht hat sich der Deutsche Bundestag auch zur Frage des Datenabgleichs geäußert. Er hat die Bundesregierung aufgefordert, jeweils zu prüfen, ob ein vorgesehenes Datenabgleichsverfahren im Interesse des Gemeinwohls zur Erreichung eines konkreten Zieles erforderlich und verhältnismäßig ist. Außerdem sollten die Bürger auf Datenabgleiche zu Verhinderung von Leistungsmißbrauch durch Hinweise in Vordrucken und Merkblättern sowie in Veröffentlichungen aufmerksam gemacht werden. Das BMA hat mir bereits zugesagt, im Merkblatt für Antragsteller auf Arbeitslosenhilfe künftig auch darauf hinzuweisen, daß Auskünfte über die Anzahl von ihnen erteilter Freistellungsaufträge eingeholt werden können.

Ob das neu eingeführte Datenabgleichsverfahren zur Verhinderung von Leistungsmißbrauch tatsächlich erforderlich und verhältnismäßig ist, kann letztlich erst anhand der damit in der Praxis gewonnen Erfahrungen festgestellt werden. Diese lagen bei Abschluß der Arbeit an diesem Bericht noch nicht vor.

7.11 TLG Treuhand Liegenschaftsgesellschaft mbH: „Totalerfassung" der Liegenschaften

Schwerpunkt eines Kontrollbesuches bei der TLG war das Projekt „Totalerfassung" des Treuhand-Liegenschaftseigentums. Dieses Projekt hatte zum Ziel, das unmittelbare und mittelbare Treuhandeigentum – deutlich unterschieden nach privatisierten und noch nicht privatisierten Liegenschaften – festzustellen, um auf diese Weise auch dubiose Eigentumsübergänge aufzudecken. Mit der Durchführung hatte die TLG die „Arbeitsgemeinschaft Totalerfassung", gebildet aus der Gesellschaft zur Erfüllung vermessungstechnischer Aufgaben mbH, Köln, und der Industrieanlagen Betriebsgesellschaft mbH, Ottobrunn, betraut. Um Datenschutzbelangen Rechnung zu tragen, wurde zunächst mit flurstückbezogenen Daten der Landesvermessungs- und Katasterämter und dem eigenen Datenbestand eine „Flurstücksgenese" erstellt. Der sich hieraus ergebende Bestand an potentiellem Treuhand-Eigentum wurde dann in

einem zweiten Schritt mit aktuellen Eigentümerdaten aus den automatisierten Liegenschaftsbüchern verglichen. Mit dieser Verfahrensweise war gewährleistet, daß die Daten der Eigentümer nur hinsichtlich der Flurstücke zur Verfügung gestellt wurden, für die der TLG ein berechtigtes Interesse im liegenschaftsrechtlichen Sinn zustand.

8 Wirtschaft und Informationsgesellschaft

Bei den Netzen für multimediale Informations- und Kommunikationsdienste wird allgemein ein erhebliches Wirtschaftswachstum erwartet. Die Einzelheiten dieser neuen Märkte sind heute erst in Umrissen erkennbar. Es steht jedoch schon fest, daß Interaktivität und das Reagieren auf individuelle Anforderungen wesentliche Aspekte des Erfolges sein werden.

Dabei wäre es ein Verstoß gegen das Persönlichkeitsrecht, wenn durch das Registrieren und Verknüpfen der Daten über die geäußerten Informations-, Unterhaltungs- und Kommunikationswünsche wesentliche Aspekte des menschlichen Verhaltens für Dritte verfügbar würden. Zum anderen müssen auch die Anbieter ihren Kunden verläßlich garantieren, daß sie deren Privatsphäre nicht verletzen, weil die Kunden, die sich dieses Risikos mehr und mehr bewußt werden, sonst von den Angeboten nicht oder nur zögerlich und mit Zurückhaltung Gebrauch machten.

Schon im Beschluß der G 7-Staaten zum Information Highway gehört daher Datenschutz ganz selbstverständlich zum Ordnungsrahmen dazu:

> *„Protecting privacy and personal data alongside the safeguarding of plurality of opinion play an essential role in maintaining citizens' confidence in the information society and thereby encourage user participation and strengthen competition and market acess."*

(Aus dem Abschlußdokument des G 7-Treffens vom 25./26. Februar 1995 in Brüssel)

8.1 Informations- und Kommunikationsdienste-Gesetz

Die Privatisierung verschiedener Monopolbereiche – wie etwa der Telekommunikation – im Zuge der europaweiten Öffnung der Märkte und die rasante technologische Entwicklung computergestützter Systeme zwingen dazu, Rahmenbedingungen für den Informations- und Kommunikationssektor zu entwikkeln. Das BMBF hat mich an der Erarbeitung des „Informations- und Kommunikationsdienste-Gesetzes" (IuKDG) von Anfang an beteiligt, das lange unter dem Arbeitstitel „Multimediagesetz" auch in der Öffentlichkeit diskutiert wurde.

Die Unsicherheit der Bürger gegenüber den neuen Informationstechnologien ist immer noch groß. Berichte über die „anarchischen" Zustände im Internet schrecken viele ab. Viele wirtschaftlich orientierte Anbieter haben ebenso wie die beteiligten Bundesressorts erkannt, daß der Datenschutz das Vertrauen des Nutzers in die Vertraulichkeit und Verläßlichkeit der neuen Dienste erheblich mitbestimmt. Datenschutz wirkt damit unmittelbar akzeptanzfördernd und ist als „Erfolgsfaktor" dieses Wirtschaftsbereiches nicht zu unterschätzen. Datenschutz, Verbraucherschutz und IT-Sicherheit werden immer deutlicher als ständige Begleiter der Bürger auf dem Weg in die Informationsgesellschaft erkannt.

Der von der Bundesregierung am 11. Dezember 1996 beschlossene Entwurf des IuKDG trägt diesen Anforderungen in dem als Artikel 2 eigens geschaffenen Teledienstedatenschutzgesetz (TDDSG) weitgehend Rechnung. Besonders positiv ist, daß die Regelungen nicht einen status quo festschreiben, sondern, z. B. durch die grundsätzliche Forderung nach Datenminimierung und nach differenziertem Umgang mit Bestandsdaten einerseits und Nutzungs- und Abrechnungsdaten andererseits, die weitere Entwicklung sinnvoll fördern. Nachdem es im Rahmen einer intensiven Abstimmung gelungen ist, in dem Entwurf des IuKDG und im Entwurf eines Staatsvertrages der Länder für den Bereich Mediendienste für parallele Sachverhalte fast wortgleiche Regelungen vorzuschlagen, ist mit einer Verabschiedung noch im Jahr 1997 zu rechnen.

Zu meinem Bedauern wurde ohne Not die zunächst im Gesetzentwurf vorgesehene Möglichkeit gestrichen, ein „Datenschutzaudit" zu etablieren, welches die Anbieter zu besonderen Bemühungen um den Datenschutz und damit zu kundenfreundlichen Angeboten animieren sollte. Den Verzicht auf diesen Anreiz halte ich für unklug, denn der typische Nutzer der neuen Dienste ist den Statistiken zufolge überwiegend ein mündiger und anspruchsvoller Kunde, der sich sehr genau informiert, wer ihm einen soliden Umgang mit seinen Daten garantieren kann. Das Fehlen eines „Qualitätssiegels", wie es durch das Audit möglich wäre, verhindert oder erschwert die Orientierung, die für eine breite Akzeptanz notwendig ist und die den massenhaften Einstieg in die Informationsgesellschaft überhaupt erst ermöglicht. Die Bundesrepublik verzichtet damit zum Teil auf einen künftig bedeutenden Standortvorteil im internationalen Wettbewerb – nämlich ihren durch Erfahrung gewonnen Vorsprung beim Datenschutz.

Bedenken habe ich gegen eine sehr weitgehende Verpflichtung der Diensteanbieter, den Polizeibehörden und Nachrichtendiensten auf Verlangen die Bestandsdaten ihrer Kunden zu übermitteln. Derart weitreichende Zugriffsbefugnisse auf personenbezogene Daten bei privaten Dienstleistern halte ich für unverhältnismäßig und mit dem bloßen Hinweis auf die entsprechende Vorschrift im Telekommunikationsgesetz nicht für ausreichend begründet. Es droht, daß mehr Schaden als Nutzen gestiftet wird, wenn man diesen entstehenden Markt durch Auflagen belastet, deren tatsächlicher Nutzen, also echter Ermittlungserfolg der Behörden, in einem schlechten Verhältnis dazu steht, daß alle Nutzer und Anbieter sich permanent weitreichenden Überwachungsbefugnissen unterworfen sehen.

8.1.1 Einführung einer Elektronischen Unterschrift – Signaturgesetz

Der Entwurf des Informations- und Kommunikationsdienste-Gesetzes (IuKDG) enthält in Artikel 3 – dem **Signaturgesetz (SigG)** – auch gesetzliche Regelungen zur sogenannten Digitalen Signatur.

Mit der „digitalen Signatur" können Dokumente, die in elektronischer Form vorliegen, so gesichert werden, daß sowohl eine Manipulation des Inhalts und der Urheberschaft des Dokumentes erkannt, als auch – bei entsprechender Verfahrensgestaltung – die Urheberschaft unbestreitbar festgestellt werden kann. Hierzu wird aus dem Originaldokument – automatisch und unter Verwendung einer speziellen mathematischen Funktion (Hash-Funktion) – eine „Kurzfassung" (Hash-Wert) des Dokumentes berechnet. Der Hash-Wert wird mit dem „**geheimen Schlüssel**" (s. u.) des Autors verschlüsselt; das so entstandene Kryptat stellt den Authentikator des Dokumentes dar. Anschließend kann das Dokument zusammen mit dem Authentikator ungeschützt – z. B. über ein offenes Netz – an den Empfänger übertragen werden (s. Abb. 2).

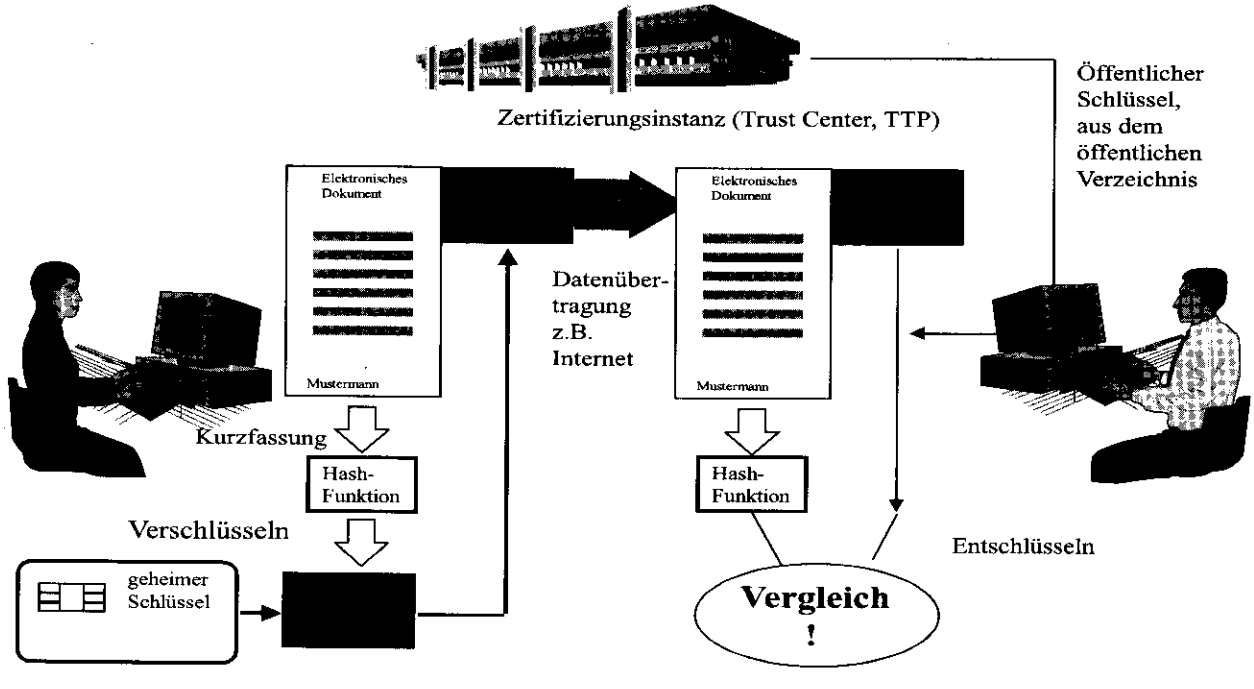
Der Empfänger prüft die Echtheit und Unversehrtheit des Dokumentes dadurch, daß er zunächst ebenfalls den Hash-Wert des empfangenen Dokumentes berechnet, sodann den Authentikator mit dem „**öffentlichen Schlüssel**" (s. u.) des Absenders entschlüsselt und das Entschlüsselungsergebnis mit dem von ihm erzeugten Hash-Wert des Dokumentes vergleicht. Wenn beides übereinstimmt, steht fest, daß weder das Dokument noch der Authentikator während der Übertragung verändert wurden: Der Authentikator des Dokumentes kann nur mit dem geheimen Schlüssel des Autors erzeugt und nur mit seinem öffentlichen Schlüssel geprüft werden. Der Empfänger kann deshalb auch sicher sein, daß nur der Besitzer des geheimen Schlüssels – also der „echte" Autor – den Authentikator des betreffenden Dokumentes berechnen konnte.

Soll die **Urheberschaft** eines Dokumentes nachgewiesen werden, benötigt man den öffentlichen Schlüssel und dessen zweifelsfreie Zuordnung zu einer (natürlichen oder juristischen) Person, das sog. **Zertifikat**. Das Zertifikat wird von einer vertrauenswürdigen Zertifizierungsinstanz („Trusted Third Party", Trust-Center) erteilt. Dort kann auch der öffentliche Schlüssel, der Name des Besitzers und beispielsweise seine Zeichnungsberechtigung hinterlegt werden. Ist der geheime Schlüssel durch sichere Zugangsmechanismen – PIN, Paßwort oder biometrisches Merkmal, z. B. Fingerabdruck – auf einer Chipkarte sicher gespeichert, besteht die Möglichkeit, mit diesem Verfahren eine zweifelsfreie Feststellung der Urheberschaft eines elektronisch vorliegenden Dokumentes zu treffen.

Die „digitale Signatur" basiert auf einem asymmetrischen Verschlüsselungsverfahren. Asymmetrische Verschlüsselungsverfahren sind dadurch gekennzeichnet, daß sie zur Ver- und Entschlüsselung nicht den gleichen Schlüssel benötigen, sondern immer ein Schlüsselpaar. Die beiden Schlüssel dieses Schlüsselpaares sind zwar verschieden, müssen aber zueinander passen. Der erste Schlüssel – er wird auch als **geheimer Schlüssel** bezeichnet – läßt sich von einem Unbefugten selbst dann nur äußerst schwer „nachmachen", d. h. berechnen, wenn der zweite Schlüssel – der **öffentliche Schlüssel** – bekannt ist. Dies ist zwar theoretisch nicht ausgeschlossen, bisher sind jedoch keine Verfahren bekannt, die das in sinnvollen Zeiträumen leisten. Einen erheblichen Einfluß auf die Berechenbarkeit hat die Schlüssellänge: Bei der derzeit angewandten Schlüssellänge von mehr als 512 Bit ergeben sich praktisch keine

Abbildung 2

Digitale Signaturen



Möglichkeiten, einen unbekannten Schlüssel zu berechnen. Der geheime Schlüssel ist – als Zeichenfolge – typischerweise auf einer Chipkarte gespeichert, die ihrerseits gegen unbefugte Benutzung geschützt ist (PIN, Paßwort usw.). Das Verfahren der „digitalen Signatur" sieht vor, daß der öffentliche Schlüssel – z. B. in einem (öffentlichen) Verzeichnis – bekannt gegeben wird, während der geheime Schlüssel nur dem Autor zur Verfügung steht. Der geheime Schlüssel dient zum Erzeugen von elektronischen Signaturen, mit dem öffentlichen Schlüssel können diese überprüft werden.

Datenschutzrechtliche Fragen treten bei dem skizzierten Verfahren besonders bei der Erhebung der Daten eines Teilnehmers, bei der Speicherung des geheimen Schlüssels, bei der Sperrung von öffentlichen Schlüsseln und in Verbindung mit den Telekommunikationsnetzen und den darin entstehenden Verbindungsdaten auf. Der vorliegende Entwurf enthält aus datenschutzrechtlicher Sicht hierzu entsprechende Regelungen. Richtungsweisend scheinen mir insbesondere die Regelungen zum Recht auf die „**Einrichtung eines Pseudonyms**" zu sein. Durch diese Technik kann der Umfang der personenbezogenen Daten, die über eine Person im Rahmen der Abwicklung des Geschäftsverkehrs über Telekommunikationsverbindungen zwangsläufig anfallen, in erheblichem Maße reduziert werden. Die Erstellung von Benutzerprofilen, die Überwachung des Einkaufverhaltens sowie die direkte Bewerbung durch Firmen ist hierdurch nahezu ausgeschlossen.

Für bedenklich halte ich allerdings die Einbeziehung von biometrischen Merkmalen, wie sie derzeit noch vorgesehen ist, ohne daß eine strikte Zweckbindung dieser Merkmale sichergestellt ist.

8.2 Datennetze

Die Behörden des Bundes nutzen Datennetze zur Zeit überwiegend zur internen Kommunikation und zur Öffentlichkeitsarbeit. Anlässe zur Datenschutzberatung im Einzelfall haben sich daraus bisher kaum ergeben. Es ist insoweit ein Sonderfall, daß die Bundeswehruniversität Hamburg der Verlockung dieser technischen Möglichkeit so sehr erlag, daß sie personenbezogene Daten ihrer Mitarbeiter mit Paßfoto, aber ohne deren Einwilligung, im WorldWide-Web veröffentlichte. Das BMVg hat aufgrund meiner Hinweise für Abhilfe gesorgt und bestätigt, daß die Datensätze der Mitarbeiter gelöscht wurden, die im Rahmen einer nachträglichen Befragung in eine solche Präsentation nicht einwilligten.

Auch wenn die Nutzung von Datennetzen durch Bundesbehörden außer Sicherheitsfragen (s. u. Nr. 8.2.3) – noch – keine besonderen datenschutzrechtlichen Probleme aufwirft, so zeigt doch die allgemeine Entwicklung, daß auch für den planmäßigen Umgang mit Daten in Netzen Datenschutzregeln erforderlich sind.

8.2.1 Verkehrsregeln auf der Datenautobahn

Der bisher in den Datennetzen, wie z. B. im Internet, praktizierte Verhaltenskodex – die „Netiquette" – reicht heute als Regelungselement nicht mehr aus. Erpressungsversuche von Firmen im Cyberspace, das Sammeln aller Daten über die Netzaktivitäten eines Nutzers und das Anbieten von Nutzerprofilen, das Anbieten von Kinderpornographie und das Auftauchen extremistischer Gewaltpropaganda machen deutlich, daß die Selbstregelungskräfte der Netzgemeinde (bei fortschreitend vereinfachtem Zugang zu den Netzen) nicht mehr genügen. Wenngleich die enormen Entwicklungspotentiale dieser Technologie, vor allem auch in wirtschaftlicher Hinsicht, nicht eingeengt oder gar ausgebremst werden sollen, so sind doch einige Regeln über die Grenzen der Netzfreiheit nötig, z. B. zum Verbraucherschutz und zum Datenschutz, um das für eine positive Entwicklung notwendige Vertrauen der Teilnehmer zu erreichen. Für den Datenschutz besonders wichtig ist dabei das Prinzip der „Datenarmut", d. h. die Beschränkung von Datenerhebung und -verarbeitung auf das unbedingt notwendige Maß. Wo keine Daten anfallen, kann kein Mißbrauch geschehen. Dadurch trägt der Datenschutz unmittelbar zu Rationalisierungseffekten beim Einsatz von Datenverarbeitungssystemen bei: Weniger Daten heißt auch weniger Kosten!

Sinnvoll ist hier auch die Forderung im Entwurf des TDDSG, dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung auch anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Die Kunden sollen diese Medien so frei und so unbeobachtet wie irgend möglich nutzen können, denn das fördert die kreativen und konstruktiven Entwicklungsmöglichkeiten, die gerade diese Technologie bietet. Dazu gehört auch, daß nicht nur technisch, sondern auch nach den sonstigen Bedingungen die Netze weltweit sind. Es kann auf die Dauer nicht dabei bleiben, daß Verbraucherschutz, Datenschutz und die Verantwortung für Inhalte an den nationalen Grenzen enden, entweder, weil im Ausland anderes Recht gilt, oder weil es praktisch unmöglich ist, sein Recht im Ausland durchzusetzen. Für die daher jetzt beginnende internationale Diskussion über international abgestimmte Regeln und damit auch über den Datenschutz bei Telediensten stellt das TDDSG einen wichtigen Beitrag dar.

8.2.2 „Freundlicher Geist" oder „Laus im Pelz"? – Heimliche Datenerhebung mit Cookies –

Jede Bewegung in den Netzen kann eine für den Nutzer oft nicht wahrnehmbare Spur, eine Art „Datenschatten" hinterlassen. Bestands-, Verbindungs- oder auch Abrechnungsdaten können neben dem eigentlichen Zweck ihrer Erhebung für vielerlei andere Nutzungen verwendet werden. Mit Hilfe automatisierter Erhebungsverfahren, die unbemerkt im Hintergrund einer Anwendung laufen und oft sogar Daten auf dem Computer des Nutzers ablegen, können mittlerweile exakte Protokollierungen der jeweiligen Aktivitäten des Nutzers erstellt werden. Einige Bürger haben sich wegen der bekanntesten Erscheinungsform solcher automatisierter Erhebungsverfahren, den sogenannten „Cookies", an mich gewandt. In diese Dateien auf der Festplatte des Nutzers speichern manche Anbieter Daten aus der aktuellen Nutzung, z. B. um mit diesen Daten über

Aktivitäten bei einem späteren Kontakt zu demselben Nutzer diesem die Suche in ihrem Angebot zu erleichtern. Der Nutzer wird jedoch vom Anbieter darüber nicht informiert. Er kann sich diesem Verfahren aber dadurch entziehen, daß er – den Ratschlägen in der Fachliteratur folgend – diese Dateien auf seiner Festplatte durch besondere Maßnahmen löscht. Unterläßt er dies, z. B. weil er wegen der Warnungen vor Benutzereingriffen in die Browser-Software und die von ihr angesprochenen Dateien das nicht riskieren möchte, so liefern die Auswertungsprogramme dem Diensteanbieter von Anwendung zu Anwendung wertvolle Hinweise über die Interessen des Nutzers, dessen Verweildauer bei bestimmten von ihm aufgerufenen Informationen oder auch über die angesteuerten Querverweise. Daraus lassen sich wiederum Nutzungs- oder Anwenderprofile erstellen, die dann helfen, den mit Cookie Überwachten vor allem direkt zu bewerben.

Sicherlich sind bei der sinnverwirrenden Vielfalt der Anwendungsmöglichkeiten in Computernetzen Erleichterungen hilfreich, etwa durch gezielte Eingrenzung und Selektion von Angeboten. Jedoch darf der kundenfreundliche Serviceaspekt nicht in ein „Ausspionieren" des Nutzers verkehrt werden, und sei es auch nur für Werbung. Der Nutzer muß selbst entscheiden können, ob er die Erstellung derartiger Profile zuläßt und damit auf ihn ganz individuell zugeschnittene Angebote erhalten möchte. Der Entwurf des TDDSG sieht deshalb vor, daß derartige Datenerhebungen nur mit der Einwilligung des Benutzers erfolgen dürfen. Und diese Einwilligung setzt voraus, daß er gut informiert wird, daß ihm die geplanten Datenverarbeitungen transparent sind. Eine europaübergreifende internationale Lösung dieses Problems kann ich für die nahe Zukunft leider noch nicht erkennen, da die Rechtspositionen dazu weltweit noch zu unterschiedlich sind. Solange eine solche Vereinbarung aber fehlt, ist nicht gewährleistet, daß der Standard, den das TDDSG für Deutschland setzt, international auch eingehalten wird.

8.2.3 Sicherheitsprobleme im Internet

Bei den Stellen meines Zuständigkeitsbereichs besteht ein zunehmender Bedarf, den Informationsaustausch untereinander, aber auch mit Stellen außerhalb der öffentlichen Verwaltung auf elektronischem Wege über Netze durchzuführen. Aus diesem Grunde haben zahlreiche Stellen bereits Zugang zum Internet, bei vielen steht seine Realisierung unmittelbar bevor. Die möglichen Gefährdungen für Datenschutz und Datensicherheit sind dabei allenfalls pauschal bekannt. Um konkrete Gefährdungen im einzelnen bewußt zu machen und geeignete Gegenmaßnahmen zu empfehlen, hat der Arbeitskreis „Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine „Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet" **(s. Anlage 21)** entwickelt. Darin werden sowohl die protokollimmanenten als auch die dienstspezifischen Sicherheitsrisiken beschrieben und Abwehrmaßnahmen mit Firewalls aufgezeigt. In einer Anlage zu der Orientierungshilfe werden die wichtigsten Dienste, die das Internet bietet (E-Mail, Usenet-News usw.), beschrieben.

8.2.4 Sicherer Internet-Zugang für die obersten Bundesbehörden

Im Juni 1995 hat die Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung (KBSt) die Studie „Internet für die obersten Bundesbehörden" veröffentlicht. Darin wird ein in ihrem Auftrag von der Gesellschaft für Mathematik und Datenverarbeitung (GMD) erstelltes Konzept für die Errichtung eines auf dem Internet-Protokoll basierenden IT-Netzes („IP-Backbone") für die obersten Bundesbehörden und die obersten Verfassungsorgane auf der Basis des Bundesbehördennetzes (BBN) vorgestellt.

Dieses „Intranet", wie solche Netze genannt werden, soll u. a. auch jeder angeschlossenen Bundesstelle – sowohl als Nutzer als auch als Informationsanbieter – Zugang zum Internet bieten. Hierzu wird die KBSt den Domain-Namen „bund.de" registrieren lassen. Mit einem Domain-Namen wird ein logisches Teilnetz des Internet bezeichnet, das einem speziellen Domain-Server zugeordnet ist. Auch dient der Name einer besseren Adressierbarkeit. Die Bundesstellen, die dieses Intranet nutzen wollen, ergänzen die Domain um einen Namen für die Subdomain; so würde ggf. der Name der Subdomain meiner Dienststelle „bfd.bund.de" lauten.

Es ist vorgesehen, drei voneinander abgeschottete Bereiche zu bilden:

1. den behördeninternen, durch eine **„Firewall"** gegenüber anderen Behörden und dem übrigen Internet abgeschotteten Bereich. Als Firewall wird dabei ein zentraler Rechner mit spezieller Software bezeichnet, über den der Internetzugang aller Benutzer erfolgt und der sämtliche eingehende Datenpakete z. B. auf unbekannte Absenderadressen überprüft und Verbindungen zu unbekannten Adressen blockiert;
2. den internen Bundesbereich, der allen angeschlossenen Bundesstellen, nicht aber der „Außenwelt" offensteht. Er ist durch eine Firewall vom lokalen Netz der angeschlossenen Bundesstelle abzuschirmen;

   und
3. den öffentlichen Bereich, der allen Internetbenutzern zur Verfügung steht.

In einem Sicherheitskonzept wird darauf hingewiesen, daß die Zahl der Benutzer des Internet derzeit explosionsartig wächst, daß die Sicherheitsmaßnahmen vielerorts rudimentär sind und Mißbrauch nicht ausgeschlossen werden kann. Wegen der exponierten Stellung des Parlaments, der Bundesregierung und vieler Bundesbehörden werden massive Eindringversuche befürchtet, sobald der Anschluß ans Internet realisiert ist. Auch wird die Gefahr von Angriffen von innen nicht ausgeschlossen.

Die zur Abwehr der beschriebenen Gefahren vorgeschlagenen Sicherheitsmaßnahmen bestehen im wesentlichen in der Protokollierung der Verbindungsdaten, der Abschottung durch Firewalls und dem Einsatz von Kryptierungssystemen, die mit mehrstufiger Verschlüsselung und privaten und öffentlichen Schlüsseln arbeiten. Es werden detaillierte Vorschläge zur Firewall-Struktur und Anforderungen an die anderen Netzwerkkomponenten – Router, Gateway- und Server-Rechner – gemacht. Zusammenfassend wird festgestellt, daß die vorgeschlagenen Firewall-Maßnahmen einen ausreichenden Schutz gegen Angriffe auf das Behördennetz aus dem Internet bieten, wenn sie durch organisatorische und personelle Maßnahmen unterstützt werden. Es wird aber auch klargestellt, daß ein vollständiger Schutz nicht möglich ist. Administrative Fehler und Fehler in der eingesetzten Hard- und Software können nicht ausgeschlossen werden, und findige Angreifer werden immer wieder neue Sicherheitslücken entdecken.

Aus datenschutzrechtlicher Sicht ist auf zwei Probleme zu verweisen:

- Es verbleibt stets ein Restrisiko bezüglich eines unbefugten Eindringens.
- Beim Betrieb des Intranet – einschließlich der „Gefahrenabwehrtechnik" – entstehen zwangsläufig zusätzliche personenbezogene Daten.

Allen Benutzern, insbesondere aber den Verantwortlichen in den Behörden, muß bewußt sein, daß die Gefahr eines Eindringens von außen nicht völlig auszuschließen ist. Daten mit erhöhtem Schutzbedarf, z. B. solche, die einem besonderen Amtsgeheimnis unterliegen, sollten in den angeschlossenen Systemen grundsätzlich nicht oder nur kryptiert verarbeitet werden (z. B. Sozialdaten, Personalaktendaten, Meldedaten).

Die aus Gründen der Systemsicherheit oder zur Abwicklung eines ordnungsgemäßen Betriebes in den Systemen gespeicherten Daten, z. B. Verzeichnisse mit Postanschriften, Protokolldaten usw. unterliegen der besonderen Zweckbindung nach § 14 Abs. 4 BDSG und dürfen ausschließlich für die Zwecke verwendet werden, für die sie gespeichert wurden, also nicht für andere Zwecke genutzt werden.

Die Hauptlast der Gefahrenabwehr wird in der Betreuung der Firewalls liegen. Für den Betrieb der zentralen Firewall (s. Bereich 2.) wurde inzwischen ein Outsourcingvertrag mit der Deutschen Telekom AG abgeschlossen

Der Betrieb der Firewalls auf lokaler Ebene (s. Bereich 1.) obliegt den einzelnen Bundesstellen; für kleinere Behörden ein nicht zu unterschätzendes Problem!

8.3 Bürgeranfragen beim Bundesaufsichtsamt für das Versicherungswesen

Verschiedene Eingaben richteten sich gegen die Behandlung von Bürgeranfragen durch das Bundesaufsichtsamt für das Versicherungswesen (BAV). Die Petenten waren mit der Weiterleitung ihrer an das BAV gerichteten Eingaben an ihre Versicherung nicht einverstanden, weil sie sich entweder ganz bewußt nicht an die Versicherung gewandt hatten, da sie Nachteile im Hinblick auf ihr Versicherungsverhältnis befürchteten, oder weil ihre Frage sich auf die Ausübung der Versicherungsaufsicht bezog und deshalb direkt an das BAV gerichtet war.

Das BAV sieht zwar das persönliche Problem des Versicherungsnehmers, hat aber die ständige Aufgabe, den Geschäftsbetrieb der Versicherungsunternehmen zu überwachen. Die Ausübung der Versicherungsaufsicht geht in der Regel über die Klärung eines einzelnen, vom Petenten geschilderten Anlasses hinaus, so daß es häufig erforderlich ist, die Stellungnahme der betroffenen Versicherung nicht nur zum vorgetragenen Fall, sondern auch zum generellen Verfahren in entsprechenden Fällen einzuholen. Die Entscheidung, ob zu diesem Zweck eine Eingabe an die zuständige Versicherung weitergeleitet wird, stellt in den – häufigen – Fällen kein Problem dar, in denen die Bürger ausdrücklich ihre Versicherungsnummer angeben. Dieser Hinweis auf das bestehende Versicherungsverhältnis ist als Aufforderung zu verstehen, sich des konkreten Falls anzunehmen. Die Notwendigkeit, die Eingabe der Versicherung personenbezogen zur Stellungnahme vorzulegen, ergibt sich aber oft auch dann, wenn die Versicherungsnummer nicht angegeben ist. Denn die vom Betroffenen kritisierte Entscheidung der Versicherung kann auf Besonderheiten des Einzelfalls beruhen, die weder dem Amt bekannt sind noch vom Versicherungsnehmer beschrieben wurden.

Nach allen Erfahrungen des Amtes aus vielen zehntausend Bürgeranfragen wirkt sich die Weiterleitung einer Eingabe an das betroffene Versicherungsunternehmen auch auf Kulanz- oder Ermessensentscheidungen des Unternehmens nicht negativ aus. Gleichwohl wird in den Fällen von einer Weiterleitung abgesehen, in denen der Petent dies ausdrücklich wünscht oder ihm dadurch aus der Sicht des Amtes möglicherweise doch Nachteile erwachsen könnten. In den sehr seltenen Zweifelsfällen wird zur Klärung die Einwilligung des Versicherungsnehmers zu der Weiterleitung seiner Anfrage erbeten.

Um mehr Transparenz und Bürgerfreundlichkeit zu erreichen, habe ich dem BAV empfohlen, die Petenten über den aufsichtsrechtlichen Hintergrund seines Vorgehens zu informieren und zugleich der nach aller Erfahrung unbegründeten Besorgnis, das Verfahren des BAV könnte sich negativ auf das bestehende Versicherungsverhältnis auswirken, vorzubeugen. In Grenzfällen sollte das BAV eher noch einmal Kontakt mit dem Petenten aufnehmen, um das Vertrauen der Bürger in das Amt nicht zu beeinträchtigen.

Das BAV hat diese Anregungen aufgegriffen und wird künftig strengere Maßstäbe bei der Einstufung von Zweifelsfällen anlegen und somit vorsorglich lieber einmal mehr die Einwilligung des Betroffenen erbitten.

8.4 Datenschutz als Allheilmittel?

Gelegentlich erreichen mich Eingaben, in denen die Betroffenen als letzte Möglichkeit für die Lösung ihrer Probleme datenschutzrechtliche Argumente anführen. Dazu zwei Beispiele:

- Auf dem nach der Viehverkehrsordnung vorgeschriebenen „Tierpaß" (Begleitpapier für Rinder) ist u. a. zum Zweck der Seuchenbekämpfung die Angabe des Erzeugerbetriebes vorgesehen. Ein Viehhändler wandte sich an mich, weil er meinte, der Herkunftsbetrieb müsse aus datenschutzrechtlichen Gründen auf dem Tierpaß verschlüsselt angegeben werden. Beweggrund für dieses Vorbringen war jedoch, daß die Kunden anhand dieses Begleitpapiers die Herkunft des Tieres erkennen können und deshalb die Händler befürchten, einige ihrer Kunden könnten künftig – unter Umgehung des Vertragshändlers – direkt beim Erzeuger kaufen. Abhilfe war hier nicht möglich, weil die Angabe des Erzeugerbetriebes dem Schutz der öffentlichen Sicherheit dient und außerdem für die am Viehhandel Beteiligten auch bei Codierung die Ermittlung des Betriebes leicht möglich wäre.

- Um Schädigungen durch betrügerische Manipulationen an Freistemplern entgegenzuwirken, hat die Deutsche Post AG die Benutzer von Freistemplern verpflichtet, regelmäßige Sicherheitsinspektionen dieser Geräte durchführen zu lassen. Die Hersteller, die entschieden hatten, diese Inspektionen selbst durchzuführen, forderten deshalb die Fachhändler auf, ihnen für die Inspektionen die Freistempler-Kunden zu benennen. Mehrere Vertragshändler, überwiegend kleine und mittelständische Unternehmen, wandten sich mit der Frage an mich, ob die Adressen der Kunden aus datenschutzrechtlicher Sicht an die Hersteller der Frankiermaschinen weitergegeben werden dürfen. Nachdem sie die Kunden beraten und geworben hatten, sahen sie sich der Gefahr ausgesetzt, daß ihnen aufgrund der von ihnen als mittelstandsfeindlich angesehenen Änderung Folgeaufträge entgehen könnten. Dazu konnte ich den Händlern nur mitteilen, daß – unabhängig von der Zulässigkeit der Datenweitergabe – Datenschutzrecht sie nicht verpflichtet, die Daten weiterzugeben. Am Ende übermittelte die Post AG diese Daten ihrer Freistempler-Kunden an die entsprechenden Hersteller mit der Auflage, sie nur für die Sicherheitsinspektionen zu nutzen, um damit die Befürchtungen der Händler so weit wie möglich zu berücksichtigen.

Auffälligerweise verfolgten in beiden geschilderten Fällen die Händler nicht ihre eigenen datenschutzrechtlichen Interessen, sondern setzten sich für den Schutz der personenbezogenen Daten ihrer Geschäftspartner ein. Deren Interessen standen der Datenweitergabe aber nicht entgegen. Hintergrund waren jeweils – wenngleich auch nachvollziehbare – wirtschaftliche Interessen der Händler, so daß ich denjenigen, die im Sinne des Datenschutzes nicht betroffen waren, die erwünschte Unterstützung nicht geben konnte.

9 Chipkarte

9.1 Technische und organisatorische Probleme mit Chipkarten

9.1.1 Schutz gegen „gezinkte Chipkarten" – aber wie ?

Die Chipkarte ist weiterhin auf Höhenflug. In immer mehr Bereichen sowohl der öffentlichen Verwaltung als auch der Privatwirtschaft werden Chipkarten eingesetzt oder erprobt. Über einige Probleme beim Einsatz von Chipkarten habe ich bereits im 15. Tätigkeitsbericht berichtet (Nrn. 1.6, 30.1).

Die neueste Generation von Chipkarten enthält einen integrierten Mikroprozessor und eine Kryptokomponente zur Verschlüsselung von Daten. Auch die Speicherkapazität der Chipkarte hat erheblich zugenommen. Während die 1994 eingeführte Krankenversichertenkarte nur eine Speicherkapazität von max. 256 Zeichen hat, werden heute bereits Chipkarten mit Kapazitäten von 8.192 Zeichen (= 8 KByte, entsprechend zwei vollgeschriebenen DIN-A-4 Seiten) angeboten. Dies entspricht einer Vergrößerung des Speicherbereiches gegenüber einer Krankenversichertenkarte auf das 32fache.

Damit wird die Chipkarte zum **Computer im Kleinstformat ohne Mensch-Maschine-Schnittstelle**. Daraus ergeben sich Konsequenzen:

- Chipkarten sind leicht transportable Rechner. Für sie gelten die gleichen Risiken der IT-Sicherheit wie bei anderen transportablen Rechnern z. B. Laptops oder Notebooks.

- Die Interaktion zwischen Mensch und Chipkarte bedarf zwischengeschalteter Systeme (Kartenterminals), die ebenfalls besonders zu sichern sind. Eine Chipkarte bildet zusammen mit dem Kartenterminal ein vollwertiges Rechnersystem mit Ein- und Ausgabe-Komponente. Die Evaluation der richtigen Funktionsweise setzt voraus, daß alle Systemkomponenten miteinander verknüpft sind.

- Aufgrund von zu geringen Speicher- und Prozessorkapazitäten lassen sich heute nicht alle aus datenschutzrechtlicher Sicht wünschenswerten Sicherheitsfunktionen realisieren. Die technische Entwicklung muß diese Engpässe jedoch bald beseitigen und, wenn möglich, Sicherheitsfunktionen schon bei der Entwicklung von Karten mit einbeziehen. Dies bedeutet, daß Chipkartenverfahren so offen gestaltet sein müssen, daß Weiterentwicklungen zur Erhöhung der Sicherheit – jedenfalls nachträglich – berücksichtigt werden können.

Mit dieser neuen Art von Karten werden auch Anwendungsfelder für den Einsatz der Chipkarte als **Informationsträger sensibler Daten** erschlossen. Die Diskussion um die Einführung einer Patientenkarte zeigt dies deutlich. In sensiblen Bereichen, wie etwa auf dem Gesundheitssektor, ist eine hochwertige sicherheitstechnische Ausstattung der Chipkarte aber Voraussetzung für die Sicherstellung des Datenschutzes. **„Gezinkte Karten" darf es daher bei sensiblen Chipanwendungen schon aus Akzeptanzgründen nicht geben.** Für den datenschutzgerechten

Einsatz einer Chipkarte ist deshalb eine konsequente und überzeugende Sicherheitstechnologie erforderlich. Da die vorhandenen Datensicherheitsmaßnahmen in ihrer Gesamtheit einen hinreichenden Schutz der Daten vor Mißbrauch gewährleisten müssen, rate ich sehr, vor der Entscheidung über den Einsatz von Chipkarten in einem Verfahren entsprechend Artikel 20 der EG-Datenschutzrichtlinie eine **Vorabkontrolle** in Sinne einer Technikfolgenabschätzung durchzuführen (zur Umsetzung der Datenschutzrichtlinie und meinen Forderungen im Hinblick auf die damit zu verbindende Modernisierung des Datenschutzrechts s. o. Nr. 2.1.5).

Dabei ist es zweckmäßig, zwischen der Ausgestaltung der Chipkarte selbst und ihrer Anwendung in einem bestimmten Kontext zu unterscheiden, da für ihre Anwendung – neben der Chipkarte selbst – eine Fülle weiterer Komponenten (Kartenterminals, Datennetze, Rechnersysteme) erforderlich sind. Denn datenschutzrechtliche Anforderungen an ein konkretes Verfahren erstrecken sich nicht nur allein auf die Chipkarte, sondern eben auch auf die verwendeten Komponenten und die technischen und organisatorischen Rahmenbedingungen bei der Herstellung, bei der Initialisierung, beim Versand und bei der Ersatzbeschaffung in Fällen des Verlustes oder der Zerstörung einschließlich des Ungültigkeitsmanagements der Chipkarte.

Da eine Bewertung sowohl der datenschutzrechtlichen Probleme als auch der technischen Risiken sich somit nur unter Kenntnis eines bestimmten Anwendungsfalls sowie der inhaltlichen und technischen Rahmenbedingungen vornehmen läßt, halte ich es für dringend geboten, bei Einführung einer Chipkarte – ob gesetzlich vorgeschrieben oder als freiwilliges Angebot z. B. einer Krankenversicherung – frühzeitig die **Beratung durch Experten** – und zwar des Datenschutzes und der IT-Sicherheit – in Anspruch zu nehmen.

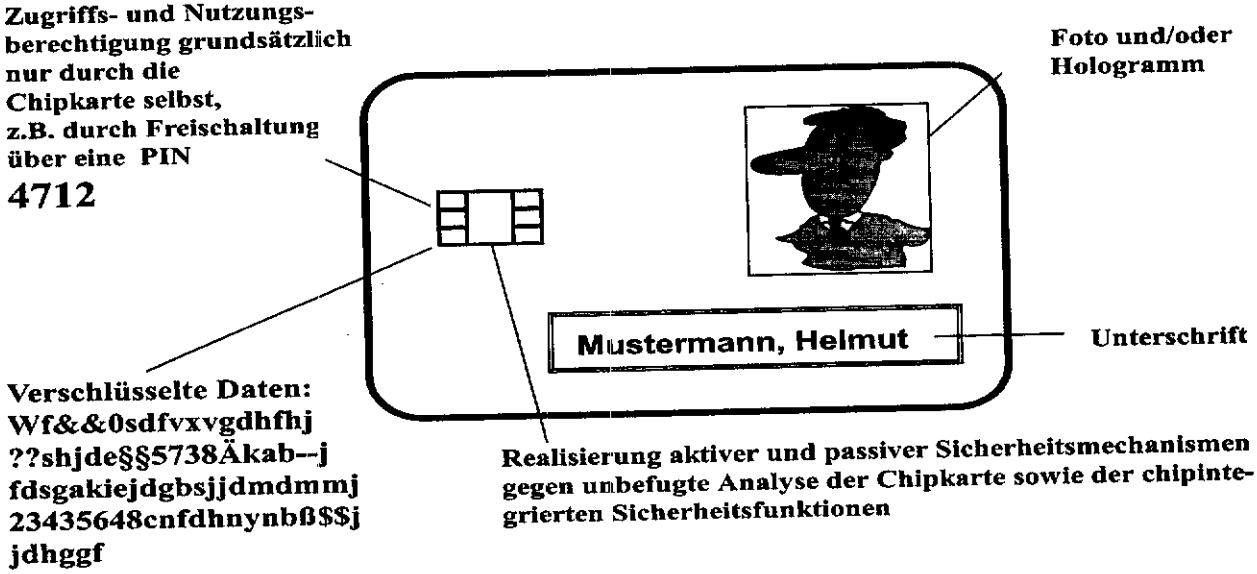
Inwieweit unabhängig von einer konkreten Anwendung allgemeine technische und organisatorische Anforderungen nur an die Chipkarte selbst definiert werden können, war Gegenstand einer Arbeitsgruppe des Arbeitskreises „Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder. Die Arbeitsgruppe kam zu dem Ergebnis, daß aus der Sicht des Datenschutzes eine Chipkarte folgende Mindestanforderungen erfüllen sollte (s. hierzu auch Abb. 3):

1. Ausstattung des Kartenkörpers mit fälschungssicheren Authentifizierungsmerkmalen, wie z. B. mit Unterschrift und/oder Foto des Inhabers bzw. Hologrammen,
2. Steuerung der Zugriffs- und Nutzungsberechtigung durch die Chipkarte selbst,
3. Realisierung aktiver und passiver Sicherheitsmechanismen gegen eine unbefugte Analyse der Chipinhalte sowie der chipintegrierten Sicherheitsfunktionen,
4. Benutzung allgemein anerkannter, veröffentlichter (oder geprüfter) Algorithmen für Verschlüsselungs- und Signaturfunktionen sowie zur Generierung von Zufallszahlen,
5. Sicherung der Kommunikation zwischen der Chipkarte, dem Kartenterminal und einem gegebenenfalls im Hintergrund wirkenden System durch kryptographische Maßnahmen.

Diese Forderungen sind als **Grundschutzmaßnahmen** beim Einsatz von Chipkarten zu verstehen und soll-

Abbildung 3

Mindestanforderungen bei Chipkarten



ten bei Realisierung schon in der Planung berücksichtigt werden.

Für besonders schutzbedürftige Verfahren – z. B. im Gesundheitswesen – empfiehlt es sich, neben den Grundschutzmaßnahmen folgende zusätzliche Sicherungsmaßnahmen zu realisieren:

1. Identifizierung und Authentifizierung der Benutzer: Hierzu eignet sich insbesondere das Challenge-Response-Verfahren. Dabei stellt die Chipkarte dem Kommunikationspartner (Kartenterminal, Rechner) eine zufällig erzeugte Frage (Challenge) und dieser berechnet eine Antwort auf der Grundlage eines vorher vereinbarten Algorithmus (und Schüssels) und sendet sie der Chipkarte zurück (Response). Nur wenn beide Partner über den gleichen Algorithmus und Schlüssel verfügen, ist die Antwort korrekt.
2. Die Datenübertragung über die Schnittstelle auf die oder von der Chipkarte ist gegen Manipulationen oder Abhören zu sichern („Secure Messaging").
3. Eingabe- und Ausgabekontrolle bei allen Schnittstellen, die Übermittlungen zulassen.
4. Interferenzfreiheit der einzelnen Anwendungen, d. h. eine gegenseitige unerwünschte Beeinflussung der Anwendungen muß ausgeschlossen sein.
5. Verzicht auf Funktionen, die eine Ausforschung der Programme ermöglichen (Trace- und Debug-Funktionen).

Ich werde auch weiterhin das Geschehen im Bereich der Chipkarten kritisch und aufmerksam beobachten. Meine Anforderungen an den Einsatz von Chipkarten werden sich dabei an den Empfehlungen des genannten Arbeitskreises der Datenschutzbeauftragten orientieren **(vgl. Anlage 22)**.

9.1.2 HPC – Eine neue Chipkarte für medizinische Berufe

Mit der flächendeckenden Einführung der Krankenversichertenkarte (KVK) gemäß § 291 SGB V wurde zwangsläufig in der gesamten Bundesrepublik Deutschland eine Infrastruktur geschaffen, die die elektronische Verarbeitung aller Leistungsdaten eines Leistungserbringers im Bereich des Gesundheitswesen (Arzt, Krankenhaus, Hebamme etc.) zur Folge hat. War vor der Einführung der KVK ein Großteil der Leistungserbringer nicht mit elektronischen Datenverarbeitungsanlagen ausgestattet, so änderte sich dies mit der Einführung schlagartig; fast jeder Leistungserbringer verfügt heute über einen Arbeitsplatzcomputer mit Drucker und Chipkartenlesegerät (Kartenterminal). Der weitere Ausbau wird – schon heute absehbar – in der Vernetzung über moderne Telekommunkationssysteme (ISDN, Internet) vorgenommen werden.

Die Nutzung der vorhandenen Infrastruktur nur zum Zweck der Abrechnung scheint auf die Dauer nicht wirtschaftlich, ließe sich doch durch den Einsatz der Technik ein Großteil der im Gesundheitswesen vorhandenen Informations- und Kommunikationsdefizite beheben. Diese wirken sich bei der Qualität der Patientenversorgung aus und verursachen in nicht unerheblichem Maße Zusatzkosten für die Versichertengemeinschaft. Typische Beispiele für die vorhandenen Defizite sind:

- Bei der Überweisung vom Haus- zum Facharzt, vom Haus- oder Facharzt ins Krankenhaus etc. werden oftmals keine Befunde oder Ergebnisse von Voruntersuchungen mitgeliefert, so daß verschiedene Untersuchungen (Röntgen, EKG, Labortests) erneut durchgeführt werden. Dies stellt nicht nur für den Patienten eine erhebliche Belastung, z. B. durch wiederholtes Röntgen dar, sondern trägt darüberhinaus zur Steigerung der Kostenbelastungen bei.

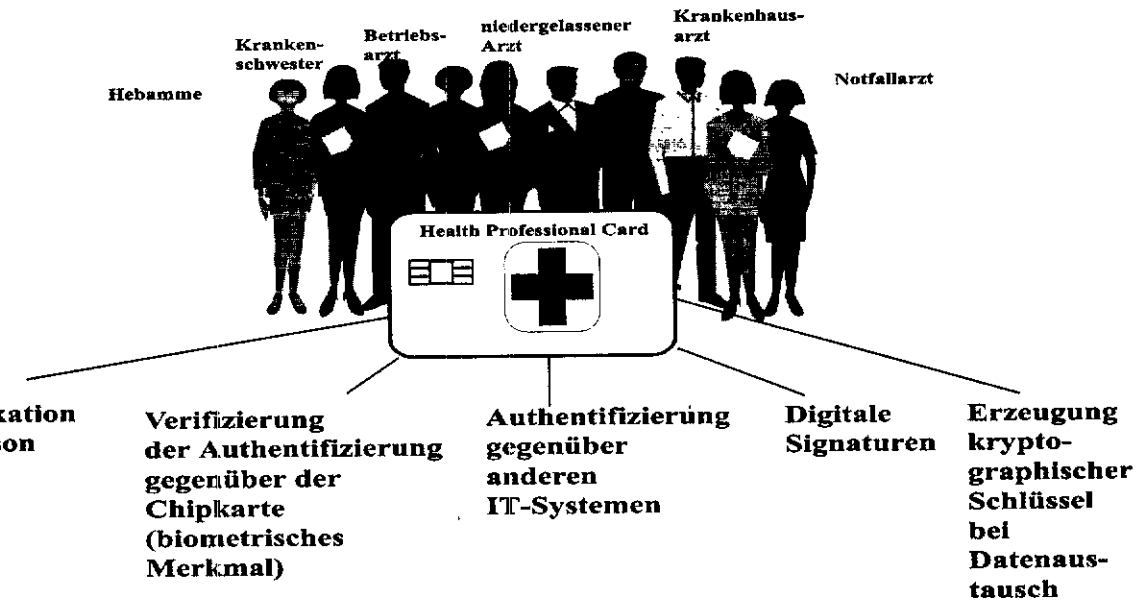
- Arztbriefe, die bei einer Krankenhausentlassung dem nach- oder weiterbehandelnen Arzt als Basisinformation dienen sollen, erreichen zum Teil erst nach Wochen ihren Empfänger. Die zumeist handschriftlichen, häufig schwer lesbaren Niederschriften wären oftmals ohne Rückfragen und den damit verbundenen Zeitverzug für eine Fortsetzung der Behandlung nicht geeignet. Die Behandlungen dauern somit länger und werden noch kostenträchtiger.

- Wichtige Informationen wie etwa solche über besondere Vorerkrankungen, Risikofaktoren, Allergien, oder Arzneimittelunverträglichkeiten, stehen zwar oftmals dem Hausarzt zur Verfügung, aber nicht den behandelnden Fachärzten oder gar dem Notfallarzt.

An der Verbesserung der Kommunikation wird seit Jahren intensiv in wissenschaftlichen Untersuchungen und Modellprojekten gearbeitet. Zum einen kommen dabei Chipkarten zur Speicherung der wichtigsten Informationen eines Patienten zum Einsatz („Patientenkarten"; Offline-Lösung), zum anderen werden die Möglichkeiten von modernen Telekommunikationsnetzen erprobt. Dies geschieht zur Unterstützung von Diagnosen durch Spezialisten über weite Entfernungen durch elektronische Übermittlung von Voruntersuchungsergebnissen per Datentransfer oder durch Zugriffe auf Patientendaten, die auf verschiedenen Rechnern – Hausarzt, Facharzt, Krankenhaus etc. – gespeichert werden. Das zentrale Problem bei den bisher geplanten oder erprobten Verfahren dreht sich um die Frage, mit welchen Maßnahmen die Daten eines Patienten gegen jeden anderen Zugriff als den der in der konkreten (Behandlungs-) Situation zugriffsberechtigten Person geschützt werden können. Dazu muß zumindest bei allen Zugriffen auf sensible medizinische Daten die Identität der berechtigten Person – des **Health Professional (HP)** – vorher zweifelsfrei feststellbar sein. Auf hohem Sicherheitsniveau müssen die Person – dies kann ein Arzt, eine Krankenschwester, eine Hebamme etc. sein – und deren Zugriffsrechte gegenüber einem IT-System – sei es eine Chipkarte oder ein Rechner – identifiziert werden. Die Frage, wie eine Identifizierung und Authentifizierung eines Beschäftigten im Gesundheitswesen gegenüber IT-Systemen vollzogen werden soll, wird auf verschiedenen europäischen und internationalen Ebenen diskutiert, beispielsweise in den Standardisierungsgremien des Comite Europeen de Normali-

Abbildung 4

Grundfunktionen der Health Professional Card (HPC)



sation (CEN), wobei einheitliche Lösungen angestrebt werden. Es besteht Konsens, den Träger der zur Identifikation erforderlichen Informationen als Chipkarte mit Mikroprozessor – **Health Professional Card (HPC)** – auszugestalten. Werden darüber hinaus auch Karten mit Krypto-Prozessoren eingesetzt, können alle Sicherheitsleistungen auf einem hohem Sicherheitsniveau ablaufen. Die HPC soll wesentlicher Bestandteil einer Sicherheitsinfrastruktur im Gesundheitswesen werden. Die Grundfunktionen der HPC sind (s. hierzu Abb. 4):

- Identifikation des HP als Person mit seiner professionellen Qualifikation und gegebenenfalls auch seiner betrieblichen Funktion (z. B. als Betriebsarzt), soweit dies für die Ausprägung der Zugriffsrechte von Bedeutung ist;
- Authentifizierung des HP gegenüber der HPC durch PIN-Prüfung und/oder biometrische Merkmale (z. B. Fingerabdruck, Augenhintergrundabbildung);
- Authentifizierung der HPC gegenüber IT-Systemen und Verifizierung der Authentifizierung von IT-Systemen gegenüber der HPC; die gleiche Funktion wird auch bei der Authentifizierung gegenüber Patientenkarten oder Gesundheitskarten („card to card") genutzt;
- Erstellung von digitalen Signaturen und Überprüfung fremder Signaturen und Zertifikate;
- Erzeugung und Austausch von kryptographischen Schlüsseln für die symmetrische Verschlüsselung beim Datenaustausch („session keys").

Die genannten Funktionen der HPC werden benötigt, um den Schutz der Gesundheitsdaten der Patienten in den geplanten IT-Anwendungen in angemessener Weise zu gewährleisten. In diesem Sinne habe ich in der Arbeitsgemeinschaft „Chipkarten im Gesundheitswesen"(s. auch Nr. 9.2) an der Festlegung wesentlicher Eigenschaften einer HPC und den Vorgaben für eine Erprobung mitgewirkt. Viele Anzeichen sprechen dafür, daß die Ergebnisse dieser Arbeiten die gegenwärtigen internationalen Normierungsverfahren für HPC, z. B. G7 Healthcards Interoperabilty Project Technical Group sowie die Standardisierungsgremien im CEN TC224 und TC 251, die die datenschutzrechtliche Aspekte bisher nur ungenügend berücksichtigt hatten, positiv beeinflussen.

9.1.3 Das Multifunktionale Kartenterminal für das Gesundheitswesen

Für die Einführung der Krankenversichertenkarte (KVK) wurde 1993 eine technische Spezifikation für Chipkartenterminals erarbeitet, die in über 100 000 Arztpraxen zum Lesen der Daten der KVK eingesetzt wird. Die Funktionalität wurde aufgrund auch datenschutzrechtlicher Aspekte auf das Lesen der Versichertenkarte beschränkt. Außerdem wird entsprechend einer Vereinbarung zwischen den Vertragspartnern nach dem Sozialgesetzbuch (SGB) diese Beschränkung durch eine Zertifizierung der Geräte gemäß der „Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC)" – Sicherheitstufe E2, Mechanismenstärke niedrig – garantiert. Ich habe diese Lösung damals schon als „zweitbeste" angesehen, denn die Sicherheit der Karte muß nach Meinung aller Experten auf der Karte selbst und nicht in anderen Systemkomponenten realisiert werden.

Mit dem Aufkommen weiterer Chipkartenanwendungen im Gesundheitswesen – Patientenkarten, Apothekenkarte, Health Professional Card etc. – ent-

steht nunmehr die Notwendigkeit des Einsatzes eines Chipkartenterminals, das keinerlei Funktionsbeschränkungen aufweist. Will man vermeiden, daß in einer Arztpraxis eine Vielzahl von Terminals zum Lesen der verschiedenen Chipkarten vorgehalten werden muß, muß ein Kartenterminal entwickelt werden, das alle möglichen Chipkarten lesen und verarbeiten kann. Sinnvoll wäre ein Terminal, das auch außerhalb des Gesundheitswesens einsetzbar ist – das Multifunktionale Kartenterminal (MKT).

Die Spezifikation eines MKT wurde von der Arbeitsgemeinschaft Karten im Gesundheitswesen (s. hierzu Nr. 9.2) und der Gesellschaft für Mathematik und Datenverarbeitung (GMD) in Darmstadt im August 1995 in der Version 0.9 vorgelegt. Die Spezifikation eröffnet viele Nutzungsmöglichkeiten, da das MKT transparent für beliebige Dialoge zwischen einem Rechner (Host) und der dort ablaufenden Applikation und einer Speicher- oder Prozessorchipkarte ist. Sie berücksichtigt die internationale Normung sowie Spezifikationen anderer Institutionen wie Europay International S.A., Mastercard International Incorporated und Visa International Service Association.

Um die Funktionsbeschränkung beim Verarbeiten einer KVK weiterhin sicherzustellen, verfügt das MKT über ein Funktionsmodul zum Lesen einer KVK. Die KVK wird dabei durch das spezifische Anwendungskennzeichen (Application-ID) identifiziert, das durch die nationale Registrierungsstelle vergeben wurde und auf allen KVK vorhanden sein muß. Damit ist aus meiner Sicht sichergestellt, daß die bislang getroffene Vereinbarung zur Zertifizierung der KVK-Lesegeräte nach wie vor erfüllt werden kann und nicht durch die Einführung neuer Anwendungen auf Chipkarten unterlaufen wird. Von einer Zertifizierung des Funktionsmoduls zum Lesen der KVK kann erst dann abgerückt werden, wenn die KVK durch andere Sicherheitsmechanismen abgesichert wird.

Das MKT kann als

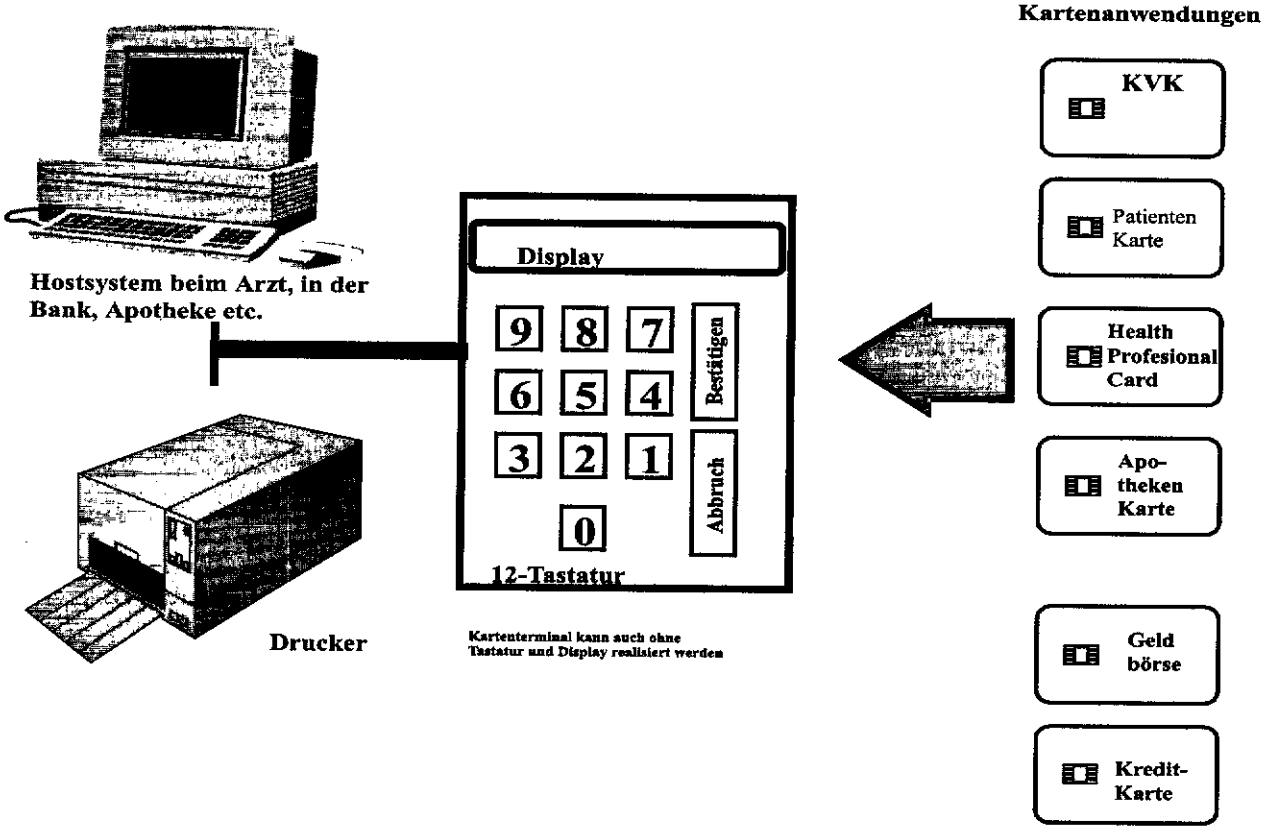
- integrierte Systemkomponente (z. B. Kartenleser integriert in die Tastatur, Kartenleser in einem Diskettenschacht etc.) oder
- als separates Endgerät

realisiert werden.

Bei der Realisierung als Endgerät können als Zusatzoptionen eine Tastatur und ein Display sowie eine zweite Kontaktiereinheit zum Lesen einer weiteren Chipkarte vorhanden sein (s. Abb. 5).

Abbildung 5

Multifunktionales Kartenterminal



Hinsichtlich der Risiken ist es gleich, welche der Möglichkeiten der Realisierung genutzt wird. Das Kartenterminal stellt nämlich in jedem Fall das Bindeglied zwischen Kartenbesitzer und der Kartenanwendung dar. Dabei ist besonders zu berücksichtigen, daß neben der Authentifizierung und der Identifizierung des Kartenbesitzers – z. B. mit Hilfe einer „Personal Identification Number (PIN)" – auch alle Daten, die eine Anwendung von einer Karte benötigt oder die während der Bearbeitung auf die Karte geschrieben werden müssen, zwangsläufig den Weg über das MKT nehmen müssen. Dabei werden gegebenenfalls auch personenbezogene Daten – im Falle von Patientenkarten sogar sehr sensibler Natur – gelesen und/oder geschrieben. Dies setzt somit voraus, daß das Kartenterminal auch wirklich so funktioniert, wie der Chipkarten-Besitzer dies erwartet. Manipulationen zum Nachteil des Kartenbesitzers, wie Änderungen der Daten im Terminal, Zwischenspeicherung der Daten z. B. der PIN, Mithören der Daten zwischen Anwendung und Karte und unberechtigtes Beschreiben der Karte sind durch technische und organisatorische Maßnahmen auszuschließen, z. B. dadurch daß die Daten nur verschlüsselt zwischen Karte und Anwendung übertragen werden. Der Einsatz des MKT ersetzt weder notwendige Sicherheitsfunktionen auf der Chipkarte (vergleiche Nr. 9.1.1) noch entsprechende Vorkehrungen in der Anwendung „hinter" dem MKT. Das MKT kann aber zum sicheren Bindeglied zwischen diesen Systemteilen werden.

Das Basiskonzept des MKT erlaubt den Einsatz verschiedener Sicherheitstechniken und verlangt die Zertifizierung besonders sensibler Funktionsmodule. Ich habe deshalb bislang keine grundsätzlichen Bedenken geäußert. Sollten die Erfahrungen in der Erprobungsphase allerdings Schwächen offenbaren, werde ich für bestimmte Anwendungen Nachbesserungen in der Spezifikation einfordern.

9.2 Chipkarten für Gesundheitsdaten

Schon als mit der Krankenversichertenkarte eine relativ schlichte Chipkarten-Anwendung in die Arztpraxen eingeführt wurde, galt das nur als ein erster Schritt, dem bald eine weitere, anspruchsvollere Nutzung einer in wenigen Jahren auch leistungsfähigeren Technik folgen sollte. Die Erwartungen an die technische Entwicklung haben sich erfüllt (s. o. Nr. 9.1) und die praktischen Anwendungsmöglichkeiten von Chipkarten mit Kryptoprozessoren werden u. a. durch die zum Jahreswechsel 1996/97 ausgegebenen multifunktionalen ec-Karten eindrucksvoll demonstriert.

Parallel zu der technischen Entwicklung von Chipkarten, die sich fortsetzen wird, wurde der Einsatz dieses Mediums zur Speicherung von Gesundheitsdaten geplant, vorbereitet und in einzelnen Versuchen auch schon erprobt. Koordinierend wirkt dabei in Deutschland die Arbeitsgemeinschaft „Karten im Gesundheitswesen", die unter der Leitung von Herrn Dr. O.P. Schaefer (bis Februar 1997 Vorsitzender der Kassenärztlichen Vereinigung Hessen) Sachverstand und Interessen auf diesem Gebiet bündelt.

Um die Bemühungen in den verschiedenen Staaten zu koordinieren, beteiligen sich mehrere Mitglieder der Arbeitsgemeinschaft an der internationalen Abstimmung über die in die Karten aufzunehmenden Inhalte sowie über deren Präsentation durch Anwendungsprogramme und andere Festlegungen, die zum Erreichen der hier offensichtlich notwendigen internationalen Interoperabilität der Systeme erforderlich sind. Ein beachtlicher Erfolg dieser Zusammenarbeit ist die auf der G7-Ebene erfolgte fachliche Einigung auf einen Patienten-Datensatz (Patient Data Set), der in allen Gesundheitskartensystemen als Mindestangabe – unter dem Vorbehalt der Einwilligung des Patienten (s. u. Nr. 9.2.2) – geführt werden soll. Dieser Datensatz geht über früher diskutierte Notfallangaben hinaus und umfaßt die wesentlichen Angaben über Erkrankungen, Allergien und Medikamente, die notwendig sind, um bei einer ärztlichen (Weiter-)Behandlung das Eintreten eines Notfalls oder einer ernsten Komplikation möglichst zu vermeiden.

Ferner besteht grundsätzliche Einigkeit darüber, daß eine Health Professional Card (s. o. Nr. 9.1.2) insbesondere die Zugriffsberechtigung auf Gesundheitsdaten und damit auch auf den Inhalt einer Chipkarte des Patienten nachweisen soll.

Der Datenschutz wird in der Arbeitsgemeinschaft und in mehreren der von ihr eingerichteten Arbeitskreisen durch eine Mitarbeiterin des Hessischen Landesbeauftragten für den Datenschutz und durch zwei meiner Mitarbeiter vertreten und allgemein als unverzichtbarer Teil der Entwicklung angesehen.

9.2.1 Vorteile und Risiken von Gesundheitsdatenkarten

Für eine erfolgreiche ärztliche Behandlung sind häufig Angaben aus früheren Behandlungen und Untersuchungen hilfreich. Der Patient hat aber möglicherweise vieles vergessen und manches nie so genau gewußt. Einiges fällt ihm gerade nicht ein und anderes fällt ihm zwar ein, aber er hält es so lange nicht für erwähnenswert, wie er sich nicht darauf angesprochen fühlt. Im Prinzip soll dieser Mangel durch die ärztliche Dokumentation der gesundheitlichen Vorgeschichte des Patienten ausgeglichen werden. Die entsprechenden Unterlagen sind aber oft nicht greifbar, z. B. wegen Arztwechsels, oder auf verschiedene Ärzte verteilt und deshalb im konkreten Bedarfsfall nur partiell nutzbar.

Deshalb ist es nicht nur für Notfälle sinnvoll, die wesentlichen Gesundheitsdaten eines Patienten auf einer Chipkarte festzuhalten, damit sie für seine späteren Behandlungen auch tatsächlich verfügbar sind. Soweit die Daten zu viel Speicherplatz belegen würden, könnte statt der Daten etwa einer Röntgenaufnahme auch die Adresse angegeben werden, von der diese Daten abgerufen werden können. Im Rahmen der in Deutschland begonnenen Kartenprojekte wird auch dieses Verfahren erprobt.

Wenn die Pläne zur Integration des Lesens und Beschreibens der Karte in der ohnehin schon in naher Zukunft sehr leistungsfähigen Datenverarbeitung in Arztpraxen, in Krankenhäusern und bei anderen Leistungserbringern des Gesundheitswesens realisiert sind, wird der zusätzliche Aufwand für die Nutzung

solcher Karten weit geringer sein als die damit erzielten Vorteile. Diese werden noch größer, wenn – wie zu erwarten ist – die internationale Zusammenarbeit das Ziel erreicht, zumindest für die Daten auf der Karte das Sprachenproblem dadurch zu lösen, daß jedem Zugriffsberechtigten die Daten der Karte durch das von ihm verwendete – nationale – Leseprogramm in seiner Sprache präsentiert werden.

Der Nutzen der Verfügbarkeit der Daten zugunsten eines Patienten ist eng mit dem Risiko verbunden, daß die Daten ohne oder gar gegen den Willen dieses Patienten aus der Karte gelesen werden könnten. Zum Schutz der Patienten gegen die unbefugte Offenbarung ihrer Gesundheitsdaten sind deshalb besondere technische, organisatorische und rechtliche Maßnahmen zu treffen. Diese Maßnahmen müssen auch gewährleisten, daß der Patient nicht zum bloßen Objekt des Kartensystems wird, etwa dadurch, daß er keinen Einfluß darauf hat, was auf seiner Chipkarte steht oder wer aus welchem Anlaß was lesen kann.

9.2.2 Entscheidungsfreiheit der Betroffenen

Gesundheitsdaten gehören zu den Angaben über eine Person, für die es besonders wichtig ist, die Selbstbestimmung der Betroffenen über den Umgang mit ihren Daten zu gewährleisten. Jeder muß deshalb selbst bestimmen können,

- ob seine Gesundheitsdaten überhaupt auf (s)einer Chipkarte gespeichert werden, es darf also keinen gesetzlichen oder sozialen Zwang geben,
- ob er seine Gesundheitsdatenkarte in einer konkreten Situation präsentiert oder statt dessen lieber die ihm sachgerecht erscheinenden Informationen vorträgt, wozu auch gehört, daß nicht oder wenigstens nicht ohne weiteres bekannt wird, wer eine Gesundheitsdatenkarte besitzt,
- welche seiner Gesundheitsdaten tatsächlich auf seine Karte aufgenommen werden sollen, was nicht nur gewisse Vorkehrungen in der Software der Kartensysteme verlangt, sondern – wenn dieses Recht zum Nutzen des Betroffenen wirken soll – in den vermutlich seltenen kritischen Fällen eine auf die jeweiligen Besonderheiten eingehende Beratung durch den Arzt erfordert, und
- welche der in der Karte enthaltenen Angaben bei welcher Gelegenheit gelesen werden sollen.

Diese Forderungen sind sowohl in den 10 Thesen der Arbeitsgemeinschaft „Karten im Gesundheitswesen" **(s. Anlage 23)** als auch in einer Entschließung der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder **(s. Anlage 14)** enthalten.

Die Erfüllung der oben zuletzt genannten Forderung trifft in der Praxis auf enge Grenzen, weil etwa die scheibchenweise Freigabe einzelner Daten im Laufe eines Arzt-Patienten-Dialogs technisch schwer realisierbar ist und das Vertrauensverhältnis belasten würde. Eher möglich ist eine Unterscheidung nach der Fachzuordnung der Lesenden, die durch deren Health Professional Card (s. o. Nr. 9.1.2) ausgewiesen ist. Es ist damit zu rechnen, daß in den nächsten Jahren für derartige Fragen unterschiedliche Lösungen untersucht und erprobt werden. Soweit dies mit der notwendigen Interoperabilität der verschiedenen Kartentypen und -systeme zu vereinbaren ist, könnten für solche Fragen auch verschiedene Lösungen auf Dauer angeboten werden.

Wie ernst die Entscheidungsfreiheit der Betroffenen in den deutschen Kartenprojekten genommen wird, zeigt – als ein Beispiel für viele – der folgende Absatz aus der vorformulierten datenschutzrechtlichen Einwilligungserklärung im Pilotprojekt „EDV-gestützte DentCard":

> *„Auf meinen Wunsch werden sämtliche oder einzelne Informationen auf der Karte gelöscht. Ich habe das Recht, jederzeit und kostenfrei Einsicht in die auf der Karte gespeicherten Informationen zu nehmen und zu erfahren, welche Informationen dort gespeichert sind."*

9.2.3 Technischer und organisatorischer Schutz für Gesundheitsdaten in Chipkarten

Die Gesundheitsdaten erzielen ihren vollen Nutzen nur dann, wenn die Inhaber sie so gut wie ständig mitführen, damit sie bei Bedarf auch verfügbar sind. Unter diesen Umständen kann die notwendige Vertraulichkeit der Gesundheitsdaten nur gewährleistet werden, wenn durch technische Maßnahmen gesichert ist, daß nicht jeder, der eine solche Karte zufällig oder gar unberechtigt in die Hand bekommt, die darin enthaltenen Daten auslesen kann. Die Möglichkeit des Lesens muß deshalb durch technische Maßnahmen auf diejenigen Personen beschränkt bleiben, die nach ihrer beruflichen Stellung dazu befugt sind.

Diese Forderung kann durch das Zusammenspiel von Patientenkarte und Health Professional Card (HPC) erfüllt werden: Das Programm in der Patientenkarte prüft, ob die korrespondierende HPC echt (und noch gültig) ist, und gibt dann nur die Daten aus, die der nachgewiesenen beruflichen Stellung entsprechen (s. o. Nr. 9.1.2). Abgesehen von dem unvermeidbaren, aber hier sehr geringen Risiko, daß die technischen Sicherungen überwunden werden könnten, bleibt dann nur das Risiko, daß ein Angehöriger der Gruppe der im Prinzip Berechtigten eine Karte außerhalb seiner kurativen Tätigkeit und ohne anderen rechtfertigenden Grund liest. Um dieses ohnehin nicht besonders große Risiko zu verringern, sollen alle Zugriffe in der gelesenen Karte protokolliert werden, was wegen des technischen Fortschritts auf diesem Gebiet keinen besonderen Aufwand erfordert.

Derartige Schutzmaßnahmen haben außer ihrer unmittelbaren Wirkung auch den Vorteil, daß jedes Lesen der so geschützten Daten durch einen Unberechtigten schon nach geltendem Recht als Ausspähen von Daten strafbar wäre, weil sie „gegen unberechtigten Zugang besonders gesichert sind" (§ 202a Abs. 1 StGB). Sie haben darüber hinaus zur Folge, daß in der Regel die Betroffenen selbst ihre in der Karte gespeicherten Gesundheitsdaten nicht ohne Hilfe eines wegen seiner beruflichen Stellung Leseberechtigten zur Kenntnis nehmen können. Dies mag zunächst nur hinderlich erscheinen, es schützt

die Betroffenen aber davor, diese Daten unter Druck unberechtigten Fragestellern zu offenbaren, und leistet auch damit einen Beitrag zur gebotenen Vertraulichkeit.

9.2.4 Gesetzlicher Schutz für Gesundheitsdaten auf Karten

Das gegenwärtige Datenschutzrecht wurde geschaffen, um den Umgang mit Daten von natürlichen Personen durch andere zu regeln. Auch der strafrechtliche Schutz des Privatgeheimnisses (§ 203 StGB) bezieht sich ebenso wie die damit korrespondierenden Beschlagnahmeverbote der Strafprozeßordnung nur auf fremde Geheimnisse. Damit könnten aber Gesundheitsdatenkarten in der Obhut der jeweils Betroffenen beschlagnahmt werden und z. B. ihre Daten von Gutachtern mit Zugangsmöglichkeiten ausgelesen und weiterverwendet werden.

Wenn diese Daten aber nicht genau so geschützt würden, als wären sie in der Obhut des behandelnden Arztes oder einer Krankenanstalt, würde den Betroffenen nicht nur der gebotene Schutz ihrer Gesundheitsdaten versagt, sondern viele würden sich auch scheuen, sich auf ein derartiges System einzulassen. Denn gerade die Daten, die besonders wichtig sind, weil sie zu beachtende Gesundheitsverhältnisse beschreiben, die nicht ohne weiteres erkannt werden können, sind als besonders heikel anzusehen. Deshalb bedarf es einer gesetzlichen Regelung, mit der die Nutzung der Gesundheitsdatenkarte strikt auf therapeutische Zwecke zugunsten des Betroffenen beschränkt wird. Dabei sind auch Vorkehrungen dagegen zu treffen, daß der Betroffene bisweilen selbst – z. B. unter Druck – in das zweckfremde Lesen der Karte „einwilligen" muß. Und immer dann, wenn die Strafverfolgung geboten scheint, um das allgemeine Vertrauen in die mit diesen Systemen geschaffene Infrastruktur zu schützen, sollte sie nicht von einem Antrag des unmittelbar Betroffenen abhängig sein.

Insgesamt muß auch der gesetzliche Schutz dieser Daten dazu beitragen, daß niemand fürchten muß, dem folgenden Szenario ausgesetzt zu sein, das sich inzwischen zu einer Art Prüfstein entwickelt hat:

> Am Ende des Einstellungsgesprächs bittet der Vertreter des Betriebes den Kandidaten, seine Gesundheitsdaten durch den dafür hinzugezogenen Betriebsarzt lesen zu lassen. Der Kandidat weiß zwar, daß schon die Bitte unzulässig ist und er sie von Rechts wegen abschlagen könnte, aber er weiß auch, daß er dann die Stelle nicht bekommt.

Technische, organisatorische und gesetzliche Vorkehrungen müssen für jedermann verständlich gewährleisten, daß solche oder ähnliche Szenen nie stattfinden.

9.3 Chipkarten als elektronische Geldbörsen

9.3.1 Geld auf Karten

Im bargeldlosen Zahlungsverkehr bestimmen schon seit langem automatisierte Datenverarbeitungsverfahren die internen Clearingsysteme. Seit vielen Jahren gibt es auch Bemühungen, Kundenkontakte zu automatisieren, statt Aufträge am Schalter oder per Brief anzunehmen und danach die Daten in die Verfahren einzugeben. Beispiele dafür sind neben Online-Verfahren für den Kontakt des Kunden mit seiner Bank der Einsatz von Geldautomaten und – im Einzelhandel – der Einsatz von Kassen, über die mit Hilfe von Kredit- oder ec-Karten eine Online-Abfrage beim jeweiligen Kreditinstitut erfolgt, mit dessen Garantie dann der Zahlungsauftrag automatisch erstellt wird. Die Datenverarbeitung, mit der diese Zahlungsaufträge durchgeführt werden, ähnelt der des Scheckeinzugs – allerdings kommt der Scheck als Gegenstand dabei nicht mehr vor.

Dem Wunsch, in automatisch zu verarbeitenden Daten nicht nur den Transfer von Geld abzubilden, sondern das Geld selbst zu verkörpern, stand lange Zeit entgegen, daß solche Daten leicht zu kopieren und die Kopien vom Original praktisch nicht zu unterscheiden waren. Um den damit möglichen Mißbrauch bekämpfen zu können, sind Kontrollverfahren erforderlich, deren Aufwand die Vorteile einer elektronischen Sofortzahlung erheblich mindert.

Die modernen Chipkarten ermöglichen es, Daten, die Geld bedeuten, in Chipkarten durch die Programme in den Karten kontrolliert zu verwalten: Geld-Daten werden nur dann an eine Empfänger-Karte gesendet, wenn zugleich der Betrag in der Absender-Karte entsprechend herabgesetzt wird, und außerdem wird der Betrag in der Empfänger-Karte nur um diesen Betrag heraufgesetzt. Durch kryptographische Verfahren kann man die Transfer-Daten zudem so „verpacken", daß keine andere Karte mit diesen Daten ihren Geldbestand erhöhen und auch die Empfänger-Karte die Daten eines Transfers nur einmal nutzen kann. Das Kopieren der Transfer-Daten kann deshalb nicht zur Geldvermehrung genutzt werden. Mit diesen Verfahren läßt sich auch das erfolgreiche Fälschen von Transfer-Daten verhindern, so daß diese Daten auf dem Weg zwischen den beteiligten Karten nicht besonders geschützt werden müssen. Damit können solche Zahlungen auch über Datennetze abgewickelt werden. Weil die Programme in den Karten so gestaltet werden können, daß sie je nach Bedarf Geldgeber oder Geldempfänger sind, ist das Übertragen von Kartengeld von Karte zu Karte im Prinzip möglich, ohne daß für diesen Geldumlauf eine Clearinginstanz benötigt würde.

Die Sicherheitsanforderungen an diese Verfahren sind sehr hoch. So müssen beispielsweise unberechtigte Änderungen durch die Karteninhaber verhindert und technische und organisatorische Vorkehrungen getroffen werden, um das unberechtigte Erschaffen von Kartengeld für den Geldumlauf zu verhindern. Trotz der hohen Anforderungen an die Sicherheit wird seit etwa 1½ Jahren ein derartiges Zahlungsverfahren in der Praxis erprobt.

9.3.2 Die GeldKarte des deutschen Kreditgewerbes

Im Frühjahr 1996 wurden im Rahmen eines Pilotprojekts in der Region Ravensburg/Weingarten ec-Karten mit Chip ausgegeben, mit denen auch Zahlungen – ähnlich wie aus einer Geldbörse – möglich sind. Der Ende 1996 für viele ec-Karten turnusmäßig erfolgende Umtausch wurde genutzt, um in ganz Deutschland solche Karten auszuliefern.

Das damit mögliche Zahlungsverfahren ist von dem oben beschriebenen Kartengeld-Umlauf (s. o. Nr. 9.3.1) noch etwas verschieden: Nur die Banken können in einem für sie reservierten Verfahren „Geld" (bis zum Höchstbetrag von DM 400,00) auf diese Karten laden, was sowohl am Schalter als – in Kürze – auch an dafür eingerichteten Automaten möglich ist. Die Kunden können diese Karten zum Bezahlen nur an sog. GeldKarten-Terminals verwenden, die insbesondere an Einzelhandelskassen und Tankstellen sowie in Fahrkarten-, Parkschein- und Warenautomaten installiert werden sollen. Ein Transfer von Karte zu Karte ist nicht möglich. Auch vom GeldKarten-Terminal können die von den einzelnen Karten abgebuchten Beträge nicht direkt in Umlauf gebracht werden. Vielmehr wird über jede einzelne Kartennutzung ein Datensatz gespeichert, den der Betreiber des GeldKarten-Terminals bei (s)einer Bank einreichen muß, um dafür eine Gutschrift zu erhalten. Die Bank reicht jeden empfangenen Datensatz an die für die darin bezeichnete GeldKarte zuständige Evidenzzentrale weiter. Dort wird für diese Karte ein Saldo geführt, von dem die Zahlungen abgebucht und zu dem die Ladebeträge zugebucht werden. Außerdem wird dort u. a. kontrolliert, ob Umsatzdaten mehrfach eingereicht wurden.

In dem Maße, in dem dieses Zahlungsverfahren Barzahlungen verdrängt, wird die Anonymität der Barzahlung durch das Erzeugen und Speichern kartenbezogener – und damit i. d. R. auch auf deren Inhaber beziehbarer – Daten abgelöst. Diese Daten können geeignet sein, die bereits jetzt aus dem bargeldlosen Zahlungsverkehr ableitbaren Ausgabe- und Konsumprofile um die Details von kleinen und kleinsten Zahlungen zu ergänzen **(s. dazu auch Anlage 11)**.

Es mag dahinstehen, ob derart detaillierte Aufzeichnungen zur Kontrolle der Zuverlässigkeit des Systems überhaupt erforderlich sind. Dagegen spricht zumindest, daß bereits ein Jahr früher in Österreich ein ähnliches Verfahren eingeführt wurde, in dem aber bereits im Terminal des Akzeptanten der Kartenzahlung die einzelnen Zahlungen so kumuliert werden, daß die Aktionen den einzelnen Karten nicht mehr zugeordnet werden können. Wenn aber solche Aufzeichnungen erfolgen und an Evidenzzentralen weitergeleitet werden sollen, dann sollte das den Kunden erläutert werden. Dazu gehören auch klare Angaben über die Speicherungsdauer und die Nutzungen dieser Daten im Regelfall und aus besonderen Anlässen. Diese stehen noch aus.

9.3.3 Neues Geld – neue Karten

In den kommenden Jahren wird durch die Einführung des Euro der Raum für Zahlungsverkehrssysteme neu geordnet, und etwa im selben Zeitraum werden neue Anforderungen des Zahlungsverkehrs in grenzüberschreitenden Netzen die Bedeutung von Landes- und Währungsgrenzen für den Zahlungsverkehr schrumpfen lassen. Eine Chipkarte des deutschen Kreditgewerbes müßte dann mit den Systemen in anderen Euro-Ländern konkurrieren, und jedes dieser Systeme müßte seine Eignung als Zahlungsmittel in einem weltweiten Informationsnetz beweisen. Wenn die Welt zum „globalen Dorf" wird, wird eben auch der Weg des Kunden zur Konkurrenz kürzer. Die Tatsache, daß ein bedeutendes Kreditkartenunternehmen jüngst eine Mehrheitsbeteiligung an einem Geldbörsensystem erworben hat, macht deutlich, daß der Wettbewerb international geführt wird.

Viele der Leistungen in einem künftigen weltweiten Netz, dessen Vorstufe das Internet in seiner heutigen Form sein dürfte, werden entgeltlich sein, und viele dieser Entgelte werden aus kleinen und kleinsten Beträgen (neudeutsch „Micropayments") bestehen. Kaum jemand wird aber unbefangen Informationen anfordern, wenn er weiß, daß jede Lieferung einen Datensatz zur Evidenzzentrale seiner Zahlungskarte in Marsch setzt. Garantierte Anonymität und damit gekoppelt die sofortige, völlig anonym zu buchende Bezahlung werden deshalb die **zugesicherten Eigenschaften** beim Vertrieb von Informationen und Unterhaltungsangeboten über Netze sein, ohne die Markterfolge bestenfalls in Nischen zu erzielen sind (s. dazu auch Nr. 8.1).

Wer damit umworben wird, daß weder sein Browsen durch das Unterhaltungsangebot noch seine Auswahl Datenspuren hinterlassen und selbst seine Zahlung sofort nach dem Mausklick so anonym durchgeführt wird, daß nicht einmal die Tatsache seines Kontaktes mit diesem Anbieter erkennbar bleibt, der wird wissen, daß anonymes Zahlen keine Utopie ist. Erreichbarer Datenschutz wird damit zwangsläufig zu einem wichtigen Beurteilungskriterium von Zahlungssystemen für alle die Fälle, in denen weder ein Kredit eingeräumt noch das Geld von Konto zu Konto bewegt werden soll. Und wer diesen Datenschutz anbietet, dessen Chipkarte wird auch für die anderen Funktionen leichter in die Hand genommen werden.

Eine elektronische Geldbörse sollte deshalb zumindest auch die Möglichkeit zum völlig anonymen Bezahlen bieten, damit jeder selbst bestimmen kann, wann seine Zahlung welche Spuren hinterläßt.

10 Telekommunikation

10.1 „Postreform III": Telekommunikationsgesetz

10.1.1 Regulierungsziele, Begriffsbestimmungen

Neben den sich an Art. 87 f GG orientierenden Regulierungszielen, auf den Märkten der Telekommunikation einen chancengleichen und funktionsfähigen Wettbewerb sicherzustellen (§ 2 Abs. 2 Nr. 2 TKG) und eine flächendeckende Grundversorgung mit Telekommunikationsdienstleistungen zu erschwinglichen Preisen zu gewährleisten (§ 2 Abs. 2 Nr. 3 TKG), sind aus meiner Sicht die Wahrung der Interessen der Nutzer auf dem Gebiet der Telekommunikation und des Funkwesens sowie die Wahrung des Fernmeldegeheimnisses (§ 2 Abs. 2 Nr. 1 TKG) von besonderem Interesse. Dieses Regulierungsziel findet seine besondere Ausprägung im elften Teil des Gesetzes (§§ 85 bis 93 TKG). Neben der Vorschrift zur Wahrung des Fernmeldegeheimnisses (§ 85 TKG) finden sich ausdrückliche Regelungen zum Datenschutz in § 89 TKG. Schon der Umfang dieser Vorschrift dokumentiert den Willen des Gesetzgebers,

das Selbstbestimmungsrecht des Bürgers weitestgehend zu schützen. Ich bin deshalb von meiner ursprünglichen Forderung abgerückt, den Datenschutz ebenfalls ausdrücklich als Regulierungsziel zu nennen. Es entsprach nicht nur den Interessen der Bundesregierung, sondern aller am Gesetzgebungsverfahren Beteiligten, das Telekommunikationsgesetz noch vor der Sommerpause in Kraft treten zu lassen. Lange Diskussionen um den Katalog der Regulierungsziele wären diesem Ziel nicht förderlich gewesen. Entscheidend ist, daß sowohl dem Fernmeldegeheimnis als auch dem Datenschutz angemessen Rechnung getragen wird.

Zu den in § 3 Nr. 1 bis 24 TKG enthaltenen Begriffsbestimmungen will ich mich auf diejenigen beschränken, die für den elften Teil des Gesetzes von besonderer Bedeutung sind: Nach § 3 Nr. 5 TKG ist „geschäftsmäßiges Erbringen von Telekommunikationsdiensten" das nachhaltige Angebot von Telekommunikation einschließlich des Angebots von Übertragungswegen für Dritte mit oder ohne Gewinnerzielungsabsicht. Durch die Einführung des Begriffs des geschäftsmäßigen Erbringens von Telekommunikationsdiensten, für die ich mich stets mit Nachdruck eingesetzt habe, ist die erforderliche Differenzierung im Anwendungsbereich gegenüber den „Telekommunikationsdienstleistungen" (§ 3 Nr. 18 TKG) gewährleistet. Insbesondere die Vorgaben im elften Teil des Gesetzes (Datenschutz, Fernmeldegeheimnis) gelten damit auch für Unternehmen, die Telekommunikationsdienste „ohne Gewinnerzielungsabsicht" anbieten (s. u. Nr. 10.1.3).

10.1.2 Auch das schnurlose Telefon des Nachbarn darf nicht abgehört werden

Durch die erste öffentliche Rundfunkübertragung der Welt aus Königs Wusterhausen im Jahre 1920 wurde einer breiten Öffentlichkeit bekannt, daß gesprochene Worte und auch Musik unsichtbar und über große Entfernungen, nämlich mittels der Funktechnik übertragen werden können. Dieses Medium fasziniert bis heute Millionen von Menschen und veranlaßt sie, auch Funksendungen zu hören – oder zu sehen –, die gar nicht für sie bestimmt sind. Lediglich schöpferischer Neugier ist es zuzurechnen, wenn Menschen erheblichen technischen Aufwand betreiben, um Rundfunksender aus Australien oder der Südsee empfangen zu können.

Probleme ergeben sich demgegenüber, wenn neugierige Zeitgenossen etwa den Funkverkehr der sogenannten **Behörden und Organisationen mit Sicherheitsaufgaben (BOS)** abhören, z. B. von Polizei, Feuerwehr oder Bundesgrenzschutz. Es leuchtet unmittelbar ein, daß es die Arbeit der Polizei gravierend beeinträchtigen kann, wenn Unbefugte durch das Abhören des Funkverkehrs z. B. Informationen über eine laufende Fahndung erhalten oder aber, wenn die Feuerwehr bei der Arbeit durch Neugierige behindert wird, die durch das Abhören des Funkverkehrs Kenntnis vom Großbrand erhalten haben. Allerdings wissen sowohl die Polizeibeamten als auch die Feuerwehrleute um die Abhörbarkeit des Funkverkehrs und versuchen – in hoffnungsvoller Erwartung längst angekündigter verbesserter und abhörsicherer Technik – sich zu behelfen.

Anders sieht dies jedoch bei den „nichtprofessionellen" Nutzern moderner Funktechnik aus. So wissen nur wenige Nutzer sogenannter **schnurloser Telefone**, von denen bereits mehrere Millionen Geräte im Einsatz sind, daß ihr Telefonat problemlos abgehört werden kann. Einzige Voraussetzung ist ein geeigneter Funkempfänger (Breitbandempfänger, „Scanner" usw.), wie er seit einigen Jahren in vielen Fachgeschäften und im Versandhandel zu moderaten Preisen erhältlich ist. Bis zum Jahre 1993 durfte die Empfangsmöglichkeit („Wellenbereich") solcher Geräte lediglich die Bereiche umfassen, die aufgrund internationaler Vereinbarungen für den Rundfunk – also für Funksendungen an alle – vorgesehen war. Nachdem das Bundesministerium für Post und Telekommunikation die entsprechenden Zulassungsbeschränkungen für Empfangsgeräte aufgehoben hat, müssen die meisten Benutzer eines schnurlosen Telefons damit rechnen, daß ihr Telefonat abgehört werden kann. Ich habe dies seinerzeit gegenüber dem Bundesministerium scharf kritisiert (14. TB Nr. 21.10) und gefordert, rechtliche Gegenmaßnahmen zu ergreifen. Hieran habe ich erinnert, als mit den ersten Überlegungen zum TKG begonnen wurde. Allerdings enthielten die ersten Entwürfe des Gesetzes lediglich ein Verbot, unbefugt Funksendungen abzuhören, die von hoheitlichen Zwecken dienenden Funkanlagen ausgesendet werden, also z. B. den Polizeifunk. Angesichts der großen Verbreitung der Funkübertragung auch im privaten Lebensbereich einerseits, der zunehmenden Verbreitung von geeigneten Abhörgeräten andererseits habe ich sowohl bei den Beratungen des Gesetzentwurfes auf Regierungsebene als auch gegenüber parlamentarischen Gremien gefordert, auch das Abhören privater Funksendungen zu verbieten und dieses ebenso wie das Abhören des Polizeifunks mit Strafe zu bewehren. Dem hat sich im übrigen der Bundesrat in seiner Stellungnahme zum Gesetzentwurf angeschlossen.

§ 86 TKG bestimmt jetzt in bemerkenswerter Deutlichkeit:

> *„Mit einer Funkanlage dürfen Nachrichten, die für die Funkanlage nicht bestimmt sind, nicht abgehört werden. Der Inhalt solcher Nachrichten sowie die Tatsache ihres Empfangs dürfen, auch wenn der Empfang unbeabsichtigt geschieht, . . . anderen nicht mitgeteilt werden."*

In § 95 TKG wird mit Freiheitsstrafen bis zu zwei Jahren oder mit Geldstrafe bedroht, wer entgegen § 86 TKG eine Nachricht abhört oder den Inhalt einer Nachricht oder die Tatsache ihres Empfangs einem anderen mitteilt.

Unberührt bleibt dabei im übrigen, daß der Empfang von Rundfunksendungen keinerlei Beschränkungen unterliegt.

Damit ist klargestellt, daß es keine „läßliche Sünde" ist, das schnurlose Telefon seines Nachbarn abzuhören, sondern eine Straftat, die mit hoher Strafe bedroht ist. Unerläßlich scheint es mir jedoch zu sein, daß diese gesetzliche Regelung – auch durch Öffentlichkeitsarbeit der zuständigen Ministerien – noch besser bekannt gemacht wird: Einer Pressemitteilung konnte ich kürzlich entnehmen, daß zu unfallträchti-

gen Zeiten – wie z. B. beim ersten Schneefall – mancher Abschleppunternehmer den Funkverkehr von Polizei und Feuerwehr abhört, um möglichst als Erster ein Unfallfahrzeug abschleppen zu können. Falls dies zutrifft, ist zu bezweifeln, ob die Abschleppunternehmer in solchen Fällen wußten, daß ihr Tun mit „Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe" bedroht ist!

10.1.3 Datenschutz auch in Corporate Networks

Relativ früh bestand zwischen den am Gesetzgebungsverfahren beteiligten Ressorts der Bundesregierung Einigkeit darüber, daß zur Wahrung des Fernmeldegeheimnisses – welches nunmehr in § 85 TKG eine einfachgesetzliche Ausprägung gefunden hat – jeder verpflichtet ist, der „geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt" (vgl. § 85 Abs. 2 TKG). Denn das Interesse der Nutzer von Telekommunikationsdiensten, den Inhalt und die näheren Umstände der Telekommunikation Dritten gegenüber geheimzuhalten, besteht unabhängig davon, ob die Dienste mit oder ohne Gewinnerzielungsabsicht angeboten werden.

Dem Fernmeldegeheimnis unterliegen damit – wie dies ebenfalls in der Begründung des Gesetzentwurfs zum Ausdruck kommt – beispielsweise auch Corporate Networks, Clubtelefone und Nebenstellenanlagen in Hotels und Krankenhäusern sowie in Betrieben und Behörden, soweit sie den Beschäftigten zur privaten Nutzung zur Verfügung gestellt sind. Nicht unter das Fernmeldegeheimnis fallen dagegen in der Regel private Endgeräte, Haustelefonanlagen und hauseigene Sprechanlagen. Bei den sog. Corporate Networks handelt es sich um geschlossene Benutzergruppen, die nicht jedermann öffentlich zugänglich sind, wie z. B. Netzwerke von Unternehmen oder Behörden. Wegen der Komplexität und der Vielfalt denkbarer Konfigurationen bei Telekommunikationsanlagen ist eine enumerative Aufzählung der Schutzbereiche des Fernmeldegeheimnisses nicht möglich. Im Einzelfall ist deshalb auf das schutzwürdige Vertrauen der Beteiligten abzustellen.

Erfolgt die Telekommunikation durch oder über Menschen, wird das Schutzanliegen des Fernmeldegeheimnisses zu dem des Datenschutzes. Um so erstaunlicher war daher für mich die anfängliche Zurückhaltung der Bundesregierung im Gesetzgebungsverfahren, mit den Vorschriften zum Datenschutz dieselben Unternehmen und Personen zu verpflichten, die auch dem Fernmeldegeheimnis unterliegen. Denn der Gesetzentwurf sah Datenschutzregelungen nur für das gewerbliche Angebot von Telekommmunikation – also mit Gewinnerzielungsabsicht – vor. Diese Haltung der Bundesregierung wurde mit Rücksicht auf die europäische ISDN-Richtlinie (s. u. Nr. 10.3) jedoch in der Schlußphase der Beratungen aufgegeben, da anderenfalls wegen der Reichweite des Fernmeldegeheimnisses etwa die Verpflichtung aus § 89 Abs. 6 TKG, u. a. Strafverfolgungsbehörden Auskunft zu erteilen (s. u. Nr. 10.1.5), nur für denjenigen bestanden hätte, der seine Dienste mit Gewinnerzielungsabsicht anbietet. Die Umgehungsmöglichkeiten, die sich daraus eröffnet hätten, liegen auf der Hand.

§ 89 Abs. 1 TKG nennt jetzt die zum Datenschutz Verpflichteten wortgleich wie diejenigen, die zur Wahrung des Fernmeldegeheimnisses verpflichtet sind: Fernmeldegeheimnis und Datenschutz muß jeder sicherstellen, der unabhängig von einer Gewinnerzielungsabsicht Telekommunikationsdienste erbringt oder daran mitwirkt.

10.1.4 Eintragung ins gedruckte und elektronische Telefonbuch – nur wenn und wie der Kunde es will!

Zu den ersten an meine Behörde gerichteten Eingaben gehörten Beschwerden über die damalige Praxis der „Zwangseintragung" von Telefonanschlüssen ins Telefonbuch – grundsätzlich mußte sich jeder Inhaber eines Telefonanschlusses in das Telefonbuch eintragen lassen. Ausnahmen wurden nur für Prominente und besonders gefährdete Personen des öffentlichen Lebens gemacht. Erst mit dem Volkszählungsurteil des BVerfG im Dezember 1983 begann auch bei der Deutschen Bundespost und dem Bundespostministerium ein Umdenken. Es dauerte jedoch bis 1991, ehe jeder Telefonkunde durch die Telekom-Datenschutzverordnung das Recht erhielt, selbst darüber zu entscheiden, ob er überhaupt in das Telefonbuch eingetragen werden will und ggf. mit welchem Text. Dieses Recht konnte er durch Widerspruch wahrnehmen; tat er dies nicht, wurde sein Anschluß ins Telefonbuch eingetragen und auch über die Auskunft bekanntgegeben.

Das TKG hat das Recht des Kunden auf Selbstbestimmung nunmehr endlich festgeschrieben: Nach § 89 Abs. 8 darf die Telekom – ebenso wie die anderen Diensteanbieter – *„Kunden mit ihrem Namen, ihrer Anschrift und zusätzlichen Angaben, wie Beruf, Branche, Art des Anschlusses und Mitbenutzer, in öffentlich gedruckte oder telefonische Verzeichnisse eintragen, soweit der Kunde dies beantragt hat. Dabei kann der Kunde bestimmen, welche Angaben in den Kundenverzeichnissen veröffentlicht werden sollen, daß die Eintragung nur in gedruckten oder elektronischen Verzeichnissen erfolgt oder daß jegliche Eintragung unterbleibt."* Die Vorschrift enthält im übrigen eine Übergangsregelung für diejenigen Kunden, die beim Inkrafttreten des Gesetzes bereits eingetragen waren.

Die Vorschrift enthält zwei wesentliche Neuerungen: Nach altem Recht durfte der Kunde grundsätzlich in Verzeichnisse eingetragen werden, wogegen er lediglich ein Widerspruchsrecht hatte. Nach neuem Recht ist die Eintragung nur zulässig, wenn der Kunde dies ausdrücklich wünscht. Hat er bei Vertragsabschluß einen solchen Wunsch nicht geäußert, darf eine Eintragung nicht erfolgen.

Eine weitere rechtliche Neuerung betrifft elektronische Teilnehmerverzeichnisse: Wenn der Kunde will, kann er sich in solche elektronische Teilnehmerverzeichnisse aufnehmen lassen. Dabei muß sich jeder Kunde jedoch über folgendes im klaren sein, daß sein Telefonanschluß über Online-Dienste – wie z. B. im T-Online-Dienst der Deutschen Telekom AG – bekanntgegeben oder aber daß der Anschluß in ein CD-ROM-Verzeichnis eingetragen wird, also in einen optisch lesbaren Datenträger, der mit Hilfe

eines PC gelesen und ausgewertet werden kann (siehe auch auf Nr. 10.4.5). Diese Bekanntgabe des Telefonanschlusses durch elektronische Verzeichnisse ist bis heute nicht nur vielen Bürgern unbekannt, sondern sie ermöglicht auch Auskünfte, gegen die viele Bürger sich auch ausdrücklich verwahren.

Ich habe mich sowohl gegenüber der Bundesregierung als auch bei den parlamentarischen Beratungen mit Nachdruck für eine Verbesserung der rechtlichen Situation der Telefonkunden eingesetzt. Durch die Neuregelung des § 89 Abs. 8 hat der Kunde jetzt abgestufte Rechte, denn er kann nicht nur entscheiden, ob er überhaupt in ein Verzeichnis, sondern auch, ob er nur in ein gedrucktes oder auch in elektronische Verzeichnisse eingetragen werden möchte.

10.1.5 Auskünfte über Telefonkunden an Strafverfolgungs-, Polizei- und Sicherheitsbehörden

Wer geschäftsmäßig Telekommunikationsdienste anbietet, ist nach § 90 TKG verpflichtet, Kundendateien zu führen, in die unverzüglich die Rufnummern und Rufnummernkontingente, die zur weiteren Vermarktung oder sonstigen Nutzung an andere – z. B. sog. Service-Provider – vergeben werden, sowie Name und Anschrift der Inhaber von Rufnummern und Rufnummernkontingente aufzunehmen sind. Das gilt auch, soweit diese nicht in öffentlichen Verzeichnissen eingetragen sind. Die aktuellen Kundendateien sind so verfügbar zu halten, daß die Regulierungsbehörde einzelne Daten oder Datensätze in einem von ihr vorgegebenen automatisierten Verfahren abrufen kann. Der Verpflichtete hat durch technische und organisatorische Maßnahmen sicherzustellen, daß ihm Abrufe nicht zur Kenntnis gelangen können.

Auskünfte aus den Kundendateien sind

- den Gerichten, Staatsanwaltschaften und andern Justizbehörden sowie sonstigen Strafverfolgungsbehörden,
- der Polizei von Bund und Ländern für Zwecke der Gefahrenabwehr,
- den Zollfahndungsämtern für Zwecke eines Strafverfahrens sowie dem Zollkriminalamt zur Vorbereitung und Durchführung von Maßnahmen nach § 39 des Außenwirtschaftsgesetzes und
- den Verfassungsschutzbehörden des Bundes und der Länder, dem MAD und dem BND

jederzeit unentgeltlich zu erteilen, soweit dies zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist. Die Regulierungsbehörde hat die Daten, die in Kundendateien gespeichert sind, auf Ersuchen der vorgenannten Stellen automatisiert abzurufen und an die ersuchende Stelle zu übermitteln.

Mit dieser Vorschrift wollte der Gesetzgeber dem Umstand Rechnung tragen, daß Auskunftsersuchen über die genannten Daten nicht mehr wie früher nur von der Telekom beantwortet werden können, sondern hierfür inzwischen mehrere Adressaten – insbesondere die Mobilfunkanbieter – in Frage kommen. Um zeitraubende Recherchen darüber zu vermeiden, bei wem diese Daten gespeichert sind, wurde die Rechtsgrundlage für ein automatisiertes Abrufverfahren geschaffen, die als Bedarfsträger auch die Sicherheitsbehörden vorsieht.

Nur wenige Vorschriften des TKG haben – schon vor dessen Inkrafttreten – eine vergleichbare Diskussion entfacht, in der ich mir auch und gerade von informierten Kreisen etwas mehr Objektivität gewünscht hätte. Die teilweise erhobene Behauptung, mit dieser Vorschrift nehme man vom Fernmeldegeheimnis Abschied, ist unzutreffend, da die genannten Daten nicht dem Fernmeldegeheimnis unterliegen. Dieses Verfahren sieht eben nicht den Abruf von Verbindungsdaten oder Gesprächsinhalten vor.

Soweit der Anbieter von Telekommunikationsdiensten durch technische und organisatorische Maßnahmen sicherzustellen hat, daß ihm Abrufe nicht zur Kenntnis gelangen können, wurde vereinzelt der Vorwurf erhoben, hierdurch erhielten die Strafverfolgungs- und Sicherheitsbehörden die Möglichkeit, sich in Telekommunikationsdatenbeständen – quasi im verborgenen – selbst zu bedienen. Auch dieser Vorwurf macht es sich etwas zu einfach. Denn mit dieser Regelung soll verhindert werden, daß in den verpflichteten Unternehmen Spekulationen etwa über die Bonität des betroffenen Kunden angestellt werden und man ihm vorsichtshalber den Vertrag kündigt nach dem Motto: „Wenn sich die Regulierungsbehörde für XY interessiert, bedeutet das nichts Gutes.".

Die Regulierungsbehörde gibt aber nicht nur die abgerufenen Daten an die ersuchende Stelle weiter, sondern protokolliert auch bei jedem Abruf den Zeitpunkt, die bei der Durchführung des Abrufs verwendeten Daten, die abgerufenen Daten, die die Daten abrufende Person sowie die ersuchende Stelle und deren Aktenzeichen. Hiermit soll auch bei der ersuchenden Behörde eine genaue Datenschutzkontrolle ermöglicht werden. Ruft die Regulierungsbehörde z. B. für die Polizei Berlins Daten ab, kann der Berliner Datenschutzbeauftragte kontrollieren, ob das erforderlich war. Die Regulierungsbehörde selbst wird von mir hinsichtlich der datenschutzrechtlichen Verpflichtungen beraten und kontrolliert.

Die technische Umsetzung dieses „automatisierten Abrufverfahrens" befindet sich noch im konzeptionellen Stadium. Anfragen an die verpflichteten Unternehmen werden von den Bedarfsträgern deshalb gegenwärtig auf § 89 Abs. 6 TKG gestützt, d. h. für Ersuchen im Einzelfall, deren Beantwortung den verpflichteten Unternehmen jedoch einen erhöhten Arbeitsaufwand verursacht. Die Vielzahl der Anfragen führte recht schnell zur Verwendung von Formblättern, wobei jedoch zwischen den beteiligten Stellen nicht nur unterschiedliche Auffassungen zu den Anforderungen an deren inhaltliche Ausgestaltung, sondern auch zur Kostenpflichtigkeit dieser Anfragen entstanden sind. Während die Unternehmen die in § 90 Abs. 1 TKG genannten Daten kostenfrei zur Verfügung zu stellen haben, enthält § 89 hierzu keine Aussage, zumal dort der Umfang einer Auskunftsverpflichtung wesentlich weiter gefaßt ist. § 89 Abs. 6 TKG zielt (nämlich) auf die sog. Bestandsdaten ab. Dies sind diejenigen personenbezogenen

Daten, die die Unternehmen für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses erhoben haben.

Nachdem die Unternehmen immer häufiger dazu übergingen, unter Berufung auf Datenschutzgründe die Beantwortung von Anfragen zu verweigern, habe ich mich um Vermittlung bemüht, um bis zur Inbetriebnahme des automatisierten Abrufverfahrens einerseits eine zügige Beantwortung von Anfragen zu ermöglichen, andererseits aber auch die Wahrung datenschutzrechtlicher Belange zu gewährleisten. Gerade ein „vereinfachtes Auskunftsverfahren" darf von den Strafverfolgungs- und Sicherheitsbehörden nicht dazu mißbraucht werden, alle Vertragsdaten eines Kunden eines Telekommunikationsunternehmens, die dort vorhanden sind, abzufordern. In diesem Zusammenhang muß insbesondere auch die Frage diskutiert werden, ob der Gesetzgeber in die im TKG geschaffenen Auskunftsverpflichtungen auch Daten einbeziehen wollte, die keinen spezifischen Telekommunikationsbezug haben. Ich denke hierbei an Angaben über Bankverbindungen oder die Zugehörigkeit zu bestimmten gesellschaftlichen Gruppen, denen Sondertarife eingeräumt werden. Ich gehe davon aus, daß mit allen Beteiligten hierüber alsbald ein Konsens erzielt werden kann.

10.1.6 Nur ein Ansprechpartner für Datenschutzfragen

In meinem 15. Tätigkeitsbericht (Nr. 20.2.3) habe ich auf die Gefahren hingewiesen, die sich aus einer regionalen Zersplitterung der Datenschutzaufsicht im Telekommunikationsbereich ergäben. Diese während der parlamentarischen Beratungen vom Postausschuß geteilten Bedenken haben den Gesetzgeber veranlaßt, in § 91 Abs. 4 TKG die Kontrollzuständigkeit für den Datenschutz meiner Dienststelle zuzuweisen. Meine Kontrolle bei den Unternehmen tritt *„an die Stelle der Kontrolle nach § 38 des Bundesdatenschutzgesetzes"*, also entsprechend den §§ 21 und 24 bis 26 des BDSG an die Stelle der Aufsichtsbehörden. Damit sind auch für den nicht-öffentlichen Bereich vorbeugende Kontrollen möglich. Hiervon unberührt bleibt die Kontrollzuständigkeit der Landesbeauftragten für den Datenschutz, soweit die öffentlichen Stellen der Länder für die geschäftsmäßige Erbringung von Telekommunikationsdiensten Daten von natürlichen oder juristischen Personen erheben, verarbeiten oder nutzen.

10.2 Weiter auf dem Weg zur Liberalisierung der Telekommunikation

10.2.1 Mehr Schutz für die Nutzer der Telekommunikation

Durch das Gesetz zur Neuordnung des Postwesens und der Telekommunikation (PTNeuOG) erfolgte im Rahmen der sog. Postreform II die entscheidende Weichenstellung zur Liberalisierung der Telekommunikation (15. TB Nr. 20.1). Art. 7 PTNeuOG, das „Gesetz über die Regulierung der Telekommunikation und des Postwesens" (PTRegG), zählt zu den Zielen der Regulierung auch „die Gewährleistung eines wirksamen Verbraucher- und Datenschutzes" (§ 2 Abs. 2 Nr. 6). In § 10 (Datenschutzverordnungen) fordert das Gesetz daher die Bundesregierung zum Erlaß u. a. einer Rechtsverordnung zum Schutz personenbezogener Daten der am Fermeldeverkehr Beteiligten auf und macht für deren Gestaltung zahlreiche konkrete Vorgaben (15. TB Nr. 20.2.2).

Im Frühsommer 1995 erhielt ich vom BMPT den ersten Entwurf einer Verordnung i.S.v. § 10 PTRegG; der Titel lautete seinerzeit „Telekommunikations- und Informationsdienstunternehmen-Datenschutzverordnung (TIDSV)". Im Juli wurde der Entwurf durch Veröffentlichung im Amtsblatt des BMPT einer öffentlichen Kommentierung zugänglich gemacht. Im Vorfeld hierzu wurden von ihm verschiedene Telekommunikationsdienstunternehmen sowie Fachkreise und Verbände angeschrieben und erhielten Gelegenheit zur Stellungnahme. Änderungs- und Ergänzungswünsche wurden – soweit sie dem BMPT nachvollziehbar und praktikabel erschienen – in den Entwurf eingearbeitet. Auch meine Dienststelle war in dieser Phase auf Arbeitsebene beteiligt.

Für die Ressortabstimmung gab ich gegenüber dem BMPT eine umfangreiche Stellungnahme zum Verordnungsentwurf ab, der eine Reihe von Kritikpunkten sowie Änderungs- und Ergänzungsvorschläge enthielt. Beispielhaft seien die folgenden Punkte genannt:

Die Verordnung unterscheidet zwischen den **Telekommunikationsunternehmen**, die lediglich – als technische Infrastruktur – Netze anbieten und den **Diensteanbietern**, die nicht über eigene Netze verfügen müssen, aber die Telekommunikationsdienstleistungen – z. B. Telefondienst, Datenübertragung usw. – dem Endkunden vermitteln und anbieten. Viele Vorschriften des Entwurfes richteten sich lediglich an die Unternehmen, ihre Geltung war jedoch auf die Diensteanbieter auszudehnen.

Mehrere Schutzvorschriften galten lediglich für die Nutzung von **Sprachkommunikationsdiensten**. Die Verordnungsermächtigung nimmt jedoch keine entsprechende Unterscheidung vor. Auch in der Verordnung darf daher keine solche Unterscheidung erfolgen, was auch sachgerecht ist, da die Übergänge hier fließend sind.

Die geltenden Verordnungen (TDSV, UDSV) enthielten in den Regelungen des sog. **Einzelverbindungsnachweises**, also der detaillierten Telefonrechnung, Vorschriften zum Schutz von Anrufen bei telefonischen Beratungsstellen, wie z. B. der Telefonseelsorge. Der Entwurf der TIDSV nahm den Mobilfunkbereich von diesem Schutz aus. Da die Verordnungsermächtigung keine Unterscheidung zwischen Mobilfunk- und Festnetz enthält, durfte auch die Verordnung Mobilfunkkunden insoweit nicht schlechter stellen.

Bereits nach geltendem Recht hatte der Kunde das Recht, seiner Eintragung in **Kundenverzeichnisse** zu widersprechen. Vor dem Hintergrund vieler Bürgerbeschwerden habe ich darüber hinaus ein **abgestuftes Widerspruchsrecht** gefordert, infolgedessen der Kunde z. B. einer Eintragung in **gedruckte** Kundenverzeichnisse zustimmen, einer Verbreitung seiner Daten über elektronische Verzeichnisse (CD-ROM,

Onlineverzeichnisse) jedoch widersprechen kann. Erfreulicherweise fanden nahezu aller meine Änderungs- und Ergänzungsvorschläge Berücksichtigung. Nicht durchsetzen konnte ich mich mit der Forderung, die Bereitstellung auch anonymer Nutzungsmöglichkeiten – z. B. mittels einer „Prepaid-Card" – in der Verordnung sicherzustellen.

In den Beratungen des Entwurfes auf Regierungsebene ergab sich auch bald, daß er ein „I" zuviel enthielt: Entsprechend der Verordnungsermächtigung – und seinem Titel – enthielt der Entwurf auch Regelungen für **Informationsdienstleistungen**. Damit waren solche Dienstleistungen gemeint, die unter Zuhilfenahme von Telekommunikations-Infrastruktur erbracht werden, ohne selbst Telekommunikationsdienstleistung zu sein. Insbesondere war hiermit der Bildschirmtext – bzw. Datex-J-Dienst der Telekom gemeint. Sehr bald wurde jedoch deutlich, daß insoweit von der Verordnungsermächtigung kein Gebrauch gemacht werden sollte, Regelungen für Informationsdienstleistungen vielmehr Gegenstand eines besonderen Gesetzes sein sollten. Den Entwurf für ein solches Gesetz hat das Bundeskabinett am 11. Dezember 1996 verabschiedet (Informations- und Kommunikationsdienste-Gesetz; s. o. Nr. 8.1).

Die Verordnung wurde als „Verordnung über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen (Telekommunikationsdienst-Unternehmen-Datenschutzverordnung – TDSV)" in der Kabinettsitzung vom 10. Juli 1996 abschließend behandelt und verabschiedet und trat am 19. Juli 1996 in Kraft. Die wichtigsten Kernpunkte sind:

- **Verbindungsdaten** (Zeitpunkt, Dauer, Zielrufnummer usw.) dürfen unter Verkürzung der Zielrufnummer um die letzten drei Stellen gespeichert werden, sofern der Kunde keine Vollspeicherung oder Löschung wünscht.
- Der Kunde kann entscheiden, ob er überhaupt nicht, nur in gedruckte Telefonbücher oder aber auch in elektronische **Verzeichnisse** eingetragen werden möchte.
- Die Voraussetzungen für das Einrichten sog. **Fangschaltungen**, mit deren Hilfe belästigende oder bedrohende Anrufe festgestellt werden können, wurden verschärft.
- Die **Telefonauskunft** darf über die in den Telefonbüchern eingetragenen Anschlüsse nicht nur die Telefonnummer, sondern auch die anderen Angaben bekanntgeben, sofern die hierüber unterrichteten Kunden dieser „Komfortauskunft" nicht widersprochen haben.
- Der Wunsch eines Telefonkunden nach **Nichtanzeige** seiner **Rufnummer** beim Angerufenen muß kostenfrei umgesetzt werden.
- Bei **Anrufen zur Polizei und zur Feuerwehr** darf die Rufnummer des Anrufers generell angezeigt werden.

Die TDSV hat eine erhebliche Verbesserung des Datenschutzes für die Nutzer der Telekommunikation gebracht. Sie ist somit eine wichtige Grundlage zum Schutz und zur Selbstbestimmung der Bürger in einem liberalisierten Telekommunikationsmarkt.

10.2.2 Rechtliche Vorgaben für die Sicherheit in der Telekommunikation

Die Sicherheit in der Telekommunikation, insbesondere im Bereich des Telefonfestnetzes, war wiederholt Anlaß für öffentliche Kritik, insbesondere im Jahre 1994 vor dem Hintergrund von manipulativen Eingriffen in das Telefonnetz und von Beschwerden über überhöhte Telefonrechnungen. Sowohl eine „Erhebung über die Sicherheit der Endverzweiger" des Bundesamtes für Post- und Telekommunikation von 1995 als auch eine Untersuchung „Überhöhte Telefonrechnungen" des Bundesamtes für Sicherheit in der Informationstechnik haben deutlich gemacht, daß hier objektiv Sicherheitslücken bestehen. Dies betrifft besonders den Teil der Telefonanschlußleitung von der Telekommunikations-Anschlußeinheit (TAE) bis zum Haus-/Straßenverteiler des Außenleitungsnetzes (APL; Abschlußpunkt des Liniennetzes), der jedenfalls seinerzeit nur unzureichend gesichert war. Es ist daher dringend geboten, den vom Gesetzgeber vorgegebenen rechtlichen Rahmen zum Schutz des Fernmeldegeheimnisses und des Datenschutzes in der Telekommunikation auszufüllen und so den Schutz der Beroffenen zu konkretisieren und zu festigen.

Am 14. September 1994 hat der Gesetzgeber durch das Postneuordnungsgesetz das Fernmeldeanlagengesetz um § 10 a ergänzt. Die Vorschrift verpflichtet in Abs. 1 Betreiber von Fernmeldeanlagen, mit deren Hilfe öffentliche Telekommunikationsdienstleistungen angeboten werden, Maßnahmen zum Schutz des Fernmeldegeheimnisses und personenbezogener Daten zu treffen und in Abs. 2 die Bundesregierung zum Erlaß einer Rechtsverordnung für entsprechende rechtliche Vorgaben. Im Februar 1995 bat ich das BMPT um Information über den Sachstand und bot meine Beratung an. Einige Monate später wurde ich auf ein vom Bundesamt für Post und Telekommunikation (BAPT) anläßlich einer Arbeitsgruppensitzung verteiltes „Arbeitspapier als Vorläufer einer Rechtsverordnung gem. § 10 a FAG zur Erstellung von Sicherungskonzepten in der Telekommunikation – Telekommunikations-Sicherungskonzepte-Verordnung – TSKV" (Stand: 7. März 1995) verwiesen. Eine redaktionell überarbeitete Fassung des „Arbeitspapiers..." wurde den Ressorts Anfang November 1995 in einer Besprechung vorgestellt.

Am 1. August 1996 trat das Telekommunikationsgesetz (TKG) in Kraft, das auch § 10a FAG außer Kraft setzte. Das TKG fordert aber technische Schutzmaßnahmen (§ 87 Abs. 1), die denen des § 10a FAG entsprechen und enthält eine entsprechende Verordnungsermächtigung des BMPT (§ 87 Abs. 3).

Das BMPT will von der Ermächtigung nur dann Gebrauch machen, wenn sich der von der Regulierungsbehörde zu erstellende „Katalog von Sicherheitsanforderungen" (§ 87 Abs. 1 Satz 3) als nicht wirkungsvoll erweist; die Aufgaben der Regulierungsbehörde werden bis zum 31. Dezember 1997 vom BMPT wahrgenommen.

Angesichts des Schutzgegenstandes der Vorschrift – Grundrechte in ihrer Ausprägung als Fernmeldegeheimnis und Datenschutz – ist mir die Haltung des

Ministeriums nicht nachvollziehbar. Unabhängig von Aktivitäten nachgeordneter Behörden hat es der Gesetzgeber dem zuständigen Ministeriums aufgegeben, durch den Erlaß einer Rechtsverordnung den Schutz der Betroffenen sicherzustellen. Im übrigen ist die Auffassung des Ministeriums „Verordnung nur bei Bedarf" allenfalls bezüglich der Selbstverpflichtung der Unternehmen gemäß § 87 Abs. 2 TKG vertretbar – wie dies auch in der Begründung des TKG ausgeführt ist.

Das BMPT hat gleichwohl an seiner Auffassung festgehalten: Den nach § 87 TKG Verpflichteten soll zunächst Gelegenheit gegeben werden, Schutzmaßnahmen im Rahmen ihrer Selbstverpflichtung umzusetzen. Dadurch kommt dem „Katalog von Sicherheitsanforderungen" herausragende Bedeutung als „Meßlatte für die Sicherheit in der Telekommunikation" zu.

Zwischenzeitlich hat das BAPT im Auftrag des Ministeriums einen Vorentwurf eines „Kataloges" erarbeitet, zu dem im Dezember 1996 eine Anhörung beim BMPT mit Vertretern von Verbraucherverbänden und Wirtschaftsverbänden der Hersteller und Betreiber von Telekommunkationsanlagen und meines Hauses stattfand. Zu dem Vorentwurf hatte ich dem BMPT vorab eine Reihe von Kritikpunkten mitgeteilt sowie Vorschläge zur Verbesserung unterbreitet.

Ich habe dazu vor allem verdeutlicht, welche Zweckbestimmung des Kataloges sich aus dem Gesetz ergibt und welchen Inhalt er danach haben muß. § 87 Abs. 1 Satz 3 TKG bestimmt: „Die Regulierungsbehörde erstellt ... einen Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen, um ... eine angemessene Standardsicherheit zu erreichen.":

- Die Regulierungsbehörde hat also ein Verzeichnis von Anforderungen zu erstellen, die von den Unternehmen zu erfüllen sind, die geschäftsmäßig Telekommunikationsdienste erbringen. Die Anforderungen betreffen zum einen die Unternehmen selbst, insbesondere deren Personal und Organisation, zum anderen die von ihnen eingesetzte Technik. Die Anforderungen sind so zu gestalten, daß durch die zu ihrer Erfüllung ergriffenen Schutzmaßnahmen eine „angemessene Standardsicherheit" für die in Satz 1 der Vorschrift genannten Schutzziele erreicht wird. Die Standardsicherheit hat „dem Stand der Technik und internationalen Maßstäben" zu entsprechen.
- Die Anforderungen selbst sowie die empfohlenen Maßnahmen müssen insgesamt – also sowohl in ihrer Anzahl als auch in ihrer (gesamten) Wirkung – ausreichend sein, um die gesetzlichen Schutzziele zu erreichen.
- Sie müssen in einer solchen Weise dargestellt werden, daß dem einzelnen Adressaten zweifelsfrei erkennbar ist, welche Anforderungen/Maßnahmen ihn betreffen. Auch muß ihr Inhalt – durch hinreichende Detaillierung, Beispiele usw. – deutliche Vorgaben für die Realisierung der Maßnahmen machen.

Diesen gesetzlichen vorgegebenen Kriterien hat der „Katalog" zu entsprechen.

Ich hoffe auf eine schnelle Vorlage des Katalogs, da – wenn schon keine zur Sicherung der Telekommunikation vorgesehene Rechtsverordnung erlassen wird – es umso wichtiger ist, daß ein hochwertiger „Katalog" erstellt und sehr bald veröffentlicht wird.

10.3 Moderne Telekommunikationsdienste bald „europäisch geschützt"

Bereits in meinem 15. TB (Nr. 20.2.10) hatte ich von dem geänderten Vorschlag der Kommission der Europäischen Gemeinschaft für eine „Richtlinie des Europäischen Parlaments und des Rates zum Schutz personenbezogener Daten und der Privatsphäre in digitalen Telekommunikationsnetzen, insbesondere im diensteintegrierenden digitalem Telekommunikationsnetz (ISDN) und digitalen Mobilfunknetzen" (im folgenden: ISDN-Richtlinie) berichtet. Ich hatte dabei betont, daß es aus Sicht des Datenschutzes hierbei darauf ankommt, daß jedenfalls gleichzeitig mit der Harmonisierung der Telekommunikationsnetze und -dienste die rechtlichen Rahmenbedingungen geschaffen werden, um ein hinreichendes Niveau zum Schutz personenbezogener Daten und der Privatsphäre von Unionsbürgern zu gewährleisten.

Nach der Verabschiedung der EG-Datenschutzrichtlinie im Oktober 1995 (s. o. Nr. 2.1.1) ist es vor allem den Anstrengungen unter der italienischen Ratspräsidentschaft im 1. Halbjahr 1996 zu verdanken, daß am 27. Juni 1996 in Luxemburg unter den Mitgliedstaaten – mit Ausnahme Portugal – ein gemeinsamer Standpunkt zur ISDN-Richtlinie erreicht wurde, der formell am 12. September 1996 beschlossen worden ist. Nachdem die Kommission dem gemeinsamen Standpunkt des Rates bereits zugestimmt hat, wird das Plenum des Europäischen Parlaments die Richtlinie Anfang des Jahres 1997 in zweiter Lesung behandeln.

Bereits in ihrem Titel wird zum Ausdruck gebracht, daß der Schutzbereich der Richtlinie sich nicht nur – wie bei früheren Entwürfen – auf den Schutz der Privatsphäre in digitalen Telekommunikationsnetzen beschränkt, sondern sich insgesamt auf die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, insbesondere im diensteintegrierenden digitalen Telekommunikationsnetz (ISDN) und in digitalen Mobilfunknetzen, erstreckt.

Als wesentlicher Fortschritt, der erst in der Schlußphase der Beratungen erreicht wurde, ist anzusehen, daß die Bestimmungen der Richtlinie auch den Schutz der berechtigten Interessen von Teilnehmern regeln, bei denen es sich um juristische Personen handelt. Hiermit geht die Richtlinie weiter als unser nationales Telekommunikationsgesetz, das lediglich solche Einzelangaben über juristische Personen dem Schutz personenbezogener Daten unterstellt, die dem Fernmeldegeheimnis unterliegen. Die Umsetzung der Richtlinie bedeutet damit zugleich eine Möglichkeit, den Anwendungsbereich des Datenschutzes im Telekommunikationsgesetz zu erweitern. Hieraus läßt sich jedoch nicht der Schluß ziehen, daß die ISDN-Richtlinie durchgängig einen höheren Datenschutzstandard bietet als unser nationales Telekommunikationsrecht.

Ich hatte mich mit Nachdruck dafür eingesetzt, die sog. Corporate Networks (s. o. 10.1.3) in den Anwendungsbereich der Richtlinie mit einzubeziehen. Daß dies nicht gelungen ist, liegt nicht etwa an mangelndem Einsatz der Bundesregierung, die sich bis in die Endphase der Beratungen für diesen Vorschlag stark gemacht hat; letztendlich ist diese Initiative jedoch an der ablehnenden Haltung des überwiegenden Teils der Mitgliedstaaten gescheitert. Zumindest wurde eine ausdrückliche Erklärung in das Ratsprotokoll aufgenommen, wonach Rat und Kommission feststellen, daß die Richtlinie Mitgliedstaaten in keiner Weise daran hindert, die Bestimmungen dieser Richtlinie auf nicht-öffentliche Telekommunikationsnetze und nicht öffentlich zugängliche Telekommunikationsdienste anzuwenden, und daß die EG-Datenschutzrichtlinie (s. o. Nr. 2.1) auf jeden Fall für die Verarbeitung personenbezogener Daten im Rahmen derartiger Netze und Dienste gilt. Es wird sich zeigen, ob der in diesem Punkt höhere datenschutzrechtliche Standard unseres Telekommunikationsgesetzes tatsächlich zu befürchteten Wettbewerbsverzerrungen führen wird, mit der Folge, daß grenzüberschreitend tätige Telekommunikationsunternehmen ihren Standort nach den geringsten datenschutzrechtlichen Anforderungen auswählen werden. Die EU-Kommission hat bereits im Februar 1995 in der Überzeugung, daß der Mensch als Verbraucher im Mittelpunkt des Wandels der Informationstechnologien steht, den EU-Kommissar Martin Bangemann beauftragt, ein „Information Society Forum" einzurichten, in dem auch die Verbraucher repräsentiert sind. Aus meinen regelmäßigen Kontakten mit Vertretern der Telekommunikationsunternehmen weiß ich, daß auch diese den Datenschutz immer mehr als ein Qualitätsmerkmal ihrer Leistungen und damit als Wettbewerbsvorteil begreifen. Es wäre fatal, wenn die Bundesregierung aus Furcht vor Wettbewerbsnachteilen für den Standort Deutschland voreilig die datenschutzrechtlichen Bestimmungen des Telekommunikationsgesetzes „zurückschneidet" und ausdrücklich auf öffentliche Dienste und Netze beschränkt.

Erfreulicherweise trägt der gemeinsame Standpunkt zur ISDN-Richtlinie nunmehr auch dem Grundsatz der Vertraulichkeit der Kommunikation angemessen Rechnung, indem er den spezifischen Tatbestandsregelungen vorangestellt wurde. Der geänderte Vorschlag der Kommission vom Juni 1994 hatte lediglich im Absatz 2 des Artikels 12 (Überwachung der Kommunikation) zu erkennen gegeben, daß man das Vertraulichkeitserfordernis nicht völlig vergessen hatte. Zwar ist die Vertraulichkeit der Kommunikation in Artikel 5 nicht durch strafrechtliche Schutzvorschriften abgesichert, die Mitgliedstaaten haben sie jedoch durch innerstaatliche Vorschriften sicherzustellen, wobei Abhör- und Überwachungsmaßnahmen nur gerechtfertigt sind, wenn entweder die betroffenen Benutzer eingewilligt haben oder das Gesetz zur Durchführung derartiger Maßnahmen ermächtigt.

Sah der ursprüngliche Vorschlag der Kommission vom 27. Juli 1990 in Artikel 4 noch eine ausdrückliche Zweckbindung für die Erhebung, Speicherung und Verarbeitung personenbezogener Daten durch eine Telekommunikationsorganisation vor, hat dieser Grundsatz im jetzigen Entwurf des gemeinsamen Standpunktes zur ISDN-Richtlinie Eingang in die bereichsspezifische Regelung zur Verarbeitung von Verkehrs- und Gebührendaten gefunden. Die im Anhang zu Artikel 6 vom Umfang her abschließend aufgezählten Teilnehmerdaten dürfen grundsätzlich zwar nur für Verbindungs- und Abrechnungszwecke verarbeitet werden, ich hätte mir jedoch eine konkretere Ausgestaltung der Verarbeitungsbefugnis zu Vermarktungszwecken mit Einwilligung des Teilnehmers gewünscht. Regelungen über Zeitpunkt, Form, Inhalt und Geltungsdauer dieser Einwilligung enthält die Richtlinie jedoch nicht. Ich bezweifle, daß somit das Erstellen von Kundenprofilen, mit dem der Teilnehmer so nicht einverstanden ist, verhindert werden kann.

Artikel 7 Abs. 1 räumt den Teilnehmern das Recht ein, Rechnungen ohne Einzelgebührennachweise zu erhalten. Die Mitgliedstaaten sind verpflichtet, bei der Anwendung innerstaatlicher Vorschriften über die Erstellung von Einzelverbindungsnachweisen das Recht anrufender Benutzer und angerufener Teilnehmer auf Vertraulichkeit miteinander in Einklang zu bringen (Artikel 7 Abs. 2). Bedauerlicherweise ist das „Holländische Modell" (15. TB Nrn. 20.2.12 und 20.3) nicht einmal in den Erwägungsgründen genannt worden. Der dortige Hinweis auf alternative Bezahlungsarten wird dem Anonymitätsinteresse der Teilnehmer nicht Rechnung tragen können.

Artikel 8 sieht eine umfangreiche, datenschutzfreundliche Regelung zur Rufnummernanzeige bzw. deren Unterdrückung vor.

Artikel 10 verpflichtet die Mitgliedstaaten sicherzustellen, daß jeder Teilnehmer die Möglichkeit hat, auf einfache Weise und gebührenfrei die von einer dritten Partei veranlaßte automatische Weiterschaltung zum Endgerät des Teilnehmers abzustellen. Eine § 9 Abs. 4 der deutschen Telekommunikationsdienstunternehmen-Datenschutzverordnung (TDSV) entsprechende Regelung, daß der anrufende Teilnehmer (z. B. durch ein akustisches Signal) automatisch über die Anrufweiterschaltung informiert wird, enthält die ISDN-Richtlinie nicht. Das Fehlen dieser Information kann Probleme in den Fällen bereiten, in denen ein Teilnehmer schon die Tatsache seines Anrufes keinesfalls einem Dritten bekannt geben wollte.

Artikel 11 (Teilnehmerverzeichnisse) sieht wesentliche Gestaltungsrechte für die Kunden vor. Zu kritisieren ist jedoch, daß juristische Personen von seiner Geltung ausgenommen werden können und auch ein sog. Nichteintrag „von der Erhebung eines vertretbaren Betrages abhängig gemacht werden kann". Wenn auch dieser Betrag nicht von der Ausübung dieses Rechts abhalten darf, bleibt offen, wann diese Grenze überschritten wird. Ein im deutschen Telekommunikationsgesetz enthaltenes selektives Widerspruchsrecht, nach dem der Teilnehmer die Eintragung seiner Daten auf gedruckte Kundenverzeichnisse beschränken und für elektronische Verzeichnisse (z. B. CD-ROM) ausschließen kann, sieht die Richtlinie nicht vor.

Insgesamt bewerte ich es als Erfolg, daß neben der EG-Datenschutzrichtlinie mit der ISDN-Richtlinie eine bereichsspezifische Regelung zum Schutz der Telekommunikation erarbeitet wurde. Sie stellt einen wichtigen Schritt auf dem Weg des europäischen Harmonisierungsprozesses dar, der aus datenschutzrechtlicher Sicht auch in anderen Bereichen der Rechtsangleichung konsequent weitergegangen werden sollte.

10.4 Datenschutzprobleme in der Telekommunikation

Größter Anbieter von Telekommunikationsdiensten in der Bundesrepublik Deutschland ist nach wie vor die Deutsche Telekom AG. Sie betreibt rund 40 Millionen Telefonanschlüsse. Diese große Anzahl erklärt, daß Beschwerden von Telefonkunden über den Datenschutz bei der Deutschen Telekom AG stets einen Schwerpunkt der Bürgereingaben an meine Dienststelle gebildet haben und bilden. Daher ist es gerade bei der Bearbeitung von Kundenbeschwerden unerläßlich, daß die Deutsche Telekom AG zu den von den Kunden vorgetragenen Sachverhalten Stellung bezieht und ggf. darlegt, aus welcher datenschutzrechtlicher Vorschrift sich ihres Erachtens die Zulässigkeit der Vorgehensweise ergibt, die von den Kunden kritisiert wird.

Zu Beginn der sog. Postreform II hatte ich den Eindruck, daß dem Anliegen und den Erfordernissen des Datenschutzes durch den Unternehmensvorstand große Bedeutung beigemessen wurde. So heißt es in den „Unternehmensgrundsätzen der Deutschen Telekom AG":

„❽ Die Telekom übernimmt gesellschaftliche Verantwortung. Wir sichern das **Fernmeldegeheimnis und den Datenschutz.**"

Bestärkt wurde mein Eindruck nicht nur durch die gute organisatorische Anbindung des Konzern-Datenschutzbeauftragten und die Ausstattung seines Bereichs mit hochqualifiziertem Personal, sondern auch durch die Einrichtung sog. Datenschutzberater. Sie sollen für die Niederlassungen der Telekom Ansprechpartner in Datenschutzfragen sein und diese insbesondere beraten. Die Datenschutzberater sind zwar bei den Direktionen der Telekom eingerichtet. Sie sind ihnen jedoch fachlich nicht unterstellt, sondern berichten der Unternehmenszentrale direkt.

Leider haben sich bislang aber weder die genannten Grundsätze noch die organisatorischen Änderungen in ihrer Wirkung vollständig entfalten können: Anders kann ich mir nicht erklären, daß es unverhältnismäßig lange dauert, bis die Telekom meine Anfragen beantwortet. Trotz wiederholter Erinnerungen dauert es oftmals mehrere Monate, in Einzelfällen bis zu einem dreiviertel Jahr, bis mir eine abschließende Äußerung vorliegt. Regelmäßig muß ich die Deutsche Telekom AG bei dieser Gelegenheit darauf hinweisen, daß die Beantwortung meiner Anfragen nicht nur eine „freundliche Geste" darstellt, sondern nach § 24 Abs. 4 BDSG eine gesetzliche Pflicht für die Deutschen Telekom AG bedeutet. Für die Bürger, die sich an mich wenden, ist es schwer verständlich, daß sie von mir immer wieder vertröstet werden müssen. Der Ärger auf die Telekom wird dann gelegentlich auch zu einem Ärger über mein Haus. Hinzu kommt, daß eine derart schleppende Bearbeitung auch zu automatischen Datenlöschungen führen kann, wodurch eine Aufklärung des Sachverhaltes zunehmend schwieriger wird.

Ich erwarte hier dringend Verbesserungen.

10.4.1 Tonbandaufzeichnung von Telefonaten mit Bundesbehörden

Große Bedeutung kommt aus verfassungsrechtlicher Sicht der **Vertraulichkeit des nichtöffentlich gesprochenen Wortes** zu (s. o. Nr. 6.6). Die Bürger müssen in der Regel davon ausgehen können, daß ein Gespräch, sei es auch noch so kurz und belanglos, das sie mit einem anderen führen, nicht heimlich belauscht oder aufgezeichnet wird. Dies gilt natürlich auch für Gespräche mit Mitarbeitern von Bundesbehörden. Nicht nur Gespräche, die innerhalb der Behörde über die TK-Anlage geführt werden, sondern auch die Gespräche mit der Vermittlung unterliegen diesem Schutz. Die Technik der modernen TK-Anlagen schafft hier jedoch Gefährdungen, auf die ich durch einen aufmerksamen Mitarbeiter einer obersten Bundesbehörde hingewiesen wurde.

Zum Zwecke der Aufzeichnung von Droh- oder Terroranrufen waren die Vermittlungsplätze der Telefonzentrale der betreffenden Bundesbehörde mit einem „Dokumentationsrecorder" verbunden. Dieser zeichnete den Inhalt **aller** ankommenden und abgehenden Telefongespräche an allen Vermittlungsplätzen bis zu einer Länge von ca. 4 Minuten automatisch auf. Nach Ablauf der 4 Minuten wurden die jeweils ältesten Gesprächsinhalte von den neuen überschrieben. In den Fällen eines Drohanrufs sollte die Telefonistin durch Knopfdruck ein Tonbandgerät in Gang setzen, wodurch die 4-Minuten-Aufzeichnung automatisch auf eine Tonbandkassette kopiert und die Speicherung des laufenden Gespräches auf der Kassette fortgesetzt wurde. Nach Beendigung eines solchen Anrufs wurde das Tonbandgerät gestoppt und die Telefonistin unterrichtete den zuständigen Sicherheitsbeamten. Dieser begab sich sodann in den Betriebsraum der TK-Anlage und entnahm dem Gerät die Bandkassette. Erfolgte der Knopfdruck irrtümlich, löschte er die Aufzeichnung. Andernfalls wurden weitere Maßnahmen entsprechend einer Bewertung des aufgezeichneten Gespräches ergriffen, d. h. die Sicherheitsbehörden wurden informiert und die Bandkassette übergeben.

Nach Dienstschluß wurden die Gespräche der Telefonzentrale zur Hauptpforte geschaltet und im übrigen wie oben beschrieben verfahren.

Die Vorratsaufzeichnung der Telefonate – also die Speicherung, ohne daß der Anruf als Bedrohung erkannt ist – verstößt gegen § 201 StGB. Nach § 201 Abs. 1 Nr. 1 StGB unterliegt das nichtöffentlich gesprochene Wort eines anderen dem Schutzbereich dieser Vorschrift. Danach wird bestraft, wer unbefugt entweder das nichtöffentlich gesprochene Wort eines anderen auf einen Tonträger aufnimmt oder eine so hergestellte Aufnahme gebraucht oder einem Dritten zugänglich macht. Gegen das Vorliegen der tat-

bestandlichen Voraussetzungen der Vorschrift spricht nicht, daß die aufgezeichneten Telefonate grundsätzlich nach ca. 4 Minuten wieder überschrieben wurden. Allein die Aufnahme genügt – ohne daß es darauf ankommt, ob die Tonbandaufnahme tatsächlich später abgehört wird oder ob der Zugriff darauf nur unter besonderen Sicherheitsmaßnahmen stattfindet.

Die Aufzeichnung ist lediglich dann nicht rechtswidrig, wenn sie befugt erfolgt. Das kann zwar durch Einwilligung der Beteiligten – Anrufer und Mitarbeiter an den Vermittlungsplätzen – erreicht werden. Dies scheidet hier aus. Bei Terror- oder Drohanrufen kann § 34 StGB als Begründung für die Aufzeichnung und damit als Rechtfertigungsgrund herangezogen werden.

Voraussetzung wäre dann, daß eine „gegenwärtige, nicht anders abwendbare Gefahr" für Leben, Leib, Freiheit, Ehre, Eigentum oder ein anderes Rechtsgut vorliegt. Tatsächlich handelt es sich jedoch bei den Telefonaten nur in geringstem Maße um Droh- oder Terroranrufe; eine Abfrage bei den obersten Bundesbehörden bestätigte mir, daß in einem Jahr oftmals kein einziger solcher Anruf ankommt. Soweit andere Rechtfertigungsgründe, wie etwa die Beweissicherung bei der Anzeige einer Straftat, in Betracht kommen, ergibt sich die gleiche rechtliche Problematik. Diese Bewertung bezieht sich auf „normale" Behörden; sie kann bezüglich der Aufzeichnung ankommender Anrufe etwa bei der Einsatzzentrale einer Polizeibehörde wie dem Bundeskriminalamt (BKA) oder im Falle der bekannten Notrufnummer 110 zu anderen Ergebnissen führen, schon weil in diesen Fällen davon ausgegangen werden kann, daß der Anrufer mit einer Aufzeichnung seines Gespräches rechnet oder zumindest rechnen muß.

Zusammenfassend ist somit festzustellen, daß – mit sehr engen Ausnahmen im Bereich der Sicherheitsbehörden – die generelle Registrierung aller ankommenden bzw. abgehenden Telefonate rechtswidrig ist. Eine Registrierung auf Knopfdruck im einzelnen, d. h. wenn ein Anruf als Droh- oder Terroranruf erkannt ist, wäre hingegen bei allen Behörden zulässig, da in diesem Fall der Rechtfertigungsgrund des § 34 StGB angenommen werden kann und die Aufzeichnung somit befugt erfolgt.

Eine klarstellende gesetzliche Normierung eng umgrenzter Ausnahmen für den Bereich der Sicherheitsbehörden würde ich begrüßen.

In einem Rundschreiben an die obersten Bundesbehörden habe ich auf die Problematik der „Vorratsaufzeichnung" hingewiesen und zur Einstellung aufgefordert. Dies ist – soweit § 34 StGB oder andere Rechtfertigungsgründe nicht vorlagen – erfolgt.

10.4.2 Die Telekom hörte Auslandsgespräche mit

Im Sommer 1996 informierte mich ein Bürger über seine Vermutung, wonach Mitarbeiter des „Telekom Operator Service-Auslandsvermittlung (TOS-AV)" in Frankfurt/M. Kenntnisse über den Inhalt von ihm geführter Telefongespräche erlangt und diese Kenntnisse an wenigstens eine andere Person weitergegeben hätten.

Die Deutsche Telekom AG betreibt diesen Service an 8 Standorten in Deutschland. Neben der Auskunft über ausländische Rufnummern wird auch ein handvermittelter Telefondienst angeboten. Hierbei vermittelt ein Operator die telefonische Verbindung zwischen den Gesprächspartnern. Vermittlungswünsche aus dem Inland werden automatisch einem dieser Standorte zugeleitet, während Vermittlungswünsche aus dem Ausland ausschließlich beim TOS-AV in Frankfurt bearbeitet werden.

Hier wird u. a. der „Deutschland Direkt"-Telefondienst der Telekom realisiert, der täglich etwa 7000 Anrufe erhält. Soll unter Nutzung dieses Dienstes aus dem Ausland ein deutscher oder ausländischer Gesprächspartner erreicht werden, vermittelt der Operator in Frankfurt das Gespräch und kümmert sich gleichzeitig um die Abrechnungsmodalitäten. Dabei legt er für jede Verbindung ein „Gesprächsblatt" an, das die für die Entgeltberechnung erforderlichen Daten – Herkunftsland des Anrufes, Anrufsziel, Tageszeit und Gesprächsdauer – enthält. Es können sowohl sogenannte „R-Gespräche" als auch Gespräche unter Nutzung der von der Telekom angebotenen „T-Card" vermittelt werden. Bei „R-Gesprächen" übernimmt der Angerufene die Kosten, bei Gesprächen mittels „T-Card" erscheinen die entstandenen Entgelte auf der Telefonrechnung des Anrufers. Zur Beobachtung des Verbindungsstatus und zur Ermittlung der Gesprächsdauer stand dem Operator neben optischen Anzeigen für bestehende Verbindungen (Kontrollampen, Rollenzähler) auch eine „Mithör"-Taste zur Verfügung.

Die an den Operatorplätzen des TOS-AV im Schichtdienst eingesetzten etwa 500 Mitarbeiter waren nach einer entsprechenden Arbeitsanweisung gehalten, sich nach Herstellung der Verbindung in etwa dreiminütigem Abstand mit Hilfe der Mithörtaste auf das Gespräch „aufzuschalten" und diese Aufschaltung unter Angabe des Zeitpunktes und ihres Namenskürzels auf der Rückseite des Gesprächsblattes zu vermerken („Sprechvermerke"). Begründet wurde dies mit der Notwendigkeit, einerseits die Qualität der bestehenden Verbindung prüfen zu müssen und andererseits – für die Bearbeitung eventueller späterer Rechnungseinwendungen – einen Nachweis für die ungefähre Dauer der Gespräche zu erhalten. Die zum Zeitpunkt meiner Kontrolle beim TOS-AV eingesetzten technischen Systeme waren dabei so gestaltet, daß das Aufschalten für die betroffenen Gesprächsteilnehmer unbemerkt erfolgte und dem jeweiligen Operator auch keine technischen Schranken hinsichtlich der Dauer der Aufschaltung gesetzt wurden.

Ich habe diese Arbeitsweise gegenüber dem Vorstand der Deutschen Telekom AG beanstandet, weil sie durch die damit gebotene und auch genutzte Möglichkeit, für die Teilnehmer unbemerkt Gesprächsinhalte zur Kenntnis zu nehmen, einen schwerwiegenden Eingriff in das Fernmeldegeheimnis und damit in das Recht auf informationelle Selbstbestimmung der betroffenen Gesprächsteilnehmer zuließ, der durch keine gesetzliche Erlaubnisnorm gerechtfertigt und somit unzulässig war.

Unmittelbar nach meiner Kontrolle hat die Zentrale der Deutschen Telekom AG den TOS-AV in Frankfurt und vier Wochen später auch die TOS-AV an den anderen Standorten angewiesen, das Hineinhören in Gespräche und das Niederschreiben der Sprechvermerke in der Handvermittlung zu unterlassen sowie die Einhaltung dieser Anweisung angemessen zu überwachen. Dies habe ich sowohl in Frankfurt als auch beim TOS-AV in Düsseldorf kontrolliert. Dabei habe ich festgestellt, daß den Operatoren – infolge technischer Veränderungen an den Operatorplätzen – ein Aufschalten auf bestehende Verbindungen nicht mehr möglich ist und die entsprechenden Passagen der Arbeitsanweisung auf Weisung des zuständigen Fachbereichs der Zentrale vorläufig mit dem Ziel außer Kraft gesetzt wurden, eine Neufassung unter Berücksichtigung des § 89 Abs. 5 TKG zu ermöglichen, in welchem abschließend geregelt ist, unter welchen Voraussetzungen und in welcher Form ein Aufschalten auf bestehende Verbindungen erlaubt ist.

In den mit der Telekom nach der Beanstandung geführten Gesprächen wurde argumentiert, daß von TOS-AV z. B. bei R-Gesprächen aus verschiedenen Staaten aufgrund der dort vorhandenen (veralteten) Technik kein Signal über das Verbindungsende („Schlußzeichen") empfangen und dieses nur durch periodisches „Hineinhören" des Operators in das Gespräch festgestellt werden könne. Die hierbei vom Operator getroffenen Feststellungen über das Bestehen/Nichtbestehen der Verbindung würden der Entgeltberechnung zugrunde gelegt.

Diese Aussage ist nicht plausibel, denn bei einem R-Gespräch zu einem deutschen Anschluß – also dem entgeltpflichtigen – wird von diesem (nach Auflegen des Hörers) das Gesprächende stets signalisiert; für solche Gespräche bedarf es also für die Entgeltberechnung keines „Hineinhörens".

Wie oben ausgeführt, berührt das Aufschalten auf Gespräche das grundrechtlich geschützte Fernmeldegeheimnis. Die Annahme des Bestehens „betriebsbedingter Schranken" des Fernmeldegeheimnisses hat das Bundesverfassungsgericht in seiner sog. Fangschaltungsentscheidung ausdrücklich verneint.

Ich habe die Telekom darauf hingewiesen, daß ich es vorbehaltlich einer eingehenderen rechtlichen Prüfung beim Aufschalten auf R-Gespräche – im genannten Zusammenhang und zum genannten Zweck – für unabdingbar halte, daß sowohl der Anrufer als auch der Angerufene vor Beginn des Gespräches kostenfrei darauf hingewiesen werden,

- daß und in welchen Zeitabständen ein Aufschalten des Operators erfolgt,
- zu welchem Zweck dies erforderlich ist,
- daß und wie das Aufschalten und Verlassen der Verbindung durch den Operator für die Teilnehmer wahrnehmbar gemacht wird.

Die Telekom hat mir ihre Absicht mitgeteilt, den handvermittelten Verkehr ab 1998 auf einen Standort zu konzentrieren und hierfür ein neues Operatorsystem zu beschaffen. In diesem System könne die handvermittelte Verbindung nicht mehr durch den Operator beobachtet werden, da sie nach Abschluß der entsprechenden Eingaben am Bildschirm durch das System automatisch aufgebaut und dann bis zum Verbindungsende „begleitet" würde. Die Verbindung stünde damit nicht mehr unter Aufsicht des Operators, womit diesem dann auch ein Aufschalten nicht möglich sei.

Dieses Vorhaben entspricht den Anforderungen zum Schutz des Fernmeldegeheimnisses. Ich werde – bei aller Rücksicht auf die wichtige Frage einer nachvollziehbaren Entgeltermittlung – bis zur Einführung des neuen Operatorsystems darauf achten, daß keine „Übergangslösung" praktiziert wird, die dem in der Regelung des § 89 Abs. 5 TKG zum Ausdruck gebrachten Willen des Gesetzgebers zuwiderläuft.

10.4.3 Die Telekom gab Auskünfte über Schulden ehemaliger Anschlußinhaber

Mehrere Kunden, die der Telekom einen Auftrag für einen Telefonanschluß erteilt hatten, erhielten nach kurzer Zeit statt des Gewünschten die Anforderung einer Sicherheitsleistung, die in Einzelfällen – je nach Art des beantragten Anschlusses – mehrere tausend DM betrug. Auf Nachfrage begründete dies die Telekom dem erstaunten Kunden damit, daß der ehemalige Anschlußinhaber noch Schulden habe, wobei weder aus dessen Namen noch über die Höhe seiner Schulden ein Geheimnis gemacht wurde. Wegen einer vermuteten räumlichen oder persönlichen Nähe des Auftraggebers zum Schuldner sei zu besorgen, daß es wieder zu Zahlungsausfällen komme. Daher müsse sich der Neukunde als „Strohmann" behandeln lassen, von dem man ebenso eine Sicherheitsleistung fordern könne.

Hatte die Telekom in früheren Jahren – in unzulässiger Weise – derartige Informationen „nur" gegenüber Familienangehörigen erteilt (s. 14. TB Nr. 21.9), erfolgten diese jetzt auch gegenüber Geschäftspartnern, Lebensgefährten und Nachbarn.

Ich habe die Deutsche Telekom AG darauf hingewiesen, daß ihre Praxis wegen Verstoßes gegen § 3 Abs. 1 TDSV rechtswidrig ist. Auf eine Beanstandung gemäß § 25 Abs. 1 BDSG konnte ich jedoch verzichten, nachdem sich die Deutsche Telekom AG sofort bereiterklärte, mit mir die Voraussetzungen abzustimmen, die kumulativ vorliegen müssen, um datenschutzrechtliche Bedenken auszuräumen:

- Das Vertragsverhältnis zwischen der Deutschen Telekom AG und dem Schuldner darf nicht mehr bestehen, d. h. der Telefonanschluß muß gekündigt sein. Damit ist die Zulässigkeit der Mitteilung nach § 16 BDSG zu beurteilen. Sie ist gegeben, wenn „sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist". Die Aufgabe ist hier die Begründung der Anforderung einer Sicherheitsleistung gemäß § 9 Abs. 1 Telekommunikations-Kundenschutzverordnung (TKV 1995) gegenüber dem Neukunden.
- Die Mitteilung über Bestehen und Höhe der Altschulden muß zur Begründung der Anforderung der Sicherheitsleistung unerläßlich sein:

Die Mitteilung lediglich der Tatsache, daß der ehemalige Anschlußinhaber noch Schulden aus seinem Vertragsverhältnis hat, ist in der Regel zur Begründung der Anforderung einer Sicherheitsleistung erforderlich und somit zulässig. Angaben über die Höhe der Schulden sind im berechtigten Interesse des Auftraggebers (Neukunden) erst dann erforderlich, wenn er der Höhe der angeforderten Sicherheitsleistung widersprochen hat und sie daher dazu dienen, ihm gegenüber die Höhe der angeforderten Sicherheitsleistung zu begründen.

- Es müssen konkrete, nachweisbare Tatsachen für die Deutsche Telekom AG die Besorgnis begründen, daß
  - = der Altschuldner – in vergleichbarem Umfang wie seinen ehemaligen eigenen – auch den Anschluß des Neukunden nutzen wird und
  - = die deshalb zu erwartenden neuen Forderungen vom Neukunden ebenfalls nicht beglichen werden können.

Auch bei Vorliegen der o. g. Voraussetzungen dürfen dem Neukunden nur die zur Begründung der Sicherheitsanforderung erforderlichen Daten bekanntgegeben werden.

Die Deutsche Telekom AG hat bisher nicht den Nachweis erbringen können, daß die genannten Voraussetzungen in einem der Beschwerdefälle erfüllt gewesen wären.

Ich sehe im übrigen durchaus die Notwendigkeit, daß sich die Telekommunikationsunternehmen vor Gebührenausfällen schützen können, die von der Gesamtheit der Kunden über die Höhe der Entgelte wieder aufgefangen werden müßten. Hierfür sollte aber die Rechtsverordnung, die als präventive Maßnahme die Erhebung einer Sicherheitsleistung vorsieht, die Voraussetzungen und Verfahrensschritte hinreichend klar regeln, damit diese auch u. U. von Dritten verlangt werden darf.

Der gegenwärtige Rechtszustand führt immer wieder dazu, daß das Bestehen von Telefonschulden sowie deren Höhe in rechtswidriger Weise Dritten mitgeteilt werden, wobei allzu oft das vordringliche Ziel erkennbar wird, durch derartige „Veröffentlichungen" im sozialen Umfeld Druck auf den Schuldner auszuüben.

10.4.4 Sektenmitgliedschaft und Telefonschulden – die Beitreibungsakten der Telekom

Zu einem Zeitpunkt, als die Aktivitäten einer auch wegen ihrer wirtschaftlichen Aktivitäten kritisierten Sekte die öffentliche Diskussion beherrschten, wandte sich eine Petentin mit dem Hinweis an mich, in ihrer Akte bei einer Beitreibungsstelle der Deutschen Telekom AG sei ein Vermerk mit folgendem Wortlaut enthalten: „... Schuldnerin soll irgendwie bei [Name der Sekte] drin sein." Sie hatte dies während eines Besuches in der Beitreibungsstelle durch „einen schnellen Blick" in ihre Akte sehen können und war über diese – wie sie sagte, unberechtigte – Verdächtigung empört.

Meine Kontrolle bei der Beitreibungsstelle bestätigte den Hinweis der Petentin. In ihrer Akte fanden sich darüber hinaus abwertende Vermutungen über ihren Ehemann. Weitere Kontrollen in zufällig ausgewählten anderen Akten ergaben, daß es sich bei den Vermerken in dieser Beitreibungsakte offensichtlich um einen Einzelfall gehandelt hat; in keiner der anderen Akten befanden sich derartige Notizen. Auf meinen Hinweis, daß die Eintragungen in der Beitreibungsakte der Petentin – unabhängig von ihrem Wahrheitsgehalt – mangels Erforderlichkeit für das Beitreibungsverfahren datenschutzrechtlich unzulässig seien, wurden diese von der Beitreibungsstelle aus der Akte entfernt und vernichtet. Ich habe daher gemäß § 25 Abs. 2 BDSG von einer Beanstandung abgesehen, zumal die Deutsche Telekom AG meiner Forderung nachgekommen ist, alle Beitreibungsstellen nochmals ausdrücklich auf die Unzulässigkeit derartiger Vermerke in den Kundenakten hinzuweisen.

Die Telekom hat mich kürzlich darüber informiert, daß ihr gesamtes Mahn- und Beitreibungswesen neu organisiert wird; die bisherige Form der Beitreibungsakten wird zukünftig entbehrlich.

10.4.5 Die CD-ROM weiß alles – nicht nur Freude über das „Elektronische Telefonbuch"

Seit Anfang der 90er Jahre hat auch in den privaten Bereich der PC-Nutzung ein Datenträger Eingang gefunden, für den es bis heute keinen deutschen Namen gibt: Die CD-ROM (compact disc – read only memory). Diese Speicherplatte, die äußerlich identisch mit der bekannten Musik-CD ist, kann – anders als die Festplatte des PC – nur gelesen, in ihrem Dateninhalt (durch Überschreiben) jedoch nicht verändert werden; zu den sich hieraus ergebenden Datenschutzproblemen siehe unten Nr. 33.3.

Die sehr große Speichermöglichkeit der CD-ROM ermöglicht Anwendungen, die vordem nur auf größeren Rechnern möglich waren. Besonderes Aufsehen – sowohl freudiges Interesse, aber auch scharfe Kritik – lösten bundesweite „Elektronische Telefonbücher" aus, insbesondere das eines Anbieters, der Anfang 1995 eines herausbrachte, das auch nur einen Bruchteil der Konkurrenzprodukte kostete.

Neu war auch die Möglichkeit der **bundesweiten** Suche eines Telefonteilnehmers: Gibt man z. B. den Namen eines ehemaligen Mitschülers ein, den man seit dem Schulende aus den Augen verloren hat, findet ihn die CD-ROM-Datenbank und zeigt seine Anschrift und seine Telefonnummer auf dem Bildschirm an. Voraussetzung ist dabei, daß er seinen Telefonanschluß auch hat ins Telefonbuch eintragen lassen, was allerdings immer noch über 90% aller Telefonkunden tun.

Bereits diese Neuerung blieb nicht ohne Kritik: Viele Bürger legen gar keinen Wert darauf, von ehemaligen Mitschülern „wiederentdeckt" zu werden, auch Geschiedene wollen oft im Sinne eines Neubeginns vom ehemaligen Ehepartner keineswegs auf diese Weise „wiedergefunden" werden.

Auch weitere „komfortable Suchmöglichkeiten" stießen und stoßen auf Kritik: So nennt einem die Datenbank auch alle Telefonteilnehmer, die in einem bestimmten Haus, gar in einer bestimmten Straße wohnen.

Die Bürger, die sich bei mir beschwert haben, sind zwar damit einverstanden, daß ihr Name, ihre Anschrift und ihre Telefonnummer ins **Telefonbuch** eingetragen sind. Sie haben aber nicht gewollt, daß diese Daten in einem **elektronischen Auskunftssystem** mit seinen vielfältigen Auswertungsmöglichkeiten angeboten werden.

Auf noch schärfere Kritik stieß eine weitere Neuerung, die **„Inverssuche**: Hierbei sagt einem die Datenbank nicht die Telefonnummer eines bestimmten Anschlußinhabers, vielmehr sagt sie einem – nach Eingabe einer Telefonnummer – wer der Inhaber dieses Anschlusses ist, wo er wohnt und ggf., welchen Beruf er hat. Diese Form der Suche ist oftmals von großer Bedeutung für die Ermittlungsarbeit der Polizei und anderer Sicherheitsbehörden (s. o. Nr. 10.1.5). Das gilt z. B. dann, wenn bei einem festgenommenen Straftäter Telefonnummern gefunden werden, die möglicherweise Mittätern zuzurechnen sind und die es zu ermitteln gilt. Wird den Sicherheitsbehörden diese Suchmöglichkeit auch eingeräumt, so wollen sehr viele Bürger sie jedoch keineswegs jedermann zugestehen.

Anfang 1995 enthielt das geltende Recht keine besondere Regelung für elektronische Verzeichnisse. Entsprechend war die datenschutzrechtliche Bewertung problematisch und die Rechte der Betroffenen waren nur mangelhaft gewahrt. Ich hatte daher seinerzeit gesetzliche Klarstellungen gefordert, damit der Bürger selbst in der Lage ist, die Entscheidung über die Verwendung seiner Daten treffen zu können. Er sollte nicht nur wissen, welche Verwendungsmöglichkeiten für seinen Eintrag bei der Aufnahme ins Telefonbuch bestehen, darüber hinaus war es erforderlich, daß er nicht nur bestimmen konnte, daß seine Daten nicht oder verkürzt ins Telefonbuch eingetragen wurden, sondern auch daß er den Eintrag auf gedruckte Verzeichnisse beschränken konnte.

Ich habe diese Problematik mit großem Nachdruck bei den Beratungen zur Telekommunikationsdienstunternehmen-Datenschutzverordnung (TDSV) vorgetragen und habe erreichen können, daß in dieser dem Telefonkunden ein solches **abgestuftes Widerspruchsrecht** eingeräumt wurde (s. o. Nr. 10.2.1). Seit deren Inkrafttreten – also dem 19. Juli 1996 – kann in der Tat jeder Telefonkunde selbst entscheiden, ob er überhaupt – und in welcher Form – in ein Verzeichnis eingetragen werden möchte und ob dies lediglich in gedruckte oder aber auch in elektronische Verzeichnisse, wie der CD-ROM, geschehen soll. Diese Rechtsposition der Telefonkunden ist durch § 89 Abs. 8 TKG noch in der Weise verstärkt worden, daß Name, Anschrift und zusätzliche Angaben, wie Beruf, Branche, Art des Anschlusses und Mitbenutzer, nur dann in öffentliche gedruckte oder elektronische Verzeichnisse eingetragen werden dürfen, soweit der Kunde dies beantragt.

Hat ein Telefonkunde von seinen Rechten Gebrauch gemacht, wird seine Telefonbucheintragung entsprechend gekennzeichnet. Damit ist jedem Nutzer der Telefonbucheintragungen – also auch Unternehmen, die diese Daten zum Erstellen elektronischer Telefonverzeichnisse, wie der CD-ROM, nutzen – zweifelsfrei verdeutlicht, daß der Kunde *„ein schutzwürdiges Interesse an dem Ausschluß der Übermittlung seiner personenbezogenen Daten"* hat (vgl. § 29 Abs. 2 Nr. 2 BDSG). Nimmt ein Anbieter die im Telefonbuch gekennzeichneten Anschlußeintragungen trotzdem in sein CD-ROM-Telefonverzeichnis auf, verletzt er damit unwiderlegbar schutzwürdige Interessen der Betroffenen und unterliegt somit den im Bundesdatenschutzgesetz vorgesehenen Sanktionen. Damit ist jetzt für die betroffenen Telefonkunden die Möglichkeit gesichert, bei Zuwiderhandlungen ihre Interessen rechtlich durchzusetzen.

Auch die Bundesregierung hat in einer Antwort auf eine parlamentarische Anfrage meine Rechtsauffassung geteilt: *„Auf diese Weise wird für den Anbieter von elektronischen Telefonverzeichnissen, der selbst keine Telekommunikationsdienstleistungen nach Maßgabe der TIDSV* (jetzt: TDSV) *zur Verfügung stellt, deutlich, daß schutzwürdige Interessen des Betroffenen einer Aufnahme in die CD-ROM entgegenstehen"* (BT-Drucksache 13/3285).

Ich hoffe, daß bei den Anbietern elektronischer Telefonverzeichnisse der Wunsch der Bürger sowie die Rechtslage künftig konsequenter umgesetzt wird – notfalls werden die Gerichte hier Klarheit schaffen.

Inzwischen haben mich bereits eine Reihe von Eingaben zur Kennzeichnung von Telefonbucheintragungen – z. B. durch einen ★ – erreicht: Diese Bürger befürchten eine „Stigmatisierung" ihrer Person, etwa als technik- oder kommunikationsfeindlich. Es gibt daher derzeit schon konkrete Überlegungen, von einer Kennzeichnung solcher Einträge abzusehen, und statt dessen in die gedruckten Verzeichnisse – an exponierter Stelle und mit drucktechnischer Hervorhebung – einen allgemeinen Hinweis anzubringen, der den gleichen Schutzeffekt hat. Dieser Hinweis müßte darauf aufmerksam machen, daß in diesem Telefonbuch auch Einträge von Kunden sind, die der Veröffentlichung ihrer Einträge in **elektronischen** Verzeichnissen widersprochen haben und müßte die Nutzer der Telefonbucheintragungen auch auf die Rechtsfolgen einer Nichtbeachtung der Widersprüche hinweisen. Der Hinweis müßte natürlich nicht nur in einzelnen, sondern in **allen** Telefonbüchern enthalten sein, also neben dem offiziellen Telefonbuch der Telekom (dem ehemaligen „amtlichen") insbesondere auch im Örtlichen Telefonbuch.

Dieses Konzept habe ich als besonders datenschutzfreundlich begrüßt, allerdings darauf hingewiesen, daß es nicht im Einklang mit dem Wortlaut des derzeit gültigen § 10 Abs. 3 Satz 1 und 2 TDSV steht. Die gemäß § 89 Abs. 1 TKG von der Bundesregierung zur erlassende „TDSV-Nachfolgeverordnung" müßte ggf. hier eine Klarstellung erhalten (s. o. Nr. 10.1.4).

10.4.6 Konferenzschaltung mit dem Anrufbeantworter – unerwünschte „Komfortleistungen" für Telefonkunden

Im Dezember 1995 erhielten viele Kunden der Deutschen Telekom AG wieder einmal eine Beilage zu ihrer Telefonrechnung. Diesmal sollten sie allerdings nicht – wie zuvor öfter – zum Kauf etwa von Heizkörperverkleidungen veranlaßt werden, vielmehr sollte sie das bunte Heftchen auf die Einführung sogenannter **Komfortleistungen** im Telefondienst aufmerksam machen. Das Heftchen lag den Rechnungen solcher Telefonanschlüsse bei, die bereits an digitalen Vermittlungsstellen angeschlossen sind; die Deutsche Telekom AG spricht in diesem Zusammenhang vom sogenannten „T-Net", das mittlerweile über 70% aller deutschen Telefonanschlüsse umfaßt.

Anfang Januar 1996 wurden dann ohne weitere Benachrichtigung die Komfortleistungen aktiviert. Zu ihnen gehört neben dem sogenannten „Anklopfen" auch die „Dreierkonferenz".

„Anklopfen" kann ein Anrufer bei einem Anschluß, der von seinem Inhaber (durch Wahl bestimmter Codeziffern) hierfür freigeschaltet wurde. Ruft man einen solchen Anschluß an, wenn er besetzt ist, hört der Benutzer des besetzten Anschlusses ein besonderes akustisches Signal („Anklopfton"). Er hat dann z. B. die Möglichkeit, das laufende Gespräch zu unterbrechen, um kurz mit den „Anklopfer" zu sprechen.

Die „Dreierkonferenz" kann z. B. für drei sportliche Radler hilfreich sein, wenn die sich für ihre nächste Tour verabreden wollen: Dazu ruft der Initiator zunächst den „zweiten Mann" an und kommt mit ihm überein, auch noch den dritten Sportsfreund in dieses Telefonat einzubeziehen. Dann drückt er entweder auf einen besonderen Knopf an seinem Apparat („R-Taste") oder tippt kurz auf die „Gabel". Um jetzt den „Dritten" zu erreichen, wählt er dessen Nummer. Hat er ihn erreicht, drückt er erneut auf die „Gabel" und wählt die Ziffer „3", woraufhin dann alle drei Sportsfreunde miteinander reden und ihren Termin vereinbaren können.

Diese „Komfortleistungen" stellen eine interessante Neuerung dar, die mancher Telefonkunde sicher gern nutzen wird – wenn er von ihrer Existenz weiß und er über die Bedienung informiert ist. Genau dort liegen aber die entstandenen Probleme: Wie ich durch viele Bürgerbeschwerden weiß, haben nämlich viele Telefonkunden das Heftchen der gleichen Kategorie wie der der Heizkörperverkleidungen zugerechnet und es ungelesen dem Papierkorb überantwortet. Große Empörung kommt in den Beschwerden insbesondere darüber zum Ausdruck, daß die Telekom mit dieser Aktion eine Verkaufsmethode gewählt hat, die aus guten Gründen inzwischen der Vergangenheit angehört, nämlich die „unverlangte Lieferung": Insbesondere Bücher waren in der Vergangenheit Bürgern mit einem Anschreiben zugesandt worden, in dem die Auffassung vertreten wurde, daß bei nicht erfolgter Rücksendung des Buches damit ein Liefervertrag über vierteljährliche Fortsetzungslieferungen vereinbart sei. Die Gerichte habe längst festgestellt, daß eine solche Annahme abwegig ist.

Durch die unbemerkte Aktivierung der „Komfortleistungen" und ihre unbewußte – und ungewollte – Nutzung kam es zu zahlreichen Störungen und Rechnungsbeanstandungen. Zu ganz gravierenden Störungen und Beeinträchtigungen kam es insbesondere dann, wenn der ahnungslose Telefonnutzer eine **Dreierkonferenz** aktivierte, ohne sich dessen bewußt zu sein: Besonders dann, wenn ein zweites Telefonat geführt werden soll, wird ein Gespräch oftmals nicht durch das Auflegen des Hörers, sondern durch drükken der „Gabel" beendet. Wählte der eilige Telefonnutzer dann eine zweite Verbindung, die mit der Ziffer „3" – der Kennziffer der Konferenzschaltung – begann, wurde der Teilnehmer des ersten Gespräches, wenn er seinerseits noch nicht aufgelegt hatte, überraschend in dieses zweite Gespräch eingeschaltet und konnte – wenn gewollt – unbemerkt mithören.

Noch problematischer und für den Anrufer mit hohen Kosten verbunden ist jedoch die folgende Variante, die mir mehrere Telefonkunden mitgeteilt haben: War der erste Telefonpartner nur ein **Anrufbeantworter** – mit dem der Anrufer sich nicht unterhalten wollte –, wurde der vollständige Inhalt des zweiten Telefonates auf dem Anrufbeantworter aufgezeichnet. Ohne es zu wollen und zu wissen tat der Inhaber des Anrufbeantworters etwas, was nach § 201 des StGB eine Straftat ist, er nahm nämlich *„das nichtöffentlich gesprochene Wort eines anderen auf Tonträger"* auf. Aber auch für den Anrufer war die Angelegenheit oftmals nicht nur teuer – er muß nämlich auch die Verbindung mit dem Anrufbeantworter bezahlen –, manchmal auch peinlich: Eine Petentin hat mir von einem Anruf beim Anrufbeantworter ihres Freundes und einem darauffolgenden, aufgezeichneten bei ihrer besten Freundin berichtet – mit der sie sich dann über Vorzüge und Schwächen des Freundes unterhielt!

Nachdem ich die ersten Beschwerden erhalten hatte, die auf diese Beeinträchtigungen hinwiesen – die zunächst jedoch nicht vollständig und in ihrer Ursache bekannt waren – habe ich dies unverzüglich der Deutschen Telekom AG mitgeteilt. Unverständlich ist, warum es danach immer noch drei Wochen dauerte, bis die „unverlangten Lieferungen wieder abgeholt", die Komfortleistungen also deaktiviert wurden. Die Deutsche Telekom AG bietet jetzt ihren T-Net-Kunden die Komfortleistungen erneut an, allerdings werden sie nur dann aktiviert, wenn der Kunde das Angebot angenommen hat. Sie hat mir darüber hinaus auch mitgeteilt, daß sie diese Komfortleistungen nur im Zusammenhang mit solchen Telefonen („Endgeräten") anbietet, bei denen die oben beschriebenen Fehlschaltungen ausgeschlossen sind. Ich werde darauf achten, daß diese Zusicherung eingehalten wird.

10.4.7 „Komfortauskunft" der Telekom: „Boxenstopp" in der ersten Runde!

In die Ferienzeit des Sommers 1996 startete die Deutsche Telekom AG ihre Kundeninformation: „Bei der Auskunft tut sich was." Diese Aktion führte bei den Kunden zu einer fast vergleichbaren Empörung wie die Panne bei der Gebührenumstellung zum Jahresbeginn. Es stellte sich im Nachhinein als kein gutes Omen heraus, daß die Telekom ihren Slogan „Mehr Leistung. Mehr Geschwindigkeit." mit einem zu einem roten Rennwagen stilisierten Telefonapparat untermalt hatte (s. Abb. 6). Etwas mehr Dynamik

Abbildung 6

bei der inhaltlichen Gestaltung der Kundeninformation, etwas mehr Sorgfalt bei der Präsentation – und es hätte sich nicht der Vergleich mit den damaligen Leistungen eines roten „Flitzers" aus dem Formel-1-Rennsport aufgedrängt. Was war geschehen?

Im August hatte die Telekom den Telefonrechnungen ein Faltblatt beigefügt, mit dem sie über die Erweiterung ihres Leistungsangebots bei den telefonischen Auskunftsdiensten zu informieren beabsichtigte. Bekanntlich durfte die Telekom bisher nur Auskunft über die Rufnummern, nicht jedoch über die Anschrift, geben. Nach Inkrafttreten der Telekommunikationsdienstunternehmen-Datenschutzverordnung (s. o. Nr. 10.2.1) war die Telekom berechtigt, im Rahmen einer sog. Komfortauskunft einem Anrufer alle Daten mitzuteilen, die im Telefonbuch über den Angefragten veröffentlicht sind. Der Gesetzgeber hatte den Telefonkunden jedoch ein Widerspruchsrecht eingeräumt, über das sie mit einer, der nächsten Fernmelderechnung beigefügten, Antwortkarte zu unterrichten waren. Dieser Vorgabe war die Telekom jedoch nur in höchst unzureichendem Maße nachgekommen. Über mehrere Wochen hinweg erreichten mich zahllose Beschwerden verärgerter und verunsicherter Bürger, die im wesentlichen folgende Kritikpunkte enthielten:

- Eine das Selbstbestimmungsrecht der Kunden berührende Information dürfe nicht in Form einer Reklame aufgemacht sein, die in den meisten Fällen sofort ungelesen in den Papierkorb geworfen wird. Derartige Beilagen zur Telefonrechnung hätten bisher immer nur Werbung für Heizkörperverkleidungen oder ähnliches enthalten.
- Die Broschüre enthalte an keiner Stelle einen Hinweis, daß die Kunden ihren Widerspruch auch noch nach Ablauf der dort genannten Vier-Wochen-Frist einlegen können. Dies wäre vor allem deshalb wichtig gewesen, weil sehr viele Kunden die Broschüre erst nach Urlaubsrückkehr – und somit oft nach Ablauf dieser Frist – erreichte. Damit setzte sich die Telekom dem Vorwurf aus, sie habe ihre Kunden bewußt an der Ausübung ihrer Rechte hindern wollen.
- Die Antwortkarte – wenn man sie denn überhaupt entdeckte – sei im Innenteil des Faltblattes „versteckt" gewesen. Mit dieser Antwortkarte konnte zudem nur Widerspruch gegen die sog. Komfortauskunft eingelegt werden: Ein Widerspruch gegen die Aufnahme der Kundendaten in elektronische Verzeichnisse (z. B. CD-ROM), über dessen Möglichkeit ebenfalls im Faltblatt „informiert" wurde, war nur telefonisch über eine dort angegebene „Hotline-Nummer" vorgesehen. Nahezu allen Kunden war diese feinsinnige – auch für mich nicht nachvollziehbare – Unterscheidung, die die zusätzliche Gefahr einer Rechtsbeeinträchtigung für die Bürger heraufbeschwor, verborgen geblieben.
- Es hätte deutlicher zum Ausdruck gebracht werden müssen, daß nur über die in den Telefonbüchern bereits veröffentlichten Daten Auskunft erteilt werden sollte und daß sich für die Kunden, die keinen Eintrag im Telefonbuch hatten, keine Änderung ergab.

Unmittelbar nach Erscheinen des Faltblattes habe ich mich mit Hilfe der Medien an die Bürger gewandt und sie über ihre Rechte informiert. Zugleich habe ich die Telekom aufgefordert, ihre Aktion nachzubessern. Nachdem auch aus dem politischen Raum entsprechende Forderungen erhoben worden waren, stellte die Telekom ihre „Komfortauskunft", die sie bis dahin im Rahmen eines Pilotprojektes in Köln und München betrieben hatte, ein. Sie hat diese Anfang November 1996 wieder aufgenommen, nachdem sie ihre Kunden erneut mit einem mit mir abgestimmten Informationsblatt über bestehende Rechte und Wahlmöglichkeiten unterrichtet hatte. Bei rechtzeitiger Annahme meines bereits frühzeitig erklärten Angebotes, an der Gestaltung der Kundeninformation mitzuwirken, hätte sich die Deutsche Telekom AG mehr als nur einen erheblichen Kostenaufwand ersparen können.

10.4.8 „Überraschende" Übertragung der Kennung des Absenders von E-Mail an den Empfänger bei T-Online

Die Deutsche Telekom AG bietet in ihrem T-Online-Dienst die Möglichkeit, anstelle der im allgemeinen aus der Telefonnummer und einem Zusatz bestehenden E-Mail-Adresse eine von ihm selbst gewählte, beliebige „Aliasadresse" zu verwenden. Das gibt dem Teilnehmer die Möglichkeit, seine eigene Telefonnummer seinen Kommunikationspartnern nicht preisgeben zu müssen.

Schreibt der Teilnehmer aber eine Nachricht und stellt sie in eine Internet-Newsgroup ein, so wird auch dort als Absender die Aliasadresse angegeben. Läßt man sich den Dokumentenquelltext zu dieser Nachricht anzeigen, so stellt man fest, daß dort neben der Aliasadresse auch die eigentliche E-Mail-Adresse mit Telefonnummer und dem Vor- und Nachnamen zu lesen ist.

Da dies offensichtlich der Mehrzahl der Teilnehmer nicht bekannt ist, waren manche überrascht, plötzlich Anrufe von Kommunikationspartnern zu erhalten, denen sie ihre Telefonnummer nicht gegeben hatten. Auch Telefonnummern, die auf Wunsch des Anschlußinhabers weder von der Auskunft genannt werden dürfen, noch in die Telefonbücher eingetragen sind, werden auf diese Weise weltweit bekannt, wenn der Betroffene ins Internet geht.

Für Telefonnummern, die in Telefonbüchern eingetragen sind, ist es zudem möglich, mit derzeit im Handel erhältlichen Telefonverzeichnissen auf CD-ROM über die Telefonnummer auch die Anschrift zu erfahren (s. o. Nr. 10.4.5).

Die Bundesregierung hat auf eine parlamentarische Anfrage zu diesem Thema geantwortet, die datenschutzrechtlichen Aspekte bei der Nutzung von T-Online würden in dem gegenwärtig als Referentenentwurf vorliegenden Informations- und Kommunikationsdienste-Gesetz – IuKDG – (s. o. Nr. 8.1) geregelt. In diesem Zusammenhang werde auch die Möglichkeit erörtert, anstelle der Telefonnummer ein vom Diensteanbieter zur Verfügung gestelltes Pseudonym zu verwenden (BT-Drucksache 13/5403 vom 6. August 1996, Seite 40).

Die Deutsche Telekom AG, die ich wegen einiger Eingaben von Teilnehmern um Stellungnahme gebeten hatte, hat mir mitgeteilt, daß die T-Online-Nummer auch bei Verwendung einer Zweitadresse („Aliasadresse") immer mit übertragen werden müsse, um eine Antwort zu ermöglichen. Auf diese Notwendigkeit seien die Nutzer von Zweitadressen durch die im System online zur Verfügung gestellten Benutzerhinweise informiert. Die „Aliasadresse" diene lediglich der Vereinfachung der Kommunikation der Teilnehmer. Es bestehe jedoch die Möglichkeit, beim T-Online-Auftragsservice eine T-Online-Nummer zu wählen, aus der sich keine Rückschlüsse auf die Telefonnummer ergeben.

Die Petenten haben die Benutzerhinweise offensichtlich nicht gekannt. Ich halte die Regelung, eine T-Online-Nummer ohne Bezug auf eine Telefonnummer zu erhalten, zwar für ausreichend, die Verwendung eines Pseudonyms, wie in der Antwort auf die parlamentarische Anfrage erwähnt, wäre aber sicherlich datenschutzfreundlicher. Sie ist bei anderen Anbietern auch gängige Praxis.

10.4.9 Erst beobachtet und dann hinausgeworfen

Wer umzieht, kann sich im allgemeinen über einen Mangel an Problemen, Schwierigkeiten und Laufereien nicht beklagen.

So erging es auch einem Bürger aus Stuttgart, der aber nicht ahnte, daß er als T-Online-Kunde infolge seines Wohnsitzwechsels ein besonderes Problem bekommen sollte. Da er die Rufnummer des Telefonanschlusses in der aufgegebenen Wohnung, unter der er auch Zugang zu T-Online hatte, nicht in die neue „mitnehmen" konnte, kündigte er den alten Telefonanschluß und beauftragte die Telekom mit der Einrichtung eines Telefonanschlusses in seiner neuen Wohnung.

Sechs Wochen später – nach überstandenen Umzugswirren – bestätigte ihm die Telekom völlig überraschend die Kündigung seiner T-Online-Zugangsberechtigung. Der Bürger hatte jedoch nie die Absicht, den T-Online-Zugang zu kündigen und versuchte nun herauszufinden, wie es wohl zu dieser irrigen Annahme gekommen sein könnte. Dabei erfuhr er telefonisch von der Telekom, daß er „im Juni und Juli T-Online nicht in Anspruch genommen habe; dann hätte man sich das im August noch 14 Tage angeguckt, da gab es auch keine Nutzung, da hätte man ihn dann rausgeschmissen".

Bei der Gestaltung der rechtlichen Rahmenbedingungen für Btx (dann Datex-J, jetzt T-Online) wurde der „Unbeobachtetheit" des Nutzers stets besondere Bedeutung beigemessen (s. auch 15. TB Nr. 20.2.6). Daher war es wichtig, zu klären, was sich hinter dem Vorwurf des Petenten verbarg. Von der Telekom erfuhr ich dann folgendes:

Bei Telefonkunden, die auch T-Online-Teilnehmer sind, werden anfallende T-Online-Entgelte auf die jeweilige Telefonrechnung gesetzt. Ordnungsmerkmal für die Rechnungserstellung ist dabei die sogenannte „Fernmeldekontonummer" (FKTO), die aus der Telefonnummer gebildet wird. Kündigt ein Kunde seinen Telefonanschluß – z. B. aufgrund eines Umzuges – wird die diesem Telefonanschluß fest zugeordnete FKTO für ihn aufgehoben und bei Neuvergabe des Anschlusses dem Nachfolger zugeteilt. Damit konnten für die alte FKTO des Petenten T-Online-Entgelte nicht mehr in Rechnung gestellt werden. Soll auch nach Kündigung des Telefonanschlusses T-Online weitergenutzt werden, müssen die Entgelte über die Rechnung eines anderen Telefonanschlusses des Kunden – sofern vorhanden – oder eines neu einzurichtenden Fernmeldekontos eingezogen werden.

Die Deutsche Telekom AG hat nach ihren Angaben die Erfahrung gemacht, daß viele Kunden nach Kündigung des Telefonanschlusses nicht auch auf T-Online verzichten möchten, dies jedoch bei der Kündigung nicht mitteilen. Wurde also ein Telefonanschluß mit T-Online-Zugang gekündigt, prüfte die Telekom, wann das letzte Nutzungsentgelt aufgekommen war. Dabei sei es also nicht um die Höhe des Entgeltes gegangen, sondern es sollte nur festgestellt werden, ob mit dem Anschluß noch gearbeitet wurde, der Wille zur vertraglich vereinbarten Nutzung also überhaupt noch bestand. Wurden **keine** Nutzungsentgelte mehr festgestellt, erfolgte zunächst eine Sperrung. Meldete der Kunde sich danach nicht mehr, wurde die Zugangsberechtigung nach einiger Zeit aufgehoben.

In den übrigen Fällen, d. h. wenn Nutzungsentgelte angefallen waren, also mit T-Online auch nach der Aufhebung des Telefonanschlusses weitergearbeitet wurde, schrieb die Telekom den Kunden an, um die zukünftige Abrechnungsmöglichkeit für die T-Online-Entgelte zu klären. Erst wenn auf dieses Schreiben keine Reaktion erfolgte, wurde auch in diesen Fällen die Online-Zugangsberechtigung aufgehoben.

Der Petent hatte nach der Kündigung seines Telefonanschlusses in der Tat – u. a. wegen eines Urlaubes – T-Online mehrere Wochen nicht genutzt; es waren also auch keine Nutzungsentgelte angefallen. Die Betrachtungsweise der Telekom hatte daher zu der falschen Annahme geführt, es fehle bei ihm der „Wille zur vertraglich vereinbarten Nutzung".

Die Telekom hat die datenschutzrechtliche Zulässigkeit ihres Vorgehens auf die Vorschriften der §§ 4 und 6 TDSV gestützt. Ob dies vertretbar ist, kann dahinstehen, denn die beschriebene Vorgehensweise führt – wie auch im vorliegenden Fall – immer wieder zu falschen Arbeitsergebnissen und ist nebenbei auch noch aufwendig. Mir ist unverständlich, warum in derartigen Fällen der T-Online-Kunde nicht einfach telefonisch oder schriftlich gefragt wird, ob er den T-Online-Anschluß ebenfalls kündigen oder diesen beibehalten möchte. Damit entfiele auch die Notwendigkeit der grundsätzlich unzulässigen Beobachtung seines Nutzungsverhaltens bei T-Online.

Ich hoffe, daß die Deutsche Telekom AG oder das Unternehmen, das von ihr zum Betrieb von T-Online ausgegliedert werden soll, hier eine Verfahrensänderung vornimmt.

10.4.10 Rabatte für Privatkunden der Telekom

Ende Juli 1996 hat die Deutsche Telekom AG bei rund einhunderttausend Teilnehmern mit dem Test zweier optionaler „City-Tarife" begonnen, die für Privatkunden gedacht sind. Es handelt sich dabei zum einen um den Tarif „City Weekend", mit dem der Kunde an Samstagen, Sonntagen und bundeseinheitlichen Feiertagen im Citybereich zum günstigen „Mondscheintarif" telefonieren kann. Zum anderen wird „City Plus" angeboten, mit dem der Kunde mit fünf zuvor von ihm festgelegten Rufnummern im Citybereich von 5 bis 21 Uhr in einem Abrechnungszeitraum 400 Tarifeinheiten im 90 Sekunden-Zeittakt telefonieren kann.

Zahlreiche Kunden hatten sich bei mir beschwert, daß sie City Plus nur nutzen können, wenn sie der Telekom ihre – wie dies naheliegt – fünf wichtigsten Telefonpartner benennen.

Ein weiteres Datenschutzproblem ergibt sich daraus, daß bei City Plus die Verbindungsdaten einschließlich der Zielrufnummern ungekürzt gespeichert und bis zu 80 Tagen nach Versendung der Rechnung aufbewahrt werden. Die Zielrufnummern werden im Einzelverbindungsnachweis auch ungekürzt ausgedruckt. Darüber hat der Kunde, der den Tarif beantragt, die Anschlußinhaber der Zielrufnummern zu informieren und ihr Einverständnis einzuholen. Die Speicherungsdauer von 80 Tagen ist notwendig, da eine ordnungsgemäße Fakturierung nur durch Auswertung der vollständigen Zielrufnummer möglich ist. Nach der Rechnungsstellung ist die Speicherung erforderlich, um eine qualifizierte Beschwerdebearbeitung vornehmen zu können. Der Ausdruck der vollständigen Zielrufnummern im Einzelverbindungsnachweis soll den Kunden in die Lage versetzen, die Richtigkeit seiner Rechnung zu überprüfen.

Sicherlich wäre auch eine Tarifkonstruktion möglich gewesen, die die genannten Datenschutzprobleme vermeidet. Die neuen Tarife werden jedoch **wahlweise** angeboten; der Kunde wird in das Verfahren nur eingebunden, wenn er in die ihm erläuterten Bedingungen einwilligt. Tut er dies nicht, hat er nicht mit Nachteilen für sein Persönlichkeitsrecht zu rechnen. Ich habe daher meine anfänglichen Bedenken gegen die Bekanntgabe der Telefonpartner und die Speicherung sowie den Ausdruck der Zielrufnummern im Interesse günstigerer Tarife für die Kunden zurückgenommen.

10.4.11 Immer wieder – und immer neuer – Ärger mit der Telefonrechnung

Seitdem telefoniert wird, gibt es Menschen, die sich über die Höhe ihrer Telefonrechnung ärgern und diese in Zweifel ziehen. Zweifellos liegt die Hauptursache in einem Mangel an Transparenz des gesamten Verfahrens der Rechnungsstellung.

Gerade beim Telefonieren könnte die Technik aber neue Lösungen ermöglichen: Beim Führen eines Telefonates erfährt der Kunde nicht, was es gekostet hat; nur ein Bruchteil aller Apparate ist mit der Anzeigemöglichkeit ausgestattet, und die hierfür erforderliche „Übermittlung der Zählimpulse" an das Kundentelefon muß die Telekom im Einzelfall erst einrichten, wofür sie dann auch noch ein zusätzliches Entgelt verlangt. Hier könnte die Telekom durch kleine Änderungen sich und ihren Kunden viel Ärger ersparen und letzteren dabei gleichzeitig die gewünschte Transparenz verschaffen.

Verschärft hat sich die Problematik nicht nur durch „Sextelefondienste", die 1995 aus dem fernen Ausland angeboten wurden, sondern auch durch die sog. Audiotex-Dienste, die unter 0190-Rufnummern angeboten werden und deren Inanspruchnahme ebenfalls sehr teuer ist (s. u. Nr. 10.4.12).

Ich habe es daher begrüßt, daß die damalige Deutsche Bundespost Telekom seit 1994 begonnen hat, einen sog. Einzelverbindungsnachweis anzubieten, heute „Einzelverbindungsübersicht (EVÜ)" genannt. Technische Voraussetzung für die Erstellung einer solchen EVÜ ist, daß der Telefonanschluß an eine digitale Vermittlungsstelle angeschlossen ist, er also zum sog. T-Net gehört (s. o. Nr. 10.4.6). Inzwischen können auf diese Weise über 70% aller Kunden eine EVÜ erhalten und – unter Zuhilfenahme ihres Gedächtnisses oder von Aufzeichnungen – die Telefonrechnung überprüfen. Das ist dadurch möglich, daß die EVÜ für jedes abgehend geführte Gespräch neben der Uhrzeit, der Dauer und der angewählten Telefonnummer – in Deutschland auch den Namen des betreffenden Zielortes – die Anzahl der Tarifeinheiten und das Gesamtentgelt des Gespräches enthält.

Von 1994 bis 1996 durfte die Telekom die Rufnummer des Angerufenen nicht vollständig im EVÜ ausdrucken, sondern mußte zu seinem Schutz (durch Ersetzen der drei letzten Stellen durch „xxx") die Verbindung anonymisieren (s. 15. TB Nr. 20.2.4). Die dafür ausschlaggebenden verfassungsrechtlichen Gründe entfielen nach Schaffung der gesetzlichen Grundlage in § 10 Abs. 2 Nr. 3a PTRegG mit Inkrafttreten der TDSV am 19. Juli 1996 , die in § 6 Abs. 7 Satz 1 die Bekanntgabe der vollständigen Rufnummer des Angerufenen ausdrücklich zuläßt. Seit dieser Zeit hätte also die Deutsche Telekom AG die Möglichkeit, die EVÜ entsprechend zu gestalten; mir ist jedoch nicht bekannt, zu welchem Zeitpunkt sie beabsichtigt, dies in Angriff zu nehmen.

Für die Erstellung einer EVÜ erhebt die Telekom ein zusätzliches Entgelt. Allerdings hat sie im Frühling 1996 die bisherige „Schlichtrechnung" wesentlich verbessert und ihr auch einen neuen Namen gegeben: Die T-Net-Kunden, die keine EVÜ wollen, erhalten seit diesem Zeitpunkt eine sog. „detaillierte Rechnung". In dieser sind die Verbindungsentgelte bestimmten Kategorien zugeordnet und dort als Summen ausgewiesen, so z. B. – in Abhängigkeit von der Entfernung des Anrufziels – City-Verbindungen, Region 50-Verbindungen, Region 200-Verbindungen usw. Gesondert ausgewiesen sind ebenfalls Verbindungen zu den Mobilfunknetzen, den Funkrufnetzen und zum „Service 0190". Verbindungen zu T-Online sind noch weiter aufgegliedert, z. B. nach „Internetzugang" und „e-Mail-Server-Zugang".

Diese verbesserte Übersicht über die Art der hergestellten Verbindungen und ihre Entgelte ist allerdings nicht von allen Bürgern mit der gleichen Freude aufgenommen worden. Einige Petenten beschwerten sich bei mir darüber, daß auf diese Weise Dritten Einblick in ihr Telefonierverhalten gegeben werde, denen sie ihre Telefonrechnung vorlegen müssen oder möchten. Ein Petent führte dazu aus, „daß Finanzämter von der Telekom nicht mit Informationen darüber versorgt werden sollten, ob und wieviel im City-Bereich und in den Bereichen der Regionen 50, 200, Fern und Ausland telefoniert wird. Das könnte z. B. bei einem von seinem Geschäftsbereich her eher lokal operierenden Unternehmen zu Nachfragen führen, warum denn soviel im Entfernungstarif 200 oder sogar ins Ausland telefoniert werde."

Ich habe den Petenten mitgeteilt, daß ich ihre Argumente zwar nachvollziehen kann, daß das Erstellen einer solchen detaillierten Rechnung gem. § 6 Abs. 2 Nr. 1 i.V. m. § 5 Abs. 1 TDSV jedoch zulässig ist. Auch das Verbot in § 6 Nr. 5, nämlich daß *„Verbindungsdaten nicht ohne Einwilligung des ... Kunden nach Rufnummern angerufener Anschlüsse ausgewertet werden dürfen"*, wird befolgt, denn zur Zuordnung in die Kategorien erfolgt nach Angabe der Telekom AG eine Auswertung lediglich nach Vorwahlnummern, also z. B. der im City-Bereich liegenden Ortsnetze. Aus Sicht des Datenschutzes bestehen selbstverständlich keine Bedenken, wenn die Deutsche Telekom AG auf Wunsch nach wie vor eine „Schlichtrechnung" erstellt; dies ist jedoch Gegenstand unternehmerischer Entscheidung und nicht datenschutzrechtlicher Erfordernisse.

10.4.12 Let's have a (Telefon-)party

In den meisten Fällen freut man sich auf eine Party oder ein geselliges Zusammensein mit Freunden und anderen netten Leuten. Groß ist die Überraschung aber, wenn sich Partygäste ankündigen, die man nicht kennt und die an einer Party teilnehmen wollen, die man angeblich selbst gibt, von der man aber gar nichts weiß.

Solch eine Überraschung erlebte ein Essener Ehepaar. Es informierte mich, daß es an einem Samstagabend im Mai 1996 mehrere Anrufe erhielt, in welchen sich die Anrufer nach Einzelheiten der an diesem Abend bei den Eheleuten stattfindenden Party erkundigen wollten. Nur, eine Party war überhaupt nicht geplant. Von einem der Anrufer erfuhren die Essener dann, daß ihre angebliche Party unter einer 0190-Rufnummer – mit Angabe von Anschrift und Telefonnummer der Eheleute – angekündigt worden war, die er ihnen auch nannte.

Sogenannte Audiotex-Dienste werden von einer Vielzahl von Anbietern unter 0190-Rufnummern inzwischen bundesweit angeboten. Hier kann man sich über aktuelle Börsenkurse oder Fußballergebnisse informieren, aber auch Telefonate jedes beliebigen Inhalts führen. Die Telekom stellt dabei lediglich „die Technik" zur Verfügung; der Dienst selbst wird inhaltlich vom Anbieter gestaltet und ist von ihm zu verantworten. Die Angebotspalette dieser Dienste ist auch deshalb sehr vielfältig, weil sie dem Anbieter angesichts der hohen Tarifentgelte – 3,60 DM pro Minute – gute Gewinne versprechen.

Die Essener Eheleute interessierte natürlich, wer auf diese Weise zu „ihrer" Party eingeladen hatte. Weil die Stellen der Telekom, bei denen sie sich nach dem Inhaber der 0190-Nummer erkundigten, ihnen aus angeblichen „Datenschutzgründen" diesen nicht mitteilen wollten, wandten sie sich hilfesuchend an mich.

Zwar trifft zu, daß nach der TDSV die Auskunftserteilung *„über Namen und andere Daten von Kunden, von denen nur die Rufnummer bekannt ist"*, unzulässig ist (§ 11 Abs. 5 TDSV). Unter dem Schutz der Verordnung stehen jedoch nur natürliche Personen; juristische Personen, wie die Anbieter von Audiotex-Diensten sind nur geschützt, soweit es um Daten geht, die dem Fernmeldegeheimnis unterliegen (§ 1 Abs. 1 Satz 3 TDSV) – was hier nicht der Fall ist.

Zur Bekanntgabe der Anbieter von Audiotex-Diensten hat mir die Zentrale der Telekom mitgeteilt:

„Hier sind die Anbieter der Rufnummer vertraglich verpflichtet, weitere Angaben wie exakte Firmenbezeichnung und Firmensitz über eine kostenlose Rufnummer zur Verfügung zu stellen. Die Verpflichtung resultiert aus dem Vertragsverhältnis, das der Anrufer mit dem Informationsanbieter eingeht. Bei diesem Vertragsverhältnis wird das Entgelt für die Informationsleistung über einen schnelleren Zeittakt bei der Verbindung als „Quasi-Inkasso-Leistung" erhoben.

Für die Mehrzahl der Anbieter wird die so festgelegte Ausunftsverpflichtung über eine telekomeigene Service-0130-Rufnummer gewährleistet, diese Rufnummer lautet 0 130 190 190. ... Daher ist für den Bereich der 0 190-Rufnummern eine Einschränkung der Auskünfte nicht erkennbar. ... Der Hinweis auf Datenschutzgründe zur Verweigerung derartiger Ausünfte ist ... nach den obigen Erläuterungen nicht zulässig und von unserem Haus auch nicht vorgesehen."

Ich habe die Zentrale der Deutschen Telekom AG aufgefordert, die zuständigen Stellen entsprechend zu informieren. Wichtig ist allerdings auch, daß nicht nur über „die Mehrzahl", sondern über alle Audiotex-Anbieter unter der o. g. Rufnummer Auskunft erteilt wird.

10.4.13 Der kleine Unterschied oder: Immer wieder Ärger mit dem Fax

Wer einen Brief verschickt, kann in der Regel darauf vertrauen, daß dieser seinen Empfänger erreicht oder zumindest nicht in falsche Hände gerät. Auch wenn der Empfänger verzogen sein sollte, sorgt die Post dafür, daß der Brief entweder nachgesandt oder als unzustellbar an den Absender zurückgegeben wird. Bei einem Telefonat kennen sich die Gesprächspartner oder stellen sich vor. Verwählt sich ein Anrufer, entschuldigt er sich in der Regel und beginnt das Gespräch gar nicht erst, gibt also keine Inhalte preis.

Oberflächlich betrachtet, geht dies beim Faxverkehr – d. h. bei der Übermittlung und dem Empfang von Fernkopien – nicht viel anders: Das Fax wird an eine bestimmte Adresse gesandt, indem eine Telefonnummer eingegeben wird, von der ausgegangen wird, daß unter ihr das Faxgerät des Empfängers erreicht werden kann. Bevor die Übertragung der eigentlichen Nachricht beginnt, tauschen die beteiligten Geräte untereinander Informationen zur gegenseitigen Identifizierung aus, anhand derer im Zweifelsfall vom Absender die Übertragung abgebrochen werden kann.

Es gibt jedoch wesentliche Unterschiede zwischen Faxverkehr und Briefpost bzw. Telefonat: Ein Fax kommt beim Empfänger gewöhnlich offen – d. h., wie eine Postkarte – an und ist damit für jeden lesbar, der sich in der Nähe des empfangenden Faxgerätes befindet. Nicht sicher ist auch der Identifizierungsvorgang zwischen den heute überwiegend eingesetzten Faxgeräten der Gruppe 3: Sie identifizieren sich mit der Rufnummer, die ihnen von ihrem Besitzer einprogrammiert wurde und die deshalb veraltet oder manipuliert sein kann. Erst ISDN-Faxgeräte der Gruppe 4 übermitteln einander die „echten" Rufnummern.

Bereits 1991 habe ich in einem Rundschreiben an die obersten Bundesbehörden ausführliche Hinweise für die sichere Nutzung von Telefaxgeräten gegeben und das Muster eines entsprechenden Merkblattes versandt (s. 13. TB Anlage 13). Gleichwohl kommt es im Faxverkehr immer wieder zu Problemen. Hier nur einige davon:

- **Rufnummernänderung**

Zieht z. B. der Steuerberater in neue Büroräume, bleiben Telefon- und Telefaxnummer unter Umständen in den alten Räumen. Die alten Rufnummern waren im Laufe der Zeit „breit" gestreut worden, eine schnelle Information aller Partner über die neuen Nummern ist kaum möglich. In der Folge erreichen den neuen Mieter noch lange Zeit Faxsendungen, die für den Steuerberater bestimmt sind.

Zwar hat sich die Praxis der Telekom bei der Neuvergabe von Rufnummern zum Positiven geändert: Mußte man Anfang der 90er Jahre noch davon ausgehen, daß gekündigte Rufnummern sofort neu vergeben wurden, so hat mir die Deutsche Telekom AG 1996 mitgeteilt, daß gekündigte Telefonanschlüsse – an denen eben (auch) Faxgeräte angeschlossen sein können – in bestimmten Fällen nicht sofort neu vergeben werden. Dies betrifft Rufnummern, die für besonders sensible Bereichen überlassen worden waren (z. B. Politiker, Behörden, Krankenhäuser, Ärzte). Sie werden, sofern nicht wichtige betriebliche Gründe – wie z. B. Rufnummernmangel – dagegenstehen, erst nach 12 Monaten neu vergeben.

Kündigt ein Kunde seinen Telefonanschluß und wünscht, daß der Übernehmende – z. B. wegen einer Konkurrenzsituation – nicht die gleiche Rufnummer erhalten soll, so wird diesem Anliegen nach Möglichkeit stattgegeben. Der Nachfolger erhält dann eine neue Rufnummer.

Trotzdem erreichen mich immer wieder Hinweise auf Faxsendungen, die wegen eines Rufnummernwechsels des gewünschten Empfängers in falsche Hände gerieten. Allerdings ist vorrangig der Absender dafür verantwortlich, daß seine Faxsendung den richtigen Empfänger erreicht. Deshalb empfehle ich in diesem Zusammenhang, regelmäßig und in kürzeren Zeitabständen die Rufnummern der Faxpartner auf Richtigkeit zu überprüfen. Dabei ist zu beachten, daß öffentliche Telefax-Verzeichnisse allenfalls halbjährlich neu erscheinen und die jährliche Veränderungsquote bei Telefon-/Telefaxanschlüssen bundesweit bei 30% liegt.

- **Falschwahl**

Will man ein Telefongespräch führen und macht einen Fehler beim Wählen der Telefonnummer, so hat das im allgemeinen keine weiteren negativen Folgen. Will man hingegen ein Fax absenden und verwählt sich dabei, können weitreichende Folgen eintreten, wenn unter der falsch gewählten Rufnummer – auch – ein Faxgerät erreicht wird. Die Sendung gelangt dann an einen unerwünschten Empfänger, der möglicherweise personenbezogene oder andere besonders schützenswerte Daten zur Kenntnis nehmen kann.

So beachteten die Mitarbeiter einer Behörde im süddeutschen Raum offensichtlich nicht, daß das von ihnen benutzte Faxgerät an einer Telekommunikationsanlage betrieben wird. Um eine Verbindung ins öffentliche Netz herstellen zu können, muß vor der gewünschten Rufnummer die Ziffer „0" (Amtsholung) gewählt werden. Wenn nicht, so wird – sofern eine Rufnummer außerhalb des Ortsnetzes gewählt wurde – die führende „0" dieser Rufnummer von der TK-Anlage als Amtsholung gewertet und die anschließende Ziffernfolge als die eigentliche Rufnummer gewählt. Demzufolge gingen eine Reihe von Faxsendungen nicht bei der adressierten Behörde, sondern in einem häufig von Journalisten aufgesuchten Café ein, in dem das Fax-Gerät zudem noch von den Gästen benutzt wurde und somit öffentlich zugänglich war.

- **Einsatz von Fax-Servern**

Fax-Server als Bestandteil von PC-Netzen ermöglichen es jedem dazu berechtigten Nutzer, vom eigenen Arbeitsplatz aus z. B. Briefe per Fax zu verschicken.

Das Versenden von Fax-Dokumenten auf diese Art und Weise erspart in jedem Fall eigene Arbeitszeit und oft auch Versandkosten, ist aber auch mit allen Risiken des „konventionellen" Faxversandes behaftet. So gestattet die Fax-Software üblicherweise das Anlegen sog. Fax-Bücher, in denen häufig genutzte Fax-Rufnummern – oft nach Adressatengruppen geordnet – verzeichnet sind und per Maus-Klick (als Sendeziel) ausgewählt werden können. Wenn jedoch nicht durch strikte Organisation die Aktualität der Fax-Bücher gesichert wird, sind Fehlsendungen vorprogrammiert.

Faxgeräte haben im allgemeinen ein Display, auf dem auch die vom angewählten Faxgerät zurückgesendete Anschlußkennung angezeigt wird und überprüft werden kann. Beim Einsatz von Fax-Servern oder PC mit Fax-Karte und entsprechender Software ist diese Möglichkeit meist nicht gegeben. Weil dann eine Falschwahl auch nicht mehr anhand der zurückgesandten Anschlußkennung des erreichten Fax-Partners erkannt werden kann, ist hier bei der Eingabe der Rufnummern besondere Sorgfalt geboten. Das Protokoll über den Versand sollte sehr genau kontrolliert werden.

Faxgeräte bieten die Möglichkeit, einen bereits begonnenen Sendevorgang – durch Drücken der dafür vorgesehenen Taste – abzubrechen, wenn beispielsweise eine Falschwahl festgestellt wurde. Die auf Fax-Servern oder Fax-PC installierte Software bietet zwar die Möglichkeit, einen Sendevorgang erst dann zu starten, wenn der Bediener ein letztes „OK" gegeben hat. Hat er es aber einmal gegeben, ist er – besonders bei Fax-Servern, auf die er im allgemeinen keinen direkten Zugriff hat – nicht mehr in der Lage, den Sendevorgang noch abzubrechen. Besonders beim Fax-Versand an Adressatengruppen kann das fatale Folgen haben, wenn dem Absender nach Auslösung des Sendevorganges bewußt wird, daß das Fax eigentlich an eine andere als die angewählte Gruppe abgesandt werden sollte.

- **Übertragung von Programmen**

Mit üblichen Faxgeräten können lediglich optisch lesbare Vorlagen übertragen werden. Mittels Fax-Server oder eines PC mit geeigneter Fax-Karte und der entsprechenden Software können demgegenüber alle Arten von Dateien übertragen werden, also auch „ausführbare Dateien", nämlich Programme. Vorteile für den Absender sind die schnellere Bearbeitung durch die Fax-Software und eine kürzere Sendezeit und damit Kostenersparnis.

Damit wurde auch im Faxbereich eine Gefährdungsmöglichkeit eröffnet, die bislang lediglich bei klassischen Formen der Datenübertragung zwischen Rechnern – mittels Leitungsverbindungen über das öffentliche Netz oder per Diskette – bestand: Das Eindringen von schädlichen Programmen (Viren, Trojanischen Pferden usw.) z. B. in das PC-Netz des Empfängers. Dabei kann beispielsweise ein Virus auch übersandt werden, ohne daß der Absender sich dessen bewußt ist oder es gar will. Bekannt sind z. B. sogenannte Winword-Viren, die als „unsichtbare Anlage" an zu übertragenden Dokumenten hängen, und im IT-System des Absenders unbemerkt – weil wirkungslos – sind, im IT-System des Empfängers jedoch Schaden anrichten.

Hier sind sorgfältig geplante, wirksame Abwehrmaßnahmen unerläßlich. Das Bundesamt für Sicherheit in der Informationstechnik – BSI – verfügt über eine Expertengruppe, die zum Schutz gegen Viren und andere schädliche Programme Beratungen durchführt und Hilfe erteilt.

Die technische Entwicklung wird auch den Faxdienst voranbringen, bis er durch E-Mail und andere Nachrichtenübermittlungsstandards verdrängt sein wird. Bis dahin wird aber noch einige Zeit vergehen und man wird bis dahin mit diesen neuen Risiken leben müssen. Meine Hinweise aus dem Jahre 1991 haben nach wie vor ihre Gültigkeit. Im Zuge der technischen Weiterentwicklung und der immer breiteren Anwendung des Faxverkehrs werden sie fortlaufend um – manchmal trivial anmutende – Details ergänzt.

Aber der Teufel steckt bekanntlich im Detail. Daher empfehle ich, den Faxverkehr auf jeden Fall in einer Dienstanweisung zu regeln, alle technischen Sicherheitsoptionen von Faxgeräten und rechnergestützten Faxanwendungen konsequent zu nutzen sowie vor jeder Übermittlung personenbezogener oder anderer besonders schützenswerter Daten per Telefax äußerst kritisch zu prüfen, ob sie auf diesem Wege notwendig und vertretbar ist.

10.4.14 Auskünfte über Telefonkunden an die Polizei und andere Sicherheitsorgane

Für die Arbeit der Polizei und anderer Sicherheitsorgane ist es oftmals wichtig zu wissen, wer der Anschlußinhaber einer bestimmten Telefonnummer ist oder welche Telefonnummer eine bestimmte Person hat – auch wenn der Anschluß nicht im Telefonbuch eingetragen ist. Nach §§ 89 Abs. 6 und 90 TKG haben die Telekommunikationsunternehmen derartigen Auskunftsersuchen zu entsprechen (s. o. Nr. 10.1.5). Über das Verfahren, nach welchem die Deutsche Telekom AG gegenwärtig diese Auskunftsersuchen entgegennimmt, bearbeitet und beantwortet, habe ich mich bei einem der insgesamt zehn „Vertriebsteams für Behörden mit Sicherheitsaufgaben (VT-BS)" informiert.

Diese Auskunftsersuchen nach dem TKG sind Anfragen der o. g. Stellen – nachstehend als Bedarfsträger bezeichnet – nach Daten aus dem Kundenauftrag bzw. aus Betriebsunterlagen der Deutschen Telekom AG. Im Regelfall nennt der Bedarfsträger die Ortsnetzkennzahl (Vorwahlnummer) und die Rufnummer, zu der dann die Telekom die gewünschten Daten ermittelt und dem Bedarfsträger mitteilt. Entscheidend für die Bearbeitung der Auskunftsersuchen ist die vom Bedarfsträger angegebene Rechtsgrundlage, auf die sich sein Auskunftsersuchen stützt.

Für jeden Bedarfsträger, der Anfragen an das für ihn zuständige VT-BS richtet, wird ein Blatt „Bedarfsträgerdaten" angelegt. Es dient zur Prüfung der Anfrageberechtigung, zur Auskunftserteilung und zur Abrechnung der Kosten. Es enthält neben den Anschriften für schriftliche Auskunftserteilungen per Post und Telefax, Rückrufnummern für telefonische Auskunftserteilung und der Rechnungsanschrift der Bedarfsträger auch die Ansprechpartner (Name, Telefon) für Stichwortvereinbarungen und sonstige Angelegenheiten sowie die Rechtsgrundlage für das Ersuchen.

Die Stichworte dienen der Identifizierung der Anfragenden. Bei einer Anfrage mit Stichwort gehen die Mitarbeiter des VT-BS davon aus, daß sich die Anfrage auf eine hinreichend geprüfte Rechtsgrundlage stützt. Aus Sicherheitsgründen habe ich empfohlen,

die Stichworte in bestimmten Zeitabständen zu ändern. Bei Anfragen ohne Nennung eines Stichworts prüft das VT-BS, ob die anfragende Stelle anfrageberechtigt und die von ihr angeführte Rechtsgrundlage plausibel ist. Diese Prüfung erfolgt auch mittels fernmündlicher Rückfragen bei der anfragenden Stelle; die Rechtsgrundlage kann – z. B. per Fax – nachgereicht werden. Ich habe empfohlen, Auskünfte in jedem Fall erst dann zu geben, wenn die Berechtigung des Anfragenden und die Rechtsgrundlage zweifelsfrei feststehen und beim VT-BS schriftlich dokumentiert vorliegen.

Anfragen können schriftlich und fernmündlich an ein VT-BS gerichtet werden. Im Regelfall gehen schriftliche Anfragen per Fax beim VT-BS ein. Die Übermittlung solcher Daten per Fax ist schon allein durch die Möglichkeit einer Falschwahl durch den Absender riskant (s. o. Nr. 10.4.13). Wenn auch die Verantwortung für die Übermittlung in diesem Fall nicht beim VT-BS liegt, habe ich die Telekom gebeten, die Bedarfsträger auf die mit dem Faxversand verbundenen Risiken mit der gebotenen Deutlichkeit aufmerksam zu machen.

Fernmündliche Anfragen in äußerst dringenden Fällen (z. B. zur Auslösung von Polizei- oder Feuerwehreinsätzen) werden nur dann direkt beantwortet, wenn die Stimme des Anrufers dem Mitarbeiter des VT-BS bekannt ist. Ansonsten wird ein Rückruf an den Anfragenden gerichtet. Gibt der Anfragende eine beim VT-BS unbekannte Rückrufnummer an, wird – bevor eine Auskunft erteilt wird – die Zuordnung dieser Nummer geprüft.

Die Identifizierung eines Anrufers anhand seiner Stimme ist wegen der vielfältigen Manipulationsmöglichkeiten problematisch. Um Mißbrauch weitestgehend einzuschränken, habe ich der Telekom nahegelegt, den Bedarfsträgern zu empfehlen, das notwendige Stichwort auch der mit der Koordinierung von Noteinsätzen zuständigen Stelle, in der Regel der Leitzentrale, mitzuteilen.

Im übrigen werden Anfragen von Personen, die einem Bedarfsträger nicht ohne weiteres zugeordnet werden können – auch aus Abrechnungsgründen – an die Stellen verwiesen, die die Telekom aufgrund der ihr zur Verfügung stehenden Daten der Bedarfsträger kennt. Diese Verfahrensweise wirkt Versuchen entgegen, sich unberechtigt Informationen zu verschaffen. Insofern habe ich empfohlen, Auskünfte möglichst immer – von den besonderen Ausnahmesituationen abgesehen – nur dem aus diesen Bedarfsträgerdaten ersichtlichen Personenkreis zu erteilen.

Für die Beantwortung von Anfragen hat das kontrollierte VT-BS seit Januar 1996 – über eine Terminalanwendung – Zugriff auf die Datenbanksysteme KONTES-ANDI (Anmeldedienst) und KONTES-BUDI (Buchdienst).

Ich habe festgestellt, daß bei der Inanspruchnahme dieser Systeme nachträglich nicht überprüft werden kann, durch wen, von welchem Terminal und zu welchem Zeitpunkt auf Daten dieser Systeme zugegriffen wurde. Der Kreis der Zugriffsberechtigten umfaßt schwerpunktmäßig alle bundesweit tätigen Mitarbeiter in den Bereichen Anmelde- und Buchdienst und ist sehr groß. Damit wäre eine nachträgliche Datenschutzkontrolle – etwa infolge einer Kundenbeschwerde – nicht vollständig möglich. Ich habe deshalb die zuständigen Stellen der Telekom gebeten, eine auswertbare Zugriffsprotokollierung einzuführen.

Die Umsetzung der §§ 89 Abs. 6 und 90 TKG, insbesondere aber die in § 90 vorgesehenen Online-Zugriffe werden in den nächsten Jahren auch mit Blick auf die Liberalisierung des Telekommunikationsmarktes ein Schwerpunkt der Arbeit meines Hauses sein. Ein Ziel dabei ist, zusammen mit dem BMPT allgemeine Empfehlungen zu diesen Vorschriften zu entwickeln, die gerade für neue oder kleine TK-Anbieter hilfreich sein können.

10.4.15 Moderne Telefonanlagen – Mehr Komfort und mehr Probleme –

Unverzichtbar für effektive Arbeitsabläufe und gute Arbeitsergebnisse sind sowohl in der Wirtschaft als auch in der öffentlichen Verwaltung moderne, leistungsfähige Telefonanlagen. Mit ihnen wird nicht nur telefoniert, es werden auch „elektronische Briefe" übersandt und Telefaxsendungen übermittelt; sie werden heute daher meist Telekommunikationsanlagen (TK-Anlagen) genannt. Die große Vielfalt von Leistungsmerkmalen ermöglicht eine hochkomfortable Kommunikation und bietet manche Arbeitserleichterung, birgt aber auch datenschutzrechtliche Risiken in sich, auf die ich schon früher hingewiesen habe (14. TB Nr. 21.11, 15. TB Nr. 20.2.10).

In der letzten Zeit wurde ich durch Eingaben auf zwei Leistungsmerkmale aufmerksam gemacht, die durchaus nicht von allen Telefonierenden uneingeschränkt begrüßt werden:

- **Anrufliste**

  Neuere TK-Anlagen besitzen – zum Teil nur für bestimmte Endgeräte – das Leistungsmerkmal „Anrufliste": Von bei einem bestimmten Teilnehmer angekommenen, nicht entgegengenommen Anrufen werden Datum, Uhrzeit und Rufnummer des Anrufers zur Nutzung durch den Angerufenen automatisch in einer „Anrufliste" gespeichert. Dabei wird die Rufnummer des Anrufers nur dann gespeichert, wenn dieser von einem ISDN-Anschluß oder aber von einem analogen Anschluß des sog. „T-Net" – der Anrufer also an eine digitale Vermittlungsstelle angeschlossen ist – angerufen hat. In letzterem Fall muß er von der Telekom die Anzeige seiner Rufnummer beim Angerufenen verlangt haben.

  Die „Anrufliste" wird von vielen gern genutzt, denn nach ihrem Aufruf ist der Rückruf zu einem der Anrufer mit lediglich einem Knopfdruck – zumeist der Wahlwiederholungstaste – möglich.

  Anrufer, die dies alles nicht wissen, sind allerdings häufig über einen solchen Rückruf („Sie stehen in meiner Anrufliste!") sehr verwundert oder auch verärgert. Dies vor allem dann, wenn sie dem Angerufenen die eigene Rufnummer gerade nicht mitteilen wollten.

Der Eintrag eines Anrufes in die Anrufliste erfolgt nur, wenn der Anrufer das Leistungsmerkmal „Rufnummernübermittlung" besitzt. Dieses kann für eine TK-Anlage an dieser selbst unterdrückt werden, für ISDN-Einzelanschlüsse durch die Telekom. Soll darauf jedoch nicht verzichtet werden, empfehle ich den Betreibern von TK-Anlagen dringend, alle Nutzer der Anlage sowohl über die Rufnummernübermittlung als auch über die Anrufliste zu informieren und diese Information in angemessenen Zeitabständen zu wiederholen.

- **Anzeige der zuletzt gewählten Rufnummer**

  Sowohl für Endgeräte von TK-Anlagen als auch bei modernen Telefonen an Einzelanschlüssen wird die zuletzt gewählte Rufnummer zumeist gespeichert, damit sie – z. B. weil der Anrufer nicht erreicht werden konnte – für die Funktion „Wahlwiederholung" genutzt werden kann.

  Bei manchen TK-Anlagen wird durch die Vorwahl einer sog. PIN (Personal Identification Number) ein danach gewähltes Gespräch als Privatgespräch gekennzeichnet.

  Einige Endgeräte, aber auch manche TK-Anlagen, speichern jedoch nicht nur die zuletzt eingegebene Telefonnummer einer gewünschten Verbindung, sondern alle eingegebenen Ziffern – auch die PIN und die Nummer zum Aufschließen des „elektronischen Telefonschlosses". Dadurch können PIN und „Schloßnummer" durch Betätigung der Wahlwiederholungstaste abgerufen und – sofern sich ein Display am Telefonapparat befindet – auch ausgespäht und unbefugt genutzt werden.

Im Dezember 1996 habe ich die obersten Bundesbehörden als Betreiber zum Teil sehr großer TK-Anlagen in einem Rundschreiben auf diese Probleme hingewiesen und ihnen empfohlen, die bei ihnen eingesetzte Technik sowie die Möglichkeit zu prüfen, die genannten Schwachstellen zu beheben. Ich habe darin auch betont, daß ich einen Hinweis an alle Nutzer der TK-Anlage sowie in der Vereinbarung mit dem Personal- bzw. Betriebsrat für unerläßlich halte **(s. Anlage 24)**.

10.5 Datenschutzkontrolle bei einer Telekom-Niederlassung

Im Herbst 1995 habe ich eine Niederlassung der Deutschen Telekom AG hinsichtlich der technischen und organisatorischen Maßnahmen zur Datensicherheit (§ 9 BDSG) beim Einsatz von Personalcomputern, UNIX-Systemen und ausgewählten Anwendungen beraten und kontrolliert.

Die Zuständigkeiten der 118 Telekom-Niederlassungen (ehemals Fernmeldeämter der Deutschen Bundespost) wurden 1995 neu geordnet, indem jede Niederlassung einen bestimmten Aktivitätsschwerpunkt erhielt, wodurch sowohl eine Aufgabentrennung als auch eine Aufgabenkonzentration erreicht werden sollte. Die Schwerpunkte dieser Aktivitäten liegen in den Bereichen Privatkunden, Geschäftskunden und Netze.

Der Schwerpunkt der von mir besuchten Niederlassung lag in der Betreuung von Privatkunden. Dadurch hatte sich die flächen- und zahlenmäßige Zuständigkeit der Niederlassung vergrößert. Äußerlich wurde das durch umfangreiche Umbaumaßnahmen deutlich, die den Geschäftsbetrieb – z. B. mit Auswirkungen auf die Zugangskontrolle – nicht unwesentlich beeinflußten. In der Niederlassung sind etwa 1 200 Mitarbeiter beschäftigt; sie betreut ca. 360 000 Telefon-Hauptanschlüsse von überwiegend Privatkunden. Die Niederlassung ist auf mehrere Standorte verteilt. In ihrem Bereich werden etwa 700 PC und Laptops, mehrere UNIX-Mehrplatzsysteme und Terminals mit Hostanbindung betrieben. Die PC waren entweder als Einzelplatzsysteme eingesetzt oder über das Inhouse-Netz „ILAN" miteinander verbunden, einige hatten – über Emulationsprogramme – Zugriff auf die UNIX-Systeme sowie auf Hosts der Telekom außerhalb der Niederlassung.

Eine Sonderstellung nimmt das DV-gestützte Arbeitssystem für Personal- und Organisationsstellen der Ämter der DBP – Bereich Telekom (DASPO-T) ein. Für dessen Betrieb ist im ILAN ein Unternetz gebildet worden.

U. a. habe ich folgendes festgestellt:

- Zum Einsatz von PC und Laptops

  Wegen der Vielzahl der eingesetzten Geräte konnte nur eine stichprobenartige Kontrolle durchgeführt werden.

  Auffällig war die nicht einheitliche Nutzung vorhandener Möglichkeiten zur elementaren Sicherung der Rechner und der darauf gespeicherten Daten:

  - In einigen Fällen war das BIOS-Paßwort aktiviert, in anderen nicht;
  - Bildschirmschoner wurden sowohl mit als auch ohne Paßwortschutz eingesetzt.

  Obwohl auf den kontrollierten Laptops keine personenbezogenen Daten gespeichert waren, birgt die in einigen Fällen angetroffene, ungesicherte Aufbewahrung ein hohes Risiko, da jederzeit die Möglichkeit besteht, personenbezogene Daten zu verarbeiten, was im übrigen auch nicht untersagt war.

- Zur Benutzerverwaltung bei DASPO-T

  Entsprechend einer Festlegung der Generaldirektion der Deutschen Telekom AG durfte die Benutzerkennung „root" (mit höchsten Rechten) nur von Mitarbeitern des Personalressorts (PE) benutzt werden. Das Ressort Informationsverarbeitungsservice (IVS) durfte nur mit der Kennung „sysadmin" mit gleichen Rechten wie „root", allerdings menügeführt, administrieren.

  Diese Anforderungen waren in der Niederlassung nicht bekannt und daher nicht umgesetzt. Die Benutzerkennung „sysadmin" war jedoch mit einem Paßwort versehen und einsatzbereit. Dem Systemadministrator war nicht bekannt, welchem Personenkreis dieses Paßwort bekannt war.

- Zur Kontrolle ausgewählter Verfahren

  TIBIS (Telekom integrierendes Büroinformationssystem)

  TIBIS ist ein speziell für die Telekom entwickeltes Büroinformationssystem für den bundesweiten Einsatz, das ebenfalls auf dem Inhouse-Netz ILAN betrieben wird. In der Niederlassung wurde es als Version 1.1 auf 10 TIBIS-Rechnern eingesetzt. Für 1995 war geplant, alle Ressorts mit mindestens einem Rechner auszustatten. Die für TIBIS einzusetzenden Rechner verfügen u. a. über Disketten- und Plattenlaufwerke, wobei das „Booten" von den Diskettenlaufwerken nicht möglich ist. Regelungen zur Rechte- und Attributsverwaltung sowie zur technisch-organisatorischen Sicherung, die gemäß der TIBIS-Dienstvereinbarung bis spätestens Februar 1995 erlassen sein sollten, lagen in der Niederlassung nicht vor. Maßnahmen gegen Winword-Viren waren nicht getroffen. Sie sind in einem solchen System jedoch dringend erforderlich.

  Da Diskettenlaufwerke hinsichtlich der Datensicherheit immer eine Schwachstelle darstellen, habe ich hinsichtlich des Endausbaus des Systems – bei flächendeckender Ausstattung der Normalbenutzer – den Ausbau oder die Sperrung der Laufwerke empfohlen.

  Der Windows-Dateimanager bietet die Möglichkeit, auf die Betriebssystemebene zu gelangen und damit Funktionen in Anspruch zu nehmen, die normalerweise nicht zur Verfügung stehen. Deshalb habe ich auf die Notwendigkeit einer äußerst restriktiven Vergabe der Berechtigung zur Benutzung des Dateimanagers hingewiesen.

- Zum Zeiterfassungssystem „Zeus"

  In der Niederlassung wird nach einem Gleitzeitverfahren gearbeitet. Zur Eingabe der Kommen- und Gehen-Zeiten („Ereignisse") werden personengebundene Karten benutzt, die sowohl eine infrarot-lesbare Markierung als auch eine Magnetstreifenmarkierung enthalten. Die Magnetstreifenmarkierung wird auch zur Kantinenabrechnung benutzt. Sie ist nicht personenbezogen (Geldbörsenfunktion).

  Für jeden der am Gleitzeitverfahren teilnehmenden Mitarbeiter wird auf dem Zentralrechner ein Stammdatensatz angelegt; zum Zeitpunkt der Kontrolle bestanden ca. 800 Sätze. Ich habe empfohlen, die Einflußmöglichkeit des einzelnen Mitarbeiters auf die Gestaltung seines Stammsatzes zu verstärken.

  Der Zeitpunkt der Ereignisse wird pro Tag in das ebenfalls auf dem Zentralrechner geführte „Monatsjournal" des jeweiligen Mitarbeiters eingetragen. An Korrekturplätzen kann eine Aktualisierung oder Korrektur der Sollzeiten unter Angabe der Gründe (Krankheit, Dienstreise usw.) vorgenommen werden. Grundlage dafür sind – vom jeweiligen Vorgesetzten unterschriebene – Korrekturbelege.

  An den Korrekturplätzen muß sich der von UNIX bereits identifizierte Benutzer gegenüber dem System Zeus erneut identifizieren. Dabei werden ihm Benutzerrechte für die Korrekturplatzfunktionalitäten zugewiesen. Da die Zahl der Fehlversuche dabei unbegrenzt ist, könnte er sich durch Ausprobieren innerhalb der Zeus-Hierarchie höhere Rechte erschleichen. Ich habe empfohlen, die Zahl der Fehlversuche auf drei zu begrenzen.

  Die Datensicherung von Zeus erfolgt zur Zeit durch wechselweise Speicherung der Daten in zwei verschiedene Partitionen einer zweiten Festplatte des Zentralrechners. Bei Totalausfall beider Platten wären die Daten verloren. Ich habe daher angeregt, ein Datensicherungskonzept unter Einbeziehung des Mediums Streamer-Band zu entwickeln, zumal ein entsprechendes Laufwerk am Zentralrechner vorhanden ist.

  Das Programm legt die Paßwörter der Korrekturplatzbenutzer unverschlüsselt im System ab. Eine Abänderung dieser Situation durch den Administrator ist nicht möglich. Der Administrator könnte sie daher auslesen und in der Rolle der Korrekturplatzbenutzer tätig werden. Dieses Verfahren birgt hohe Risiken und entspricht nicht dem Stand der Technik. Daher habe ich dringend empfohlen, das Programm entsprechend ändern zu lassen.

  Das Verfahren zur Einrichtung von neuen Benutzern der Korrekturplätze ist ungeregelt, die Einrichtung erfolgte „auf Zuruf". Ich halte es für geboten, ein schriftlich geregeltes Verfahren einzurichten.

Die Zentrale der Deutschen Telekom AG hat meine Empfehlungen angenommen und begonnen, sie umzusetzen, so daß ich von einer Beanstandung abgesehen habe.

Seit Anfang 1996 hat die Telekom bezirkliche Datenschutzberater eingesetzt, die unabhängig von den Funktionsträgern der Niederlassungen arbeiten und nur den fachlichen Weisungen der Zentrale unterstehen. Sie sollen u. a. durch effektivere Kontrollen die Einhaltung datenschutzrechtlicher Vorschriften gewährleisten.

Ich begrüße diesen Ansatz und hoffe auf einen Qualitätssprung bei der Bewältigung besonders der datenschutzrechtlichen Telekom-Probleme, die die Bürger tagtäglich an mich herantragen.

11 Bundeskriminalamt

11.1 Bundeskriminalamtgesetz und Errichtungsanordnungen

Auch 13 Jahre nach dem Volkszählungsurteil des Bundesverfassungsgerichts (BVerfGE 65, 1 ff.) erfolgt die Verarbeitung personenbezogener Daten beim Bundeskriminalamt noch ohne ausreichende gesetzliche Grundlage, denn die rudimentären Regelungen des Bundeskriminalamtgesetzes in der Fassung aus dem Jahre 1973 entsprechen bei weitem nicht den Vorgaben des Bundesverfassungsgerichts zur Sicherung des informationellen Selbstbestimmungsrechts. Aus diesem Grund hat der Hessische VGH in mehre-

ren Entscheidungen aus dem Jahre 1995, die allerdings noch nicht rechtskräftig sind, die Verarbeitung personenbezogener Daten beim Bundeskriminalamt für rechtswidrig erklärt, weil der Übergangsbonus für eine gesetzliche Neuregelung abgelaufen sei.

Im Februar 1995 hat das Bundeskabinett den Entwurf eines Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten – BKAG – beschlossen, der nach der Beteiligung des Bundesrates und weiterer Absprachen innerhalb der Koalitionsfraktionen noch erhebliche Veränderungen erfahren hat. Die parlamentarischen Beratungen im Deutschen Bundestag waren bei Redaktionsschluß dieses Berichtes noch nicht abgeschlossen.

Mit dem Gesetzentwurf werden insbesondere Aufgaben und Befugnisse des BKA

- als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen einschließlich Regelungen zu INPOL,
- bei der internationalen Zusammenarbeit,
- bei der Strafverfolgung sowie
- beim Schutz von Mitgliedern der Verfassungsorgane

geregelt.

Während der Vorbereitung und Beratung des Gesetzentwurfs habe ich mehrfach schriftlich und mündlich Stellung bezogen. Nach seinem derzeitigen Stand scheint mir der Entwurf ein angemessener Kompromiß zwischen dem Informationsbedürfnis der Polizeibehörden und dem informationellen Selbstbestimmungsrecht der Betroffenen zu sein. Mein besonderes Augenmerk galt den schutzwürdigen Interessen derjenigen Personen, die nicht als Tatverdächtige oder Beschuldigte ins Visier der Polizei geraten, deren Daten aus polizeilicher Sicht aber gespeichert werden müssen, weil sie für unverzichtbar gehalten werden. Zu dem betroffenen Personenkreis zählen potentielle Zeugen und Opfer, Kontakt- und Begleitpersonen von Tatverdächtigen oder Beschuldigten sowie Hinweisgeber und sonstige Auskunftspersonen. Für die Speicherung von Daten potentieller Straftäter ist statt des konturlosen Begriffs „Straftaten von erheblicher Bedeutung" nunmehr ein Straftatenkatalog mit Regelbeispielen als Voraussetzung vorgesehen.

Der Entwurf sieht ferner den Einsatz technischer Mittel (z. B. Tonaufzeichnungsgeräte) in Wohnungen zur Eigensicherung von Beamten vor, wenn diese im Rahmen der Befugnisse des BKA bei der Strafverfolgung tätig werden. Zwar halten sich diese Maßnahmen noch im Rahmen des Artikels 13 Abs. 3 GG. Um jedoch möglichen Mißbräuchen vorzubeugen, habe ich verschiedene verfahrenssichernde Schritte bei dieser Art der heimlichen Datenerhebung vorgeschlagen. So sollte die Anordnung der Maßnahme in jedem Einzelfall von der Leitung des BKA gebilligt werden. Schließlich sollte die Verwendung von Erkenntnissen, die bei solchen Einsätzen anfallen, als Ermittlungsansatz für andere Straftaten ausgeschlossen sein. Damit sollte jedem Anschein einer akustischen Wohnraumüberwachung durch die Hintertür – also ohne Grundgesetzänderung – vorgebeugt werden. Leider ist der Gesetzgeber der letztgenannten Anregung in den bisherigen Beratungen nicht gefolgt.

Das Bundeskriminalamt hat im Sinne von § 18 Abs. 2 Satz 2 BDSG für jede neueingerichtete automatisierte Datei eine Dateianordnung aufzustellen, die vor der Inbetriebnahme vom BMI zu genehmigen ist. Vor Genehmigung soll ich vom BMI um Stellungnahme gebeten werden. Dieses Verfahren soll im neuen BKAG gesetzlich geregelt werden. Dies wird auch für temporäre Dateien, wie z. B. einer SPUDOK, gelten. Im Rahmen laufender Beteiligungsverfahren habe ich festgestellt, daß das Ministerium seiner Rolle als Genehmigungsbehörde häufig in nicht zureichendem Maße nachkommt, indem die vorgesehene Beteiligung meiner Dienststelle unterbleibt oder nicht rechtzeitig eingeleitet wird.

Der Gesetzentwurf sollte wegen der dringend notwendigen Rechtsgrundlage für die Arbeit des BKA möglichst bald vom Gesetzgeber verabschiedet werden, zumal auch das in Vorbereitung befindliche Vertragsgesetz zu EUROPOL (vgl. Nr. 11.5.1) in erheblichem Umfang auf die Regelungen des BKAG Bezug nehmen wird.

11.2 Rechtstatsachensammelstelle beim BKA

Bereits im 15. Tätigkeitsbericht (Nr. 4.1.1) habe ich mich für eine effektive Erfolgskontrolle polizeilicher Befugnisse eingesetzt. Das vorhandene Wissen über Anwendung und Auswirkungen besonders einschneidender strafprozessualer Ermittlungsbefugnisse, wie z. B. der Telefonüberwachung, ist eher lückenhaft und unzureichend. Wenn der Gesetzgeber seinen verfassungsrechtlichen Auftrag zur strafrechtlichen Gewährleistung der Grundrechte auf körperliche Unversehrtheit, Freiheit und Eigentum wahrnimmt und zu diesem Zweck eine effektive Strafverfolgung mit häufig einschneidenden, neuen Befugnissen schafft, will er hierbei sowohl ein Unter- als auch ein Übermaß vermeiden. *„Die Vorkehrungen, die der Gesetzgeber trifft, müssen für einen angemessenen und wirksamen Schutz ausreichend sein und zudem auf sorgfältigen Tatsachenermittlungen und vertretbaren Einschätzungen beruhen"* heißt es im Urteil des Bundesverfassungsgerichts vom 28. Mai 1993 zur staatlichen Schutzpflicht gegenüber dem ungeborenen Leben (BVerfGE 88, S. 203ff. (254). Diese Forderung gilt auch für die Prüfung neuer staatlicher Eingriffsbefugnisse. Bei der gesetzlichen Definition der erforderlichen, geeigneten und angemessenen Eingriffsbefugnisse, bedarf es – ex ante – einer gründlichen Bestandsaufnahme und Evaluierung des strafprozessualen und polizeirechtlichen Instrumentariums, um – sowohl mit Blick auf die gebotene Effizienz als auch mit Blick auf die Einschränkung von Grundrechten Verdächtiger und erst recht Unbeteiligter – das rechte Maß zu finden. Deshalb müssen neue Eingriffsbefugnisse – ex post – nach ihrer Einführung und Anwendung hinsichtlich ihrer Wirkungen bewertet werden können, um spätestens in dieser Phase sowohl Unter- als auch Überreaktionen auszuschließen.

1994 zeichnete sich die Einrichtung einer sog. Rechtstatsachensammlung ab, mit der Erhebungen zu polizeilichen Ermittlungsmethoden und Eingriffsbefugnissen durchgeführt werden sollen. Ein entsprechender Beschluß wurde von der Innenministerkonferenz gefaßt.

Insbesondere mit Blick auf nicht verdächtige Kontakt- und Begleitpersonen, die z. B. als Familienangehörige von einer Telefon- oder Wohnraumüberwachung im innersten Bereich ihrer persönlichen Lebensgestaltung erfaßt werden, unterbreitete die 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder im selben Jahr Vorschläge, die helfen sollten, die Erforderlichkeit polizeilicher Befugnisse und deren Auswirkungen auf die Rechte der Betroffenen zu überprüfen (vgl. 15. TB Anlage 9). Dabei sollten insbesondere Angaben über den Anlaß einer Datenerhebung mit besonderen Mitteln, die Örtlichkeit und die Dauer der Maßnahme, den Umfang der überwachten Gespräche, z. B. bei der Telefonüberwachung, den betroffenen Personenkreis sowie die Anzahl der ermittelten, verurteilten, aber auch der entlasteten Personen einbezogen werden.

Im Dezember 1994 erhielt das BKA von der IMK den Auftrag, eine sog. Bund/Länder-Fallsammlung einzurichten, und – gemeinsam mit den Landeskriminalämtern – ein einheitliches Themenraster für die Anlieferung von Informationen durch die beteiligten Dienststellen zu erarbeiten. An der 1995 angelaufenen Informationserhebung haben sich bis Anfang Dezember 1996 allerdings neben dem BKA nur sechs Landeskriminalämter, das Zollkriminalamt und die Grenzschutzdirektion beteiligt. Aufgrund der jedenfalls zur Zeit noch geringen Beteiligung der Polizeidienststellen und wegen der zunächst eher knappen Personalausstattung der Rechtstatsachensammelstelle habe ich gewisse Zweifel, ob gegenwärtig eine hinreichend breit angelegte, analytische und objektive Aufarbeitung von Rechtstatsachen möglich ist.

Ich hoffe, daß bei der Arbeit der Rechtstatsachensammelstelle ein „Ungleichgewicht" zwischen – grundsätzlich legitimen – polizeilichen Interessen und verfassungsrechtlich geschützten Individualinteressen vermieden und eine einseitig erkenntnisgeleitete Vorgehensweise ausgeschlossen werden kann. Ich gehe davon aus, daß die weitere Entwicklung und Arbeit der Rechtstatsachensammelstelle beim BKA und insbesondere die Beteiligung der Länderpolizeibehörden auch von den Landesbeauftragten für den Datenschutz aufmerksam verfolgt wird **(s. auch Anlage 7)**. Gesetzgeberische Aktivitäten kann es nur mit ausreichender Begleitung durch rechtstatsächliche Auswertungen geben.

11.3 INPOL-neu

Das gemeinsame Informationssystem der Polizeibehörden des Bundes und der Länder, INPOL, soll neu konzipiert werden. Hiermit sind datenschutzrechtliche Probleme verbunden (Näheres s. 15. TB Nr. 23.5). Die konzeptionellen Arbeiten an diesem Projekt sind zwischenzeitlich soweit fortgeschritten, daß im Herbst 1996 mit der Realisierungsphase begonnen wurde, wozu die Erarbeitung eines technischen Feinkonzeptes gehört. Das Bundesministerium des Innern hat den Datenschutz- und Datensicherheitsfragen eine hohe Priorität eingeräumt und im Rahmen des Projektes eine Stabsfunktion Datenschutz/Datensicherheit gebildet. Sie soll u. a. durch Kontakt mit den Datenschutzbeauftragten dafür sorgen, so früh wie möglich einen Konsens über die Einhaltung von datenschutzrechtlichen Bestimmungen zu erreichen.

Die Datenschutzbeauftragten haben hierzu eine Arbeitsgruppe gebildet. Sie steht den Projektbetreibern beratend zur Verfügung. Im Juli 1996 fand eine erste Besprechung der Arbeitsgruppe mit Vertretern des Bundesministeriums des Innern und des Bundeskriminalamtes in meiner Dienststelle statt. Neben den Fragen des weiteren Vorgehens wurden materiell-rechtliche Fragen erörtert, z. B. in welchem Verhältnis landesrechtliche Vorschriften und Regelungen des zukünftigen BKAG (vgl. Nr. 11.1) zueinander stehen. Nach Auffassung des BMI stellt das BKAG im übrigen das materielle Polizeirecht der Länder unberührt bleibt. Das neue INPOL-Verfahren begründet im Verhältnis zum Bürger keine Eingriffsbefugnisse. Für den Bereich der Gefahrenabwehr gilt auch weiterhin ausschließlich Landesrecht; das gleiche gilt im Hinblick auf die Vorsorge für die Verfolgung zukünftiger Straftaten. Datenschutzrechtliche Detailfragen bezüglich des Zugriffsschutzes, der Verschlüsselung, der Protokollierung usw. werden erst in einem späteren Stadium ausführlich diskutiert werden können. Hierzu ist es notwendig, daß Vorlagen erstellt werden, die bewertende Aussagen zulassen.

11.4 Automatisiertes Fingerabdruck-Identifizierungssystem – AFIS –

AFIS wird beim Bundeskriminalamt eingesetzt, um verformelte Fingerabdrücke von Asylbewerbern, von sonstigen Personen, die nach dem Ausländergesetz erkennungsdienstlich behandelt worden sind, sowie von mutmaßlichen Straftätern automatisiert zu speichern. In meinem 15. Tätigkeitsbericht (Nr. 23.3) habe ich das Verfahren im einzelnen dargestellt und über eine Kontrolle im Jahre 1994 berichtet. Ich hatte insbesondere gerügt, daß der Abgleich der Daten von mutmaßlichen Straftätern gegen den gesamten AFIS-Bestand und damit auch gegen den Datenbestand von Asylbewerbern mit § 16 Abs. 5 Asylverfahrensgesetz nicht vereinbar und somit unzulässig sei. Von einer förmlichen Beanstandung nach dem Bundesdatenschutzgesetz hatte ich nur unter der Voraussetzung abgesehen, daß durch technische und organisatorische Maßnahmen sichergestellt wird, daß ein Abgleich der vorgenannten Datenbestände nur unter den einschränkenden Voraussetzungen des § 16 Abs. 5 Asylverfahrensgesetz erfolgt. Eine Äußerung des Bundesministeriums des Innern zu meinen Forderungen liegt mir trotz wiederholter Erinnerungen bisher nicht vor.

Auch mangelt es immer noch an einer vom BMI endgültig genehmigten Errichtungsanordnung für die Datei AFIS, die immerhin einen Bestand von 2,2 Millionen Datensätzen hat. Eine Errichtungsanordnung ist eine Beschreibung der Datei (u. a. welche Daten,

wer greift auf diese zu, wann werden die Daten gelöscht), zu der das BMI rechtlich verpflichtet ist. Das Verfahren wird somit seit der Inbetriebnahme im Jahre 1992 immer noch auf der Grundlage einer vorläufigen Errichtungsanordnung betrieben. Dies halte ich für nicht mehr vertretbar. Eine weitere Verzögerung des Erlasses wäre datenschutzrechtlich zu beanstanden.

11.5 EUROPOL-Drogenstelle

11.5.1 Überblick

Die EUROPOL-Drogenstelle – EDS – hat ihre Aktivitäten im Berichtszeitraum intensiviert. Maßgebliche Rechtsgrundlage ist weiterhin die Ministervereinbarung vom 2. Juni 1993 (siehe 15. TB Nr. 23.2.3.1). Danach ist eine eigenständige Verarbeitung personenbezogener Daten bei der EDS bis zum Inkrafttreten der EUROPOL-Konvention nicht gestattet. Umfassende polizeiliche Analysen zur Verhütung und Bekämpfung des illegalen Drogenhandels, des illegalen Handels mit nuklearen und radioaktiven Substanzen, der Schleuserkriminalität, des Menschenhandels und der Kraftfahrzeugkriminalität unter Nutzung sensibler personenbezogener Daten werden deshalb erst nach Ratifizierung der Konvention durch die Mitgliedstaaten bei der EDS aufgenommen. Bis dahin werden lediglich Daten und Informationen zwischen den nationalen Verbindungsbeamten der Mitgliedstaaten ausgetauscht. Dieser Informationsaustausch wurde im Berichtszeitraum erheblich intensiviert. Die EDS beschäftigt bereits jetzt vier polizeiliche Analytiker, die – ohne personenbezogene Daten zu nutzen – strategische Verbrechensanalysen, beispielsweise zu den Vertriebswegen von Drogen, erstellen. Das zunächst auf die Bekämpfung des Drogenhandels beschränkte Mandat der EDS wurde durch die gemeinsame Maßnahme vom 10. März 1995 auf die Bekämpfung der Nuklearkriminalität, der Kfz-Verschiebung und der Schleuserkriminalität sowie der damit jeweils zusammenhängenden Geldwäsche erweitert. Ende 1996 wurde das Mandat ferner um die Bekämpfung des Menschenhandels und der sexuellen Ausbeutung von Kindern ergänzt.

Die EUROPOL-Konvention wurde nach langen und intensiven Beratungen am 26. Juli 1995 von den Mitgliedstaaten gezeichnet. Nunmehr laufen die Beratungen für eine innerstaatliche Ratifizierung. Der Arbeitsentwurf eines EUROPOL-Vertragsgesetzes wurde im Oktober 1996 den Bundesländern zur Stellungnahme übersandt. Über den Ausgang des Gesetzgebungsverfahrens im Laufe des Jahres 1997 läßt sich derzeit keine Prognose abgeben, jedoch hält die Bundesregierung den Entwurf für vordringlich.

Um EUROPOL rechtlich, finanziell, organisatorisch und personell auf die Aufnahme der Analysetätigkeit vorzubereiten, bedarf es neben der Verabschiedung der EUROPOL-Konvention mehrerer Durchführungsbestimmungen, die so verschiedene Bereiche, wie z. B. die Einrichtung der Arbeitsdateien zu Analysezwecken, den EUROPOL-Haushalt, die dienstrechtliche Stellung der EUROPOL-Mitarbeiter oder den Geheimschutz bei EUROPOL betreffen. Diese Regelungen werden – wie schon die EUROPOL-Konvention – in der Ratsarbeitsgruppe EUROPOL in Brüssel von Vertretern der Mitgliedstaaten unter Beteiligung nationaler Datenschutzbeauftragter vorbereitet. Ich war von Anfang an intensiv daran beteiligt. Mein besonderes Augenmerk gilt den Durchführungsbestimmungen für die Analysedateien, die als „Herzstück" von EUROPOL nach der Ratifizierung der Konvention umgesetzt werden sollen (siehe dazu Nr. 11.5.2). Einen weiteren Schwerpunkt sehe ich bei der Vorbereitung der Geschäftsordnung für die Gemeinsame Kontrollinstanz, die die Einhaltung datenschutzrechtlicher Vorschriften durch EUROPOL kontrollieren wird. Das EUROPOL-Computersystem soll nach dem gegenwärtigen Planungsstand rechtzeitig mit dem Inkrafttreten der Konvention, also voraussichtlich 1999, zur Verfügung stehen. Auch bei dieser Konzeption stellen sich schwierige datenschutzrechtliche und technische Fragen. Ich begrüße es daher ausdrücklich, daß das BMI und das BKA mich auch insoweit intensiv beteiligen.

Die Tätigkeit der deutschen Verbindungsbeamten bei der Europol-Drogenstelle habe ich im August 1995 (vgl. Nr. 11.5.4) kontrolliert. Im März 1996 habe ich mich mit anderen europäischen Datenschutzbeauftragten bei der EDS über deren Aufgaben informiert. Im Anschluß daran haben die Datenschutzbeauftragten gegenüber dem Rat der Justiz- und Innenminister ihre Bereitschaft zur Zusammenarbeit beim Aufbau von EUROPOL unterstrichen.

Für 1997 ist eine weitere datenschutzrechtliche Kontrolle beabsichtigt.

11.5.2 Durchführungsbestimmungen für die Arbeitsdateien zu Analysezwecken

Die Durchführungsbestimmungen für die Arbeitsdateien zu Analysezwecken ergänzen und konkretisieren die Vorgaben der Artikel 10 und 12 der EUROPOL-Konvention. Damit soll insbesondere geregelt werden, welche Daten zu unterschiedlich „tatnahen" und „tatfernen" Personen, wie z. B. Verdächtigen oder Zeugen, in den Analysedateien gespeichert und verarbeitet werden dürfen. Sie bilden damit die eigentliche Grundlage für Art und Umfang der EUROPOL-eigenen Informationsverarbeitung im Bereich der kriminalpolizeilichen Analyse.

Ein erster Entwurf der Durchführungsbestimmungen für die Analysedateien wurde Ende Juli 1995 von der damaligen spanischen EU-Präsidentschaft vorgelegt und seitdem mehrfach überarbeitet. Die Beratung dieser besonders wichtigen Regelungen über z. T. sensible Daten ist noch nicht abgeschlossen, ein Ergebnis wird für 1997 erwartet. Bei der Erörterung der verschiedenen, von der spanischen, italienischen, irischen und niederländischen Präsidentschaft vorgelegten Entwürfe wurde deutlich, daß aus polizeilicher Sicht eine Option für eine möglichst umfassende Verarbeitung personenbezogener Daten angestrebt wird, um die Chancen zur Aufklärung kriminalistisch relevanter Verbindungen von Personen oder Personengruppen zu einzelnen Delikten oder Deliktkomplexen zu erhöhen. Dagegen zielt der datenschutzrechtliche Ansatz darauf ab, die Verarbeitung der Daten „tatferner" Personen, wie insbesondere der Zeu-

gen und Opfer, auf das unabdingbar erforderliche Minimum zu reduzieren, um den Schutz der Persönlichkeitsrechte dieser Menschen sicherzustellen. Dies gilt vor allem für so schützenswerte Daten, wie rassische Herkunft, politische Anschauungen, religiöse oder andere Überzeugungen, sowie Daten zur Gesundheit i.S.d. Artikels 6 Satz 1 der Datenschutz-Konvention des Europarates vom 28. Januar 1981. Die Verarbeitung und Nutzung personenbezogener Daten im Rahmen der Analyse steht unter dem Vorbehalt der Erforderlichkeit (Artikel 10 Abs. 1 Satz 1 des EUROPOL-Übereinkommens). Für die vorstehend aufgeführten Daten sieht Artikel 10 Abs. 1 Satz 2 der Konvention eine strenge Prüfung der Erforderlichkeit vor. Derartige Daten dürfen nur dann verarbeitet werden, wenn sie für den – hinreichend deutlich und präzise zu definierenden – Zweck einer bestimmten Analyse unbedingt notwendig sind und wenn sie andere personenbezogene Daten in dieser Datei ergänzen.

Mit Blick auf diese strenge Vorgabe des Europaratsübereinkommens und der EUROPOL-Konvention sind in den Durchführungsbestimmungen verfahrenstechnische Vorkehrungen festzuschreiben, die eine umfassende und effektive Kontrolle der Speicherung und Verarbeitung besonders schützenswerter personenbezogener Daten ermöglichen. Insoweit ist sicherzustellen, daß die Gemeinsame Kontrollinstanz (s. u. Nr. 11.5.3) jederzeit einen vollständigen statistischen Überblick über Art und Zahl der zu den verschiedenen Personengruppen gespeicherten Daten erhalten kann, um diesen als Prüfungsansatz und Einstieg in eine effektive Kontrolle der Datenverarbeitung im Einzelfall zu nutzen.

Von grundsätzlicher datenschutzrechtlicher Bedeutung ist auch die Umsetzung der Regelungen des Artikels 12 der Konvention, der eine Errichtungsanordnung für jede automatisierte Analysedatei vorsieht und dabei eine unverzügliche Unterrichtung der Gemeinsamen Kontrollinstanz über jeden Entwurf einer Errichtungsanordnung anordnet. In den Durchführungsbestimmungen ist insoweit auch zu klären, welche „Sperrwirkung" Beanstandungen der Gemeinsamen Kontrollinstanz haben, wenn nach deren Ansicht datenschutzrechtliche Regelungen der EUROPOL-Konvention oder der Durchführungsbestimmungen verletzt sind.

Umzusetzen und zu konkretisieren sind in den Durchführungsbestimmungen ferner die Artikel 20 und 21 der EUROPOL-Konvention, die die Berichtigung und Löschung von Daten sowie die Speicherungs- und Löschungsprüffristen regeln. Vor allem die gebotene gründliche Prüfung der Erforderlichkeit einer weiteren Speicherung und Nutzung der Daten durch die Analytiker kann die betroffenen Personen vor einer unverhältnismäßig umfangreichen und unangemessen langen Aufbewahrung ihrer Daten schützen. Ich setze mich insofern dafür ein, daß in den Durchführungsbestimmungen eine jährliche Prüfung der weiteren Speicherung dieser empfindlichen Daten vorgesehen wird. Ich gehe davon aus, daß die Einhaltung dieser Prüffristen und auch der in Artikel 21 Abs. 3 der EUROPOL-Konvention leider nur unvollständig geregelten Speicherhöchstfristen einen Prüfungsschwerpunkt der Gemeinsamen Kontrollinstanz darstellen werden.

11.5.3 Gemeinsame Kontrollinstanz

Die unabhängige Gemeinsame Kontrollinstanz hat nach Maßgabe der Konvention insbesondere folgende Aufgaben:

- Prüfung, ob durch die Speicherung, die Verarbeitung und die Nutzung personenbezogener Daten durch EUROPOL die Rechte von Personen verletzt werden,
- Prüfung der Zulässigkeit der Datenübermittlung der von EUROPOL stammenden Daten,
- Prüfung von Anwendungs- und Auslegungsfragen im Zusammenhang mit der Verarbeitung und Nutzung personenbezogener Daten durch EUROPOL sowie
- Prüfung von Rechtsfragen und Entscheidungen im Zusammenhang mit der Geltendmachung des Auskunftsanspruchs.

Diesem umfassenden Prüfungs- und Beratungsauftrag entspricht das jedermann eröffnete Recht, die Gemeinsame Kontrollinstanz um Prüfung der Zulässigkeit und Richtigkeit einer etwaigen Speicherung, Erhebung, Verarbeitung und Nutzung von Daten zu ersuchen, soweit diese den Antragsteller betreffen.

Die Gemeinsame Kontrollinstanz besteht aus dem Plenum sowie dem Ausschuß nach Artikel 24 Abs. 7 und hat einen Präsidenten, dessen Aufgaben bei der Leitung der Plenarberatungen und des Ausschusses nach Artikel 24 Abs. 7 in der Geschäftsordnung der Gemeinsamen Kontrollinstanz bestimmt werden sollen. Die Mitglieder der Gemeinsamen Kontrollinstanz sind bei der Wahrnehmung ihrer Aufgaben weisungsunabhängig (Artikel 24 Abs. 1 S. 7). Soweit sie als Mitglieder des Ausschusses gerichtsähnliche Aufgaben wahrnehmen, halte ich es mit Blick auf die Vorgaben des Grundgesetzes für geboten, ihre Rechtsstellung am Maßstab der Anforderungen zu orientieren, die „verfassungskräftig" die Unabhängigkeit deutscher Richter definieren.

Neben dem Präsidenten, dem Plenum sowie dem Ausschuß sieht die EUROPOL-Konvention in Artikel 24 Abs. 8 des weiteren Kommissionen vor, denen nach Maßgabe der Geschäftsordnung und im Rahmen der rechtlichen Vorgaben der Konvention einzelne Aufgaben übertragen werden können. Damit ist die Möglichkeit eröffnet, durch ad hoc einzuberufende oder bei Beginn einer jeden Amtsperiode vorsorglich einzusetzende, kleine und flexible Kommissionen datenschutzrechtliche Probleme kurzfristig aufzugreifen, zu untersuchen und – soweit erforderlich – Beanstandungen gegenüber der Leitung von EUROPOL und dem Verwaltungsrat vorzubereiten. Alle genannten Organe der Gemeinsamen Kontrollinstanz werden von einem Sekretariat unterstützt, dessen Aufgaben ebenfalls durch die Geschäftsordnung zu präzisieren sind (Artikel 24 Abs. 10). Die Entsendung der deutschen Mitglieder in der Gemeinsamen Kontrollinstanz soll in dem Vertragsgesetz zur EUROPOL-Konvention geregelt werden.

11.5.4 Kontrolle der deutschen Verbindungsbeamten bei der EUROPOL-Drogenstelle – EDS –

Im August 1995 habe ich die deutschen Verbindungsbeamten bei EUROPOL kontrolliert und bera-

ten. Prüfungsschwerpunkte waren die internen Kommunikationsverfahren zwischen den deutschen Verbindungsbeamten und den Verbindungsbeamten der anderen Mitgliedstaaten sowie die externen Kommunikationsverfahren zwischen den deutschen Verbindungsbeamten und insbesondere dem BKA.

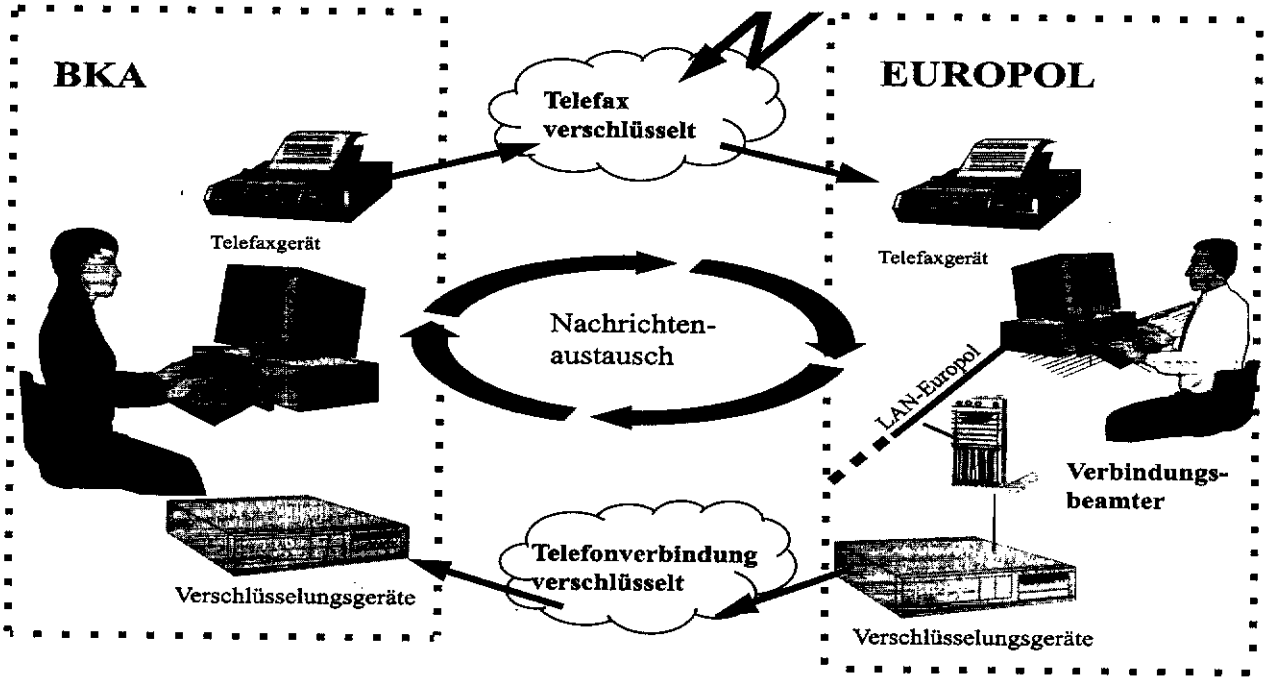
Die Kommunikation unter den Verbindungsbeamten wird über ein Netzwerk (Local Area Network, LAN) und damit quasi papierlos durchgeführt. Das Netzwerk besteht aus mehreren Arbeitsplatzcomputern und drei zentralen Servern. Jedem Verbindungsbeamten stehen die heute üblichen Bürokommunikationskomponenten – Textverarbeitung, Tabellenkalkulation, Graphik, Mail – zur Verfügung. Die Kommunikation zwischen den Verbindungsbeamten wird über ein Mail-Programm abgewickelt (vgl. 15. TB Nr. 23.2.3.1). Die netzwerkinterne Kommunikation der Verbindungsbeamten beginnt nach Eingang der Anfrage einer nationalen Stelle, indem der jeweilige nationale Verbindungsbeamte diese Anfrage mit Hilfe des Mail-Programms an die betroffenen Verbindungsbeamten anderer Mitgliedstaaten weitergibt. Die mittlerweile getroffenen Sicherheitsmaßnahmen, vor allem den Zugriffsschutz bei der Nutzung des Mail-Programms halte ich für effizient und stelle meine im 15. TB geäußerten Bedenken zurück.

Alle Arbeitsstationen der Verbindungsbeamten im EUROPOL-Netzwerk waren im Zeitpunkt der Prüfung mit Diskettenlaufwerken ausgestattet. Diskettenlaufwerke gelten wegen der erleichterten Möglichkeiten des unbefugten Kopierens von Daten und des Einschleusens von Viren als sehr große Gefahrenquelle. Ich habe angeregt, entweder dort auf die Diskettenlaufwerke zu verzichten, wo sie nicht wirklich benötigt werden, oder – sofern an einzelnen Arbeitsstationen die Verwendung von Disketten unabdingbar ist – durch Installation geeigneter Software den Zugriff auf das Diskettenlaufwerk nur besonders berechtigten Benutzern zu erlauben. Ferner habe ich auf einige Schwächen bei der Gestaltung von Paßwörtern hingewiesen. Meine Vorstellungen hat das Bundesministerium des Innern aufgegriffen und sie den zuständigen Gremien vorgetragen mit der Bitte, geeignete Maßnahmen zu ergreifen. Mögliche Änderungen sind mir noch nicht mitgeteilt worden.

Der wesentliche Vorteil der Arbeitsweise von EUROPOL liegt in der Gewährleistung schneller Kommunikation mit den nationalen Stellen und damit eines schnellen Informationsaustausches. Um einem Mißbrauch der übertragenen Informationen durch unbefugtes Mithören vorzubeugen, ist die nationale Stelle von EUROPOL – das BKA – über eine verschlüsselte Telefonwählverbindung mit Hardwareverschlüsselung und Einwählkontrolle (Zugriffsschutz) mit EUROPOL verbunden. Über diese kryptographisch verschlüsselte Wählverbindung wird der E-Mail-Verkehr abgewickelt. Diese Kommunikationsverbindung wird gegenwärtig nur in einer Richtung für den Datenverkehr von EUROPOL an das BKA benutzt. Antworten vom BKA an EUROPOL bzw. Anfragen des BKA an EUROPOL werden noch über sichere Faxgeräte übermittelt, die über eine Verschlüsselungsfunktion verfügen (s. Abb. 7).

Abbildung 7

Informationsaustausch EUROPOL – BKA



In absehbarer Zeit wird aber auch diese Kommunikation über verschlüsselte E-Mail-Verbindungen ablaufen.

Der Informationsaustausch zwischen EUROPOL und den Landeskriminalämtern soll grundsätzlich auf demselben, sicheren Weg unter Einschaltung des Bundeskriminalamtes erfolgen. Soweit unmittelbare Kommunikation zwischen Dienststellen der Länder und EUROPOL stattfindet, habe ich mich sowohl beim BKA als auch bei den Landesbeauftragten für den Datenschutz dafür eingesetzt, kurzfristig die technischen und organisatorischen Voraussetzungen für eine sichere Übermittlung personenbezogener Daten zu schaffen.

11.6 Schengener Durchführungsübereinkommen

11.6.1 Überblick

Das Schengener Durchführungsübereinkommen (SDÜ) vom 19. Juni 1990 ist durch Beschluß des Exekutivausschußes zwischen den Gründerstaaten Belgien, Frankreich, Luxemburg, Niederlande, Bundesrepublik Deutschland sowie Portugal und Spanien mit Wirkung vom 26. März 1995 in Kraft gesetzt worden. Seit diesem Zeitpunkt finden an den Binnengrenzen zwischen den Vertragsparteien, mit Ausnahme derjenigen Frankreichs mit Belgien und Luxemburg, keine Personenkontrollen mehr statt. Zum selben Zeitpunkt hat auch das Schengener Informationssystem (SIS), das aus der zentralen Unterstützungseinheit in Straßburg (C.SIS) und je einem nationalen SIS in den Mitgliedstaaten besteht, seinen Betrieb aufgenommen (vgl. 15. TB Nr. 23.2.1). Nach anfänglichen Kinderkrankheiten hat das SIS – auch durch Nachrüstung – mittlerweile eine hohe technische Verfügbarkeit erreicht. Dies ist auch aus Sicht des Datenschutzes von großer Bedeutung, da die Fahndungsausschreibungen auf aktuellem Stand gehalten werden müssen. Zum Jahreswechsel 1996/1997 zählte das SIS insgesamt mehr als 4,5 Millionen Datensätze, darunter ca. 600 000 personenbezogene Ausschreibungen und ca. 400 000 Alias-Datensätze zu mißbräuchlich verwandten Personalien, sowie mehr als 3 Millionen Ausschreibungen zur Sachfahndung.

In naher Zukunft wird das Schengener Vertragsgebiet erweitert werden. Die Beitrittsabkommen mit Griechenland und Italien sind bereits ratifiziert. Die Ratifizierung des Beitritts von Österreich steht bevor. Sobald die rechtlichen sowie technisch-organisatorischen Voraussetzungen von den Beitrittsländern erfüllt sind, wird das Durchführungsübereinkommen mit ihnen in Kraft gesetzt, und das jeweilige nationale SIS wird seinen Betrieb aufnehmen. Dies setzt jedoch für Griechenland noch den Erlaß der notwendigen datenschutzrechtlichen Regelungen voraus (s. u. Nr. 32.3.1). Das italienische Datenschutzgesetz ist im Januar 1997 in Kraft getreten, während das griechische Datenschutzgesetz noch für die erste Hälfte 1997 erwartet wird.

Inzwischen wurden Beitrittsverhandlungen mit den nordischen Staaten aufgenommen. Dänemark, Finnland und Schweden erhielten bereits im April 1996 den Beobachterstatus mit der Perspektive des Beitritts zum SDÜ. Mit Norwegen und Island, die nicht Mitglieder der EU sind, wurde über Kooperationsabkommen verhandelt. Nach Abschluß der Beratungen haben die fünf Länder am 19. Dezember 1996 das SDÜ bzw. das Kooperationsabkommen unterzeichnet. Im Hinblick auf diese Beitritte und weitere mögliche Beitrittswünsche anderer Staaten werden bereits Überlegungen über die Aufrüstung des bestehenden SIS bzw. über die Neukonzeption eines erweiterten SIS angestellt.

11.6.2 Gemeinsame Kontrollinstanz

Für die datenschutzrechtliche Kontrolle des SIS, insbesondere im Hinblick auf den Zentralcomputer in Straßburg, ist eine gemeinsame Kontrollinstanz (GKI) zuständig, die sich aus je zwei Vertretern der nationalen Kontrollinstanzen zusammensetzt. Unberührt hiervon bleibt meine Zuständigkeit für den beim BKA geführten nationalen Teil des SIS (N.SIS). Nach Inkraftsetzung des SDÜ am 26. März 1995 hat sich die GKI am 17. Mai 1995 konstituiert. Die deutsche Delegation in dem Gremium besteht aus einem Vertreter meiner Dienststelle und einer Vertreterin des Hessischen Landesbeauftragten für den Datenschutz. Letztere wurde auf Vorschlag der Landesbeauftragten in das Gremium berufen. Zu den ersten Amtshandlungen der GKI zählten der Erlaß einer Geschäftsordnung sowie die Wahl des Vorsitzenden. Diese fiel auf ein Mitglied der französischen Delegation.

Neben der Überwachung der technischen Unterstützungseinheit in Straßburg ist die GKI u. a. zuständig für Fragen der Anwendung und Auslegung im Zusammenhang mit dem SIS sowie für die Erarbeitung von Lösungsvorschlägen für aufkommende Fragen, z. B. zur Rechtsgrundlage der nationalen SIRENE-Büros (s. auch Nr. 11.6.3). Die GKI legte von Anfang an Wert auf eine unabhängige, weisungsfreie Aufgabenerfüllung und verlangte deshalb von den dafür zuständigen Schengener Gremien einen eigenständigen Haushalt. Bei einigen Regierungsdelegationen stieß dieser Wunsch aber leider auf Ablehnung. Mit einem eigenen Haushalt könnte das Gremium jedoch seinen Auftrag wirkungsvoller erfüllen, z. B. bei Bedarf auch externe Berater zur Beurteilung schwieriger Probleme bei der Datenverarbeitung und der Kommunikation mit den N.SIS hinzuziehen. Schließlich gilt es, ein recht komplexes Datenbanksystem wirksam zu kontrollieren.

Eine Arbeitsgruppe der GKI mit Vertretern aus vier Ländern (Frankreich, Luxemburg, Spanien, Deutschland) hat vom 7.–10. Oktober 1996 erstmalig die technische Unterstützungseinheit in Straßburg kontrolliert, und zwar

- die technisch-organisatorischen Maßnahmen am dortigen Standort, in dem sich auch DV-Einrichtungen des französischen Innenministeriums befinden,
- die Gewährleistung der absoluten Identität zwischen dem Datenbestand des zentralen SIS und den Datenbeständen der SIS auf nationaler Ebene, wie das im Übereinkommen vorgeschrieben ist, und
- das Verfahren, mit dem Daten gelöscht werden.

Über die Ergebnisse der Kontrolle möchte ich auf den Bericht der GKI verweisen, den diese dem Exekutivausschuß zuleitet. Bedauerlicherweise endete der Kontrollbesuch mit einem Eklat, weil die spanischen Mitglieder der Kontrollgruppe vom französischen Leiter des Zentrums gegen Ende der Prüfung – angeblich auf mündliche Weisung aus Paris – ultimativ aus dem Schengen-Zentrum verwiesen wurden. Dies hat zu einer scharfen Protestnote des Vorsitzenden der GKI gegenüber den zuständigen französischen Regierungsstellen geführt. Auch dieser Vorfall zeigt, wie wichtig es ist, die Unabhängigkeit der gemeinsamen Kontrollinstanz im Verhältnis zu den Schengen-Gremien und den nationalen Regierungen zu stärken.

11.6.3 Schengen-Kontrollen bei BKA und BGS

Im Berichtszeitraum habe ich die Datenverarbeitung im Zusammenhang mit dem SDÜ beim BKA und beim BGS kontrolliert, und zwar beim deutschen SIRENE-Büro, das beim BKA in Wiesbaden eingerichtet wurde, beim BKA am Standort Meckenheim und beim Grenzschutzamt Frankfurt/Main.

Im deutschen SIRENE-Büro – mittlerweile eine BKA-Organisationseinheit mit über 40 Mitarbeitern – habe ich u. a.

- die Übermittlungen an die anderen Schengen-Vertragsparteien,
- die Übernahme erledigter Fahndungsunterlagen der deutschen SIRENE in Kriminalakten des BKA und
- die Dokumentation der Bearbeitung von Ausschreibungsfällen in der Vorgangsnachweisdatei (VNS).

überprüft.

Nach Artikel 103 SDÜ ist durchschnittlich jede zehnte Übermittlung von „Schengen-Daten" zu protokollieren, um die Zulässigkeit der Abrufe datenschutzrechtlich überprüfen zu können. Das SIRENE-Büro beim BKA protokolliert gegenwärtig nur jeden zehnten der Fälle, in denen zu den Daten der abgefragten Person Daten im SIS gefunden wurde, sogenannte Trefferfälle. Diese Praxis verstößt schon gegen den Wortlaut des Art. 103 SDÜ. Nach meinem Verständnis liegt nämlich auch dann eine Datenübermittlung vor, wenn die Abfrage im SIS keinen Treffer erzielt, also kein Bestand vorhanden ist. Im BKA wurden mir zudem Protokollausdrucke vorgelegt, die eine Kontrolle nicht erlaubten: Die Zulässigkeit der Übermittlungen konnte nicht kontrolliert werden, weil z. B. weder der Abfragegrund noch die „einschlägige" Aktenfundstelle im Protokolldatensatz enthalten waren. Ich habe das BMI und das BKA gebeten, diese Art der Protokollierung aussagekräftiger zu gestalten. Das BMI lehnt dies als derzeit nicht machbar ab. Das Problem einer angemessenen Protokollierung habe ich auch der GKI mit dem Ziel einer schengenweiten Lösung unterbreitet.

Das BKA hat bisher in wenigen Fällen Unterlagen aus erledigten Fahndungsausschreibungen anderer Schengen-Vertragsstaaten gemäß Art. 95 SDÜ (Festnahme mit dem Ziel der Auslieferung) in hauseigene Kriminalakten übernommen. Sofern die betroffenen Personen in Deutschland als Straftäter noch nicht in Erscheinung getreten waren und deshalb deutsche Kriminalakten bisher nicht existierten, habe ich Bedenken dagegen, deutsche Kriminalakten nur mit aus anderen Staaten übernommenen Fahndungsunterlagen anzulegen. Artikel 102 Abs. 1 SDÜ sieht ausdrücklich vor, daß die nationalen Zentralstellen die Fahndungsdaten *„nur für die der jeweiligen Ausschreibung entsprechenden Zwecke nutzen"* dürfen. Fraglich ist, ob nach Erledigung einer „Schengen-Fahndung", z. B. nach Festnahme, eine Nutzung für „entsprechende Zwecke" im Sinne des Artikel 102 Abs. 1 SDÜ noch möglich ist. Nach Rücknahme der „einschlägigen" Schengen-Ausschreibung durch den zuständigen Mitgliedstaat sind meines Erachtens Speicherungen im nationalen deutschen Informationssystem zu löschen und gegebenenfalls angelegte Akten zu vernichten. Dies gilt dann nicht, wenn zur Person des Betroffenen bereits polizeirelevante Erkenntnisse im Inland vorliegen. In diesem Falle bestehen gegen die Übernahme der Fahndungsunterlagen keine datenschutzrechtlichen Bedenken.

Der im Zusammenhang mit dem Schengener Informationssystem anfallende begleitende Informationsaustausch mit den SIRENE-Büros anderer Staaten wurde zunächst im sog. Vorgangsnachweis Personen (VNP) dokumentiert. Der VNP ist eine automatisierte Amtsdatei des BKA. Ausweislich ihrer Errichtungsanordnung dient diese Datei jedoch nur dem Nachweis von Vorgängen administrativer Art im BKA, nicht aber der Speicherung von Informationen des polizeilichen Nachrichtenaustausches im Rahmen des SDÜ. Das BKA hat daher inzwischen eine besondere Amtsdatei „Vorgangsnachweis SIRENE" (VNS) eingerichtet und in Betrieb genommen.

Das Konsultationsverfahren nach Artikel 17 Abs. 2 SDÜ dient einer abgestimmten Entscheidung der Vertragsparteien über die Erteilung sogenannter Schengen-Visa, wenn die Antragsteller aus bestimmten Drittländern stammen. Vor Erteilung des Visums sind in solchen Fällen insbesondere die Sicherheitsbehörden aller Vertragsparteien zu konsultieren, um eine sachgerechte Entscheidung über den Antrag zu ermöglichen (s. 15. TB Nr. 23.2.1.2).

Zentrale Sammel- und Verteilerstelle für die von den deutschen diplomatischen und konsularischen Vertretungen und von den anderen Schengen-Vertragsstaaten eingehenden Anfragen ist das Auswärtige Amt (AA). Bereits im 15. TB (Nr. 23.2.1.2) habe ich darauf hingewiesen, daß für den gegenseitigen Informationsaustausch zwischen dem AA und den inländischen Sicherheitsbehörden sowie zwischen dem AA und den ausländischen Zentralstellen eine bereichsspezifische Rechtsgrundlage fehlt. Leider zeichnet sich auch keine gesetzgeberische Initiative ab.

Auf dem Flughafen Frankfurt/Main wie auch auf den übrigen internationalen Flughäfen der Schengen-Vertragsstaaten werden ankommende Passagiere bei der grenzpolizeilichen Einreisekontrolle getrennt nach EU-Staatsangehörigen und Drittausländern abgefertigt. Bei einreisenden Drittausländern werden zunächst der INPOL- und der Grenzfahndungsbestand abgefragt. Sofern darüber hinaus Daten im

N.SIS gespeichert sind, erscheint in der INPOL-Anzeige des Kontrollterminals nach einem Merker auch der im N.SIS gespeicherte Datensatz zu der abgefragten Person. Im Trefferfall wird anschließend in einem automatisierten Verfahrens der Lage- und Einsatzzentrale des Grenzschutzamtes ein Berichtsvorgang angelegt und eine SIS-Treffermeldung gefertigt. Die Treffermeldung wird automatisiert an das deutsche SIRENE-Büro beim BKA und nachrichtlich an die Grenzschutzdirektion übermittelt. Sofern der Bundesgrenzschutzaktennachweis (BAN als Nachfolgesystem des früheren Grenzaktennachweises – GAN –) zu den Daten der abgefragten Person bereits einen Fundstellenhinweis enthält, wird der neue Vorgang mit dem Aktenzeichen des schon im BAN gespeicherten „alten" Falles erfaßt. Der „Treffer" wird befristet beim Grenzschutzamt gespeichert und programmgesteuert gelöscht, sofern der Sachbearbeiter im Einzelfall eine weitere Aufbewahrung der Unterlagen und weitere Speicherung der Daten nicht ausdrücklich verfügt. Gegen diese Verfahrensweise bestehen aus meiner Sicht keine Bedenken.

11.7 Europäisches Informationssystem

Über die Zielsetzung und den Beginn der Arbeiten an dem Übereinkommen über ein Europäisches Informationssystem – EIS – habe ich bereits in meinem 14. (Nr. 24.2.1) und in meinem 15. Tätigkeitsbericht (Nr. 23.2.2.) berichtet. Der Entwurf des EIS-Übereinkommens wurde im Berichtszeitraum nur geringfügig weiterentwickelt. Ursache hierfür sind Meinungsverschiedenheiten über den Entwurf eines Übereinkommens über das Überschreiten der Außengrenzen. Die datenschutzrechtlich bedeutsamen Regelungen des aktuellen Entwurfs (Stand: 1. Dezember 1995) sind gegenüber dem im letzten Tätigkeitsbericht berücksichtigten Vorentwurf (Stand: 25. März 1994) unverändert. Ich begrüße vor allem die Beibehaltung der Artikel 26 und 27, die den Datenschutz bei konventioneller Datenübermittlung gewährleisten. Gegen die Einrichtung eines automatisierten Abrufverfahrens zugunsten von EUROPOL habe ich Bedenken, solange die Erforderlichkeit eines solchen Direktzugriffes von EUROPOL nicht hinreichend dargelegt ist. Die zuständige Ratsgruppe „EUROPOL" hat sich seither mit dieser Frage noch nicht befaßt.

11.8 IKPO-Interpol – Kommission für die interne Kontrolle der Dateien der IKPO-Interpol –

Im März 1995 bin ich vom Exekutiv-Komitee auf Vorschlag der deutschen Delegation für drei Jahre zum Mitglied der Kommission für die interne Kontrolle der Dateien der IKPO-Interpol gewählt worden. Über Aufgaben und Funktionsweise dieses Datenschutz-Gremiums habe ich bereits in meinem 15. Tätigkeitsbericht berichtet (Nr. 23.6). Die fünf neu ernannten Mitglieder des Ausschusses haben sich im Dezember 1995 zu ihrer konstituierenden Sitzung getroffen und Herrn Paul Thomas, den Vorsitzenden der belgischen Datenschutzkommission, zu ihrem Vorsitzenden bestimmt. Das Kontrollgremium wird demnächst einen eigenen Jahresbericht über seine wichtigsten Aktivitäten im Zeitraum 1995/1996 vorlegen.

11.9 Verträge über internationale polizeiliche Zusammenarbeit

Das BMI hat im Berichtszeitraum mehrere Abkommen über die polizeiliche Zusammenarbeit mit west- und osteuropäischen Nachbarstaaten vorbereitet. Während die Verträge mit den westeuropäischen Nachbarstaaten primär die polizeiliche Zusammenarbeit in den Grenzgebieten verbessern sollen, wird mit den osteuropäischen Staaten insbesondere eine verbesserte kriminalpolizeiliche Zusammenarbeit bei der Bekämpfung der sprunghaft angewachsenen grenzüberschreitenden organisierten Kriminalität angestrebt.

Im Rahmen des Informationsaustausches sollen auch besonders schützenswerte, personenbezogene Daten an die osteuropäischen Vertragspartner übermittelt werden. Die Empfängerstaaten sind darum bemüht, ihre datenschutzrechtlichen Standards dem westeuropäischen Niveau anzugleichen und dabei insbesondere die vertrauliche und zweckgebundene Behandlung personenbezogener Informationen sicherzustellen. Eine möglichst kurzfristige Angleichung des datenschutzrechtlichen Niveaus und insbesondere auch der Standards im Bereich der Datensicherheit sind für mich essentielle Voraussetzungen eines polizeilichen Informationsaustausches. Ich gehe davon aus, daß das BKA nach Inkrafttreten der Vereinbarungen gerade in der gegenwärtigen Übergangsphase in jedem Einzelfall besonders sorgfältig prüfen wird, ob die angeforderten Informationen übermittelt werden dürfen, und dabei berücksichtigen wird, daß eine „unkontrollierte" Übermittlung „weicher", noch nicht abgeklärter, polizeilicher Informationen unter Umständen zu schweren Nachteilen für den möglicherweise unschuldigen Betroffenen führen kann. Vor allem aus diesem Grunde ist eine allenfalls restriktive Regelung für eine Datenübermittlung mit zweckändernder Nutzung im Empfängerstaat bezüglich Behörden außerhalb des polizeilichen Bereiches geboten. Nach deutschem Recht sind hiesige Polizeibehörden als Empfänger ausländischer Polizeiinformationen nur in gesetzlich eng definierten Fällen verpflichtet, personenbezogene Daten an die Nachrichtendienste weiterzugeben, z. B. für Zwecke der Spionageabwehr oder zur Bekämpfung terroristischer Bestrebungen. Sofern Entsprechendes in den osteuropäischen Empfängerstaaten mit deutschen Polizeiinformationen aus Gründen der Gegenseitigkeit angestrebt wird, darf eine eng begrenzte Weitergabe und Nutzung nur bei angemessen hohem Datenschutzniveau beim Empfänger erfolgen.

Die Verträge mit den westeuropäischen Ländern dienen der Konkretisierung der Regelungen zur polizeilichen Zusammenarbeit im Schengener Durchführungsübereinkommen (vgl. Nr. 11.6). Die Vereinbarung zwischen dem BMI und dem niederländischen Innen- und dem Justizminister über die polizeiliche Zusammenarbeit im Grenzgebiet wurde am 17. April 1996 unterzeichnet. In den Abkommen sind u. a. die Koordination polizeilicher Einsätze im Grenzgebiet, die Verbesserung der Kommunikationstechnik und die Intensivierung der gemeinsamen Aus- und Fortbildung vorgesehen. Der Entwurf des deutsch-französischen Abkommens sieht darüber

hinaus die Einrichtung gemeinsamer Zentren als Kommunikationsstellen sowohl der beteiligten deutschen Länderpolizeien als auch des Bundesgrenzschutzes und der Zollverwaltung auf der einen und der entsprechenden Partnerbehörden Frankreichs auf der anderen Seite vor. Dies soll einer Intensivierung des Informationsaustausches z. B. über die Personalien von Beteiligten an Straftaten in den Grenzgebieten sowie über Täterverbindungen, typisches Täterverhalten und über deliktische Sachverhalte dienen. Der Ausbau der polizeilichen Zusammenarbeit mit den Schengen-Staaten erfolgt auf der Grundlage der guten datenschutzrechtlichen Vorgaben des SDÜ.

Die polizeiliche Zusammenarbeit mit der Schweiz kann dagegen nicht auf grundlegenden Regelungen und Standards des Schengen-Verbundes aufbauen, weil die Schweiz diesem nicht beigetreten ist. Ein erster Entwurf der deutsch-schweizerischen Vereinbarung sieht – über das „allgemeine" Schengen-Niveau hinausgehend – auch die Zulassung grenzüberschreitender verdeckter Ermittlungen vor. Dies bedarf aus datenschutzrechtlicher Sicht einer sorgfältigen rechtlichen Absicherung (vgl. zur selben Problematik Nr. 13.4.2 – Neapel II –). Vorgesehen ist ferner, sog. kontrollierte Lieferungen u. a. bei Bekämpfung der BtM-Kriminalität, des illegalen Waffenhandels und der Geldwäsche gegenseitig zu ermöglichen. Die Einrichtung eines automatisierten Verfahrens zum Abruf von Sachfahndungsdaten soll insbesondere der Bekämpfung der Kfz-Kriminalität dienen. Die erste Verhandlungsrunde über einen Vertragsentwurf hat Anfang 1997 stattgefunden. Mit Blick auf die hohen datenschutzrechtlichen Standards in der Schweiz bestehen aus meiner Sicht keine grundsätzlichen Bedenken gegen die beabsichtigte Intensivierung der Zusammenarbeit, sofern insbesondere die Weiterübermittlung und Zweckänderung von Daten in einer hinreichend präzisen und klaren Datenschutzklausel geregelt werden.

12 Bundesgrenzschutz

12.1 Erste Erfahrungen mit dem Bundesgrenzschutz-Neuregelungsgesetz

Das BGS-Neuregelungsgesetz, das richtungsweisend datenschutzrechtliche Prinzipien verwirklicht (vgl. 15. TB Nr. 24.1), trat zum 1. November 1994 in Kraft.

Ein wesentlicher Punkt der Neuregelung ist die gesetzliche Definition der Anforderungen an die sog. Errichtungsanordnungen (§ 36 BGSG). Diese Vorschrift verpflichtet den BGS, für automatisierte polizeiliche Dateien mit personenbezogenen Daten vor Inbetriebnahme der Datei jeweils unter anderem Rechtsgrundlage und Zweck der Datei, den Personenkreis, über den Daten gespeichert werden sollen, die Arten der zu speichernden personenbezogenen Daten und die Voraussetzungen, unter denen gespeicherte personenbezogene Daten an welche Empfänger und in welchem Verfahren übermittelt werden, zu definieren. Derartige Dateien bedürfen der Zustimmung des BMI; der Bundesbeauftragte für den Datenschutz ist vor Erlaß der Errichtungsanordnung zu hören. Damit habe ich die Möglichkeit, einer unzulässigen Datenverarbeitung rechtzeitig entgegenzuwirken. Der zunehmende Einsatz von Informationstechnik beim BGS bringt es mit sich, daß seine polizeiliche Datenverarbeitung in den nächsten Jahren vielschichtiger und intensiver werden wird und meine Beteiligung anläßlich der Einführung neuer Dateien und DV-Verfahren sich daher ebenfalls verstärken wird. Das neue BGSG enthält keine besondere Regelung zur Auskunftserteilung an den Betroffenen. Diese richtet sich daher nach § 19 BDSG.

12.2 Aktennachweis des Bundesgrenzschutzes – BAN –

Der BGS übernahm zum 1. April 1992 bahnpolizeiliche und Luftsicherheitsaufgaben; damit war die Datei Grenzaktennachweis – GAN – nicht mehr ausreichend. Der GAN diente dem Nachweis personenbezogener Akten, deren Führung bei der Grenzschutzdirektion und den Grenzschutzämtern zur Erfüllung der ihnen obliegenden, grenzpolizeilichen Aufgaben bei der Verbrechensbekämpfung und der Gefahrenabwehr erforderlich war. Den GAN habe ich im August 1993 beim Grenzschutzamt Frankfurt/Oder kontrolliert (s. 15 TB Nr. 24.3.1). Als „Nachfolgemodell" des GAN wurde die Datei „Aktennachweis des Bundesgrenzschutzes – BAN –" eingerichtet.

Bei der Konzeption dieses neuen Systems wurde ich frühzeitig und intensiv beteiligt. Der BAN dient dem Nachweis von personenbezogenen Akten und deren Führung bei den Dienststellen des BGS sowie bei den ebenfalls mit der Wahrnehmung grenzpolizeilicher Aufgaben betrauten Polizeibehörden des Freistaates Bayern und der Hansestädte Hamburg und Bremen auf dem Gebiet der Strafverfolgung, der Ahndung von Ordnungswidrigkeiten und der Gefahrenabwehr. Der BAN soll vor allem helfen, als Störer einschlägig in Erscheinung getretene Personen zu erkennen und grenz- und bahnpolizeiliche Akten schnell zu finden. Damit sollen in möglichst kurzer Zeit sachgerechte polizeiliche Entscheidungen herbeigeführt und polizeiliche Kontrollen und Ermittlungen durchgeführt werden. Im Rahmen der sog. „Vorgangsverwaltung" soll mit dieser DV-Anwendung die fristgerechte Aktenaussonderung und Datenlöschung sichergestellt werden. Aus Kapazitäts- und Kostengründen wird der BAN auftragsweise beim BKA geführt.

In den BAN werden Daten folgender Personengruppen aufgenommen:

- Beschuldigte im Rahmen strafrechtlicher Ermittlungsverfahren sowie Betroffene im Rahmen von Bußgeldverfahren,
- Verdächtige, bei denen Anhaltspunkte dafür vorliegen, daß sie Täter oder Teilnehmer einer Straftat sind,
- Personen, bei denen erkennungsdienstliche Maßnahmen vorgenommen worden sind,
- Personen, bei denen Fahndungsmaßnahmen in Betracht kommen sowie

- Personen, bei denen die Führung von Akten zur Abwehr von Gefahren in der Zuständigkeit des BGS erforderlich ist.

Nach dem Stand vom 15. Dezember 1996 sind im BAN rund 710 000 Personendatensätze gespeichert. Die zu speichernden Daten beschränken sich im wesentlichen auf Personengrunddaten wie z. B. Vorname, Nachname, Geburtsdatum, Spitzname, Geschlecht und Staatsangehörigkeit, die einen Identitätsabgleich und damit das Auffinden von Akten bei einer anderen Dienststelle des BGS bzw. der Länder Bayern, Bremen und Hamburg im grenz- und bahnpolizeilichem Aufgabenbereich ermöglichen. Im „Trefferfall" gibt der BAN auch Auskunft über die zuständige, aktenführende und sachbearbeitende Dienststelle sowie Tagebuchnummer und über das Datum der Aussonderungsprüfung für die Löschung von Daten und die Vernichtung von Akten.

Vorgesehen sind ferner sogenannte „personengebundene Hinweise", die insbesondere der Eigensicherung von Polizeibeamten, z. B. im Zusammenhang mit Personenfeststellungen im Bahnhofsbereich oder an der Grenze, dienen sollen. Einige der personengebundenen Hinweise dienen dagegen dem Schutz des Betroffenen selbst, z. B. wegen Suizidgefahr. Die Beschränkung der personengebundenen Hinweise auf das unabdingbar notwendige Maß ist mir ebenso wie die Einhaltung angemessener Speicherungsfristen ein besonderes Anliegen.

12.3 Dienstanweisung Gruppe Fernmeldewesen

Die Gruppe Fernmeldewesen – neuerdings Bestandteil der Zentralstelle für Information und Kommunikation des BGS – unterstützt die Grenzschutzämter und -abteilungen sowie – in Einzelfällen – das BKA und die Polizeien der Länder auf dem Gebiet der Funktechnik. Unterstützt wird ferner das BfV auf der Grundlage des § 10 BGSG. Aufgaben- und Befugnisrahmen der Auftragsdatenerhebung für das BfV bestimmen sich nach dem Bundesverfassungsschutzgesetz (s. 15. TB Nr. 24.2).

Die strikte organisatorische Trennung und Abgrenzung der Unterstützungstätigkeit für das BfV von den polizeilichen Aufgabenbereichen beruht auf dem Gebot der Trennung polizeilicher und nachrichtendienstlicher Aufgabenwahrnehmung. § 10 Abs. 3 BGSG entspricht dieser Verpflichtung, indem er die Regelung der Detailfragen durch eine Dienstanweisung vorsieht. Bei der Erarbeitung dieser Dienstanweisung war ich intensiv beteiligt. Die Dienstanweisung sieht eine strikte organisatorische und räumliche Trennung der Sachgebiete bei der Gruppe Fernmeldewesen vor. Die Lenkungsbefugnisse des zuständigen Grenzschutzpräsidiums für die Wahrnehmung polizeilicher Aufgaben einerseits und die Lenkungbefugnisse des BfV für die Wahrnehmung der Aufgaben nach § 10 Abs. 1 BGSG andererseits sind ausdrücklich getrennt und dürfen nicht vermischt werden. Für die Wahrnehmung der Aufgaben nach § 10 Abs. 1 BGSG wird ein besonderes, nur diesen Zwecken dienendes, abgeschottetes IT-System verwendet. Die verfassungsrechtlichen und datenschutzrechtlichen Vorgaben zur organisatorischen und technischen Gestaltung der Überwachungspraxis werden somit durch die Dienstanweisung erfüllt.

12.4 Video-Anlagen im Bahnhofsbereich

Mit ihrem sogenannten 3-S-Konzept möchte die Deutsche Bahn AG Service, Sicherheit und Sauberkeit im Bahnhofsbereich verbessern. Sukzessiv werden zu diesem Zweck die großen Bahnhöfe mit Video-Anlagen ausgerüstet, die über ferngesteuerte Speed-Dome-Kameras verfügen, sich automatisch auf die verschiedenen Lichtsituationen bei Tag und Nacht einstellen und weite Bereiche des Bahnhofes erfassen. Die Mitarbeiter der Bahn in den 3-S-Zentralen haben den Bahnhofsbereich über mehrere Monitore im Blick und stehen mittels modernster Kommunikationstechnik mit bahneigenen Stellen, aber auch mit der Bahnpolizei in Verbindung. Ein Monitor in der jeweiligen BGS-Bahnpolizeidienststelle ist an die Videoanlage des 3-S-Systems angeschlossen und wird aktiviert, wenn die Videobeobachter der Bahn in der 3-S-Zentrale polizeirechtlich relevante Störungen bemerken. Die Steuerung der in Echtzeit auf den Monitor der Bahnpolizei übertragenen Bilder erfolgt in der 3-S-Zentrale. Eine selbständige Bildsteuerung durch die Mitarbeiter der Bahnpolizei ist nicht vorgesehen. Der Entwurf einer Vereinbarung über die Zusammenarbeit zwischen Bahnpolizei und Deutscher Bahn AG in den 3-S-Zentralen (Stand: August 1996) sieht vor, daß alle Sachverhalte von polizeilicher Relevanz unverzüglich der Bahnpolizei zu melden sind, damit diese in eigener Zuständigkeit Maßnahmen ergreift oder ggf. die Landespolizei verständigt. Ferner ist vorgesehen, bei besonderen Lagen (z. B. Bundesligaspiele, Großdemonstrationen) einen Bahnmitarbeiter als Verbindungskraft zur Bahnpolizei einzusetzen. Ständige Präsenz der Beamten der Bahnpolizei in der 3-S-Zentrale selbst ist nicht vorgesehen. Die Bahn soll jedoch verpflichtet werden, der Bahnpolizei lageabhängig die Nutzung eines ständig für bahnpolizeiliche Zwecke vorgehaltenen, besonderen Arbeitsplatzes zu ermöglichen. Der BGS und die Deutsche Bahn AG haben mich frühzeitig bei der Erarbeitung des Konzeptes beteiligt und mir eine der ersten Anlagen, nämlich auf dem Hauptbahnhof in Mainz, vorgeführt.

Aus meiner Sicht ist wesentlich, daß die bahneigenen Aufgaben, die sich aus dem Hausrecht ergeben, und die spezifisch bahnpolizeilichen Aufgaben des BGS grundsätzlich getrennt bleiben. So habe ich angeregt, den besonderen Arbeitsplatz in der 3-S-Zentrale optisch und akustisch abzuschotten, der Bahnpolizei für den dortigen Monitor die ausschließliche Bildsteuerung zuzuweisen und Zugriffsmöglichkeiten der Bahnmitarbeiter in der 3-S-Zentrale auf das vom BGS im Rahmen polizeilicher Maßnahmen genutzte Bild auszuschließen. Ferner sollte eine getrennte Archivierung von Videobändern des BGS und der Deutschen Bahn AG vorgesehen werden.

Bei Einhaltung dieser Vorgaben bestehen aus datenschutzrechtlicher Sicht keine Bedenken gegen die Einbeziehung der Bahnpolizei, die nach § 27 S. 1 Nr. 2 BGSG zur Verwendung selbsttätiger Bildauf-

nahme- und Bildaufzeichnungsgeräte in Verkehrsanlagen und öffentlichen Verkehrsmitteln oder in unmittelbarer Nähe ermächtigt ist. Die Bahnpolizei ist verpflichtet, Videoaufzeichnungen unverzüglich zu vernichten, wenn sie nicht mehr zur Abwehr gegenwärtiger Gefahren oder zur Verfolgung von Straftaten oder Ordnungswidrigkeiten benötigt werden.

13 Zollfahndung und Außenwirtschaftskontrolle

13.1 Post- und Telefonüberwachung nach dem Außenwirtschaftsgesetz auf dem verfassungsgerichtlichen Prüfstand / Kontrolle beim Zollkriminalamt

Als Konsequenz des illegalen Technologietransfers und schwerer Verstöße gegen das Kriegswaffenkontrollgesetz in den 80er Jahren ist das Zollkriminalamt als Bundesoberbehörde mit erweiterten Aufgaben und Befugnissen errichtet worden. 1992 wurde durch Änderung des Außenwirtschaftsgesetzes (AWG) für das Zollkriminalamt (ZKA) die Ermächtigung zur Überwachung des Brief-, Post- und Fernmeldeverkehrs geschaffen (s. 14. TB Nr. 26.1). Die Beschränkung des Brief-, Post- und Fernmeldegeheimnisses wurde entsprechend meiner damaligen Anregung auf zwei Jahre bis 31. Dezember 1994 befristet. Inzwischen wurde die Geltungsdauer jedoch zum zweiten Mal verlängert und zwar zuletzt für die Dauer von drei Jahren, womit die §§ 39–43 des AWG jetzt bis zum 31. Dezember 1999 gelten.

Trotz umfangreicher verfahrenssichernder Maßnahmen habe ich gegen die Vorschrift auch unter datenschutzrechtlichen Aspekten Bedenken. Das Land Rheinland-Pfalz hat im August 1992 beim Bundesverfassungsgericht (BVerfG) gegen diese Änderung des AWG einen Antrag auf abstrakte Normenkontrolle gestellt. Diesen Antrag hat es neben Zweifeln an der Zuständigkeit des Bundes im wesentlichen auch auf datenschutzrechtliche Aspekte gestützt. So ist das Land der Auffassung, daß es der Regelung des § 39 AWG wegen einer Kombination zahlreicher unbestimmter Rechtsbegriffe an der notwendigen Bestimmtheit fehle, die das Grundgesetz für Eingriffe in Artikel 10 GG (Schutz des Brief-, Post- und Fernmeldegeheimnisses) fordert. Außerdem verstoße § 39 AWG gegen das Übermaßverbot in Form des Grundsatzes der Verhältnismäßigkeit. Schließlich hält es Rheinland-Pfalz für verfassungswidrig, daß für die Behörden der Länder keine hinreichende Zweckbindung für die Verwendung von Erkenntnissen aus solchen Eingriffen besteht.

Ich habe in meiner Stellungnahme zu diesem Verfahren, um die das BVerfG die Datenschutzbeauftragten des Bundes und der Länder im Dezember 1995 gebeten hatte, zwar einerseits Verständnis für die Notwendigkeit derartiger Überwachungsmaßnahmen, andererseits aber auch verfassungsrechtliche Bedenken gegen die Ausgestaltung der Eingriffsbefugnisse geäußert. Dabei habe ich mich im wesentlichen auf die Argumente gestützt, die ich schon während der Vorbereitung der gesetzlichen Regelungen geäußert hatte. So erlaubt § 39 AWG Eingriffe in die durch Artikel 10 GG geschützten Rechte u. a. gegenüber Personen, bei denen Tatsachen die Annahme rechtfertigen, daß sie Straftaten von erheblicher Bedeutung planen. Zum Ausschluß vager, gerichtlich nicht verwertbarer Hinweise aus dem nachrichtendienstlichen Bereich als Auslöser für solche Maßnahmen habe ich in Anlehnung an die Telefonüberwachungsbefugnisse im Strafverfahrensrecht (§ 100 a StPO) gefordert, daß zumindest „**bestimmte**" Tatsachen diese Annahme rechtfertigen müssen. Weitere Zweifel habe ich dazu geäußert, ob der Begriff „**Straftaten von erheblicher Bedeutung**" im gegebenen Zusammenhang dem verfassungsrechtlichen Bestimmtheitsgebot entspricht, da in dem Straftatenkatalog des § 39 AWG z. B. auch solche Delikte enthalten sind, deren Versuch grundsätzlich nur als Ordnungswidrigkeit geahndet wird, die aber dann zur Straftat hochgestuft werden, wenn die Handlung geeignet ist, die auswärtigen Beziehungen der Bundesrepublik Deutschland zu gefährden. Dem Betroffenen solcher Maßnahmen dürfte es kaum möglich sein, immer vorauszusehen, wann eine derartige Gefährdung vorliegt. Auch der unbestimmte Rechtsbegriff des „**Planens**" solcher Handlungen ist problematisch, da damit die grundlegende rechtsstaatliche Klarstellungs- und Garantiefunktion der strafrechtlichen Tatbestandsmäßigkeit weitgehend außer Kraft gesetzt wird. Jeder dieser unbestimmten Rechtsbegriffe begegnet schon verfassungsrechtlichen Bedenken, erst recht ihre Kumulation.

Angreifbar ist die Vorschrift auch unter dem Gesichtspunkt, daß zwar bei Bundesbehörden die aus diesen Maßnahmen erlangten personenbezogenen Daten einer strengen Zweckbindung unterliegen, eine solche Zweckbindung für Landesbehörden aber nicht normiert wurde. Wie bereits in meinem 14. TB (Nr. 26.1) berichtet, wurde eine Zweckbindung für Landesbehörden nicht vorgesehen, um zu vermeiden, daß das Gesetz der Zustimmung des Bundesrates bedurfte. Da gem. § 39 Abs. 4 AWG die Staatsanwaltschaft (i. d. R. eine Landesbehörde) vom Ergebnis der beantragten Maßnahme zu unterrichten ist, könnte sie – mangels Zweckbindung – Erkenntnisse aus Eingriffen in Artikel 10 GG für solche strafrechtliche Ermittlungsverfahren verwenden, bei denen ein solcher Eingriff unverhältnismäßig oder sonst unzulässig wäre.

Bei Redaktionsschluß hatte das Bundesverfassungsgericht über den Antrag auf Normenkontrolle noch nicht entschieden.

Im Herbst 1996 habe ich beim Zollkriminalamt die Informationsverarbeitung im Zusammenhang mit Maßnahmen gemäß § 39 ff. AWG kontrolliert und festgestellt, daß das ZKA mit diesen Eingriffsbefugnissen verantwortungsbewußt umgeht. Die Prüfung hatte das Ziel, die technischen und organisatorischen Verfahrensabläufe kennenzulernen und einen Überblick über Art und Umfang der Maßnahmen zu gewinnen. Anträge auf Genehmigung von Maßnahmen zur Beschränkung des Brief-, Post- und/oder Fernmeldegeheimnisses werden vor allem aufgrund eigener Feststellungen des ZKA (z. B. aus der Marktbeobachtung), Feststellungen anderer Dienststellen der Zollfahndung, aufgrund der Ergebnisse von Außen-

wirtschaftsprüfungen oder aufgrund von Hinweisen sonstiger Behörden, wie z. B. der Nachrichtendienste, vorbereitet. Diese vorläufigen Erkenntnisse werden durch das ZKA daraufhin überprüft, ob Anlaß für Überwachungsmaßnahmen besteht. Sofern nach intensiver und gründlicher Prüfung hinreichende Anfangserkenntnisse für eine Maßnahme nach § 39 AWG angenommen wurden, unterrichtete das ZKA zunächst die jeweils örtlich zuständige Staatsanwaltschaft (§ 39 Abs. 4 Satz 1 AWG). Allen bisher gestellten Anträgen hat das bundesweit zuständige Landgericht Köln entsprochen. Nach Mitteilung des ZKA wurde eine mögliche Eilentscheidung des BMF (§ 40 Abs. 2 Satz 1 AWG), mit der die gerichtliche Entscheidung – vorübergehend – ersetzt werden kann, bisher in keinem einzigen Fall notwendig. Ich habe daher angeregt zu prüfen, ob bei einer künftigen Novellierung des AWG diese Eilkompetenz entfallen kann. Nach Abschluß von Überwachungsmaßnahmen sollten die anläßlich der Kontrollmaßnahmen gewonnenen Unterlagen erst angemessene Zeit nach Benachrichtigung des Betroffenen vernichtet werden, damit sein verfassungsrechtlich gebotenes Auskunftsrecht und auch sein Grundrecht auf Gewährung effektiven, gerichtlichen Rechtsschutzes im Sinne des Artikel 19 Abs. 4 GG nicht leerlaufen. Dieser Anregung hat sich das BMF angeschlossen. Die anläßlich der Überwachungsmaßnahmen gewonnenen Unterlagen sollen künftig erst einen Monat nach Zugang der Benachrichtigung vernichtet werden.

13.2 Bekämpfung der Drogenkriminalität durch Grundstoffüberwachung und Monitoring

Das Grundstoffüberwachungsgesetz vom 7. Oktober 1994 (GÜG, BGBl. I S. 2835) ist am 1. März 1995 in Kraft getreten. Insbesondere mit Blick auf die dramatisch steigende Produktion sog. Designerdrogen ist die Grundstoffüberwachung ein wichtiges Instrument im Kampf gegen die Drogenkriminalität. Die Bundesopiumstelle beim Bundesinstitut für Arzneimittel und Medizinprodukte überwacht die Herstellung und das Inverkehrbringen von Grundstoffen (Precursern), die für die Drogenherstellung geeignet sind. Einfuhr, Ausfuhr und die sog. Durchfuhr von Grundstoffen sowie den Warenverkehr mit diesen Stoffen innerhalb der EU überwachen die Zollbehörden, deren Maßnahmen durch das Zollkriminalamt (ZKA) koordiniert werden. Eine weitere wichtige Rolle kommt der Gemeinsamen Grundstoff-Überwachungs-Stelle des BKA und des ZKA beim BKA (GÜS) zu (15. TB Nr. 25.5). Betroffene Unternehmen sind verpflichtet, Tatsachen, die die Annahme eines Verdachtes der Abzweigung von Grundstoffen zur unerlaubten Herstellung von Betäubungsmitteln rechtfertigen, der GÜS mitzuteilen. Diese veranlaßt die notwendigen Ermittlungen der Zoll- und Polizeibehörden und informiert das Bundesinstitut für Arzneimittel und Medizinprodukte über Sicherstellungen sowie über Abzweigungs- und unerlaubte Methoden der Herstellung. Das Bundesinstitut kann Unternehmen die notwendige Erlaubnis zur Herstellung und zum Inverkehrbringen von Grundstoffen entziehen. Gegenwärtig verfügen knapp 500 deutsche Unternehmen über eine solche Erlaubnis. Die Unternehmen sind verpflichtet, Einfuhr, Ausfuhr und Abgabemengen von Grundstoffen dem Bundesinstitut detailliert mitzuteilen, wobei auf Verlangen auch Name und Anschrift des jeweiligen Erwerbers sowie die Abgabemenge im Einzelfall mitzuteilen sind. Das ZKA ist berechtigt, diese Daten im automatisierten Verfahren abzurufen.

Eine effektive Grundstoffüberwachung setzt insbesondere voraus, daß alle zur Drogenherstellung geeigneten Grundstoffe und deren Ersatzstoffe erkannt und einbezogen werden. Sie ist jedoch nur dann wirklich effektiv, wenn alle Fälle unerlaubter Abzweigung rechtzeitig erkannt und der GÜS mitgeteilt werden. Die Liste der 22 überwachungspflichtigen Grundstoffe (Precurser) wird durch supranationales Recht vorgegeben. Weitere Chemikalien unterliegen der Überwachung im sog. „Monitoring-Verfahren". Grundlage des Monitoring ist nicht das GÜG, sondern eine Vereinbarung mit dem Verband der Chemischen Industrie. Die Regelung sieht u. a. die Meldung verdächtiger Bestellungen an die GÜS vor.

BKA, ZKA und Bundesopiumstelle verfolgen die Entwicklung neuer synthetischer Drogen, von Precursern und Pre-Precursern (Grundstoffen für die Gewinnung von Grundstoffen) sowie die Verwendung von Ersatzstoffen sehr aufmerksam, um ggf. eine Ausweitung der Erlaubnispflicht anzuregen. Eine verläßliche Bewertung des „Meldeverhaltens" im Rahmen der Grundstoffüberwachung und des Monitoring liegt mir nicht vor. Mitarbeiter der GÜS haben darauf hingewiesen, daß die meisten Unternehmen und nicht nur die großen deutschen Chemiehersteller bestrebt seien, Abzweigungen rechtzeitig vorzubeugen und – im Verdachtsfall – die GÜS frühzeitig zu informieren.

Die gesetzlichen Instrumente des GÜG und die freiwillige Zusammenarbeit im Rahmen des Monitoring sollen durch weitere, vertragliche Regelungen ergänzt werden. Der Entwurf einer Vereinbarung zwischen dem Verband der Deutschen Chemischen Industrie (VCI) will die Zusammenarbeit bei der Bekämpfung der Abzweigung von Chemikalien verstärken, die für die unerlaubte Herstellung von Betäubungsmitteln mißbraucht werden könnten. Die geplante Vereinbarung sieht u. a. vor, daß die Industrieunternehmen ihre Sachkenntnis über mögliche Vorläufersubstanzen zur illegalen Rauschgiftherstellung den Zoll- und Polizeibehörden zugänglich machen. Die Zoll- und Polizeibehörden sollen Methoden der Abzweigung und illegalen Drogenherstellung analysieren, den VCI und seine Mitgliedsunternehmen informieren und – soweit erforderlich – auf Schwachstellen hinweisen. Dieser Maßnahmenkatalog würde die Instrumente des GÜG und des bereits seit einigen Jahren praktizierten Monitoring in sinnvoller Weise ergänzen. Die Verpflichtung zur Mitteilung verdächtiger Bestellungen und aller in diesem Zusammenhang relevanten Umstände ist auch in dieser Vereinbarung vorgesehen. Da die Vereinbarung mit dem VCI, also nicht unmittelbar mit einzelnen Mitgliedsunternehmen geschlossen werden soll, wird damit keine unmittelbare rechtliche Verpflichtung der Unternehmen begründet, Zoll- und Polizei in der beschriebenen Weise zu unterstützen. Die Ver-

einbarung dürfte jedoch einen gewissen „Konformitätsdruck" auslösen, der letztlich zur Umsetzung der vertraglichen Maßnahmen führen dürfte.

Diese – eher „moralische" als unmittelbar rechtlich verbindliche – Verpflichtung der Mitgliedsunternehmen des VCI ist aus meiner Sicht insoweit unbedenklich, als gesetzliche Regelungen für die mit der Vereinbarung bezweckte Datenübermittlung und -verarbeitung nicht geboten sind und die Regelungszuständigkeit von Bundestag und Bundesrat daher nicht umgangen wird. Die Frage des parlamentarischen „Regelungsvorbehaltes" stellt sich aber dann, wenn die Chemieunternehmen der GÜS nicht nur verdächtige Bestellungen mitteilen sollen, sondern darüber hinaus alle sonstigen Umstände, die für die Erforschung eines Verdachts von Bedeutung sein können. Ob damit über die Verpflichtung nach § 4 Abs. 1 Nr. 3 GÜG hinaus durch eine „gesetzesvertretende" vertragliche Regelung und insofern „auf Umwegen" weitergehende Verpflichtungen begründet werden sollen, bedarf intensiver Prüfung. Jedenfalls sind Verpflichtungen Privater zur Mitwirkung bei der Strafverfolgung und der Verhütung von Straftaten insbesondere dann klar und deutlich durch Gesetz zu regeln, wenn diese dabei zur Übermittlung personenbezogener Daten Dritter an staatliche Stellen verpflichtet werden sollen.

Das BMF hat mir Ende 1996 den Entwurf einer Errichtungsanordnung für ein DV-Verfahren zur Grundstoffüberwachung übersandt, mit dem dem ZKA u. a. Recherchen für Überwachungs- und Ermittlungszwecke, die Erkennung spezifischer Verfahrensweisen, die Verknüpfung von Erkenntnissen aus nationalen und internationalen Quellen sowie die Erstellung spezifischer Lagebilder und Statistiken ermöglicht werden soll.

13.3 Rechtsverordnung über die Übermittlung von Daten durch das Zollkriminalamt gemäß § 5a Abs. 2 des Finanzverwaltungsgesetzes

Bei Errichtung des ZKA als Reaktion auf illegale Rüstungs- bzw. Technologieexporte (s. o. Nrn. 13.1 und 13.2) bestand Einvernehmen, für die Aufgaben und Befugnisse eine bereichsspezifische Regelung durch ein ZKA-Gesetz zu schaffen; bis zu dessen Inkrafttreten gilt für das ZKA bei der Verarbeitung personenbezogener Daten das BDSG. Nach § 5a Abs. 1 Nr. 2 FVG (BGBl. 1992 I S. 1222) kann das Amt im Rahmen seiner Mitwirkung bei der Überwachung des Wirtschaftsverkehrs mit dem Ausland anderen Behörden unter bestimmten Voraussetzungen über ihm vorliegende Erkenntnisse berichten. Der Kreis der Empfänger ist in einer gemäß § 5a Abs. 2 FVG vom BMF zu erlassenden Rechtsverordnung festzulegen. Das BMF hat bereits 1992 einen ersten Entwurf dieser Rechtsverordnung den Ressorts und mir übersandt. Dieser stieß wegen des großen Empfängerkreises (mehr als 40 Behörden) sowie einer Öffnungsklausel für weitere Empfänger auf breite Ablehnung. Mittlerweile ist zwar der Kreis der potentiellen Datenempfänger erheblich reduziert worden, das BMF beharrt jedoch auf einer Öffnungsklausel. Darüber hinaus gibt bereits der Wortlaut der Regelungen zu Zweifeln Anlaß, ob auch die Nachrichtendienste als Datenempfänger in die Rechtsverordnung aufgenommen werden sollen. Unbestritten können illegale Technologietransfers bzw. Waffenexporte auch einen nachrichtendienstlichen Hintergrund haben. Vor dem Hintergrund der Entstehungsgeschichte des Gesetzes vertrete ich indessen die Auffassung, daß der Gesetzgeber nicht ausschließen wollte, Erkenntnisse mit personenbezogenen Daten über illegalen Technologietransfer unter bestimmten Voraussetzungen zwar auch dem BfV und dem BND zukommen zu lassen, nicht jedoch dem MAD. Dabei sehe ich die Regelung in § 5a Abs. 2 i.V. m. Abs. 1 Nr. 2 FVG lediglich als Aufgabenbeschreibung an, während sich die Befugnis zur Übermittlung von personenbezogenen Daten aus den Dienstegesetzen, also dem BVerfSchG und dem BND-Gesetz, ergibt. Auch diese Frage muß jedoch noch abschließend geklärt werden.

Da sich nach Informationen des BMF die Vorlage eines ZKA-Gesetzes weiter verzögern wird, halte ich den Erlaß der Rechtsverordnung § 5a Abs. 2 FVG für umso dringlicher.

13.4 Internationales

Im Berichtszeitraum wurden zahlreiche Verträge der Europäischen Union mit amerikanischen und asiatischen Staaten vorbereitet, um die internationale Zusammenarbeit bei der Bekämpfung der illegalen Verbreitung von Grundstoffen zu verbessern. So wurden 1995 Verträge der EU mit Bolivien, Ecuador, Kolumbien, Peru und Venezuela unterzeichnet.

Die Vereinbarung zwischen der EU und den USA wird voraussichtlich im Frühjahr 1997 paraphiert werden. Dieser – hier exemplarisch vorgestellte – Entwurf sieht u. a. gegenseitige Informationen bei Verdacht auf rechtswidrige Abzweigung von Precursern und die Zulassung bestimmter Grundstoffexporte nur mit Zustimmung des Empfängerlandes vor. Transporte von Grundstoffen sind zu unterbinden, sofern nach Auffassung einer Vertragspartei vernünftigerweise Grund zu der Annahme einer Abzweigung vorliegt. Geregelt wird nicht nur der bilaterale Grundstoffhandel der Vertragsparteien, sondern auch der Export in Drittstaaten, die nicht am Vertrag beteiligt sind. Mit der „pre-shipment consultation" verpflichten sich die Vertragsparteien zur Abstimmung vor der Ausfuhr von Grundstoffen in Drittstaaten, sofern der Verdacht illegaler Verwendung der Chemikalien besteht. Im Rahmen der Konsultation sind die Vertragspartner zur Abfrage eigener Dateien und anderer Informationsquellen und zur Übermittlung von Erkenntnissen an den anfragenden Konsultationspartner verpflichtet. Vor Zulassung des fraglichen Exports ist der konsultierende Vertragspartner verpflichtet, die zuständige Behörde des konsultierten Vertragsstaates über die getroffene Entscheidung zu informieren. Unabhängig von Einzelfällen sollen Informationen auch zu solchen Chemikalien ausgetauscht werden, die (noch) nicht als Grundstoffe definiert sind, jedoch häufig zur Drogenherstellung verwendet werden.

Der Umgang mit besonders schützenswerten personenbezogenen Daten – etwa bei einer amerikanischen Zollbehörde, die diese Daten anläßlich der pre-shipment consultation ohne Wissen und Mitwirkung eines deutschen Grundstoffexporteurs erhält – bedarf einer sorgfältigen Regelung. Der Entwurf sieht insoweit die Gewährleistung eines gegenseitigen Schutzniveaus vor. Dabei sollen – auf der Grundlage der Datenschutzstandards der Vertragsparteien EU und USA – auch nationale, unter Umständen sogar höhere Datenschutzstandards der einzelnen Mitgliedstaaten der Europäischen Union zur Geltung kommen. Ich hätte es begrüßt, wenn die vorrangige Anwendung hoher Standards des nationalen Datenschutzrechts des übermittelnden Staates in der Vereinbarung noch deutlicher niedergelegt worden wäre.

Der Entwurf sieht darüber hinaus vor, daß übermittelte Informationen grundsätzlich nur für die Zwecke des Vertrages genutzt werden dürfen. Ist eine Zweckänderung im Empfängerstaat beabsichtigt, ist dieser verpflichtet, zuvor um schriftliche Einwilligung des übermittelnden Staates zu ersuchen. Die Einrichtung gemeinsam genutzter, neuer Datenbanken durch die EU und die USA ist nicht beabsichtigt.

Die für die Grundstoffüberwachung durch die EU-Mitgliedstaaten eingerichtete Datenbank „Prexco" existiert bereits seit einigen Jahren in Brüssel. Dieses System war bisher als „Sachdatenbank" ohne personenbezogene Daten konzipiert und enthielt insbesondere Informationen zur Zuordnung und Bestimmung von Chemikalien sowie Export-Verfahrensinformationen. Gegenwärtig wird durch die Kommission geprüft, ob weitere Funktionen hinzukommen sollen. Vertreter der zuständigen Generaldirektion der Kommission haben im Frühjahr und Sommer 1996 in den Mitgliedstaaten Vorschläge und Anregungen zur Erweiterung des Systems gesammelt. Dabei bin ich frühzeitig beteiligt worden. Ein Konzept für den weiteren Ausbau dieser Datenbank liegt aber noch nicht vor.

13.4.1 Internationale Zollinformationssyteme im Rahmen der EU

Bereits im 14. (Nr. 26.3) wie auch im 15. Tätigkeitsbericht (Nr. 25.2) hatte ich über die geplanten Zollinformationssysteme der EU-Mitgliedstaaten und der EU selbst berichtet. Bedauerlicherweise wird für beide Datensammlungen der Begriff Zollinformationssystem – ZIS – verwendet, obwohl es sich um zwei Systeme mit unterschiedlichen Rechtsgrundlagen und Zweckbestimmungen handelt. Die Konvention für das Zollinformationssytem der Mitgliedstaaten wurde ebenso wie das EUROPOL-Übereinkommen am 26. Juli 1995 in Brüssel unterzeichnet. Die Arbeiten am Entwurf des nach Artikel 59 Abs. 2 GG notwendigen Vertragsgesetzes werden voraussichtlich im Laufe des Jahres 1997 aufgenommen werden.

Die neue EG Amtshilfe-Verordnung, die als Rechtsgrundlage für das EG-Zollinformationssystem – EG-ZIS – dienen soll, wurde bislang nicht verabschiedet.

13.4.2 Verstärkte Zusammenarbeit der nationalen Zollverwaltungen auf europäischer Ebene – „Neapel II" –

Mit der Verwirklichung des Europäischen Binnenmarktes soll auch die Zusammenarbeit der europäischen Zollverwaltungen intensiviert werden (vgl. 14. TB Nr. 26.3), die bisher auf dem Neapeler Übereinkommen vom 7. September 1967 beruht. Ein erster Schritt hierzu war die Unterzeichnung der ZIS-Konvention am 26. Juli 1995 (s. o. Nr. 13.4.1). Derzeit wird im Rat ein Übereinkommen über die gegenseitige Unterstützung der Zollverwaltungen („Neapel II") beraten, das die Zusammenarbeit der Zollverwaltungen in der Europäischen Union im Hinblick auf die Aufklärung von Zuwiderhandlungen gegen nationale Zollvorschriften und die Verfolgung von Zuwiderhandlungen gegen gemeinschaftliche und nationale Zollvorschriften weiter verbessern soll. Regelungen der Rechtshilfe in Strafsachen sollen durch das Übereinkommen nicht berührt werden. Der Entwurf sieht die Einrichtung zentraler Koordinierungsstellen in jedem Mitgliedstaat vor, die alle Anträge auf gegenseitige Amtshilfe entgegennehmen und die Koordinierung der Maßnahmen sicherstellen sollen. Die unmittelbare Zusammenarbeit zwischen den nachgeordneten Zollbehörden der Mitgliedstaaten, insbesondere in dringenden Fällen, bleibt weiterhin möglich. Vorgesehen ist der Einsatz von Verbindungsbeamten, die unter anderem den Informationsaustausch zwischen den Mitgliedstaaten fördern und beschleunigen, Ermittlungen unterstützen, soweit diese Bezüge zu ihrem Heimatstaat haben, und das Gastland bei der Vorbereitung und Durchführung von grenzüberschreitenden Operationen beraten und unterstützen. Die Einrichtung neuer, gemeinsam genutzter DV-Systeme ist nicht vorgesehen. Den Zollbehörden der EU-Mitgliedstaaten soll die Möglichkeit zur grenzüberschreitenden Nacheile und Observation eingeräumt werden, wie sie für Polizeivollzugsbeamte der Schengen-Staaten nach dem SDÜ bereits möglich ist.

Ein Novum gegenüber dem Instrumentarium des SDÜ stellt die Zulässigkeit der sogenannten kontrollierten Lieferung sowie der grenzüberschreitende Einsatz verdeckter Ermittler dar. Die Datenerhebung durch verdeckte Ermittlungen greift besonders tief in das Persönlichkeitsrecht ein und erfordert deshalb eine besonders sorgfältige und gründliche Regelung. Aus datenschutzrechtlicher Sicht bedarf der Einsatz verdeckter Ermittler grundsätzlich der richterlichen Anordnung und sollte nur als „ultima ratio" zugelassen werden, wenn die Sachverhaltsaufklärung andernfalls wesentlich erschwert oder unmöglich wäre. Der Entwurf knüpft dabei an die Voraussetzungen des nationalen Rechts an (Artikel 21 Abs. 3). Das deutsche Strafprozeßrecht ermöglicht gegenwärtig den Einsatz verdeckter Ermittler zur Aufklärung von Zolldelikten nur in beschränktem Umfang. Nicht erst bei einer Umsetzung des Übereinkommens in das nationale Recht sollte insoweit eine restriktive Linie verfolgt und insbesondere der Deliktskatalog des Entwurfs kritisch überprüft werden, damit der Einsatz verdeckter Ermittler auf Fälle der Schwerkriminalität beschränkt bleibt. Einer „Sogwirkung" unangemessen weiter zwischenstaatlicher Regelungen,

die zu einer Aufweichung sachgerechter und ausgewogener nationaler Vorschriften führen könnte, ist vorzubeugen. Aus datenschutzrechtlicher Sicht für wünschenswert halte ich ferner die ausdrückliche Verpflichtung zur Benachrichtigung des Betroffenen nach Abschluß solcher Maßnahmen.

Unerläßlich ist ferner die Gewährleistung eines hohen Standards auch beim sog. konventionellen Datenaustausch. Insbesondere die Garantie des Auskunftsrechts, die Verpflichtung der Zollbehörden zur Berichtigung und Löschung unrichtiger Daten und die Verpflichtung der Mitgliedstaaten zu effektiver datenschutzrechtlicher Kontrolle halte ich – wie auch die übrigen Garantien und Verpflichtungen des Artikels 25 des Entwurfs – für unabdingbar.

13.5 INZOLL

INZOLL ist das Informations- und Auskunftssystem über Straftaten und Ordnungswidrigkeiten (OWi) im Zuständigkeitsbereich der Zollverwaltung. In dem System werden primär personenbezogene Daten von ermittelten Tatverdächtigen sowie Sachverhalts- und Firmendaten erfaßt. Die Datei besteht seit 1980 und umfaßte Ende 1996 ca. 943 100 Sachverhalts- und ca. 528 200 Personen-/Firmendatensätze.

Das BMF hat mir im Berichtszeitraum auf meine Bitte den Entwurf des Dateistatuts für INZOLL übersandt. Diese Datei wird seit Jahren ohne ausreichende Rechtsgrundlage betrieben. Ein Rückgriff auf die allgemeinen Regelungen des BDSG als Befugnisnorm für die Datenverarbeitung ist 13 Jahre nach der Entscheidung des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 kaum noch vertretbar. Das BMF hat zwar einen Arbeitsentwurf zu einem ZKA-Gesetz erstellt, dieser soll aber erst nach Verabschiedung des in parlamentarischer Beratung befindlichen Bundeskriminalamtgesetz-Entwurfs (vgl. Nr. 11.1) auf den Weg der Gesetzgebung gebracht werden.

Nach dem Entwurf des Dateistatuts haben das Zollkriminalamt, die Zollfahndungsdienststellen, die Zoll- und Verbrauchssteuerabteilungen der Oberfinanzdirektionen (OFD), die Straf- und Bußgeldstellen der Hauptzollämter sowie das Fachaufsichtsreferat im BMF Zugriff auf diese Datei. Letzteres habe ich kritisiert. Das BMF vertritt die Meinung, daß die direkte Abrufbarkeit der INZOLL-Daten für Zwecke der Fach- und Geschäftsaufsicht über die Zollfahndungsbehörden erforderlich sei, um den Einsatz der Kräfte bei Bedarf steuern zu können und eine einheitliche Aufgabenerledigung sicherzustellen. Darüber hinaus werde der Online-Anschluß benötigt für eine schnelle Unterrichtung der Hausleitung des BMF in konkreten Ermittlungsverfahren.

Der Datenkatalog von INZOLL ist nach meiner Überzeugung jedoch nicht geeignet, zuverlässige und umfassende Angaben über diese Zwecke zu vermitteln. Im übrigen halte ich eine Zugriffsmöglichkeit des für die Fachaufsicht zuständigen Referates im BMF auf sämtliche Datensätze der Datei INZOLL für nicht erforderlich, da die Speicherung der personenbezogenen Daten primär dazu dient, Ermittlungsansätze zu liefern und eingeleitete Strafverfahren zu dokumentieren. Allenfalls wäre ein Zugriff des BMF auf die Sachverhaltsdaten – ohne Personenbezug – vertretbar.

In meiner Stellungnahme zum Entwurf des Dateistatuts habe ich ferner bemängelt, daß von den Zollfahndungsbehörden eingeleitete OWi-Verfahren sowie solche ohne Mitwirkung des Zollfahndungsdienstes, die von den OFD und Hauptzollämtern eingeleitet worden sind, in INZOLL erfaßt werden. Dies bedeutet, daß ein Nachweis aller von der Zollverwaltung eingeleiteten OWi-Verfahrens mittels INZOLL geschaffen wurde. Eine solche zentrale Datei eingeleiteter OWi-Verfahren ist in der Bundesrepublik Deutschland einzigartig und verstärkt meine Bedenken, zumal es sich nicht um Strafverfahren, sondern lediglich um Bußgeldverfahren handelt. Ich verkenne nicht, daß es beispielsweise gerade im Bereich des Außenwirtschaftsrechts OWi-Verfahren von erheblicher Bedeutung geben kann, denen im Einzelfall eine gravierende Rechtsverletzung zugrunde liegt. Diese unreflektiert in einer Datei zu erfassen, wäre allenfalls hinnehmbar, wenn eine sachgerechte Differenzierung bei der Speicherung von OWi-Verfahren erreicht werden kann.

Nach dem Entwurf des Dateistatuts werden in INZOLL auch Amtshilfeersuchen ausländischer Behörden erfaßt. Die Erforderlichkeit der – personenbezogenen – Datenspeicherung ist bereits wegen fehlender Rechtsgrundlage nicht zulässig. Die bisherige Praxis krankt auch daran, daß es grundsätzlich keine Rückmeldung der ersuchenden ausländischen Behörden über den Verfahrensausgang gibt. Dies wiederum hat zur Folge, daß die personenbezogenen Daten unterschiedslos zehn Jahre lang in INZOLL gespeichert bleiben. Das BMF begründet die Notwendigkeit dieser Datenverarbeitung mit den INZOLL-Richtlinien (Teilziffer 1.1 Abs. 2,4. und 5. Tiret). Auch sei der Informationswert dieser Daten angesichts der Durchlässigkeit der nationalen Grenzen in der EU und der wachsenden Mobilität der Täter genauso hoch einzuschätzen wie der von Daten aus „inländischen" Ermittlungsverfahren. Die Verarbeitung dieser Daten sei deshalb für die rechtmäßige Aufgabenerfüllung des Zollfahndungsdienstes erforderlich. Daneben würden die Sachverhaltsdaten auch zu statistischen Zwecken ausgewertet.

Die Speicherungsdauer personenbezogener Daten in der Datei INZOLL ist im Entwurf des Dateistatuts unzureichend und undifferenziert geregelt. Als allgemeine Löschungsfrist der gespeicherten Daten gilt grundsätzlich zehn Jahre; bei Verfahren, die mit einer Verwarnung abgeschlossen wurden und bei ähnlichen Fällen mit geringem Unrechtsgehalt werden die erfaßten Daten nach drei Jahren gelöscht. Die Frist beginnt am Tag der letzten Verarbeitung und endet mit Ablauf des dritten bzw. zehnten darauffolgenden Kalenderjahres nach Verarbeitung. Besondere Löschungsfristen (sofortige Löschung) sieht der Entwurf des Dateistatuts in Fällen der Abstandnahme, der Verfahrenseinstellung und bei Wegfall der Erforderlichkeit vor. Meine Kritik an diesen Regelungen bezieht sich darauf, daß die Speicherungsdauer nicht an den Tag der letzten Verarbeitung per-

sonenbezogener Daten anknüpfen darf, sondern an den Tag des Ereignisses, das eine Datenspeicherung begründet. Weiterhin sollte die Löschung der gespeicherten Daten nicht am Jahresende, sondern „taggenau" vorgenommen werden. Im übrigen habe ich angeregt, von der grundsätzlichen Speicherungshöchstdauer von zehn bzw. drei Jahren abzusehen und statt dessen individuelle, auf die Lage des Einzelfalls bezogene Wiedervorlagefristen (Aussonderungsprüffristen) vorzusehen.

Das BMF hat in einem Zusatz in dem Entwurf des Dateistatuts bereits kenntlich gemacht, daß die Löschungsfristen derzeit überarbeitet werden.

13.6 Kontrollen bei Zollfahndungsdienststellen

Mehrere Zollfahndungsdienststellen habe ich vor allem mit Blick auf INZOLL beraten und kontrolliert. Im einzelnen habe ich folgendes festgestellt:

- **Speicherungen aufgrund von Amtshilfeersuchen ausländischer Behörden**

  Im Rahmen eines Amtshilfeersuchens wurde eine Zollfahndungszweigstelle von einer österreichischen Finanzbehörde ersucht, Ermittlungen zu führen, weil der Verdacht der Hinterziehung österreichischer Eingangsabgaben durch österreichische Staatsbürger entstanden war. Obwohl sich weder dieser Verdacht noch ein Verstoß gegen deutsche Zollbestimmungen erhärtete, wurde der Sachverhalt in INZOLL für die Dauer von zehn Jahren erfaßt. Auch wurde die dem Sachverhalt zugrunde liegende Akte, aus der der Personenbezug leicht hergestellt werden konnte, zehn Jahre aufbewahrt. Ich halte die Speicherung der Sachverhaltsdaten sowie die Aufbewahrung der zugrunde liegenden Aktenunterlagen in diesen und gleichgelagerten Fällen für nicht zulässig und habe Löschung angeregt. Das BMF lehnt dies unter Hinweis auf die INZOLL-Richtlinien ab und verweist im übrigen darauf, daß keine Anhaltspunkte für die Festsetzung einer kürzeren Speicherungsfrist bekannt seien, da weder der Verfahrensausgang der ersuchten Behörde mitgeteilt wurde, noch die Straf- bzw. Bußgeldnormen angegeben wurden (s. auch Nr. 13.5).

- **Datenspeicherung bei inländischen Amtshilfeersuchen**

  Eine ermittelnde Zollfahndungsdienststelle kann im Rahmen der Amtshilfe eine andere Zollfahndungsbehörde um teilweise Aufgabenerledigung ersuchen. Die ersuchende Stelle erfaßt die Personen- und Sachverhaltsdaten in INZOLL (E-Vorgang), die ersuchte Behörde speichert sodann ihren Vorgang (I-Vorgang) ebenfalls in INZOLL und vergibt eigene Speicherungsfristen (im Regelfall zehn Jahre). Unabhängig von dem bereits oben dargestellten grundsätzlichen Problem der Speicherungsfristen habe ich in meinem Kontrollbericht angeregt zu prüfen, ob überhaupt eine Speicherung von I-Vorgängen in INZOLL erforderlich ist. Dies erscheint bereits deshalb entbehrlich, da keine neuen Sachinformationen gespeichert werden und die von der ersuchten Stelle ermittelten Sachverhalte ohnehin dem originär zuständigen Zollfahndungsamt in Berichtsform übersandt werden. In der Speicherung des I-Vorganges in INZOLL liegt für den Benutzer des Systems kein eigener Informationswert im Sinne der Zweckbestimmung der Datei. Darüber hinaus habe ich bei einer Zollfahndungszweigstelle festgestellt, daß insbesondere zum Jahreswechsel unterschiedliche Aussonderungsprüffristen bestehen können, was sich bei der jetzigen INZOLL-Konzeption dahingehend auswirkt, daß die personenbezogenen Daten – nur aufgrund der Beteiligung einer weiteren Zollfahndungsbehörde am Ermittlungsverfahren – ein Jahr länger gespeichert bleiben können.

- **Speicherung von Daten Heranwachsender**

  Die INZOLL-Richtlinien sehen keine differenzierenden Fristen vor, wenn Daten von Heranwachsenden gespeichert werden müssen, weil ihnen ein Zollvergehen angelastet wird. Die Konsequenzen habe ich anhand eines Falles thematisiert: Ein zwanzigjähriger österreichischer Staatsangehöriger wurde beim Grenzübertritt mit elf Gramm Haschisch angetroffen, das sich in seinem Pkw befand. Nach seinen Angaben bei der Vernehmung stammte das Rauschgift von einer deutschen Anhalterin, die er nicht näher gekannt habe. Das eingeleitete Ermittlungsverfahren gegen ihn wurde nach § 170 Abs. 2 StPO eingestellt. Gleichwohl führte dieser Sachverhalt zu der Speicherung der personenbezogenen Daten für die Dauer von zehn Jahren in INZOLL. Dies habe ich gerügt: Das BMF hat mir zunächst mitgeteilt, die Löschung der personenbezogenen Daten sei versehentlich unterblieben, obwohl sie wegen der Verfahrenseinstellung hätten gelöscht werden müssen. Auf meine Nachfrage, ob sie denn in der Zwischenzeit gelöscht worden seien, erfuhr ich nunmehr vom BMF, daß für die Aussonderung von Akten die „Bestimmungen über Aufbewahren und Aussondern in der Finanzverwaltung" maßgeblich seien. Diese sähen im vorliegenden Fall eine Aussonderungsfrist von zehn Jahren nach Ablauf des Kalenderjahres vor, in dem das Strafverfahren abgeschlossen wurde.

  Das BMF hat auf nochmalige Nachfrage nunmehr mitgeteilt, daß die im dargestelten Einzelfall gespeicherten personenbezogenen Daten gleichwohl gelöscht wurden.

- **Speicherungen aufgrund des Verdachts der Einfuhr von Betäubungsmitteln in geringen Mengen**

  Schon geringste Mengen von Rauschgift führen bei Aufgriffen an der Grenze zur Einleitung eines Ermittlungsverfahrens und somit auch zur Erfassung der personenbezogenen Daten in INZOLL. Die Strafverfahren werden meistens gegen Zahlung einer geringen Geldbuße abgeschlossen. In einem konkreten Fall führte der Aufgriff einer Person, die drei Gramm Haschisch und 0,5 Gramm

Marihuana mit sich führte, zu einer Speicherung Ihrer Daten in INZOLL für zehn Jahre. In solchen Bagatellfällen halte ich eine Datenspeicherung für die Dauer von zehn Jahren für nicht angemessen. Das BMF sieht keine Möglichkeit für die Anwendung einer besonderen – verkürzten – Löschungsfrist aufgrund der Vorläufigkeit von Einstellungen nach § 153a StPO. Im übrigen erhalte die speichernde Stelle nicht immer sachausgangsbezogene Auskünfte von den Justizbehörden. Auf meine Anregung, bei der Datenerfassung kurze Prüffristen (im Sinne von Wiedervorlagefristen) im Hinblick auf eine Aussonderung zu verwenden und diese je nach Erkenntnisstand zu aktualisieren, ist das BMF bisher noch nicht eingegangen.

Auch im vorliegenden Fall hat das BMF eine Löschung des Datensatzes veranlaßt.

– **Speicherung von Bußgeldtatbeständen**

Ordnungswidrigkeitsverfahren werden nach den INZOLL-Richtlinien grundsätzlich für zehn Jahre im System gespeichert. Unabhängig von der generellen Frage der Zulässigkeit der Speicherung ist es jedenfalls nicht sachgerecht und auch nicht verhältnismäßig, unterschiedslos die mit solchen Verfahren zusammenhängenden Daten stets für zehn Jahre in INZOLL zu speichern. Zunächst sah das BMF nach den INZOLL-Richtlinien keine Möglichkeit zu unterscheiden; es hat jedoch angedeutet, bei der Neufassung der Richtlinien solle die Speicherungsdauer entsprechend der Höhe der Geldbuße verkürzt werden. Es sei vorgesehen, bei Geldbußen bis 50 000 DM die Daten für fünf Jahre und bei höheren Geldbußen für zehn Jahre zu speichern. Ich sehe in diesem Vorschlag einen positiven Aspekt und die Bereitschaft des BMF zu einer sachgerechten Lösung. Gegen eine Verallgemeinerung der Speicherungsfristen im Sinne einer einheitlichen Handhabung und aus praktischen Gründen habe ich keine Bedenken. Die zukünftige Regelung sollte jedoch deutlicher zum Ausdruck bringen, daß die Datenspeicherung einzelfallorientiert erfolgt und daher weitere sachgerechte Differenzierungen durchaus angemessen sind.

– **Zollrechtliche Überwachung**

Die zollrechtliche Überwachung ist ein Fahndungsinstrument der Zollfahndungsbehörden, das in einer Polizei-Dienstvorschrift (PDV) geregelt ist. Danach ist bei begründeter Vermutung von Verstößen in den Deliktsbereichen Rauschgift- und Waffenschmuggel die Ausschreibung von Personen oder Fahrzeugen im polizeilichen Informationssystem INPOL möglich. Diese Fahndungsausschreibung schon bei geringem Tatverdacht ist ein gesetzlich nicht geregelter Eingriff in das Persönlichkeitsrecht des Betroffenen. Ich habe daher eine gesetzliche Regelung gefordert, die auch für die zollrechtliche Überwachung konkrete Voraussetzungen festlegt. Das BMF sieht für Letzteres aus Praktikabilitätsgesichtspunkten keine Notwendigkeit. Das Verfahren selbst soll jedoch in dem noch ausstehenden ZKA-Gesetz geregelt werden.

Die Diskussion mit dem BMF über meine Forderungen ist noch nicht abgeschlossen.

14 Verfassungsschutz

14.1 Probleme bei der Anwendung des Bundesverfassungsschutzgesetzes

Nach der Novellierung des Bundesverfassungsschutzgesetzes (BVerfSchG) im Jahre 1990 hat sich dessen Anwendung aus datenschutzrechtlicher Sicht weitgehend eingespielt und normalisiert. Zu einigen wesentlichen Punkten bestehen aber noch erhebliche Differenzen mit dem BMI:

– So bestreitet das BMI, daß es mich vor Erlaß von Dateianordnungen für das BfV für Dateien, die im Zusammenhang mit Maßnahmen nach dem G 10-Gesetz (Eingriffe in das Brief-, Post- und Fernmeldegeheimnis) stehen, anhören muß. Es verweist darauf, daß gem. § 24 Abs. 2 Satz 4 Nr. 1 BDSG personenbezogene Daten, die der Kontrolle durch die G 10 Kommission unterliegen, meiner Kontrolle entzogen seien. Hierbei verkennt das BMI jedoch, daß

  - für Dateien des BfV das Bundesverfassungsschutzgesetz eine eindeutige Regelung trifft und daher als Spezialgesetz dem allgemeineren Bundesdatenschutzgesetz vorgeht;
  - selbst wenn man § 24 Abs. 2 Satz 4 Nr. 1 BDSG anwenden wollte, die Verpflichtung zur Anhörung des Bundesbeauftragten für den Datenschutz hierdurch nicht verdrängt würde, weil § 14 Abs. 1 Satz 2 BVerfSchG keinen ausschließlichen Bezug nur zur datenschutzrechtlichen Kontrolle aufweist, sondern meine Anhörung auch im Hinblick auf meine Beratungskompetenz vorschreibt;
  - § 24 Abs. 2 Satz 4 Nr. 1, 2. Halbsatz BDSG ausdrücklich die Möglichkeit vorsieht, daß mich die G 10 Kommission um Kontrolle der Einhaltung datenschutzrechtlicher Vorschriften ersuchen kann. Da sich danach also auch die G 10 Kommission meiner datenschutzrechtlichen Sachkompetenz bedienen kann, war es nicht der Wille des Gesetzgebers, meine Anhörung vor Erlaß solcher Dateianordnungen auszuschließen. Eine andere Auslegung würde auch bereits dem eindeutigen Gesetzeswortlaut zuwiderlaufen.

Daraus ergibt sich, daß das BMI zu Unrecht mein Anhörungsrecht bestreitet. Es hat mir gleichwohl – wenn auch relativ spät – Gelegenheit zur Stellungnahme zur Dateianordnung über Telefonüberwachungsmaßnahmen nach dem G 10 Gesetz gegeben. Meine Anhörung erfolgte jedoch mit dem ausdrücklichen Hinweis des BMI, diese Anhörung sei gesetzlich nicht vorgeschrieben.

Im übrigen vertrete ich (unter Berufung auf eine Entscheidung des Bundesverfassungsgerichts (BVerfG) aus dem Jahre 1984 (BVerfGE 67, 157,

185) die Auffassung, § 24 Abs. 2 Satz 4 Nr. 1 BDSG schließe von Verfassungs wegen meine Kontrollkompetenz nur insoweit aus, als Vorgänge der Kontrolle der G 10 Kommission unterliegen. Damit keine Kontrollücke entstehen kann, bedeutet dies, daß der Zuständigkeitsausschluß für mich nur insoweit greift, als die G 10 Kommission ihrerseits bereits von ihrem Prüfungsrecht Gebrauch gemacht hat. In diesem letztgenannten Punkt wird meine Auffassung aber sowohl vom Bundeskanzleramt als auch von der G 10 Kommission bestritten. Ich hoffe, daß die für dieses Jahr zu erwartende Entscheidung des BVerfG über drei Verfassungsbeschwerden zum Verbrechensbekämpfungsgesetz (s. u. Nr. 16.1) auch diese Frage klären wird.

- Ein weiteres Problem zwischen BK, BMI, BMVg und mir ist die noch immer offene Frage der Zusammenarbeit der Nachrichtendienste des Bundes mit den Strafverfolgungsbehörden (insbes. Polizeien und Staatsanwaltschaften des Bundes und der Länder). Die derzeit offiziell noch gültigen Zusammenarbeitsrichtlinien in der Fassung vom 23. Juli 1973 sind durch die Gesetze für die Nachrichtendienste (BVerfSchG, MADG und BNDG) von 1990 weitgehend überholt. Ich hatte vorgeschlagen, diese Richtlinien neu zu fassen und hierbei das Trennungsgebot zwischen Polizei und Nachrichtendiensten für die Anwender deutlich hervorzuheben. BK, BMI, BMJ und BMVg waren hingegen in einer Besprechung am 24. Oktober 1995 der Auffassung, in Anbetracht der neuen veränderten Rechtslage seien solche Zusammenarbeitsrichtlinien obsolet, da die Zusammenarbeit ausdrücklich gesetzlich geregelt sei. Auch die Dienste haben nur noch Bedarf für Regelungen im Verhältnis zu den Staatsanwaltschaften gesehen. Eine Hervorhebung des Trennungsgebots wurde, außer von mir, von den Beteiligten nicht für erforderlich gehalten. Ich habe nach wie vor Zweifel, ob in Anbetracht der Rechtslage der völlige Wegfall solcher Richtlinien zweckmäßig ist. Die Zusammenarbeit der Nachrichtendienste erfolgt durch Behördenmitarbeiter mit unterschiedlichem rechtlichem Ausbildungsstand. Daher wären solche Richtlinien gerade für weniger rechtskundige Behördenmitarbeiter eine wichtige Hilfe im ungewohnten Umgang mit den Nachrichtendiensten.

- Nach wie vor ist das BfV nicht bereit, seiner gesetzlichen Verpflichtung nach § 6 Abs. 2 BDSG nachzukommen (vgl. 15. TB Nr. 26.11). Danach wird für Verbunddateien – also Dateien, bei denen mehrere Stellen speicherungsberechtigt sind – vorgeschrieben, daß der Betroffene sich an jede dieser Stellen zwecks Auskunft wenden kann. Die angesprochene Stelle ist gegebenenfalls verpflichtet, das Ersuchen an die speichernde Stelle weiterzuleiten und den Betroffenen zu unterrichten. Die Vorschrift erlaubt den Nachrichtendiensten jedoch, mich an Stelle des Betroffenen zu unterrichten. Nur einige Regelungen des BDSG sind von den Nachrichtendiensten neben ihren Spezialgesetzen noch anzuwenden. Diese Vorschrift ist nach dem BVerfSchG nicht ausgeschlossen. Das BMI vertritt dennoch die Auffassung, die Vorschrift stehe im Zusammenhang mit § 19 BDSG, der die Auskunftserteilung an den Betroffenen regelt und diese Vorschrift finde nach § 27 BVerfSchG keine Anwendung. Daher sei aus Akzessorietätsgründen auch § 6 Abs. 2 BDSG nicht anwendbar. Wenn also ein Betroffener sich zwecks Auskunft an das BfV wendet, und in NADIS gibt es nur eine Speicherung durch eine Landesbehörde, erhält er die zumindest zweideutige Antwort, von ihm seien beim BfV keine Daten erfaßt. Ich kann das Interesse des BfV nachvollziehen zu vermeiden, daß ein Betroffener durch Nachfrage bei einer beliebigen, am Verbundsystem beteiligten Stelle erfahren oder zumindest erahnen kann, ob und von welcher Landesbehörde seine Daten gespeichert wurden. Doch das ist gerade der Sinn dieser Regelung. Im übrigen könnte ein Betroffener aus der bloßen Mitteilung, daß seine Daten von einer bestimmten Landesbehörde in NADIS eingestellt wurden, keine wesentlichen Rückschlüsse auf mögliche Quellen ziehen oder darauf, was konkret über ihn gespeichert ist. Erst recht wären solche Rückschlüsse nicht möglich, wenn das BfV von seinem Recht Gebrauch macht, mich statt des Betroffenen in Kenntnis zu setzen. Obwohl die genannte Regelung sich auch auf § 19 BDSG bezieht, halte ich die Argumentation des BMI nicht für vertretbar, weil es hier nicht um den nach § 27 BVerfSchG ausgeschlossenen Auskunftsanspruch des Betroffenen über Art, Herkunft, Empfänger oder Zweck gespeicherter Daten geht, sondern dem Betroffenen mit § 6 BDSG die Möglichkeit gegeben werden soll zu erfahren, welche Stelle Daten über ihn in einer Verbunddatei gespeichert hat, damit er in die Lage versetzt wird, gegebenenfalls den Rechtsweg zu beschreiten.

- Bereits in meinem 15. TB (Nr. 26.11) habe ich über die Praxis des BfV berichtet, unzulässig gespeicherte Daten eines Betroffenen zu löschen, wenn dieser einen Antrag auf Auskunft über von ihm gespeicherte Daten stellt. Dem Betroffenen wurde dann mitgeteilt, daß keine Daten über ihn gespeichert sind, was nach deren Löschung dann ja auch zutrifft. Soweit Auskunftsanträge durch mich an das BfV gerichtet werden, hat mir die Behörde glaubhaft versichert, daß die Daten erst nach meinem Einverständnis gelöscht würden. Soweit der Betroffene selbst anfragt, setzt sich die bisherige Verfahrensweise fort, selbst wenn der Betroffene vom BfV ausdrücklich den Hinweis erhält, er könne sich an mich wenden. Diese Verfahrensweise halte ich für rechtswidrig.

14.2 BfV will einige Daten unbefristet speichern

Das BfV hat gespeicherte personenbezogene Daten über Bestrebungen gegen die freiheitliche demokratische Grundordnung, gegen Bestand oder Sicherheit des Staates oder gegen Verfassungsorgane bzw. Informationen über gewaltsame Bestrebungen gegen auswärtige Belange der Bundesrepublik Deutschland im Inland (§ 3 Abs. 1 Nr. 1 oder 3 BVerfSchG) grundsätzlich spätestens zehn Jahre nach Speicherung der letzten relevanten Information zu löschen,

wobei nach spätestens fünf Jahren eine erste Überprüfung zu erfolgen hat (§ 12 Abs. 3 BVerfSchG). Eine darüber hinausgehende Speicherung ist nur im Einzelfall auf Anordnung der Leitung des BfV zulässig. Mit dem BMI und dem BfV bin ich unterschiedlicher Auffassung darüber, ob diese Löschungsfristen auch für solche Daten von Betroffenen gelten, zu deren Person selbst keine tatsächlichen Anhaltspunkte für solche Bestrebungen bestehen. Das Ministerium vertritt die Auffassung, daß zwar die beim BfV (gem. § 10 Abs. 1 Nr. 1 BVerfSchG) gespeicherten Daten über Personen, bei denen tatsächliche Anhaltspunkte für solche Bestrebungen nach § 3 Abs. 1 BVerfSchG bestehen, in der Regel nach 10 Jahren zu löschen sind. Daten, die gem. § 10 Abs. 1 Nr. 2 BVerfSchG „nur" zur Erforschung oder Bewertung solcher Bestrebungen erforderlich sind und beispielsweise solche Personen betreffen, die selbst nicht extremismus- oder spionageverdächtig sind, sollen der gesetzlichen Höchstspeicherdauer von 10 Jahren dagegen nicht unterliegen. Denn es handele sich in diesen Fällen nicht um Daten über extremistische Bestrebungen, sondern diese Daten seien nur zu deren Erforschung erforderlich.

Diese schwer nachvollziehbare Rechtsauffassung führt in der Praxis dazu, daß etwa Daten von Extremisten grundsätzlich 10 Jahre nach dem Zeitpunkt der letzten gespeicherten Information zu löschen sind, während die Daten sonstiger Personen den Schutz dieser regelmäßigen Höchstspeicherfrist nicht genießen, es sei denn, es bestünden gleichzeitig tatsächliche Anhaltspunkte für extremistische Bestrebungen zu ihrer Person.

Zwar ist es zutreffend, daß das BfV nach § 12 Abs. 3 Satz 1 BVerfSchG ohnehin spätestens nach fünf Jahren zu prüfen hat, ob gespeicherte Daten zu berichtigen oder zu löschen sind, doch führt das nicht zwangsläufig zur Löschung solcher zur Erforschung und Bewertung erhobener Daten. Ich kann nicht erkennen, warum die Daten von Personen, bei denen tatsächliche Anhaltspunkte für extremistische Bestrebungen bestehen, durch eine solche Praxis besser geschützt sind als die Daten von Personen ohne Anhaltspunkte für eigene extremistische Bestrebungen.

14.3 BfV arbeitet noch überwiegend mit nur vorläufig genehmigten Arbeitsplänen

Nach wie vor sind die Arbeitspläne für die einzelnen Abteilungen des BfV noch nicht vollständig an das Ende 1990 novellierte BVerfSchG angepaßt worden (s. auch 15. TB Nr. 2.6.5). Das BMI hat mir inzwischen zwar weitere Neufassungen zur Stellungnahme übersandt und im Hinblick auf den Beschluß des Deutschen Bundestages vom 5. Februar 1993 (vgl. 14. TB Anlage 1) die Arbeitspläne zunächst vorläufig genehmigt, doch sind noch immer nicht alle Arbeitspläne endgültig genehmigt. Lediglich für die Abteilungen I und V existiert ein endgültiger Arbeitsplan. Abteilung I ist zuständig für zentrale Fachfragen der anderen Abteilungen des BfV, die Abteilung V für sicherheitsgefährdende Bestrebungen von Ausländern. Die übrigen Abteilungen arbeiten nach wie vor mit vorläufig genehmigten Arbeitsplänen (Abteilung II: Rechtextremismus und -terrorismus, Abteilung IV: Spionagebekämpfung, Geheim- und Sabotageschutz). Für die Abteilung III (Linksextremismus und -terrorismus) liegt mir ein überarbeiteter Entwurf vor, den das BMI für genehmigungsreif hält.

Bezüglich dieser Arbeitspläne sind zwischen dem BMI und mir im wesentlichen einige wenige, jedoch gewichtige Punkte strittig, wie z. B. die Frage, ob Daten bestimmter, nicht selbst extremismus- oder spionageverdächtiger Personen auch ohne ihr Wissen oder ihr Einverständnis gespeichert werden dürfen (§ 10 Abs. 1 Nr. 2 BVerfSchG) und, wenn ja, ob für solche Speicherungen die grundsätzlich zu beachtende Höchstspeicherfrist nach § 12 Abs. 3 Satz 2 BVerfSchG gilt (s. auch Nr. 14.2).

Zur Zeit ist nicht absehbar, ob ich mit dem BMI zu einer einvernehmlichen und ausgewogenen Lösung der noch offenen Punkte kommen werde; so habe ich – unter Aufrechterhaltung meiner in diesen Punkten abweichenden Rechtsauffassung – gegen die endgültige Genehmigung des Arbeitsplanes der Abteilung V keine Einwände mehr erhoben, damit das BfV trotz weiterbestehenden Dissenses wenigstens auf der Basis des zuletzt genehmigten Arbeitsplans arbeitet, der gegenüber der früheren Fassung aus Sicht des Datenschutzes immerhin einige Verbesserungen enthält.

14.4 Dateianordnung zu NADIS-PZD

In meinem 15. TB (Nr. 26.6) habe ich über einen Dissens mit dem BMI über den zulässigen Umfang der Speicherung personenbezogener Daten in der Personenzentraldatei des Nachrichtendienstlichen Informationssystems der Verfassungsschutzbehörden – NADIS-PZD – berichtet. Ich hatte damals die Auffassung vertreten, daß – abgesehen von den Personengrunddaten – weitere Zusatzinformationen zum Betroffenen über den nach § 6 Satz 2 BVerfSchG zulässigen Umfang der Datei hinausgehen, da sie zum Auffinden der Akten und der dazu notwendigen Identifizierung von Personen nicht erforderlich sind. Das BMI hatte meiner Auffassung widersprochen, indem es die Speicherung dieser Zusatzinformationen im Rahmen von § 6 Satz 2 BVerfSchG für zulässig hielt.

Da auch nach zahlreichen weiteren Erörterungen mit dem BMI eine Annäherung der Rechtsstandpunkte nicht erzielt werden konnte, habe ich mich beim BfV über die Praxis der Speicherung und Nutzung solcher Zusatzinformationen durch das BfV in der Datei NADIS-PZD informiert. Auch danach hat sich an meiner grundsätzlichen Auffassung nichts geändert, daß die Speicherung der oben genannten Merkmale eines Betroffenen in NADIS-PZD nicht in erster Linie dem Wiederauffinden von Akten und der dazu notwendigen Identifizierung von Personen dient, wie dies § 6 Satz 2 BVerfSchG ausdrücklich vorsieht. Denn es geht nach den mir beim BfV vorgeführten Anwendungsfällen um die Identifizierung von Personen mittels recherchefähiger Suchvorgänge, um damit bestimmte Sachverhalte einer Person zuordnen zu können. Insofern geht der in NADIS-PZD gespeicherte Datenumfang über die in § 6 Satz 2 BVerfSchG genannte Hinweisfunktion der Datei hin-

aus. Eine solche Speicherung wäre allenfalls nach § 6 Satz 8 BVerfSchG zulässig und auch nur für eng umgrenzte Anwendungsgebiete, z. B. zur Aufklärung geheimdienstlicher Tätigkeiten für eine fremde Macht.

Das BfV hat mir aber auch bestimmte Fallbeispiele vorgestellt, nach denen nicht auszuschließen ist, daß diese Daten im Einzelfall auch zum Wiederauffinden von Unterlagen geeignet sein können. Das erweiterte Suchverfahren in NADIS-PZD mittels weiterer Datenarten als den Personengrunddaten war auch schon vor dem Inkrafttreten des neuen Bundesverfassungsschutzgesetzes gängige Praxis. Es ist deshalb nicht davon auszugehen, daß der Gesetzgeber trotz des engen Wortlauts des § 6 Satz 2 BVerfSchG seinerzeit eine Einschränkung des NADIS-PZD-Datensatzes vornehmen wollte.

Ich habe dem BMI in der abschließenden Stellungnahme zum Entwurf der Dateianordnung für die „Personenzentraldatei" mitgeteilt, daß ich meine datenschutzrechtlichen Bedenken gegen die Speicherung bestimmter weiterer Angaben zurückstelle. Dabei habe ich jedoch betont, daß der vorerwähnte Katalog von Zusatzinformationen abschließend sein muß.

14.5 Aufbewahrung von Akten zu Personen des öffentlichen Lebens

Das BfV möchte Akten zu Personen des öffentlichen Lebens sowie zu zeitgeschichtlich bedeutsamen Personen über das zu seiner Aufgabenerfüllung erforderliche Maß hinaus aufbewahren, um sich im Falle eventuell denkbarer späterer Vorwürfe entlasten zu können. Es geht hierbei um Daten eines Personenkreises, die ursprünglich in NADIS-PZD (s. o. Nr. 14.4) aufgrund besonderer Eigenschaften gespeichert waren, inzwischen aber gelöscht wurden. Ich lehne eine solche weitere Aufbewahrung „ins Blaue hinein" ab, soweit keine Anzeichen für solche späteren Vorwürfe erkennbar sind. Mit der Anerkennung einer Aufbewahrung personenbezogener Daten in Akten, ohne daß dies für die laufende Aufgabenerfüllung erforderlich ist, würde ein Präzedenzfall geschaffen, und das BfV erhielte eine Möglichkeit zur Vorratshaltung personenbezogener Daten. Die Mehrzahl der Bundesländer hat in ihren Verfassungsschutzgesetzen ausdrücklich die Vernichtung von Akten vorgesehen, in denen zur Aufgabenerfüllung nicht mehr erforderliche personenbezogene Daten enthalten sind.

Das BMI argumentiert, § 12 BVerfSchG schreibe zwar eine Löschung solcher personenbezogener Daten in Dateien vor, für entsprechende Daten in Akten sei eine Vernichtung aber gerade nicht vorgesehen, da § 13 Abs. 2 BVerfSchG ausdrücklich nur deren Berichtigung und Sperrung regle.

Soweit sich das BMI auf § 13 BVerfSchG beruft, habe ich darauf hingewiesen, daß diese gesetzliche Bestimmung im Lichte der Verfassung auszulegen ist, d. h. eine verfassungsrechtlich unzulässige Vorratsspeicherung nicht zu rechtfertigen vermag.

Bei der Anhörung zu den Arbeitsplänen der einzelnen Abteilungen des BfV (s. o. Nr. 14.3) konnte ich mich mit meiner Auffassung bisher nicht durchsetzen. Soweit das Ministerium auf seiner Auffassung beharrt, sollte die Frage der Vernichtung von Unterlagen in Akten vom Gesetzgeber behandelt werden.

14.6 Kontrollen beim BfV

1995 habe ich beim BfV in der Abteilung III (Linksextremismus/-terrorismus) die Verarbeitung personenbezogener Daten in Zusammenhang mit der Beobachtung einer linksextremistisch beeinflußten Organisation kontrolliert. Das BfV unterscheidet bei seinem Auftrag nicht zwischen extremistischen und extremistisch beeinflußten Organisationen.

Aus NADIS-PZD, dem System, mit dem – ähnlich einem Aktennachweissystem – vorhandene Unterlagen nachgewiesen und gefunden werden können, habe ich zu dieser linksextremistisch beeinflußten Organisation 40 Fälle zufällig ausgewählt und kontrolliert. Von diesen habe ich 10 Fälle zur Löschung empfohlen; das BfV ist dem nachgekommen. Aufgrund dieses Ergebnises habe ich dem BMI empfohlen, den Gesamtbestand der zu dieser Organisation gespeicherten personenbezogenen Daten zu überprüfen. Das BMI hat dies mit der Begründung abgelehnt, daß die zu der Organisation gespeicherten Daten im Rahmen der laufenden Sachbearbeitung regelmäßig auf Erforderlichkeit der weiteren Aufrechterhaltung der Speicherung überprüft werden, so daß eine Sonderaktion nicht erforderlich sei.

Ich habe die Kontrolle auch zum Anlaß genommen, das BMI und das BfV auf folgende Punkte hinzuweisen, die immer wieder zu Problemen führen:

- Konsequente Beachtung der nach dem Bundesverfassungsschutzgesetz vorgesehenen Fristen für die Überprüfung personenbezogener Daten mit dem Ziel der Löschung,
- Berücksichtigung des Lebensalters betroffener Personen bei der Überprüfung (z. B. hohes Lebensalter) zwecks Löschung,
- Berufung auf den Quellenschutz bei Kontrollen mir gegenüber. Diese Berufung sollte nur erfolgen, wenn mit der Einsicht in Unterlagen des BfV eine Quelle namentlich bekannt würde. Denn meine Kontrollen werden hierdurch erschwert. Auch ist dieser Grund für meine kontrollierenden Mitarbeiter nicht immer nachvollziehbar, da sie selbst sicherheitsüberprüft sind. Zu verbleibenden Einzelfällen zum Quellenschutz ist eine handhabbare Lösung gefunden worden.

15 Militärischer Abschirmdienst – MAD – Schleppende Umsetzung datenschutzrechtlicher Regelungen –

Im 15. Tätigkeitsbericht (Nr. 27) hatte ich berichtet, daß sich der MAD in einer Phase der Umorganisation befindet. Seitdem ist die Datenverarbeitung beim MAD kaum vorangekommen, was überwiegend mit der noch laufenden Neuorganisation begründet wurde. So dauerte es von März 1995 bis Mitte Juli 1996, bis der Entwurf einer Dateianordnung für die Perso-

nenzentraldatei des MAD zwischen dem BMVg und mir soweit abgestimmt war, daß gegen den Erlaß der Dateianordnung aus datenschutzrechtlicher Sicht keine Einwände mehr bestanden.

Zum Entwurf der Richtlinien über die Dauer der Speicherung personenbezogener Daten in Dateien des MAD habe ich im Januar 1996 Stellung genommen. Trotz Erinnerung habe ich noch keine Antwort des BMVg erhalten.

Bereits im Mai 1995 hatte ich ein Gespräch mit dem BMVg und dem MAD über Fragen der Zusammenarbeit geführt. Dabei wurde mir zugesichert, nach erfolgter personeller Neuorganisation würden die ausstehenden datenschutzrechtlichen Regelungen zur Durchführung des MAD-Gesetzes vom 20. Dezember 1990 zügig in Angriff genommen. Viel mehr als diese mündlichen Ankündigungen ist aber bisher nicht festzustellen.

16 Bundesnachrichtendienst

16.1 Drei Verfassungsbeschwerden gegen Brief-, Post- bzw. Fernmeldeüberwachung des BND beim Bundesverfassungsgericht anhängig

Im Jahr 1994 wurden das Gesetz zu Artikel 10 GG (G 10) durch das Verbrechensbekämpfungsgesetz (BGBl. I, S. 3186) geändert und die Befugnisse des BND zur Fernmeldeaufklärung erheblich erweitert (vgl. 15. TB Nr. 28.2). Die Prinzipien der Fernmeldeaufklärung – zu denen ich in den vergangenen Jahren immer wieder befragt wurde – sind in der Abbildung 8 und die der Auswertung in der Abbildung 9 dargestellt. Die getroffenen Regelungen hatte ich in Hinblick auf Artikel 10 GG kritisiert, aber nicht grundsätzlich in Abrede gestellt.

Beim Bundesverfassungsgericht sind zwischenzeitlich drei Verfassungsbeschwerden gegen die Befugnisse des BND zur Brief-, Post- und Fernmeldeüberwachung nach dem G 10 anhängig. Davon richten sich zwei Beschwerden schwerpunktmäßig gegen § 3 G 10 im ganzen und eine Beschwerde überwiegend gegen die nach dem Verbrechensbekämpfungsgesetz in § 3 G 10 neu eingefügten Befugnisse. Ich habe nach §§ 94, 77 BVerfGG gegenüber dem Bundesverfassungsgericht zu diesen Verfahren Stellung genommen und im wesentlichen meine bereits im 15. TB dargestellte Position vertreten.

Darüber hinaus habe ich zur Frage der sog. strategischen Kontrolle zur Abwehr der Gefahr eines bewaffneten Angriffs auf die Bundesrepublik Deutschland nach § 3 Abs. 1 Satz 2 Nr. 1 G 10 darauf hingewiesen, daß zwar nach den Grundsätzen, die das Bundesverfassungsgericht in seiner Entscheidung vom 20. Juni 1984 (BVerfGE 67, 157 ff.) aufgestellt hat, eine solche

Abbildung 8

Prinzipien der Fernmeldeaufklärung durch den BND nach § 3 Abs. 1 G 10

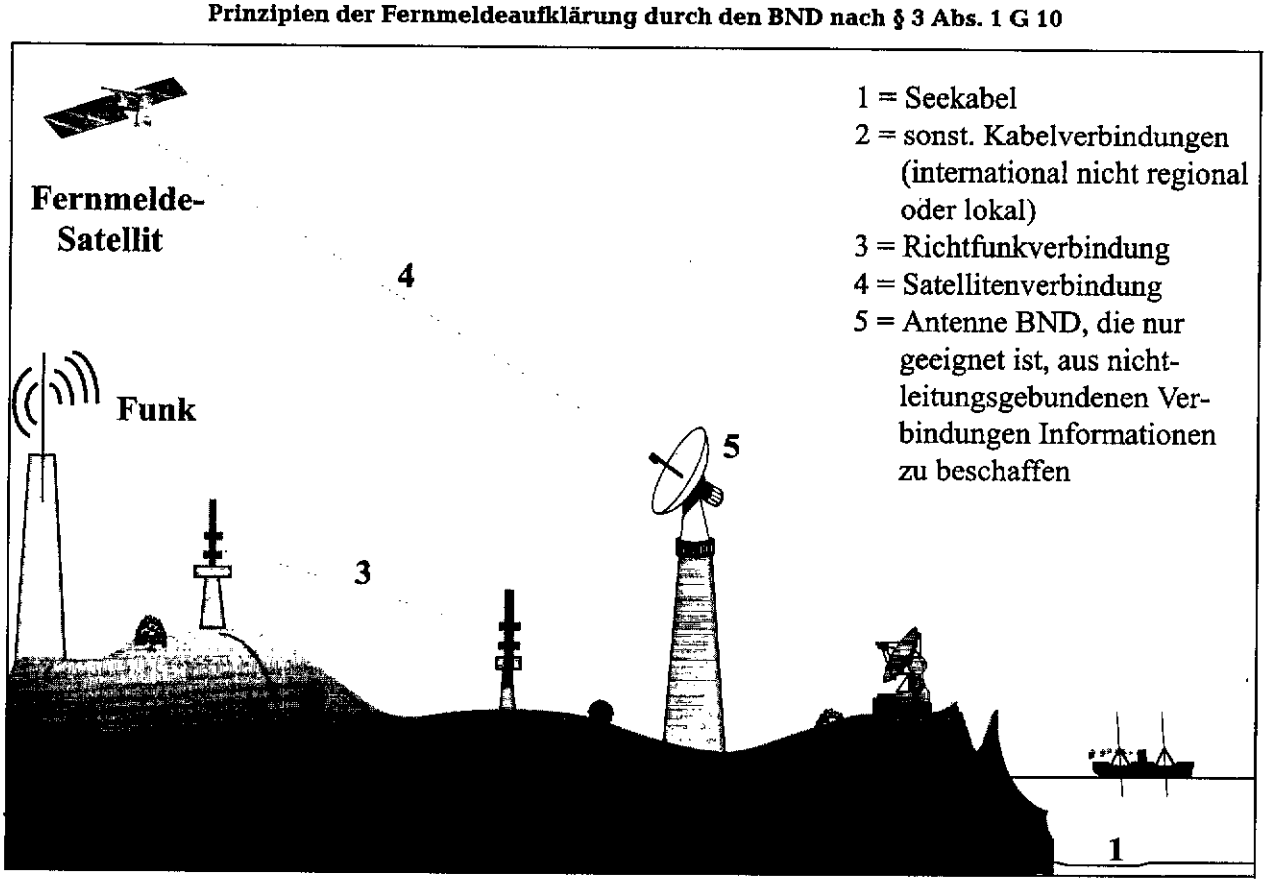
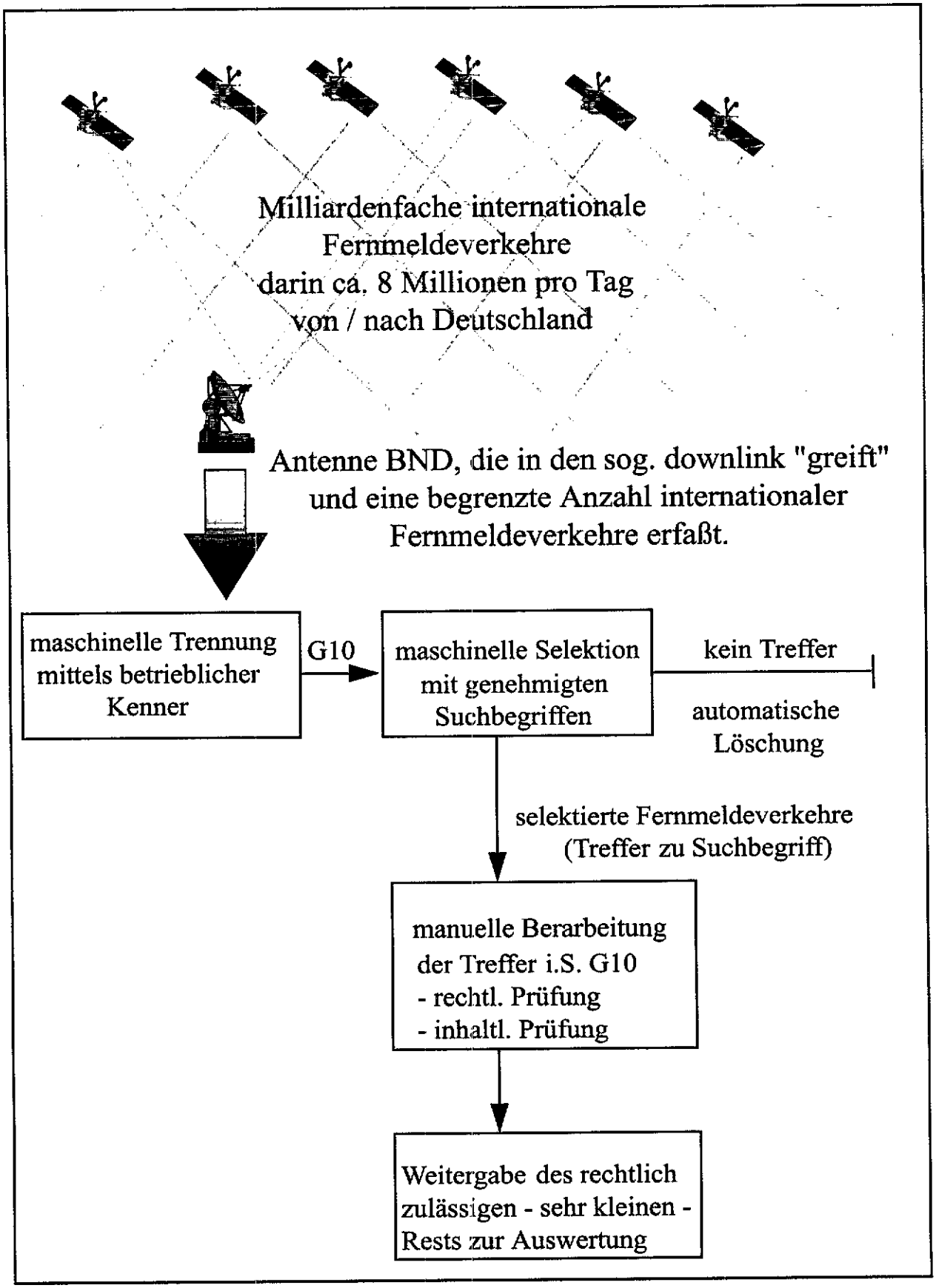


Abbildung 9

Prinzipien der Auswertung der Informationen aus der Fernmeldeaufklärung nach § 3 Abs. 1 G 10



Kontrolle der Post- und Fernmeldeverkehrsbeziehungen heute nicht mehr zulässig wäre, da z. B. der Warschauer Pakt nicht mehr existiert. Die Grundsätze dieser Entscheidung können aber heute nicht mehr uneingeschränkt Anwendung finden, denn inzwischen sind nach Wegfall des Warschauer Paktes neue, z. T. schwer überschaubare Bedrohungspotentiale und Krisenherde (z. B. militanter islamistischer Fundamentalismus) entstanden, die der BND im Sinne § 3 Abs. 1 G 10 – zur Abwehr eines bewaffneten Angriffs auf die Bundesrepublik Deutschland – beobachten können sollte. Auch die technische Entwicklung konnte 1984 so noch nicht vorausgesehen werden. Im Hinblick auf die gesetzlich vorgesehenen verfahrenssichernden Maßnahmen und darauf, daß die strategische Kontrolle nicht dazu dienen soll, Einzelpersonen oder bestimmte Anschlüsse zu erfassen bzw. zu identifizieren, halte ich sie für noch vertretbar. Dabei habe ich jedoch auch deutlich gemacht, daß ich in Anlehnung an die Rechtsprechung des BVerfG neben der Kontrolle durch die G 10 Kommission auch die ergänzende und unterstützende Kontrolle durch eine weitere unabhängige Institution, wie den Bundesbeauftragten für den Datenschutz für erforderlich halte, der personell und materiell in der Lage ist, die Einhaltung der gesetzlichen Einschränkungen auch in komplexen Fällen intensiv zu prüfen.

Als verfassungsrechtlich bedenklich sehe ich im übrigen an, daß dem BND im Rahmen seiner Berichtspflicht an die Bundesregierung gem. §§ 3 Abs. 3 Satz 2 G 10 i.V. m. 12 BNDG eine fast grenzenlose Ermächtigung zur Übermittlung auch personenbezogener Daten zusteht, die aus dem Eingriff in das Grundrecht aus Artikel 10 GG stammen. Nach den genannten Vorschriften könnte die Übermittlung dieser personenbezogenen Daten zur Unterrichtung der Bundesregierung erfolgen, ohne daß sie dort einer Zweckbindung unterliegen.

Eine Entscheidung des BVerfG ist dieses Jahr zu erwarten.

16.2 Innerdienstliche Vorschriften des BND

Der BND hat mich bei mehreren innerdienstlichen Vorschriften zur Umsetzung des BND-Gesetzes und bei Dateianordnungen beteiligt. So habe ich u. a. zu Regelungen zur Personendokumentation einschließlich der Dateianordnung zur zentralen Personendatei, zu den Amtshilferichtlinien, den Richtlinien für die Überprüfung und Speicherung personenbezogener Daten, den Richtlinien über die Berichtigung, Löschung und Sperrung personenbezogener Daten sowie zu zahlreichen als geheim oder vertraulich eingestuften Vorgängen Stellung genommen. Ich begrüße die Verbesserung der Zusammenarbeit mit dem BND. Jedoch sind einige Fragen noch offen. So bestreitet der BND z. B., daß für ihn die Speicherfristen nach § 5 BNDG i.V. m. § 12 Abs. 3 Satz 2 BVerfSchG von höchsten 10 Jahren mit begrenzten Ausnahmemöglichkeiten gelten.

Auch zur Frage, ob Löschungs- bzw. Wiedervorlagefristen ab dem Zeitpunkt des letzten relevanten Ereignisses oder ab der letzten Speicherung zu laufen beginnen, vertritt der BND eine von meiner und den anderen Sicherheitsbehörden abweichende Auffassung, wonach es auf das Datum der letzten Speicherung ankommen soll. Aus Kontrollen ist mir bekannt, daß zwischen Ereignis und Speicherung im Einzelfall mehrere Jahre liegen können. In den entsprechenden Vorschriften macht der BND mittels Fußnote auf meine abweichende Auffassung aufmerksam und verweist darauf, der Deutsche Bundestag werde bei Behandlung meines 15. TB über diese Frage entscheiden.

Der BND hat mir zugesagt, seine Altdatenbestände, die schon seit über einem Jahr hätten überprüft und bereinigt sein müssen, bis Ende 1997 endgültig zu bereinigen.

16.3 Datenschutzrechtliche Kontrollen beim BND

Die Schwerpunkte zweier Kontrollen beim BND, die jeweils den Stand der Informationsverarbeitung beim BND und die Umsetzung des BND-Gesetzes vom 20. Dezember 1990 mit einschlossen, bildeten u. a. das Verfahren der Gruppenauskunft nach § 12 AZRG, soweit der BND Antragsteller war, und eine zentrale Personendokumentation.

Bereits wenige Monate nach Inkrafttreten des neuen Gesetzes über das AZR habe ich beim BND das Verfahren der Einholung von Gruppenauskünften nach § 12, insbesondere Abs. 1 Nr. 3 AZRG kontrolliert. Die Gruppenauskunft war bei der Novellierung des AZRG datenschutzrechtlich besonders umstritten, weil mit einer Anfrage möglicherweise Daten über eine Vielzahl von Ausländern übermittelt werden, also zwangsläufig auch von solchen, die vom Grund für die Anfrage nicht unmittelbar betroffen sind. Zum Zeitpunkt der Kontrolle lag die Anzahl der Gruppenauskunftsersuchen des BND noch bei weniger als 20. Auch im weiteren Verlauf des Berichtszeitraums hat sich gezeigt, daß von diesem rasterähnlichen Instrumentarium nicht in unvertretbarer Weise Gebrauch gemacht wird. Gemäß § 12 Abs. 3 AZRG bin ich über die erteilten Auskünfte an die berechtigten Behörden zu unterrichten, was in der Regel monatlich erfolgt.

Ich habe aber mehrere Verstöße gegen § 12 Abs. 2 AZRG festgestellt. So waren die Ersuchen nicht jeweils vom Leiter des BND gebilligt, der seine Befugnis vielmehr delegiert hatte. Dies ist mittlerweile nicht mehr der Fall. Ferner waren die Ersuchen nicht ausreichend schriftlich begründet, was der Registerbehörde keine angemessene Beurteilung der Zulässigkeit des Ersuchens im Einzelfall ermöglichte. Zwar habe ich Verständnis für Geheimschutzerwägungen des BND, doch ist nunmehr in den Verwaltungsvorschriften zu dem AZR-Gesetz (AZR-VV) geregelt, daß die Ersuchen schriftlich zu begründen sind. Der BND kommt mittlerweile den gesetzlichen Anforderungen nach, wovon ich mich auch beim Bundesverwaltungsamt als Registerbehörde überzeugen konnte. Schließlich habe ich bemängelt, daß die Ersuchen im Hinblick auf die Zielpersonen nicht hinreichend eingegrenzt waren. Dies führte dazu, daß im Einzelfall wesentlich mehr Daten übermittelt wurden, als für den spezifischen Anfragegrund erforderlich waren.

Weiterhin bestehen Differenzen zwischen dem BND und mir über den Kreis der gesuchten Zielpersonen. Während der BND das Instrument der Gruppenauskunft umfassend zur Erfüllung seiner Aufgaben einschließlich der Anknüpfung nachrichtendienstlicher Verbindungen nutzen will, vertrete ich unter Berufung auf den Wortlaut des § 12 Abs. 1 Nr. 3 AZRG die Auffassung, daß von der Gruppenauskunft im Hinblick auf § 2 Abs. 1 Nr. 4 BND-Gesetz nur restriktiv Gebrauch gemacht werden soll. Diese Differenzen sind noch nicht ausgeräumt.

Schließlich habe ich erstmals eine zentrale Personendokumentation beim BND anhand zufällig ausgewählter Datensätze kontrolliert. Dabei hat sich bestätigt, daß der BND mit der sog. Altdateienbereinigung noch erheblich im Rückstand ist. So waren beispielsweise noch Daten von über 90jährigen Betroffenen gespeichert. Hier ist mir der nachrichtendienstliche Erkenntniswert dieser Speicherungen nicht nachvollziehbar.

Die zufällig ausgewählten Daten betrafen auch BND-Bedienstete und damit auch deren Personal- und Sicherheitsakten. Bei deren Kontrolle wurde ich erheblich behindert, weil der BND mir nur diejenigen Datensätze und Akten von aktiven und ehemaligen Bediensteten vorlegen wollte, die – nach einem speziellen Anschreiben durch den Dienst – ausdrücklich in die Einsichtnahme eingewilligt hatten. Ich habe dieses Verhalten als Verstoß gegen § 24 BDSG förmlich beanstandet, zumal auch kein wirksamer Widerspruch der Betroffenen vorgelegen hatte. Dieser ist im übrigen nach § 24 Abs. 2 BDSG mir gegenüber zu erklären. Mittlerweile ist sichergestellt, daß der BND künftig entsprechend dieser Vorgaben verfahren wird. Bei der Durchsicht der vorgelegten restlichen Sicherheitsakten habe ich festgestellt, daß die Unterlagen zum Teil wesentlich mehr Daten enthielten als nach dem Sicherheitsüberprüfungsgesetz von 1994 zulässig ist. Über die Frage einer retrograden Datenbereinigung stehe ich mit dem BND noch in der Diskussion.

17 Sicherheitsüberprüfung

17.1 Umsetzung des Sicherheitsüberprüfungsgesetzes

Nach Inkrafttreten des SÜG vom 20. April 1994 (BGBl. I S. 867) haben sich Petentinnen darüber beschwert, daß sie aufgrund der sicherheitserheblichen Tätigkeit des Ehemannes oder Lebenspartners in die Sicherheitsüberprüfung einbezogen wurden. Wenn Personen, die Zugang zu Verschlußsachen erhalten sollen, einer erweiterten Sicherheitsüberprüfung oder einer Sicherheitsüberprüfung mit Sicherheitsermittlungen unterzogen werden, soll der volljährige Ehegatte oder Partner, mit dem der Betroffene in eheähnlicher Gemeinschaft lebt (Lebenspartner), in die Sicherheitsüberprüfung einbezogen werden (§ 2 Abs. 2 SÜG). Bestehen Sicherheitsrisiken bezüglich des Ehegatten oder des Lebenspartners, so können sich diese aufgrund der engen persönlichen Beziehung auf denjenigen auswirken, der die sicherheitserhebliche Tätigkeit übernehmen soll. Somit wird auch zu dem Ehe- oder Lebenspartner bei den Nachrichtendiensten, Polizeibehörden und in bestimmten Fällen auch beim Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR nachgefragt, ob dort Erkenntnisse vorliegen, die für die Sicherheitsüberprüfung relevant sein können. Für den Ehegatten oder Lebenspartner ist die Einbeziehung in die Überprüfung ein erheblicher Eingriff in sein Recht auf informationelle Selbstbestimmung. Nach dem Gesetz darf die Einbeziehung nur mit seiner Zustimmung erfolgen. Die Verweigerung der Zustimmung durch den Ehegatten oder den Lebenspartner hat jedoch für denjenigen, der wegen zukünftigen Zugangs zu Verschlußsachen sicherheitsüberprüft wird, erhebliche Folgen. Kann z. B. die Sicherheitsüberprüfung wegen der Verweigerung nicht abgeschlossen werden, so kann dies dazu führen, daß der Betroffene nicht oder nicht weiterhin in einem sicherheitsempfindlichen Bereich beschäftigt werden kann.

Der Petitionsausschuß des Deutschen Bundestages hat mich zu dem Fall einer Petentin, die die Zustimmung zur Einbeziehung in die Sicherheitsüberprüfung verweigert hatte, um Stellungnahme gebeten, ob die Entscheidung des BMVg, die Sicherheitsüberprüfung eines Beamten deswegen nicht fortzuführen, das Recht der Petentin auf informationelle Selbstbestimmung nicht unverhältnismäßig beeinträchtige. Ich habe gegenüber dem Petitionsausschuß dargelegt, daß das BMVg – abweichend von dem üblichen Verfahren – im einzelnen prüfen muß, ob wegen der Konsequenzen für ihren Ehemann auf die Einbeziehung der Petentin verzichtet werden kann. Dies habe ich dann auch gegenüber dem BMVg angeregt, der mir jedoch mitteilte, daß wegen der bisherigen Tätigkeit des Ehemannes in einem sicherheitsempfindlichen Bereich ein Verzicht nicht in Betracht komme. Diese Auffassung hat dann auch der Petitionsausschuß geteilt.

In einem anderen Fall hat mich die Wehrbeauftragte des Deutschen Bundestages um Stellungnahme gebeten, weil das BMVg die Fortführung der Sicherheitsüberprüfung eines Soldaten verweigert hatte, nachdem dessen Ehefrau zwar nicht die Zustimmung zu ihrer Einbeziehung in die Sicherheitsüberprüfung, wohl aber zur Speicherung ihrer personenbezogenen Daten in automatisiert geführten Dateien des MAD verweigert hatte. Das BMVg vertrat die Auffassung, eine ordnungsgemäße Durchführung der Sicherheitsüberprüfung sei nicht möglich, weil der MAD ohne diese Speicherung den mit anderen Sicherheitsbehörden in dieser Sache geführten Schriftverkehr nicht wiederauffinden könne. Als Konsequenz aus dieser Entscheidung wurde der Soldat aus seiner bisherigen Verwendung im sicherheitsempfindlichen Bereich versetzt, der neue Standort war allerdings 600 km von seinem bisherigen Familienwohnort entfernt. Ich habe der Wehrbeauftragten mitgeteilt, daß ich die Ablehnung der Fortführung der Sicherheitsüberprüfung des Soldaten für unverhältnismäßig halte. Eine Fortsetzung der Sicherheitsüberprüfung sei möglich, da es dem BMVg und dem MAD nicht verwehrt sei, die personenbezogenen Daten der Ehefrau zu erheben und auch manuell zu speichern.

Außerdem könnten ihre Daten auch in die Sicherheitsakte ihres Ehemannes aufgenommen werden. Somit wäre es dem MAD ohne große Schwierigkeiten möglich, die erforderlichen Anfragen bei den Sicherheitsbehörden durchzuführen und gegebenenfalls hätten auch weitere Sicherheitsermittlungen eingeleitet werden können. Da das BMVg auf seiner Rechtsauffassung beharrte, hat der Betroffene eine gerichtliche Entscheidung herbeigeführt. In seinem letztinstanzlichen Urteil vom 2. April 1996 – BVerwG 1. WB 71.95 – ist das Bundesverwaltungsgericht meiner o. g. Auffassung gefolgt und hat das BMVg zur Fortsetzung der Sicherheitsüberprüfung verurteilt.

17.2 Zahlreiche Personenüberprüfungen nach Luftverkehrsgesetz

Der Gesetzgeber hat in § 29 d LuftVG der Bundesregierung aufgegeben, die Einzelheiten für die Prüfung der **Zuverlässigkeit** zum Zugang zu den nicht allgemein zugänglichen oder sicherheitsempfindlichen Bereichen von Verkehrsflughäfen in einer Rechtsverordnung zu regeln. An der Vorbereitung des Entwurfs dieser Verordnung war ich beteiligt. Der Entwurf, der sich noch in der Abstimmung mit den Ländern befindet, sieht vor, grundsätzlich alle Personen, die zum nicht für jedermann zugänglichen Bereich eines solchen Flughafens Zutritt erhalten sollen, wie z. B. Personal von Luftverkehrsunternehmen und von Flughäfen bis hin zur Reinemachefrau, das in diesen Bereichen eingesetzt wird, zu überprüfen. Auch Personen, die ansonsten die Möglichkeit hätten, Sprengstoffe, Waffen o. ä. in diese Bereiche zu lenken, wie zum Beispiel das Personal am Gepäckabfertigungsschalter, soll einer besonderen Zuverlässigkeitsüberprüfung unterfallen. Diese Überprüfung beinhaltet u. a. Abfragen bei den Polizei- und Verfassungsschutzbehörden des Bundes und der Länder sowie in bestimmten Fällen auch beim Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik.

Die Kosten für die Sicherheitsüberprüfung haben die Veranlasser, also die Luftverkehrsunternehmen oder Flughafenbetreiber, ggf. die Betroffenen zu tragen. Die Höhe der Kosten ist in einer Kostenverordnung geregelt.

Wegen der Vielzahl möglicher Betroffener würde die Verordnung nach § 29 d LuftVG dazu führen, daß z. B. allein am Flughafen Frankfurt/Main bis zu 20 000 oder gar 30 000 Zuverlässigkeitsüberprüfungen durchzuführen sind. Ich habe die Erforderlichkeit einer solch großen Zahl von Überprüfungen mit dem Hinweis problematisiert, daß es nicht unbedingt nachvollziehbar sei, wenn die Sicherheitsüberprüfung von 'zigtausend Personen bis hin zur Putzfrau und zum Schalterpersonal für notwendig erachtet wird.

17.3 Kontrolle der Sicherheitsüberprüfung beim Bundeswirtschaftsministerium

1995 habe ich die Verarbeitung personenbezogener Daten in Zusammenhang mit der Sicherheitsüberprüfung von Beschäftigten im nicht-öffentlichen Bereich beim BMWi kontrolliert. Das BMWi ist nach dem SÜG zuständige Stelle für die Sicherheitsüberprüfung von Beschäftigten der nicht-öffentlichen Stellen (siehe auch Nr. 17.4). Es prüft die von den Sicherheitsbevollmächtigten der einzelnen Unternehmen eingehenden Sicherheitserklärungen auf etwaige sicherheitserhebliche Tatsachen und legt je nach dem Grad der beantragten Ermächtigung fest, welche Art der Sicherheitsüberprüfung für den Betroffenen angemessen ist. Durchgeführt werden die Überprüfungsarten Ü 1 (einfache Sicherheitsüberprüfung), Ü 2 (erweiterte Sicherheitsüberprüfung) und Ü 3 (erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen). Die Überprüfung selbst nimmt das BfV als mitwirkende Behörde vor. Das BfV teilt dem BMWi das Ergebnis samt etwaiger sicherheitserheblicher Erkenntnisse und dem Votum mit, ob ein Sicherheitsbescheid erteilt werden kann. Der Geheimschutzbeauftragte des BMWi hat den Betroffenen nach dem SÜG grundsätzlich zu etwaigen Erkenntnissen anzuhören, um ihm so die Gelegenheit zu geben, diese Bedenken auszuräumen. Der nicht-öffentlichen Stelle, bei der der Betroffene beschäftigt ist, dürfen die sicherheitserheblichen Erkenntnisse nicht übermittelt werden. Dem Sicherheitsbevollmächtigten des Unternehmens wird lediglich mitgeteilt, ob ein Bescheid erteilt werden kann oder nicht. Die von mir beim BMWi eingesehenen Sicherheitsakten entsprachen den rechtlichen Anforderungen bis auf einen Fall, bei dem die Erkenntnisse aus der Überprüfung dem Unternehmen mitgeteilt worden waren, die dort aber auch schon bekannt waren.

Die Sicherheitsüberprüfung ist immer ein Eingriff in das Recht des Betroffenen auf informationelle Selbstbestimmung. Sie sollte deshalb dann erfolgen, wenn der Zugang zu Verschlußsachen oder zu einem sicherheitserheblichen Bereich bevorsteht, wenn sich also abzeichnet, daß das Unternehmen den entsprechenden Auftrag bekommt, und nicht bereits zu Beginn des Ausschreibungsverfahrens. Leider ist das BMWi meiner Anregung nicht gefolgt, weil es der Auffassung ist, eine solche Praxis könnte zu möglichen Verzögerungen bei der Auftragsvergabe führen. Ich halte meine Bedenken gegen jegliche Sicherheitsüberprüfung auf Vorrat aufrecht.

Weiter habe ich festgestellt, daß bis zum Inkrafttreten des SÜG im Jahre 1994 die Beschäftigten im nicht-öffentlichen Bereich grundsätzlich der Sicherheitsüberprüfung Ü 2 unterzogen worden waren. Ü 2 bedeutet, daß neben den Nachrichtendiensten auch bei den Polizeibehörden angefragt wird. Hier hätte in der Regel eine einfache Sicherheitsüberprüfung (Ü 1) ausgereicht. Die Praxis hat sich aber nach Inkrafttreten des SÜG geändert, weil der Sicherheitsbevollmächtigte des Unternehmens auch aufgrund meiner Anregung gehalten ist zu begründen, wenn er Sicherheitsüberprüfungen nach Ü 2 oder gar nach Ü 3 für erforderlich hält.

Nach meiner Auffassung werden von den Unternehmen auch Sicherheitsüberprüfungen für zu viele Beschäftigte beantragt, wohl um für einen möglichen Ausfall von Personal gerüstet zu sein. Im Hinblick auf den damit verbundenen Eingriff in das Persönlichkeitsrecht, aber auch wegen der Kosten, die eine

Sicherheitsüberprüfung verursacht, habe ich dem BMWi empfohlen, ähnlich wie bei der vergleichbaren Zuverlässigkeitsüberprüfung für Bedienstete in Kernkraftwerken Gebühren von den Unternehmen zu erheben. Damit würde m.E. Einfluß darauf genommen, daß nur im erforderlichen Umfang sicherheitsüberprüft wird. Das Ministerium hat dies abgelehnt, weil es einen Wettbewerbsnachteil kleinerer Unternehmen befürchtet, die diese Kosten möglicherweise nicht in ihre Preiskalkulation aufnehmen könnten und so bei der Auftragsvergabe gegen den größeren Anbieter ohne Chance wären. Außerdem hält das Ministerium die Sicherheitsüberprüfung im nicht-öffentlichen Bereich für eine hoheitliche Aufgabe, deren Kosten von der öffentlichen Hand zu tragen seien. Dieser Auffassung hat sich der Innenausschuß des Deutschen Bundestages angeschlossen. Ich habe daraufhin dem BMWi mitgeteilt, daß ich davon ausgehe, daß es seine Geheimschutzberatung der Unternehmen intensiviert und durch kritische Überprüfung der von den Sicherheitsbevollmächtigten der Unternehmen abgegebenen Begründungen zur Art der Sicherheitsüberprüfung sichergestellt wird, daß nur im erforderlichen Umfang überprüft wird.

Die ca. 120 000 Sicherheitsakten, die zum Zeitpunkt meiner Überprüfung beim BMWi geführt wurden, werden in einer eigenen Registratur verwaltet. Datensicherungsprobleme habe ich nicht festgestellt. Allerdings hat die Durchsicht der Sicherheitsakten von Personen, denen die Sicherheitsermächtigung entzogen worden war, ergeben, daß die Akten entgegen der nach dem SÜG zulässigen Aufbewahrungsfrist von fünf Jahren doppelt so lange aufbewahrt wurden. Daneben waren diese Daten auch noch in der Datenbank des BMWi zu SÜG-Maßnahmen. Von einer Beanstandung habe ich abgesehen, da inzwischen durch entsprechende Arbeitsanweisungen gewährleistet ist, daß die Fristen eingehalten werden.

Das BMWi betreibt eine Datenbank, in der die Daten der Sicherheitsüberprüften, aber auch die Daten, die bei der Geheimschutzberatung der Unternehmen anfallen, verarbeitet werden (z. B. Daten über Schulungen der Beschäftigten). Die im Zusammenhang mit der allgemeinen Geheimschutzberatung anfallenden Daten sind für die Aufgaben eines anderen Referates des BMWi erforderlich. Es muß deshalb sichergestellt werden, daß die für die Durchführung der Sicherheitsüberprüfung zuständigen Bediensteten des BMWi nur auf die Daten zugreifen können, die nach dem SÜG zulässig sind. Das ist bei der derzeitigen Datenbankstruktur, die bereits 1989 entwickelt worden ist, nicht hinreichend gewährleistet. Darüber hinaus habe ich noch verschiedene Mängel bei den technischen und organisatorischen Maßnahmen festgestellt, die eine sichere Datenverarbeitung gewährleisten sollen. Die damit zusammenhängende notwendige Umorganisation der Datenbank ist nur mit einem erheblichen fachlichen und finanziellen Aufwand möglich. Das BMWi beabsichtigt, ein neues Informationssystem zu entwickeln, das dann auch datenschutzrechtliche Belange umfassend berücksichtigen soll. In diese Neuentwicklung soll ich mit einbezogen werden. Leider ist es aber nach über einem Jahr seit meiner Kontrolle nicht dazu gekommen.

17.4 Kontrolle der Sicherheitsüberprüfung bei Unternehmen

Beschäftigte von Unternehmen der Privatwirtschaft, die Aufträge erhalten, für die sie den Zugang zu sicherheitsempfindlichen Bereichen und zu Verschlußsachen benötigen, sind einer Sicherheitsüberprüfung nach dem SÜG zu unterziehen (s. o. Nr. 17.3). Der Sicherheitsbevollmächtigte des Unternehmens, der besonders überprüft und vom BMWi ausdrücklich ermächtigt wird, leitet die von den Beschäftigten ausgefüllten Sicherheitserklärungen, die die gleichen Angaben enthalten wie im öffentlichen Bereich, nach Prüfung auf Vollständigkeit und Richtigkeit der Erklärung an das BMWi weiter, das dann die Sicherheitsüberprüfung veranlaßt. Ein Exemplar der Sicherheitserklärung wird zur Sicherheitsakte des Beschäftigten genommen, die beim Sicherheitsbevollmächtigten geführt wird und getrennt von den Personalakten aufbewahrt werden muß. Zur Erfüllung seiner Aufgaben im Geheimschutzbereich des Unternehmens kann der Sicherheitsbevollmächtige die erforderlichen personenbezogenen Daten in automatisierten Dateien verarbeiten und nutzen.

Nach dem SÜG vom 20. April 1994 (BGBl. I S. 867) ist mir die Zuständigkeit für Kontrollen der personenbezogenen Datenverarbeitung bei den Sichheitsbevollmächtigten von Unternehmen übertragen worden. Ich habe im Jahre 1996 erstmals bei zwei Unternehmen die Einhaltung datenschutzrechtlicher Vorschriften in Zusammenhang mit der Sicherheitsüberprüfung ihrer Beschäftigten überprüft. Es handelte sich um ein mittleres Unternehmen und um einen Konzern mit Verbundunternehmen, die von der Konzernzentrale sicherheitsmäßig mitbetreut werden. Allgemein kann ich feststellen, daß beide kontrollierten Unternehmen im Bereich des Geheimschutzes einen hohen datenschutzrechtlichen Standard aufwiesen.

Das mittelgroße Unternehmen beschäftigte zum Zeitpunkt meiner Kontrolle ca. 2 100 Mitarbeiter, von denen ca. 130 sicherheitsermächtigt waren. Die Sicherheitsakten werden zentral beim Sicherheitsbevollmächtigten, jedoch getrennt von den Personalunterlagen aufbewahrt. Die technisch-organisatorischen Maßnahmen zur Datensicherheit sind insgesamt angemessen. Die stichprobenweise Prüfung von Sicherheitsakten der Beschäftigten hat ergeben, daß diese nur Unterlagen enthalten, die nach dem SÜG zulässig sind.

Allerdings habe ich im Rahmen meiner Prüfung auch Akten von Beschäftigten vorgefunden, die seit mehr als 5 Jahren nicht mehr im sicherheitsempfindlichen Bereich beschäftigt bzw. ausgeschieden sind. Sicherheitsakten sind aber nach Ablauf dieser Frist zu vernichten. Nach Angaben des Sicherheitsbevollmächtigten waren bisher jedoch noch nie Akten ausgesondert worden. Er sagte zu, diese Akten umgehend auszusondern und zu vernichten.

Die Speicherung personenbezogener Daten der Sicherheitsermächtigten in einer Datenbank, die mittels Paßwort nur dem Sicherheitsbevollmächtigten zugänglich ist, hält sich im zulässigen Rahmen des § 31 SÜG. Auch Datensicherheitsprobleme haben sich insoweit nicht ergeben.

Bei dem kontrollierten Konzern waren zum Zeitpunkt der Prüfung ca. 2 900 Personen sicherheitsermächtigt. Der Sicherheitsbevollmächtigte ist auch für den Geheimschutz in den rechtlich selbständigen Konzernunternehmen zuständig. Die Sicherheitsakten aller Beschäftigten werden derzeit noch zentral am Hauptsitz des Unternehmens aufbewahrt. Für die Standorte außerhalb der Zentrale sind örtliche Sicherheitsbevollmächtigte bestellt, die aber nur eine Vorprüfung der Sicherheitserklärungen vornehmen und die dann an die Zentrale weiterleiten. Die Aufbewahrung der Sicherheitsakten erfolgt – jeweils nach Mutterunternehmen und verbundenen Unternehmen getrennt – in dem nur mittels Codekarte zugänglichen Arbeitsbereich des Sicherheitsbevollmächtigten. Zugriffsberechtigt sind nur er und seine für den Geheimschutz zuständigen Mitarbeiter. Die Sicherheitsakten sind streng von den Personalakten getrennt. Die Akten von Personen, bei denen die Sicherheitsermächtigung aufgehoben wurde, weil sie nicht mehr im sicherheitsempfindlichen Bereich eingesetzt werden, werden gesondert aufbewahrt. Die zulässige Aufbewahrungsfrist von fünf Jahren war in keinem Falle überschritten. Die Einhaltung dieser Frist wird durch die zuständigen Sachbearbeiter laufend kontrolliert. Auch die Sicherheitsakten der aktuell Ermächtigten enthalten nur Unterlagen, die nach dem SÜG zulässig sind. In zahlreichen Akten von Beschäftigten, die bereits seit längerer Zeit sicherheitsermächtigt waren, habe ich Unterlagen gefunden, deren weitere Aufbewahrung ich nach den politischen Entwicklungen seit 1990 und nach dem neuen SÜG für nicht mehr erforderlich halte, z. B. Reisemeldungen über Besuche in der ehemaligen DDR. Ich habe dem BMWi in meinem Kontrollbericht empfohlen, den Sicherheitsbevollmächtigten des Unternehmens zu ersuchen, im Rahmen der laufenden Bearbeitung die Sicherheitsakten entsprechend zu bereinigen.

Die Mitarbeiter des Unternehmens, die für den Geheimschutz zuständig sind, betreiben zur Erfüllung ihrer Aufgaben eine Datenbank mit den personenbezogenen Daten der aktuell Ermächtigten und in einem separaten Abschnitt derjenigen Beschäftigten, bei denen der Sicherheitsbescheid aufgehoben war. Auch hier werden nur Daten verarbeitet, die nach dem SÜG zulässig sind. Auch Datensicherheitsmängel konnte ich nicht feststellen.

Der Sicherheitsbevollmächtigte betreut auch die rechtlich selbständigen Tochterunternehmen des Konzerns in den Aufgaben des Geheimschutzes. Um sicherzustellen, daß für die Beschäftigten dieser Tochterunternehmen die Zweckbindung von Daten aus der Sicherheitsüberprüfung auch gegenüber den anderen rechtlich selbständigen Konzernteilen gilt, also diese Daten grundsätzlich nicht an diese Konzernteile übermittelt werden dürfen, habe ich empfohlen, in die Arbeitsverträge der Geheimschutzbearbeiter eine entsprechende Zusatzvereinbarung aufzunehmen.

Der Konzern beabsichtigt, die Aufbewahrung der Sicherheitsakten und die Verarbeitung personenbezogener Daten aus der Sicherheitsüberprüfung auf die einzelnen Betriebsstandorte zu dezentralisieren. Letzteres soll durch eine vernetzte Datenverarbeitung unterstützt werden. Wie bei allen Netzen entstehen hier vor allem besondere Sicherheitsprobleme, die wegen der zu übermittelnden besonders schützenswerten Daten datenschutzrechtlich nicht unproblematisch sind. Ich habe dem Unternehmen meine Beratung angeboten.

17.5 Vorbeugender personeller Sabotageschutz – sicherheitsempfindliche Stellen von lebens- und verteidigungswichtigen Einrichtungen –

Ich hatte bereits früher (zuletzt 15. TB Nr. 29.2.1) berichtet, daß auf meine Anregung hin (vgl. 14. TB S. 141 f.) die Innenminister von Bund und Ländern prüfen wollten, was unter lebens- und verteidigungswichtigen Einrichtungen im Sinne des § 3 Abs. 2 Satz 1 Nr. 2 BVerfSchG zu verstehen ist. Auch die 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich in einer Entschließung **(vgl. Anlage 8)** für einen behutsamen Umgang mit Sicherheitsüberprüfungen in diesem Bereich ausgesprochen. Nachdem inzwischen die Frage der lebens- und verteidigungswichtigen Einrichtungen innerhalb der Bundesressorts weitgehend geklärt ist, hat mir das BMI auf Anfrage mitgeteilt, daß innerhalb der Bundesregierung derzeit mehrheitlich kein Handlungsbedarf für zusätzliche gesetzgeberische Maßnahmen zum vorbeugenden personellen Sabotageschutz gesehen werde. Dies bedeutet, daß über den Anwendungsbereich der § 12 b AtomG und § 29 d LuftVerkG hinaus bis auf weiteres keine Überprüfungsmaßnahmen für den personellen Sabotageschutz geplant sind. Damit dürfte gewährleistet sein, daß keine Sicherheitsüberprüfungen „auf Vorrat" stattfinden.

18 Personaldaten

18.1 Arbeitnehmer-Datenschutzgesetz

Die Notwendigkeit eines Arbeitnehmer-Datenschutzgesetzes wird auch vom Deutschen Bundestag anerkannt, der zu meinem 14. Tätigkeitsbericht (Nr. 9.1) beschlossen hatte: „Die Bundesregierung wird aufgefordert, bereichsspezifische Regelungen zum Arbeitnehmerdatenschutz baldmöglichst vorzulegen." Daraufhin hat die Bundesregierung die Erarbeitung eines Arbeitnehmer-Datenschutzgesetzes angekündigt. Im 15. Tätigkeitsbericht (Nr. 32.4) habe ich die Dringlichkeit nochmals hervorgehoben. In ihrer Stellungnahme dazu bekräftigt die Bundesregierung, sie habe die Arbeiten erneut aufgenommen und bleibe bemüht, den Referentenentwurf sobald wie möglich vorzulegen. Leider muß ich erneut feststellen, daß die Bundesregierung entgegen ihrer Ankündigung einen Gesetzentwurf immer noch nicht vorgelegt hat.

18.2 Immer wieder umfangreiche ärztliche Unterlagen in Personalakten

Ein Mitarbeiter der Zollverwaltung wandte sich an mich, weil ein vollständiges nervenärztliches Gutachten in seine Personalakte gelangt war. Er bat

mich, dafür zu sorgen, daß diese Unterlage aus der Personalakte entfernt wird. Die Oberfinanzdirektion hatte sein entsprechendes Ersuchen mit der Begründung abgelehnt, daß die ärztliche Schweigepflicht gegenüber der ein Gutachten veranlassenden Behörde nicht gelte und daß nach dem Prinzip der Vollständigkeit der Personalakte sämtliche Unterlagen und Vorgänge, die das Beamtenverhältnis betreffen, zur Personalakte zu nehmen seien. Hierzu zähle auch das vollständige Gutachten, das auf Veranlassung des Dienstherrn zur Überprüfung der Dienstfähigkeit erstellt worden ist.

Grundsätzlich bin ich der Auffassung, daß die Teile des Gutachtens in die Personalakte gehören, die für die dienstliche Entscheidung erforderlich sind, ob ein Beamter aus gesundheitlichen Gründen in den Ruhestand zu versetzen ist. Sie stehen in einem unmittelbaren Zusammenhang mit dem Dienstverhältnis und sind daher zur Personalakte zu nehmen (vgl. § 90 Abs. 1 Satz 2 BBG).

Vor dem Hintergrund, daß die Regelungen der §§ 90ff. BBG das früher geltende Vollständigkeitsprinzip für die Führung der Personalakten durch das Erforderlichkeitsprinzip ersetzt haben, habe ich die Sach- und Rechtslage mit dem BMF mit dem Ergebnis erörtert, daß folgende Teile des nervenärztlichen Gutachtens entfernt und vernichtet wurden:

- biographische Anamnese,
- Familienanamnese,
- somatische Anamnese,
- Drogen-, Alkohol-, Suchtmittel- und Medikamentenanamnese,
- die Untersuchungsbefunde (somatischer, neurologischer und psychischer Befund),
- Teile der zusammenfassenden Beurteilung.

Da die Verwaltung im Rahmen von § 45 BBG verpflichtet ist, regelmäßig zu prüfen, ob ein aus gesundheitlichen Gründen vorzeitig in den Ruhestand versetzter Beamter wieder dienstfähig ist, damit ggf. Entscheidungen über die Wiederverwendung vorbereitet werden können, ist die personalbewirtschaftende Stelle auf die Angaben des in der Personalakte verbliebenen Teils des Gutachtens angewiesen, insbesondere wenn eine Besserung des Gesundheitszustandes grundsätzlich möglich erscheint.

Im Hinblick darauf, daß die Kenntnisnahme des Inhalts von ärztlichen Gutachten durch Beschäftigte, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten befaßt sind, nicht für jede Personalentscheidung erforderlich ist, sind entsprechende Unterlagen in einem verschlossenen Umschlag mit der Kennzeichnung „ärztliches Gutachten" in der Personalakte aufzubewahren. Der Umschlag ist zu versiegeln. Bei jedem Öffnen ist das Handzeichen mit dem Datum und dem Grund des Öffnens auf dem Umschlag zu vermerken (vgl. 14. TB Nr. 9.14.4). Das BMF hat mir inzwischen mitgeteilt, daß eine entsprechende Regelung in den Entwurf der Personalaktenrichtlinie aufgenommen wird.

18.3 Geburtstagslisten in Dienststellen

Es ist eine verbreitete Übung und ein Zeichen guten Betriebsklimas, wenn sich Kollegen untereinander zum Geburtstag gratulieren. Deshalb gibt es in vielen Dienststellen auch sogenannte Geburtstagslisten, die helfen sollen, den „Ehrentag" des Kollegen nicht zu verpassen. Mit der Frage, ob eine solche Liste gegen den Datenschutz verstößt, hat sich eine Bundesbehörde an mich gewandt, nachdem u. a. ihr Personalrat den Dienststellenleiter um Zulieferung von Geburtstagslisten gebeten hatte. Beim Geburtstag handelt es sich um ein personenbezogenes Datum, das angesichts seines unmittelbaren inneren Zusammenhangs mit dem Dienstverhältnis sogar die Qualität eines Personalaktendatums trägt.

In der Tat wäre die Verbreitung eines listenmäßigen Ausdrucks der Namen und Geburtstage aller Bediensteten als Ergebnis einer Abfrage aus dem Personalinformationssystem der Dienststelle unzulässig. Denn das für die Zwecke von Personalverwaltung und Personalwirtschaft erhobene Geburtsdatum unterliegt dem Schutz des Personalaktengeheimnisses.

Die üblichen Geburtstagslisten entspringen allerdings kollegialer Initiative. Neue Mitarbeiter werden unter Hinweis auf eine beabsichtigte Aufnahme in die Geburtstagsliste um Angabe ihres Geburtstages und -monats gebeten. Deren Angabe für diesen Zweck erfolgt dann entsprechend § 4 Abs. 1 BDSG mit Einwilligung des Bediensteten in diese Verwendung. Es entspricht der Praxis und ist sinnvoll, daß derartige Listen in größeren Behörden auf die Referats- oder allenfalls Abteilungsebene beschränkt bleiben, weil nur in diesem Kreis so enge Zusammenarbeitsbeziehungen bestehen, daß ein gegenseitiges Gratulieren zum Geburtstag naheliegt.

18.4 Wenn der interne Datenschutzbeauftragte gleichzeitig Dienstvorgesetzter ist – Eklatante Unverträglichkeit!

Über einen Mitarbeiter eines Fernmeldeamtes der Telekom AG wurde ein postbetriebsärztliches Gutachten zur Überprüfung seiner Dienstfähigkeit wegen einer gegebenenfalls einzuleitenden Versetzung in den Ruhestand nach § 42 Abs. 1 BBG erstellt. Später wurde dieses Gutachten für die Umsetzung des Mitarbeiters an einen anderen Arbeitsplatz genutzt, obwohl eine erneute Untersuchung zur Klärung seiner Einsatzfähigkeit auf dem neuen Arbeitsplatz grundsätzlich hätte durchgeführt werden müssen (vgl. § 14 Abs. 2 SchwbG). Außerdem wurde dem Mitarbeiter entgegen der Regelung des § 90c Abs. 1 u. 3 Satz 2 BBG eine Ablichtung des Gutachtens mit der Begründung verweigert, daß dies nicht üblich sei.

Dagegen hat sich der Mitarbeiter an den internen Datenschutzbeauftragten seiner Dienststelle gewandt. Dieser hat die Eingabe an die nächsthöhere Dienststelle weitergeleitet, da er sich als Leiter der Zentralabteilung und damit als Dienstvorgesetzter des Mitarbeiters für befangen hielt.

Vom internen Datenschutzbeauftragten der übergeordneten Dienststelle wurde der Petent angewiesen,

den weiteren Schriftverkehr in seiner datenschutzrechtlichen Angelegenheit ausschließlich mit ihm zu führen. Außerdem wurde er gebeten, die von ihm vermuteten datenschutzrechtlichen Verstöße unter Angabe von Personen, Daten und Beweismitteln bis zu einem bestimmten Termin genau darzulegen. Soweit dies nicht innerhalb dieser Frist geschehe, solle er die Vorwürfe schriftlich zurücknehmen oder er müsse mit der Einleitung juristischer Schritte rechnen.

Nach der derzeit noch in Kraft befindlichen vorläufigen Anweisung zur Ausführung des Datenschutzes bei der Deutschen Bundespost Telekom (DS-Anweisung) sind jeweils Personen mit der Wahrnehmung der Aufgaben des internen Datenschutzbeauftragten betraut, die darüber hinaus noch Personalentscheidungen zu treffen bzw. daran mitzuwirken haben.

Diese Regelung ist nicht akzeptabel. Denn die Wahrnehmung von Aufgaben in Bereichen, in denen Personalentscheidungen vorbereitet oder getroffen werden, ist regelmäßig unvereinbar mit der Tätigkeit als interner Datenschutzbeauftragter. Die besondere Vertrauensstellung des internen Datenschutzbeauftragten läßt eine gleichzeitige Aufgabenwahrnehmung als Dienstvorgesetzter nicht zu. Sie erfordert vielmehr eine Trennung dieser Aufgabenbereiche, damit die Mitarbeiter eindeutig davon ausgehen können, daß datenschutzrechtliche Ansprüche unabhängig von Personalentscheidungen geltend gemacht werden können.

Nach Erörterung der Rechtslage hat der zuständige Fachbereich der Zentrale der Deutschen Telekom AG den internen Datenschutzbeauftragten der Direktion angewiesen, in der Angelegenheit nicht weiter tätig zu werden, da der Petent einen Anspruch darauf hätte, „daß der vorgetragene Sachverhalt allein aus datenschutzrechtlicher Sicht gewürdigt würde".

Die Zentrale der Deutschen Telekom AG hat mir mitgeteilt, daß die o. g. „vorläufige Dienstanweisung Datenschutz" in Kürze außer Kraft treten soll. Neben den zwischenzeitlich bestellten hauptamtlichen Datenschutzberatern (s. Nr. 10.1.6) werden nebenamtlich regionale Datenschutzberater eingesetzt, die deren Tätigkeit unterstützen sollen.

18.5 Weitergabe von Personalakten an andere Dienststellen ohne Mitwirkung der Betroffenen

Das BAFl sucht wegen des vorgesehenen Personalabbaus seit Anfang 1995 für ca. 1 500 Bedienstete neue Aufgaben. Tatsächlich konnten bisher aber nicht für alle Mitarbeiter neue Stellen gefunden werden. Um bei Kündigungen zu differenzieren, wurde gemeinsam mit der Schwerbehindertenvertretung, der Frauenbeauftragten und der Personalvertretung eine Auswahl nach sozialen Kriterien getroffen. Im Anschluß daran war man bemüht, die Betroffenen durch Gespräche zunächst für freie Stellen im Geschäftsbereich des BMI, z. B. beim Bundesgrenzschutz (BGS), zu interessieren. In zahlreichen Fällen haben sich Betroffene aber nicht auf die angebotenen Stellen beworben, so daß die Möglichkeit geprüft wurde, sie an andere Ressorts bzw. deren nachgeordnete Dienststellen abzuordnen oder zu versetzen. Zur Vorbereitung hierauf oder im Rahmen der entsprechenden Beteiligung wurden die in Frage kommenden Dienststellen über Inhalte aus den Personalakten der Betroffenen informiert. In mir vorliegenden Eingaben wurde eine Verletzung des Personalaktengeheimnisses beklagt, da das BAFl ohne Mitwirkung oder wenigstens Kenntnis der Betroffenen Personalakten an andere Behörden – auch Landes- und Kommunalbehörden – weitergegeben habe.

Hierzu ist zu bemerken, daß es grundsätzlich zulässig ist, die Personalakte eines Beamten ohne dessen Einwilligung für Zwecke der Personalverwaltung oder Personalwirtschaft der jeweiligen obersten Dienstbehörde, einer im Rahmen der Dienstaufsicht weisungsbefugten Behörde, Behörden desselben Geschäftsbereiches sowie Behörden eines anderen Geschäftsbereichs desselben Dienstherrn vorzulegen, soweit die Vorlage zur Vorbereitung oder Durchführung von Personalentscheidungen notwendig ist oder die Behörden an einer Personalentscheidung mitzuwirken haben (§ 90 d Abs. 1 BBG).

Grundsätzlich unbedenklich ist daher die Vorlage von Personalakten an

- andere Behörden oder Stellen desselben Geschäftsbereichs oder
- andere Ressorts oder deren Geschäftsbereich, soweit diese die Aufnahme eines konkret benannten Beamten im Wege einer Abordnung oder Versetzung vorbereiten, sie also an einer Abordnung oder Versetzung zwangsläufig beteiligt werden müssen.

An Dritte, das sind andere Dienstherren, z. B. Landes- oder Kommunalbehörden, dürfen Auskünfte nur mit Einwilligung des Beamten erteilt werden (§ 90 d Abs. 2).

Das BAFl hat eingeräumt, daß ein Versand von Personalakten an Landes- oder Kommunalbehörden in Einzelfällen zwar angekündigt, tatsächlich jedoch in keinem Falle ohne Mitwirkung der Betroffenen vorgenommen worden sei. Die Rechtslage wolle man gegenüber den Mitarbeitern klarstellen.

Daneben stellte sich die weitere Frage, wie für den Betroffenen und die Dienststelle eine eventuelle Versendung der Personalakten nachvollzogen werden kann.

Die Bemühungen des BAFl, für die vom Personalabbau betroffenen Mitarbeiter eine anderweitige Beschäftigung zu finden, dienen der Vorbereitung von Abordnungs- und Versetzungsverfahren. Die sich entwickelnden personalwirtschaftlichen Aktivitäten müssen in der Personalakte oder einer Teilakte dokumentiert werden, da durch die Weitergabe von Personalaktendaten an andere Behörden entstandene Unterlagen mit dem Dienstverhältnis der Betroffenen in einem unmittelbaren inneren Zusammenhang stehen (§ 90 Abs. 1 BBG). Anlage und Führung von Personalakten erfolgen entsprechend dem Erlaß des BMI vom 25. März 1993. Die Dokumentationspflicht ermöglicht es den Betroffenen, durch Einsichtnahme in die Personalakte oder Teilakte zu erfahren, welche Behörde Informationen aus seiner Personalakte erhalten hat.

Nach Mitteilung des BAFl erfolgt die Dokumentation in einer Teilakte, die auch den Fragebogen zur Sozialauswahl enthält. Die Teilakte soll nach Abschluß des Personalabbauverfahrens vernichtet werden. Damit sind einer möglichen Einstellungsbehörde die vorausgegangenen Bewerbungen nicht aus der Personalakte des Bewerbers ersichtlich.

18.6 Beratungen im Bereich der automatisierten Personaldatenverarbeitung

Verstärkt berate ich zahlreiche Bundesbehörden bei der Einführung oder Umstellung von Systemen der automatisierten Personaldatenverarbeitung. Hierdurch kann ich bewirken, daß Datenschutzaspekte in einem frühen Entwicklungsstadium der Vorhaben berücksichtigt werden und mit geringem Aufwand in die Entwicklung oder Umstellung der Systeme einfließen können.

Die in diesem Zusammenhang mit den beteiligten Stellen der Bundesbehörden geführten Gespräche verliefen stets in einer konstruktiven Atmosphäre. So war es möglich, die verschiedenen datenschutzrechtlich relevanten Punkte auf der Basis des jeweiligen Entwicklungsstadiums zu erörtern und entsprechende Hinweise und Empfehlungen zu geben. Hierbei waren unter Datenschutzaspekten folgende Punkte immer wieder Erörterungsgegenstand: Sicherstellung der gesetzlichen Vorgaben des Bundesbeamtengesetzes (§§ 90ff., insbesondere § 90g BBG), Datenumfang, Zugriffsregelungen, Auswertungsmöglichkeiten, Protokollierungen, Löschungsfristen, Bemerkungs-/Freitextfelder, technisch-organisatorische Maßnahmen gemäß § 9 BDSG und Anlage sowie datenschutzrechtliche Regelungen in Dienstvereinbarungen und -anweisungen.

Im Zuge meiner Beratungen weise ich immer wieder darauf hin, daß sich diese nur auf die jeweils konkret vorhandenen Bedingungen bzw. die tatsächliche Systemumgebung sowie die konkrete inhaltliche Ausgestaltung des Systems der automatisierten Personaldatenverarbeitung bezieht. Denn ein System, das bei der einen Bundesbehörde den Datenschutzanforderungen genügt, muß nicht zwangsläufig auch bei einer anderen Behörde diesen Anforderungen entsprechen.

Meine Beratungen richteten sich sowohl auf „kleinere" automatisierte Systeme, mit denen Mitarbeiterdaten verarbeitet werden (z. B. TK-Anlagen, IT-gestützte Reisekostensysteme oder elektronische Zeiterfassungssysteme) als auch auf die Einführung neuer Personalinformations-/Personalverwaltungssysteme. Hierbei habe ich im Berichtszeitraum Beratungen beim BMBF, BMI, BMJ, BMU, BMV, BAFl sowie beim Deutschen Patentamt durchgeführt, die teilweise noch nicht abgeschlossen sind.

18.7 Zugriffsrechte von Vorgesetzten in einem Personalinformationssystem

Im Rahmen meiner datenschutzrechtlichen Beratung über Personalinformationssysteme stellte sich erneut folgendes Problem, das von grundsätzlicher Bedeutung ist.

Eine Bundesbehörde mit über 3000 Mitarbeitern plant und entwickelt die Erhebung von Personal- und Stellendaten sowie ihre Verarbeitung in einem Personalinformationssystem und ihre Nutzung für die dienstlichen Zwecke der Personalverwaltung und Personalwirtschaft. Durch Benutzeridentifizierungen und Benutzerauthentifizierung wird sichergestellt, daß nur die abschließend festgelegten Berechtigten unmittelbaren Zugriff auf das Personalinformationssystem haben. Die einzelnen Arbeitsbereiche der Personalreferate erhalten durch technische Maßnahmen jeweils nur in dem Umfang Zugang zu den Personaldaten, wie es für deren Aufgabenerfüllung erforderlich ist. Daher ist vorgesehen, daß der Leiter der Zentralabteilung (AL Z) sowie sein Vertreter lesenden Zugriff auf alle im Personalinformationssystem gespeicherten Personalaktendaten haben. Fraglich ist, ob dies mit den Regelungen der §§ 90 ff. BBG, insbesondere des § 90 Abs. 3 BBG vereinbar ist. Danach dürfen Zugang zur Personalakte – hierzu gehören auch Personalaktendaten, die in Dateien verarbeitet oder genutzt werden – nur Beschäftigte haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind, und zwar nur, soweit dies für Zwecke der Personalverwaltung oder der Personalwirtschaft erforderlich ist.

In der von mir hierzu erbetenen Stellungnahme hat die betroffene Bundesbehörde zur vorgesehenen Nutzung des Personalinformationssystems durch den AL Z u. a. vorgetragen, Schwerpunkt seiner Arbeit im Personalbereich sei, die Behördenleitung bei der Personalpolitik des Hauses zu beraten und zu unterstützen. Hieraus ergebe sich, daß der AL Z alle die Zugriffe insgesamt haben müsse, die seine Personalreferate im einzelnen besäßen. Ferner bedeute dies im Hinblick auf die Personalpolitik, daß der AL Z und sein Vertreter auch von den Möglichkeiten Gebrauch machen müßten, die sich gerade aus der Gesamtnutzbarkeit des Datenbestandes ergäben. Dies treffe auch für die Notwendigkeit und den Umfang der Möglichkeiten zu, den Datenbestand auszuwerten und zu sortieren. Um einzelne Personalmaßnahmen zu überprüfen, sei nicht nur der Zugriff auf die „elektronische Personalakte" des Einzelfalls, also auf den unter einem bestimmten Namen enthaltenen Datenbestand (ohne Listensortierung) nötig. Die Möglichkeiten des Systems auszuwerten und zu sortieren seien stets erforderlich, wenn einzelne Maßnahmen auf die optimale Alternativentscheidung hin geprüft werden müßten.

Um die Angelegenheit abschließend bewerten zu können, habe ich das Bundesministerium des Innern im Hinblick auf dessen Zuständigkeit für das Beamtenrecht um eine grundsätzliche Stellungnahme zu der Frage gebeten, ob die vorgesehenen umfassenden Zugriffsrechte der Abteilungsleitung insbesondere mit den Regelungen des Bundesbeamtengesetzes (§§ 90ff.) vereinbar sind.

Hierzu hat das BMI ausgeführt, daß nach den einschlägigen Vorschriften des Beamtenrechts (§§ 90 Abs. 3, 90g BBG) zu den Zugangsberechtigten bei automatisiert verarbeiteten Daten auch der Leiter einer Personalabteilung sowie sein Vertreter gehör-

ten. Aus den Aufgaben eines AL Z könnten sich unter Umständen auch Zugriffsrechte ergeben, die über die Befugnisse der einzelnen ihm unterstellten Personalreferate hinausgehen. Das dürfe jedoch nicht dazu führen, daß in der Hand des Abteilungsleiters ein Personalinformationssystem entstehe, das durch bestimmte Verknüpfungen geeignet sei, Persönlichkeitsprofile zu erstellen und zu erfassen oder als umfassendes Kontrollinstrument zu dienen.

Die Bundesregierung habe sich in der Vergangenheit wiederholt verpflichtet, keine derartigen Personalinformationssysteme einzuführen (vgl. BT-Drucksache 10/4594; Begründung zum Entwurf eines Neunten Gesetzes zur Änderung dienstrechtlicher Vorschriften – BT-Drucksache 12/544, Seite 14). Die Beschränkung der Personalinformationssyteme auf Hilfs- und Unterstützungsfunktionen sei schon bei der Einrichtung dieser automatisierten Verfahren zu berücksichtigen. Insbesondere sei darauf zu achten, daß die Vorschrift des § 90 d Abs. 4 BBG nicht umgangen werde, nach der beamtenrechtliche Entscheidungen nicht allein auf Informationen oder Erkenntnisse gestützt werden dürfen, die unmittelbar durch Personalinformationssysteme gewonnen werden. Außerdem sei dafür Sorge zu tragen, daß sensible Daten wie Personalaktendaten im Sinne des § 90 a BBG (z. B. Unterlagen über Beihilfen) so abgeschottet werden, daß sie nicht mit anderen Personalaktendaten verknüpft werden können. Diese Abschottung dürfe auch nicht durch umfassendere Zugriffsrechte von Vorgesetzten wieder aufgehoben werden.

Damit entspricht die Rechtsauffassung des BMI auch meiner datenschutzrechtlichen Bewertung. Dies habe ich der Bundesbehörde mitgeteilt und gebeten, diese Rechtsauffassung bei der automatisierten Verarbeitung von Personalaktendaten in ihrem Personalinformationssystem entsprechend zu berücksichtigen.

Eine abschließende Bewertung aus datenschutzrechtlicher Sicht ist derzeit noch nicht möglich, da die bei dem Personalinformationssystem vorgesehenen Abfragemöglichkeiten oder Möglichkeiten der Auswertung und des Sortierens noch von der Bundesbehörde in Zusammenarbeit mit der Personalvertretung definiert und festgeschrieben werden müssen. Auf meine Anregung hin hat die Bundesbehörde in ihrer vorläufigen Dienstvereinbarung über die elektronische Verarbeitung von Personaldaten festgelegt, daß sich der Einsatz derartiger Programmfunktionen des Personalinformationssystems an den von mir dargelegten Grundsätzen orientieren wird. Diese „Hinweise zum Einsatz von Datenbanksprachen bei der automatisierten Personaldatenverarbeitung" habe ich den obersten Bundesbehörden in einem Rundschreiben (s. 15. TB Anlage 19) mitgeteilt.

18.8 Personaldisketten im Bäckerladen gefunden

In einer Bonner Bäckerei waren Disketten mit der Bemerkung: „Die werden gleich abgeholt" abgegeben worden. Nach zwei Wochen gab der Bäcker die Disketten einem Kunden, der diese Disketten lesen konnte. Dieser fand hochinteressante Daten/Personaldaten eines Ministeriums. Daraufhin wurden mir die Disketten übergeben, damit ich der Angelegenheit nachgehen konnte. Meine Prüfung der Disketten bestätigte, daß es sich um wichtige Personaldaten eines Ministeriums handelte u. a. personenbezogene Hinweise zu einem staatsanwaltschaftlichen Ermittlungsverfahren gegen einen Beamten und Stellenbesetzungsvermerke mit Angaben zu dienstlichen Leistungen von Beamten.

Ich habe die Disketten umgehend der Leitung des Ministeriums übergeben und um Prüfung gebeten.

Nach der Stellungnahme des Ministeriums habe ein Mitarbeiter entgegen der bestehenden Weisungslage unverschlüsselte Disketten aus der Dienststelle mit nach Hause genommen, um außerhalb der Arbeitszeit dienstliche Aufgaben auf seinem privaten PC zu erledigen. In der Bäckerei seien die Disketten offenbar aus seiner Aktentasche gefallen. Aufgrund der eingeleiteten Verwaltungsermittlungen liege aber kein Verdacht einer strafbaren Handlung vor.

Zur abschließenden Bewertung des Falles habe ich mir von dem Ministerium noch mitteilen lassen,

- welche konkreten technischen und organisatorischen Maßnahmen dort zum Zeitpunkt des Vorfalles getroffen waren, die eine sichere Datenverarbeitung im Sinne des § 9 BDSG gewährleisten sollen, und
- welche Vorschriften den Fall regelten, daß ein Mitarbeiter personenbezogene Daten des Ministeriums zu Hause auf seinem privaten PC weiterbearbeiten will.

Nach den im Ministerium bestehenden Regelungen ist es den Mitarbeitern seit Jahren u. a. ausdrücklich verboten, private PC für dienstliche Zwecke einzusetzen. Auch die technischen und organisatorischen Maßnahmen zur Gewährleistung der IT-Sicherheit habe ich für ausreichend erachtet.

Der Datenschutzverstoß wurde vom Ministerium eingeräumt und u. a. zum Anlaß genommen, die vorhandenen Sicherheitsmechanismen sowie technische und organisatorische Regelungen erneut zu überprüfen und zu verbessern. Insofern habe ich bei diesem Datenschutzverstoß in einem Einzelfall von einer Beanstandung abgesehen (§ 25 Abs. 2 BDSG).

18.9 Übersicht über Arbeitsergebnisse von Einzelentscheidern gibt erneut Anlaß zu Diskussionen beim BAFl

Die Führung von Übersichten über Arbeitsergebnisse von Einzelentscheidern hat beim BAFl unter der Bezeichnung „Einzelentscheiderstatistik" eine Vorgeschichte. Die Übersicht soll der Einsatzplanung, der Beurteilung, der Erstellung von Zeugnissen sowie zur Feststellung der Bewährung der Einzelentscheider dienen. Sie enthält neben dem Namen des Einzelentscheiders und dessen Beschäftigtenstatus (Voll- oder Teilzeitbeschäftigung) Angaben zum Aktenzeichen des bearbeiteten Vorganges, Anhörungsdatum, Bearbeitungsdauer, Schwierigkeitsgrad, Besonderheiten bei der Bearbeitung (z. B. ausschweifende Antworten, umfangreicher Vortrag, Anhörung in JVA) sowie Bemerkungen über Abwesen-

heitstage wegen Urlaubs, Krankheit oder sonstiger Tätigkeiten. Die Übersicht ist vom Einzelentscheider sowie vom Referatsleiter (Außenstellenleiter) zu unterzeichnen.

Dazu haben Einzelentscheider in Eingaben die Übersicht als unzulässige Verhaltens- und Leistungskontrolle bezeichnet. Aufgrund meiner Nachfrage zur Erforderlichkeit dieser Übersicht wurde vom Präsidenten des BAFl zunächst entschieden, daß sie mit Wirkung vom 1. März 1996 nicht mehr benötigt wird. Mit Dienstanweisung vom 18. September 1996 wurde den Leitern der Außenstellen jedoch freigestellt, selbst zu entscheiden, ob sie die Einzelentscheiderstatistik für erforderlich halten.

Hierzu ist festzustellen, daß der Dienstherr über Mitarbeiter personenbezogene Daten nur erheben darf, soweit dies zur Begründung, Durchführung, Beendigung oder Abwicklung des Dienstverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwekken der Personalplanung und des Personaleinsatzes erforderlich ist oder eine Rechtsvorschrift dies erlaubt (§ 90 Abs. 4 BBG).

Die mit der Dienstanweisung vom 18. September 1996 wieder eingeführten Erhebungsbögen beim BAFl sollen, soweit ihr Einsatz von den Leitern der Außenstellen für erforderlich gehalten wird, der Einsatzplanung und Beurteilung der Mitarbeiter sowie der Erstellung von Zeugnissen und zur Feststellung der Bewährung der Mitarbeiter dienen.

Ob der Fragebogen damit die Voraussetzungen des § 90 Abs. 4 BBG erfüllt, erschien mir aufgrund der Vorgeschichte zweifelhaft, da die Erforderlichkeit des Erhebungsbogens nur bejaht werden kann, wenn Einsatzplanung und Beurteilung der Mitarbeiter sowie die Erstellung von Zeugnissen und die Feststellung der Bewährung ohne die mit der Übersicht erhobenen Angaben allgemein nicht möglich wären. Insofern ist auch die Frage klärungsbedürftig, wieso die Übersicht in einzelnen Außenstellen erforderlich sein soll, in anderen wiederum nicht. Soweit die aktuelle Dienstanweisung vorsieht, „die Erforderlichkeit unter Berücksichtigung der örtlichen Gegebenheiten" zu beurteilen, ist bisher nicht nachvollziehbar, welche örtlichen Gegebenheiten die Erforderlichkeit eines Fragebogens unterschiedlich beeinflussen könnten. Besondere Kriterien hierzu sind in der Dienstanweisung vom 18. September 1996 nicht ersichtlich.

Falls und soweit die Erhebung der in Rede stehenden Daten letztlich doch erforderlich sein sollte, wäre das Verfahren zu den genannten Zwecken nur mit Genehmigung des BMI (§ 90 Abs. 4 Satz 2 BBG) zulässig. Darüber hinaus wäre die Personalvertretung zu beteiligen und eine Dienstvereinbarung abzuschließen (§§ 75 Abs. 3 Nrn. 8 und 9, 76 Abs. 2 Nrn. 2 und 3 BPersVG).

Die Erörterung der dargestellten Problematik mit dem BMI und dem BAFl hat verdeutlicht, daß die Erhebung der genannten Daten im wesentlichen der Steuerung der Geschäftsverteilungs-, Organisations- und Fortbildungsplanung dienen soll. In die Beurteilung der Einzelentscheider soll sie nur teilweise, als ein Aspekt von vielen, einfließen.

Es bestand Einigkeit darüber, daß entsprechende Erhebungsbögen der Genehmigung des BMI bedürfen. Ich habe darauf hingewiesen, daß der Zweck der Erhebung in einer entsprechenden Dienstanweisung eindeutig festgelegt und gegenüber den Mitarbeitern ggf. auch näher erläutert werden muß.

Von BMI und BAFl wurde mir zugesagt, für die Übersicht über die Arbeitsergebnisse im Bereich der Einzelentscheider ein neues Konzept zu entwickeln, wobei auch geprüft wird, ob die Personalvertretung zu beteiligen ist.

18.10 Kontrollen im Personalwesen

Im Berichtszeitraum habe ich wieder mehrere Beratungen und Kontrollen im Bereich der Personaldatenverarbeitung durchgeführt:

18.10.1 Bewerberverfahren verbessert

In der Außenstelle Berlin des BMWi habe ich festgestellt, daß bei Ablehnung die Unterlagen von Bewerbern – mit Ausnahme der Bewerbungsschreiben selbst – den Bewerbern zurückgesandt werden. Die Bewerbungsschreiben werden danach in der allgemeinen Registratur und nicht in der Personalregistratur aufbewahrt. Die zurückgehaltenen Bewerbungsschreiben enthalten oftmals sensible Angaben, z. B. über Qualifikationen, Fähigkeiten, Werdegang usw. der Betroffenen.

Weiterhin habe ich festgestellt, daß im Bereich der Außenstelle eine automatisierte Bewerberdatei geführt wird, in der Bewerbernummer, Ausschreibungsnummer, Familien- und Vorname, Geschlecht, die Funktion, für die die Bewerbung erfolgte sowie ggf. allgemeine Vermerke über abgelehnte Bewerber gespeichert werden. Die Notwendigkeit einer derartigen Datei wurde damit begründet, daß beim endgültigen Vollzug des Umzuges von Bonn nach Berlin möglichst kurzfristig geeignete Mitarbeiter ausgesucht und eingestellt werden müßten. Die abgelehnten Bewerber wurden über diese Datenspeicherung nicht informiert.

Die Speicherung dieser Daten ist jedoch im Falle einer endgültig abgelehnten Bewerbung für die Aufgabenerfüllung des BMWi nicht mehr erforderlich. Dies gilt auch z. B. im Hinblick auf die Rechnungsprüfung, Reisekostenerstattung. Diese Zwecke könnten auch dadurch erfüllt werden, daß nur eine Kopie des Antwortschreibens an den Bewerber in den Akten verbleibt. Diese Kopie würde gleichzeitig die Funktion erfüllen, zu einem späteren Zeitpunkt festzustellen, ob sich der Betreffende bereits früher einmal beim BMWi beworben hat.

Diese Datenspeicherungen sind rechtlich problematisch, da es sich um unzulässige Vorratsspeicherungen handelt. Denn zum Zeitpunkt der Kontrolle war in keiner Weise absehbar, ob die Betroffenen jemals wieder für eine Anstellung im BMWi in Betracht kommen würden. Ein datenschutzrechtlich korrektes Vorgehen wäre hier gewesen, die Einwilligung der

Betroffenen zu einer entsprechenden Speicherung einzuholen oder diese hierüber zu informieren und ihnen eine Widerspruchsmöglichkeit einzuräumen.

Inzwischen hat mir das BMWi zugesagt, die Bewerbungsschreiben bei endgültiger Absage zu vernichten und hinsichtlich der Bewerberdatei künftig wie von mir vorgeschlagen zu verfahren.

18.10.2 Mängel bei der Personalaktenführung

Bei der Außenstelle Berlin des BMWi und bei zwei Arbeitsämtern habe ich den Inhalt von Personalakten geprüft, die nach dem Zufallsprinzip aus unterschiedlichen Laufbahngruppen ausgewählt worden waren.

In keiner der eingesehenen Personalakten befand sich ein Verzeichnis über Teil- und Nebenakten i.S.d. § 90 Abs. 2 BBG. Weiterhin waren die Seitenzahlen in einigen Personalakten nicht ordnungsgemäß numeriert. Teilweise war die Paginierung unvollständig oder mangelhaft oder sie fehlte ganz.

Ich habe von den geprüften Stellen gefordert, die Paginierung wie auch die Aufnahme der Verzeichnisse über Teil- und Nebenakten kurzfristig nachzuholen. Beides ist unerläßlich, um das Einsichtsrecht der Betroffenen nach § 90c Abs. 1 BBG sicherzustellen. Nur wer Kenntnis hat, in welchen Unterlagen sich Personaldaten über ihn befinden, und außerdem davon ausgehen kann, daß seine Personalakte keine ihm nicht bekannten Lücken aufweist, kann sein Einsichtsrecht umfassend wahrnehmen.

Sowohl BMWi als auch die BA haben meinen Empfehlungen inzwischen entsprochen.

18.10.3 Verstöße gegen das Personalaktengeheimnis

Bei den kontrollierten Arbeitsämtern habe ich weiterhin festgestellt, daß in einigen Personalakten Unterlagen abgelegt waren, die Informationen über andere Mitarbeiter enthielten, die u. a. Anfragen an die Gauck-Behörde zu mehreren Mitarbeitern betrafen.

Dies ist mit dem Personalaktengeheimnis nicht vereinbar. Nach der Aufnahme dieser Unterlagen in die Personalakte hätte der betroffene Mitarbeiter bei Gelegenheit der Einsichtnahme in seine Personalakte gleichzeitig die Möglichkeit, Personalaktendaten seiner Kollegen zur Kenntnis zu nehmen.

Soweit für die Aufgabenerfüllung der Personalabteilung erforderlich, sollten Unterlagen mit Angaben zu mehreren Mitarbeitern in einer Sachakte abgelegt werden oder es sollten, soweit Ablichtungen zu den einzelnen Personalakten der betroffenen Mitarbeiter verfügt werden, in diesen die Namen der anderen Mitarbeiter unkenntlich gemacht werden.

Weiterhin habe ich in mehreren Personalakten Unterlagen mit teilweise besonders schützenswerten personenbezogenen Daten (auch Dritter) festgestellt, die nach § 90 Abs. 1 BBG nicht in die Personalakte aufgenommen werden dürfen – so beispielsweise die Ablichtung eines vollständigen Mutterpasses mit zahlreichen Diagnose-/Anamneseangaben.

Die BA hat inzwischen hinsichtlich der konkreten Feststellungen und für die Zukunft eine datenschutzgerechte Verfahrensweise im Umgang mit Personalakten ihrer Mitarbeiter zugesagt.

19 Sozialwesen – Allgemeines

19.1 Status des internen Datenschutzbeauftragten bei Sozialleistungsträgern

19.1.1 Zulässigkeit der Bestellung eines externen Datenschutzbeauftragten

Eine große Berufsgenossenschaft hat die Frage an mich herangetragen, ob sie auch einen externen Datenschutzbeauftragten als gesetzlichen Datenschutzbeauftragten nach § 81 Abs. 4 SGB X bestellen kann.

Aus § 81 Abs. 4 Satz 1 SGB X i.V.m. § 36 Abs. 1 BDSG folgt für die Sozialleistungsträger die Pflicht, einen Beauftragten für den Datenschutz zu bestellen. § 36 Abs. 1 BDSG schließt die Bestellung externer Personen zum Datenschutzbeauftragten nicht ausdrücklich aus; die Vorschrift stellt Anforderungen an die Person, läßt aber offen, ob sie fest angestellt sein muß. Nach meiner Kenntnis bestellen vor allem solche kleinere Unternehmen einen externen Datenschutzbeauftragten, in denen die datenschutzrechtlichen Erfordernisse und die personellen Ressourcen die Bestellung eines eigenen Mitarbeiters zum Datenschutzbeauftragten nicht nahelegen oder ermöglichen.

Derartige Gründe können aber nicht ohne weiteres auf die gesetzliche Sozialversicherung übertragen werden. Diese unterscheidet sich vom nicht-öffentlichen Bereich bereits durch die besondere Schutzwürdigkeit der Daten und des vielfältigen gesetzlich bestimmten Umgangs mit ihnen. Im Fall der Berufsgenossenschaft kommt hinzu, daß die zu schützenden Betroffenen aufgrund gesetzlicher Vorschriften unfallversichert sind und daher – anders als im nicht-öffentlichen Bereich – auf eine Rechtsbeziehung zum Unfallversicherungsträger nicht verzichten können. Diese und andere Besonderheiten haben sich in bereichsspezifischen Regelungen zum Sozialdatenschutz niedergeschlagen, die im Vergleich zum BDSG einen höheren Schutz festlegen.

Diese Erwägungen lassen die Bestellung eines externen Datenschutzbeauftragten im Bereich der gesetzlichen Sozialversicherung daher allenfalls in Ausnahmefällen zu, wie z. B. bei sehr kleinen Sozialleistungsträgern.

19.1.2 Zulässigkeit einer befristeten Bestellung des gesetzlichen Datenschutzbeauftragten

Ein Sozialleistungträger wollte wissen, ob eine befristete Bestellung des gesetzlichen Datenschutzbeauftragten nach § 81 Abs. 4 SGB X zulässig ist.

Bei einer befristeten Bestellung besteht die Gefahr, daß der Abberufungsschutz des § 36 Abs. 3 Satz 4 BDSG unterlaufen wird, der insbesondere auch eine von Konformitätsmotiven unbeeinflußte unabhängige gesetzliche Aufgabenerfüllung des Daten-

schutzbeauftragten gewährleisten soll. Für die Beurteilung der Zulässigkeit der Befristung im Bereich der gesetzlichen Sozialversicherung kommt es unter dem Aspekt der Aufgabenerfüllung zudem entscheidend auf die Zahl der von der Datenspeicherung betroffenen Personen, die Sensibilität der zu verarbeitenden Daten, den Umfang der Datenspeicherung je betroffener Person sowie auf Umfang und Häufigkeit der Datenweitergabe an Dritte an. Eine zu kurz bemessene Befristung dürfte einer gesetzlichen Aufgabenerfüllung im Wege stehen. Daher halte ich eine befristete Bestellung zwar nicht von vornherein für unzulässig, aber doch für problematisch.

Der anfragende Sozialleistungsträger hat das Problem der Befristung durch eine Regelung gelöst, die eine einvernehmliche Beendigungsmöglichkeit der Amtsausübung nach 5 Jahren vorsieht. Diesen Weg halte ich für akzeptabel.

19.2 Prüfungspflicht und Verantwortlichkeit bei Übermittlungen

Auskunftsersuchen von oder bei Sozialleistungsträgern gehören zu den notwendigen Routinevorgängen im Bereich der Sozialversicherung. In § 67d SGB X hat der Gesetzgeber festgelegt, in welchen Fällen solche Datenübermittlungen zulässig sind. Dabei trägt immer die übermittelnde Stelle die Verantwortung für die Entscheidung, ob die Übermittlung von Sozialdaten zulässig ist. Das gilt auch, wenn die Übermittlung die Antwort auf ein Auskunftsersuchen ist (§ 67d Abs. 2 SGB X). Also muß die Anfrage der ersuchenden Stelle hinreichende Angaben enthalten, die es der ersuchten Stelle ermöglicht, die Rechtmäßigkeit der Datenübermittlung zu prüfen.

Ich habe festgestellt, daß solche Angaben in der Praxis zuweilen fehlen oder vielfach nur oberflächlich erfolgen, besonders wenn es sich um standardisierte Auskünfte in Massenverfahren handelt. Auch in diesen Fällen ist ein bloßer allgemeiner Hinweis auf den Grund des Auskunftsersuchens oder lediglich auf „Aufgaben nach dem SGB" nicht ausreichend. Das BMA hat hervorgehoben, daß ein Auskunftsersuchen sich auf die Übermittlung besonders schützenswerter personenbezogener Daten beziehen kann und daher in jedem Einzelfall abzuwägen ist, wie konkret die jeweilige Begründung sein muß. Im Hinblick auf den Ersterhebungsgrundsatz (§ 67a Abs. 2 Satz 1 SGB X) gehört es zu den notwendigen Angaben der ersuchenden Stelle, warum die Erhebung beim Betroffenen für sie einen unverhältnismäßigen Aufwand erfordert oder daß die bisher vom Betroffenen vorliegenden Angaben unvollständig, widersprüchlich oder offensichtlich unrichtig sind. Beruht die Anforderung der Daten auf der Zustimmung des Betroffenen (§ 60 Abs. 1 Nr. 1, 2. Alt. SGB I) oder auf seiner Einwilligung (§ 67b SGB X), so ist auch dies anzugeben. Bei der Anforderung von medizinischen Daten halte ich die Angabe für geboten, daß der Versicherte auf sein Widerspruchsrecht hingewiesen wurde, hiervon aber keinen Gebrauch gemacht hat (§ 76 Abs. 2 SGB X).

Ich habe die Spitzenverbände der Sozialleistungsträger entsprechend informiert und um Berücksichtigung dieser Rechtslage gebeten. Von diesen und aus dem Kreis der Landesbeauftragten für den Datenschutz habe ich erfahren, daß die Überprüfung und gegebenenfalls eine Anpassung der Verwaltungsverfahren an die genannten Darlegungserfordernisse begonnen hat.

19.3 Zusammenarbeit mit den Spitzenverbänden der Sozialleistungsträger

Wegen der Vielzahl der meiner Kontrolle unterliegenden Sozialleistungsträger werde ich oft mit vergleichbaren Fragestellungen innerhalb eines Versicherungszweiges befaßt. Um meiner Beratungsaufgabe nach § 81 Abs. 2 SGB X i. V. m. § 26 Abs. 3 BDSG umfassend nachkommen zu können, bin ich darauf angewiesen, daß ich insbesondere bei übergreifenden Problemen und bei der Mitwirkung an Gesetzgebungsvorhaben von den Spitzenverbänden der einzelnen Versicherungszweige unterstützt werde. Gespräche sowohl auf Initiative von Spitzenverbänden als auch auf meine Initiative gaben im Berichtszeitraum Gelegenheit, Form und Wege der Zusammenarbeit grundsätzlich zu besprechen. Damit ist für die künftige Arbeit eine gute Grundlage gelegt. Auf die Sachkompetenz und Koordinierungsfunktion der Spitzenverbände kann ich nicht verzichten und werde daher stärker als bisher auf sie zurückgreifen.

19.4 Sonstige Gesetzgebungsvorhaben

Im Berichtszeitraum gab es mehrere datenschutzrechtlich relevante Gesetzgebungsvorhaben im Sozialrecht. In gesonderten Kapiteln dieses Berichts sind das Arbeitsförderungs-Reformgesetz (AFRG, Einordnung des AFG in das SGB als dessen Drittes Buch), und das Unfallversicherungseinordnungsgesetz – UVEG – (s. u. Nrn. 20.5 und 23.1) behandelt.

- **Gesetz zur Änderung des Asylbewerberleistungsgesetzes und anderer Gesetze**

  Der Entwurf eines Gesetzes zur Änderung des Asylbewerberleistungsgesetzes und anderer Gesetze sieht Datenabgleichs- und -übermittlungsverfahren zwischen den Sozialleistungsträgern einerseits und den für die Ausführung des Asylbewerberleistungsgesetzes zuständigen Behörden und anderen Stellen andererseits vor.

  Es ist unbestritten, daß sich der Staat gegen Leistungsmißbrauch schützen muß, nicht zuletzt auch, um das System der sozialen Sicherung im Interesse aller Berechtigten zu schützen. Da von Datenabgleichsverfahren immer jedoch auch redliche Bürger erfaßt werden und ihre persönlichen Verhältnisse mit jedem zusätzlichen Datenabgleich an einer Stelle immer transparenter und für den jeweiligen Bearbeiter umfassender offengelegt werden, ist vor ihrer Einrichtung jeweils zu prüfen, ob sie im Interesse des Gemeinwohls zur Erreichung eines konkreten Zieles erforderlich und verhältnismäßig sind. Dies hat der Deutsche Bundestag auf Empfehlung des Innenausschusses am 22. Juni 1995 beschlossen. Darauf habe ich im Rahmen

meiner Beteiligung am Gesetzgebungsverfahren hingewiesen. Ein Datenabgleich kann nicht etwa mit der damit verbundenen Geschäftserleichterung begründet werden, sondern er muß erforderlich sein, um tatsächlich bestehende Mißstände, insbesondere unberechtigten Leistungsbezug, zu vermeiden. Wird der Datenabgleich für erforderlich gehalten, sind die Daten, die zwecks Abgleich übermittelt werden sollen, im Gesetz selbst oder in einer Rechtsverordnung aufzuführen und die Stellen zu nennen, zwischen denen der Datenabgleich zulässig ist. Die Betroffenen sollten auf Datenabgleiche zur Verhinderung von Leistungsmißbrauch durch Hinweise in Vordrucken und Merkblättern aufmerksam gemacht werden.

Der Bundesrat hat dem Gesetz zur Änderung des Asylbewerberleistungsgesetzes und anderer Gesetze insgesamt die Zustimmung versagt. Bei Redaktionsschluß war der vom Bundestag angerufene Vermittlungsausschuß mit den Entwürfen befaßt.

– **Gesetz zur Reform der Sozialhilfe**

In Kraft getreten ist eine Ergänzung von § 117 Abs. 3 BSHG, die den Datenabgleich auch zwischen den Trägern der Sozialhilfe und *„anderen Stellen ihrer Verwaltung, bei ihren wirtschaftlichen Unternehmen und bei den Kreisen, Kreisverwaltungsbehörden und Gemeinden"* ermöglicht. Hierdurch soll beispielsweise festgestellt werden können, ob ein Sozialhilfeempfänger Halter eines Kraftfahrzeuges ist. Der Wortlaut der Vorschrift ist auf meine Empfehlung hin präzisiert worden.

Entsprechend meinem Votum wurde davon abgesehen, einen Abgleich von Sozialhilfedaten mit Sozialversicherungsdaten, die bei der Datenstelle der Rentenversicherungsträger beim Verband Deutscher Rentenversicherungsträger (VDR) gespeichert sind, einzuführen. Diese Änderung hätte der Datenstelle eine neue Aufgabe zugewiesen, die quantitativ wie qualitativ eine erhebliche Erweiterung bedeutet hätte. Die Zweckbestimmung und die Grenzen zulässiger Übermittlung durch Einrichtung automatisierter Abrufverfahren wären überschritten worden (§ 150 Abs. 4 SGB VI). Ein umfassender „Sozialdatenpool" wäre aus verfassungsrechtlichen Gründen höchst problematisch.

– **Gesetz zur Änderung des Gesetzes zur Regelung von Vermögensfragen der Sozialversicherung im Beitrittsgebiet**

Dieses Änderungsgesetz regelt den Verbleib, die Speicherung und die Nutzung des Gesundheitsdatenarchivs des Uranerzbergbaus „SDAG Wismut" (Sowjetisch-Deutsche Aktiengesellschaft Wismut).

Im Süden Sachsens und Thüringens betrieb die ehemalige DDR von 1946 bis 1989 einen Uranerzbergbau. Hier wurden 200 000 t Uran gefördert. Insgesamt waren ca. 600 000 Personen bei der SDAG Wismut beschäftigt. 7 000 von ihnen sind bislang an Lungenkrebs erkrankt. Die Gesamtzahl der zu erwartenden Fälle wird auf 20 000 geschätzt.

Das Gesundheitswesen Wismut war umfassend für die ärztliche Betreuung der Beschäftigten des Uranerzbergbaus und ihrer Angehörigen zuständig (s. auch 14. TB Nr. 2.4). Behandelt wurden vielfach auch andere Bewohner der Region. Hieraus ist ein Gesundheitsdatenarchiv entstanden, das u. a. etwa 1,2 Millionen Krankenakten, 1,2 Millionen pathologische Präparate und 45 000 Sektionsprotokolle verwahrt. Zudem existieren genaue Aufzeichnungen über den betrieblichen Einsatz der Beschäftigten, wie beispielsweise Schichtpläne, die Rückschlüsse auf Art und Intensität ihrer Exposition durch Uran ermöglichen.

Zur Abwicklung des ehemaligen Uranerzbergbaus einschließlich der Sanierung der betroffenen Natur ist im Geschäftsbereich des Bundesministeriums für Wirtschaft die Wismut GmbH gegründet worden, in deren Besitz und Verwahrung sich auch das Gesundheitsdatenarchiv befand.

Nach Auflösung des Gesundheitswesens der SDAG Wismut sind Fortbestand und Zugang zu den Gesundheitsdaten von erheblicher Bedeutung, und zwar für die ehemaligen Beschäftigten und Angehörigen für deren weitere ärztliche Behandlung sowie deren unfallversicherungsrechtliche Betreuung in Verfahren zur Anerkennung von Berufskrankheiten. Aber auch zur Erforschung von Risiken und Folgen der Uranexposition sowie zur Gewinnung von Erkenntnissen für Präventivmaßnahmen und für den Arbeitsschutz stellt der Datenbestand ein weltweit einmaliges Material dar.

In intensiver und konstruktiver Zusammenarbeit unter Federführung des BMA mit dem BMJ, dem BMWi, dem BMU, der Bundesanstalt für Arbeitsmedizin (BAfAM) und dem Bundesversicherungsamt ist es gelungen, der außergewöhnlichen Situation angemessene Regelungen zu schaffen, die den Interessen sowohl der individuell Betroffenen als auch der wissenschaftlichen Forschung gerecht wird.

Das Gesundheitsdatenarchiv wurde auf die BAfAM übertragen. Sie darf Daten an Sozialleistungsträger im Rahmen deren gesetzlicher Aufgaben übermitteln. Für die wissenschaftliche Forschung darf die BAfAM die Daten selbst nutzen oder dem Bundesamt für Strahlenschutz (BfS) oder anderen wissenschaftliche Forschung betreibenden öffentlichen oder privaten Stellen übermitteln. Für solche an den Forschungszweck gebundene Übermittlungen gelten strenge Anforderungen an die Person des Empfängers, den Standard des bei ihr einzuhaltenden Datenschutzes und die Einhaltung der Zweckbindung für die Forschung. Zudem sind die Daten sobald wie möglich zu anonymisieren. Die Befugnisse der für den Datenschutz zuständigen Aufsichtsbehörde sind über § 38 BDSG hinaus erweitert. Eine ergänzende Regelung betrifft Daten, die zu einem früheren Zeitpunkt den gewerblichen Berufsgenossenschaften zugewiesen worden waren.

Mit dem Inkrafttreten dieses Änderungsgesetzes wird nunmehr eine datenschutzgerechte gesetzliche Regelung für diese sensiblen Gesundheitsdaten geschaffen.

- **Unterhaltsvorschußgesetz**

  Durch eine Änderung des Unterhaltsvorschußgesetzes sollen auch Versicherungsunternehmen verpflichtet werden, Auskünfte über den Wohnort und über die Höhe von Einkünften des Elternteils, bei dem der Unterhaltsberechtigte nicht lebt, zu geben. Die bisherige Übermittlungsbefugnis der Sozialleistungsträger wurde durch eine entsprechende Verpflichtung präzisiert. Diese Änderung des Gesetzes wurde wegen der steigenden Zahl unterhaltsflüchtiger Väter geschaffen.

  Für mich zählt das Recht des Kindes auf angemessenen Unterhalt höher als die mit den Gesetzesänderungen vorgesehenen möglichen Eingriffe in das Persönlichkeitsrecht des Unterhaltspflichtigen. Insofern habe ich lediglich Empfehlungen zur Durchführung gegeben.

  So habe ich dem zuständigen BMFSFJ empfohlen, daß grundsätzlich zuerst der unterhaltsverpflichtete Elternteil selbst aufgefordert wird, seiner Auskunftspflicht nachzukommen. Die Anfrage sollte mit dem Hinweis verbunden werden, daß bei Zweifeln an seiner Auskunft auch eine Anfrage bei Sozialleistungsträgern, privaten Versicherungen und seinem Arbeitgeber (bisheriges Recht) möglich ist. Über die Anfrage bei Dritten sollte der Unterhaltsverpflichtete, beispielsweise durch Überlassung einer Kopie des Auskunftsersuchens, informiert werden.

  Das zuständige BMFSFJ hat mir zugesagt, meine Empfehlungen in der Verwaltungsvorschrift zur Durchführung des Unterhaltsvorschußgesetzes zu berücksichtigen.

19.5 Sozialdaten auf Überweisungsträgern

Sozialleistungen, die in Geld zu erbringen sind, erfolgen meist durch Überweisung auf ein Girokonto. Als Erläuterungstext wurde bisher die Art der Sozialleistung oder allgemein „Sozialleistung" angegeben, bisweilen ergänzt durch das Aktenzeichen. Für die Zahlung der Sozialhilfe hat das Bundesverwaltungsgericht (BVerwG) 1994 entschieden, daß die Angabe „Sozialleistung" im Feld „Verwendungszweck" des Überweisungsträgers bzw. im Feld Buchungserläuterung im Kontoauszug ohne Zustimmung des Hilfeempfängers unzulässig ist. Das BVerwG hat zurecht darauf hingewiesen, daß es sich schon bei der Tatsache des Bezugs von Sozialhilfe um Sozialdaten handelt. Für die Qualifizierung als Sozialdaten spiele es keine Rolle, ob den Daten etwas anhaftet, das als diskriminierend empfunden werden kann.

Die Übermittlung von Sozialdaten an Dritte, wie eben an die mit der Ausführung der Überweisung betrauten Geldinstitute, ist ohne Zustimmung des Betroffenen nach dem Gesetz nur zulässig, soweit es für die Aufgabenerfüllung des Sozialleistungsträgers erforderlich ist. Erforderlich ist die Kennzeichnung der Überweisung als „Sozialleistung" aber selbst unter dem Gesichtspunkt des Informationsbedürfnisses des Empfängers nicht, weil die Angabe „Leistung gemäß Antrag vom ..." im Erläuterungstext eine ebenso eindeutige Zuordnung ermöglicht.

Da das Urteil des BVerwG Bedeutung für alle Sozialleistungsbereiche hat, hat die BA auch aufgrund einer Eingabe ihr Verfahren ab Anfang 1997 dahin gehend geändert, daß das Kürzel „ALHIA" bei der Zahlung von Arbeitslosenhilfe entfällt.

Auch bei der Überweisung von Leistungen nach dem Bundesausbildungsförderungsgesetz (BAföG) ist eine entsprechende Neutralisierung des Erläuterungstextes geboten. Hier besteht nach der aktuellen Rechtslage allerdings die Besonderheit, daß in der Allgemeinen Verwaltungsvorschrift zum BAföG ein Hinweis darauf, daß der gezahlte Betrag eine Leistung nach dem BAföG ist, ausdrücklich vorgesehen ist. Ich habe, der Anregung eines Landesbeauftragten für den Datenschutz folgend, das BMBF gebeten, die Verwaltungsvorschrift an die Rechtslage nach dem Urteil des BVerwG anzupassen.

Betroffen ist auch die Rentenversicherung. Allerdings geht es hier um über 22 Millionen monatliche Rentenzahlungen, die die Rentenrechnungsstellen der Deutschen Post AG anweisen. Jede Änderung dieses Massenverfahrens muß deshalb auch zuvor mit dessen Auswirkungen sorgfältig abgewogen werden. Die Deutsche Post AG hat zurecht darauf hingewiesen, daß die bloße Bezugnahme auf den Rentenantrag des Versicherten nicht ausreicht, weil die regelmäßigen Rentenanpassungen antragslos erfolgen. Ich bin zuversichtlich, daß ich im Kontakt mit der Deutschen Post AG auch für den Bereich der Rentenüberweisungen eine ebenso sachgerechte wie datenschutzgerechte Lösung finden werde.

19.6 Aktenarme Verwaltung

In der Praxis wird der Inhalt routinemäßiger Auskünfte zwischen Sozialleistungsträgern oftmals nicht – etwa in Form einer Aktennotiz – protokolliert. Festgehalten werden lediglich Tatsache und Datum der Auskunft. Gegenstand solcher Datenübermittlungen sind nicht nur Angaben geringerer datenschutzrechtlicher Sensibilität, sondern etwa auch solche über Gesundheitsdaten. Unter dem Stichwort „aktenarme Verwaltung" wird die dokumentationslose Auskunftserteilung als entbürokratisierende Aufwandminimierung und damit als vorteilhaft bewertet.

Dieses Verfahren ist nicht unproblematisch. So kann der Betroffene seinen Auskunftsanspruch gegen die Verwaltung in den Fällen derartiger Datenübermittlungen nicht oder nur sehr schlecht realisieren. Denn soweit eine Datenübermittlung nicht dokumentiert wird, erschließt sie sich dem Betroffenen auch im Wege der Akteneinsicht nicht. Zum einen wird das gesetzliche Einsichts- und Auskunftsrecht des Versicherten (§§ 25 und 83 SGB X) fraglich: Der Versicherte kann nicht mehr feststellen, „wer was wann und bei welcher Gelegenheit" über ihn weiß, wie das BVerfG das Transparenzgebot im Volkszählungs-

gesetz formuliert hat. Zum anderen werden auch die Kontrollpflichten und -befugnisse der internen Datenschutzbeauftragten (§ 81 Abs. 4 SGB X i.V. m. § 37 BDSG) und der Aufsichtsbehörden, insbesondere des Bundesversicherungsamtes und meines Hauses, beeinträchtigt.

Wird die Auskunft beispielsweise urschriftlich auf dem Anforderungsschreiben erteilt, so läßt sich später nicht nachprüfen, ob das Übermittlungsersuchen hinreichende Angaben zur Begründung der Übermittlungsbefugnis enthielt (§ 67 d Abs. 2 SGB X). Auch ließe sich nicht mehr feststellen, ob der Versicherte auf sein Widerspruchsrecht hingewiesen wurde, das ihm das Gesetz insbesondere bei der Übermittlung von ärztlichen Daten zugesteht (§ 76 Abs. 2 Nr. 1 SGB X).

Gegen eine Protokollierungsverpflichtung der Übermittlungen ist vom BMA eingewandt worden, es könnten gerade durch sie „Datenfriedhöfe" entstehen; auch schreibe das Gesetz die Protokollierung nicht ausdrücklich vor.

Diese Argumentation überzeugt aber nicht, weil sie den Verfassungsrang des informationellen Selbstbestimmungsrechts des Versicherten nicht berücksichtigt. Die Frage, welche konkreten Folgerungen sich aus dem Transparenzgebot ableiten, wird derzeit in meiner Dienststelle unter verfassungsrechtlichen Gesichtspunkten geprüft. Eine Lösungsmöglichkeit könnte darin bestehen, daß der Versicherte eine Kopie der urschriftlich erteilten Auskunft erhält. Dadurch würde er informiert, ohne daß eine Speicherung des Auskunftsinhalts bei der übermittelnden Stelle erforderlich wäre. Ein ähnliches, datenschutzgerechtes Verfahren hat der Gesetzgeber jüngst in § 188 Satz 3 und 4 SGB VII eingeführt.

20 Arbeitsverwaltung

20.1 Beratungsvermerke in der computerunterstützten Arbeitsvermittlung

In meinem 15. Tätigkeitsbericht (Nr. 11.2) hatte ich zuletzt darüber berichtet, daß die Erhebung und die Speicherung personenbezogener Daten für die Arbeitsvermittlung und -beratung in einem für alle Arbeitsämter geltenden Runderlaß der BA grundsätzlich datenschutzgerecht geregelt sind. Ich hatte dargestellt, daß ich die Weisungslage zu Form und Inhalt individueller Beratungsvermerke für ausreichend erachte, wonach Arbeits- und Ratsuchende weder negativ gekennzeichnet noch subjektive Eindrücke und Bewertungen in den Vermerken aufgenommen werden dürfen, daß es in Einzelfällen allerdings immer wieder Probleme bei der Umsetzung dieser Regelung in der Praxis gibt.

Die BA hatte im Anschluß an die Kontrolle eines Arbeitsamtes (s. Nr. 20.3) zugesagt, meine Anregungen aufzugreifen und die gesamte o.a. Problematik den Fachkräften der Arbeitsvermittlung und Arbeitsberatung durch eine konkretisierende Darstellung von Positiv- und Negativbeispielen zu verdeutlichen. Sie hatte dargelegt, daß es wegen der erheblichen Auswirkungen auf die Vermittlungstätigkeit der BA jedoch noch intensiver Beratungen auch in der Praxis bedürfe; der danach zu erarbeitende Erlaß würde mit mir abgestimmt werden.

Der erste Entwurf des neuen Erlasses zu den Eintragungen in den Beratungs- und Vermittlungsunterlagen enthält neben entsprechenden Grundsätzen hierfür erstmalig Beispiele für zulässige Formulierungen aber auch unzulässige Eintragungen, die einen Datenschutzverstoß darstellen:

- Nicht zu beanstanden wären Formulierungen wie:
  - Tätigkeit mit Ausnahme im Arzneimittelbereich (bei Drogenabhängigen)
  - Tätigkeit ohne Kontakt mit Spirituosen (bei Alkoholabhängigen)
  - Tätigkeit ohne besondere Streßbelastung (bei psychisch Kranken)
  - Tätigkeit ohne schweres Heben und Tragen
  - keine ausschließlich stehende Tätigkeit
  - kann aus gesundheitlichen Gründen Beruf nicht mehr ausüben
- Nicht statthaft sind Eintragungen wie:
  - Arbeitslosmeldung nach Drogentherapie/Entziehungskur
  - hat Alkoholprobleme
  - verdeckte Kennzeichnung, wie ***/—/YYY
  - rassistische Kennzeichnung
  - einschlägig vorbestraft
  - destruktives und unsoziales Verhalten
  - anscheinend psychische Probleme

Der vorgesehene Erlaß wird den Datenschutz im Arbeitsamt weiter fördern.

20.2 Neue Wege der Selbstinformation bei der Bundesanstalt für Arbeit

Die BA hat mir mitgeteilt, daß im Zuge der Weiterentwicklung der Arbeitsberatung und der Arbeitsvermittlung ein Selbstinformationssystem in ausgewählten Modellregionen bzw. Modellarbeitsämtern seit Januar 1996 erprobt werde, das aus den Komponenten Arbeitgeber-Informations-Service, Stellen-Informations-Service und Informationspräsentation der BA besteht. Für die Erprobungszeit dieses Systems, mit dem Arbeitgeber und Arbeitnehmer über öffentliche Netze Stellenangebote, Bewerberangebote und Informationen über das Dienstleistungsangebot der BA aufrufen und die für sie geeigneten Angebote auswählen können, sind laut BA etwa 18 bis 24 Monate vorgesehen.

Bei dem Selbstinformationssystem handelt es sich um ein ergänzendes zusätzliches Service-Angebot der Arbeitsverwaltung. Arbeitsuchende und Arbeitgeber können selbst bestimmen, in welchem Umfang und mit welcher Intensität sie Informationen zum Dienst-

leistungsangebot, zu Stellenangeboten und zu Bewerberprofilen abrufen wollen. Unabhängig von diesen Möglichkeiten, sich selbst – ohne Hilfe von Mitarbeitern eines Arbeitsamtes – zu informieren, kann jeder Arbeitgeber und jeder Arbeitsuchende das gesamte Dienstleistungsangebot der BA einschließlich individueller Beratung und Vermittlung in Anspruch nehmen.

Sowohl der Arbeitgeber-Informations-Service wie auch der Stellen-Informations-Service sind von datenschutzrechtlicher Relevanz, da sie Sozialdaten enthalten können. Beim Arbeitgeber-Informations-Service handelt es sich dabei im wesentlichen um Sozialdaten der Bewerber (§ 67 Abs. 1 SGB X), während beim Stellen-Informations-Service überwiegend Sozialdaten von Arbeitgebern bzw. diesen gleichstehende Betriebs- und Geschäftsgeheimnisse (§ 35 Abs. 4 SGB I) verarbeitet und genutzt werden.

Die Veröffentlichung eines Angebotes im Stellen-Informations-Service setzt voraus, daß Arbeitgeber ausdrücklich einwilligen (§ 67 b SGB X). Den mir von der BA zur Verfügung gestellten Unterlagen habe ich entnommen, daß derzeit etwa 80% der Stellenangebote im Stellen-Informations-Service deanonymisiert sind, so daß sich der Arbeitsuchende in diesen Fällen direkt mit dem Arbeitgeber in Verbindung setzen kann. In etwa 20% der Fälle wünschen Arbeitgeber einen Kontakt ausschließlich über die entsprechende Vermittlungsfachkraft des Arbeitsamtes.

Die Arbeitsuchenden, die ihre Daten und damit ihr Bewerberprofil dem Arbeitgeber-Informations-Service zur Verfügung stellen, willigen in deren Veröffentlichung – im Sinne des § 67 b SGB X – ausdrücklich ein. Für den Service wird das Bewerberprofil anonymisiert. Damit sind die Daten der Arbeitsuchenden optimal vor Mißbrauch geschützt.

Anläßlich eines Besuches bei der BA habe ich mir den Arbeitgeber-Informations-Service und den Stellen-Informations-Service vorführen lassen. Die Verfahren berücksichtigen die erforderlichen datenschutzrechtlichen Belange.

20.3 Kontrollen bei Arbeitsämtern

Ohne nennenswerte Probleme bei der Umsetzung des Sozialdatenschutzes zeigten sich folgende Aufgabenbereiche bei mehreren Arbeitsämtern:

- Eintragungen in die Bewerberangebote im System CoArb (s. o. Nr. 20.1)
- Zusammenarbeit zwischen Arbeitsamt und Maßnahmeträgern
- Inhalt und Umfang der im Bereich des ärztlichen und psychologischen Dienstes erstellten Gutachten
- Einsichtsrecht des Betroffenen in Gutachten des ärztlichen und psychologischen Dienstes
- Außenprüfungen des Arbeitsamtes nach dem Arbeitsförderungsgesetz (§ 150 a AFG)
- Inhalt von Leistungsakten
- Verfahren der Berufsberatung und
- Datenträgerentsorgung im Bereich der Verwaltungsabteilung des Arbeitsamtes.

Besonders herausstellen möchte ich den Umgang eines Arbeitsamtes mit den personenbezogenen Daten ausländischer Arbeitnehmer:

Hier habe ich u. a. das Arbeitserlaubnisverfahren geprüft und mir das Verfahren und die Kommunikation des Arbeitsamtes mit Ausländerbehörden darstellen lassen. Ich konnte feststellen, daß Art und Umfang der Übermittlung von Kopien der Arbeitserlaubnisse an die zuständigen Ausländerbehörden den Vorgaben der Ausländerdatenübermittlungsverordnung (§ 5) entsprachen. Auch wenn in Einzelfällen weitere Daten benötigt wurden, war deren Übermittlung rechtlich zulässig und lag im Interesse der Betroffenen.

Datenschutzprobleme ergaben sich bei der stichprobenweisen Prüfung der Arbeitserlaubnis-Datei. Diese Datei wird sowohl auf Papier als auch automatisiert geführt. Sie enthielt teilweise nicht erforderliche Unterlagen wie z. B. Kopien der Aufenthaltserlaubnisse aus Pässen. Ich habe Einvernehmen mit dem Arbeitsamt dahingehend erzielt, daß grundsätzlich entsprechende Vorlage-/Prüfvermerke in der Datei ausreichen und daß die nicht benötigten Anlagen vernichtet werden. Ausnahmsweise dürfen Belege, die zur Beweissicherung benötigt werden, wenn die Arbeitserlaubnis abgelehnt wird, weiterhin – bis längstens zum Eintritt der Rechtskraft – aufbewahrt werden.

Auch gab es zum Zeitpunkt der Kontrolle keine Aufbewahrungs- und Löschungsregelungen für die Arbeitserlaubnis-Datei. Ich habe der BA empfohlen, für dieses Problem eine übergreifende – also nicht nur auf das geprüfte Arbeitsamt bezogene – Regelung zu schaffen. Ziel dieser Regelung muß sein, die Anforderungen zur Berichtigung, Löschung und Sperrung von Daten nach § 84 SGB X hier umzusetzen.

Keine Probleme gab es beim Umgang mit den personenbezogenen Daten ausländischer Arbeitnehmer in der Leistungsabteilung, in der Abteilung Arbeitsvermittlung/-beratung sowie im Ärztlichen Dienst.

20.4 Projekt „Arbeitsamt 2000"

Die Bundesanstalt für Arbeit hat unter der Bezeichnung „Arbeitsamt 2000" ein Gesamtkonzept über die künftige Struktur ihrer Organisation entwickelt, das sich nicht nur auf die Arbeitsämter bezieht, sondern die Landesarbeitsämter und die Hauptstelle mit einschließt.

Die Bundesanstalt für Arbeit hat mich über dieses Organisationsprojekt und die damit verbundenen Organisationsänderungen informiert. Im Konzept „Arbeitsamt 2000" wird dem Datenschutz – wie bisher – ein hoher Stellenwert eingeräumt. Der vorhandene Datenschutz-Standard soll nicht nur gehalten, sondern ausgebaut werden.

Ich werde das Projekt weiterhin beratend begleiten.

20.5 Gesetzgebungsverfahren AFRG

Die parlamentarische Beratung des Entwurfs eines „Gesetzes zur Reform der Arbeitsförderung" war bei Redaktionsschluß noch nicht abgeschlossen. Mit dem Gesetz soll das Arbeitsförderungsgesetz (AFG) in das SGB als dessen Drittes Buch eingeordnet werden.

Im Rahmen meiner Beteiligung am Gesetzgebungsverfahren habe ich darauf hingewirkt, daß ein eigener Abschnitt mit bereichsspezifischen Datenschutzvorschriften aufgenommen wird. Er enthält neben einer zentralen Vorschrift über die Erhebung, Verarbeitung und Nutzung von Daten (§ 403 Entwurf SGB III) ein Kennzeichnungs- und Maßregelungsverbot (§ 404 Entwurf SGB III).

Ebenfalls in einem eigenen Abschnitt ist die Arbeitsmarkt- und Berufsforschung der BA geregelt. Die vom Institut für Arbeitsmarkt- und Berufsforschung verarbeiteten und genutzten Daten unterliegen einer Zweckbindung für die wissenschaftliche Forschung und sind zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist (§ 280 Entwurf SGB III).

Auch zu vielen hier nicht näher darstellbaren Einzelaspekten wurden datenschutzrechtlich gut vertretbare Lösungen gefunden.

21 Krankenversicherung

21.1 Übermittlung von Leistungsdaten in der gesetzlichen Krankenversicherung

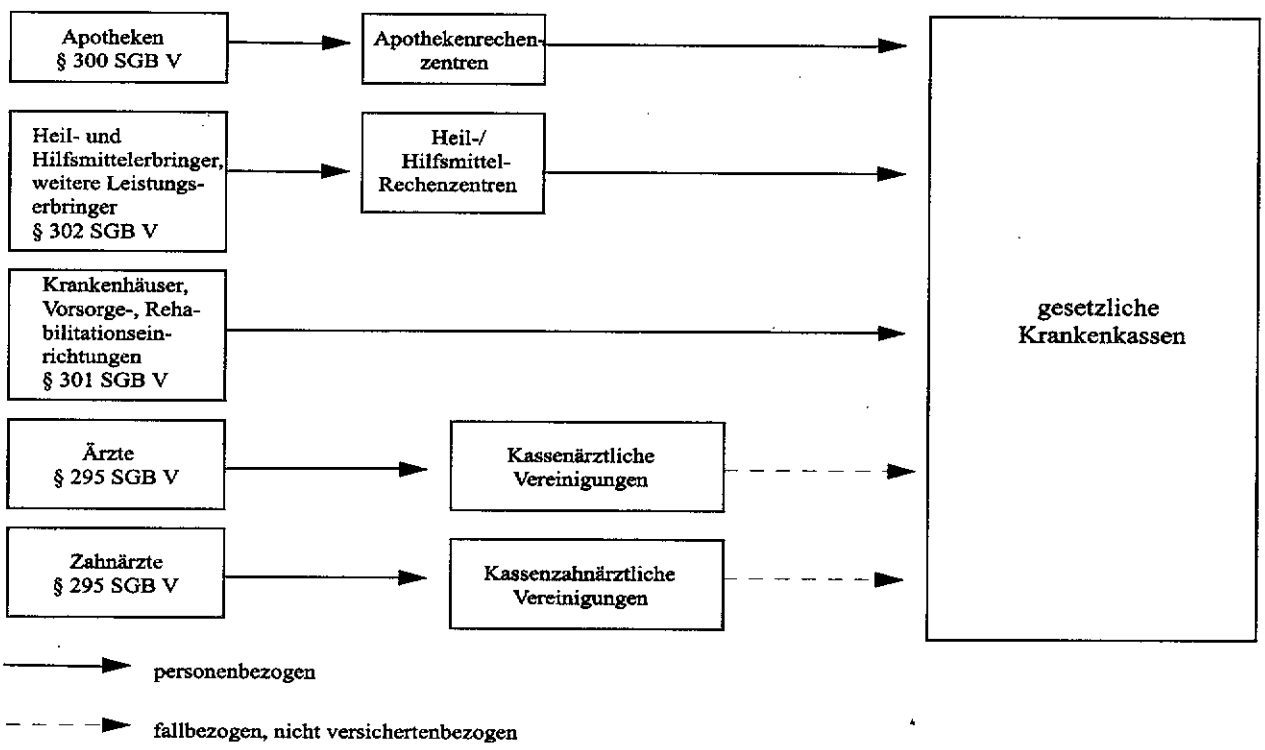
Das Gesundheitsreformgesetz 1989 und das Gesundheitsstrukturgesetz 1992 verfolgten das Ziel, dem Kostenanstieg in der gesetzlichen Krankenversicherung entgegenzuwirken, was nicht zuletzt durch den Einsatz automatisierter Datenverarbeitung ermöglicht werden soll. Die Vorschriften der §§ 294 ff. SGB V geben dabei den Rahmen für die Datenübermittlungen der Leistungserbringer an die Krankenkassen für Zwecke der Leistungsabrechnung (s. Abb. 10) und der Wirtschaftlichkeitsprüfungen vor.

21.1.1 Abrechnung zahnärztlicher Leistungen

Nach § 295 Abs. 3 SGB V sind die Spitzenverbände der Krankenkassen und die Kassenzahnärztliche Bundesvereinigung (KZBV) aufgerufen, die Einzelheiten der Übermittlungen von Leistungsdaten zwischen Zahnarzt, Kassenzahnärztlicher Vereinigung und Krankenkasse zu vereinbaren. Da eine derartige Vereinbarung nicht zustande kam, setzte daraufhin das angerufene Bundesschiedsamt für die vertragszahnärztliche Versorgung eine Vereinbarung in Kraft, die von der KZBV unter zwei Aspekten heftig

Abbildung 10

Übermittlung von Daten bei der Abrechnung von Leistungen in der gesetzlichen Krankenversicherung (Leistungserbringer – Krankenkassen)



kritisiert wurde: Zum einen sprenge der Umfang der Übermittlung an die Kassen den Rahmen des Erforderlichen; zum anderen ermögliche der Vertrag unzulässigerweise die Herstellung eines Personenbezuges.

Diese Kritik geht von § 295 Abs. 2 SGB V aus, wonach die Kassenzahnärztlichen Vereinigungen den Krankenkassen die erforderlichen Angaben über die abgerechneten Leistungen zwar fallbezogen, nicht jedoch versichertenbezogen übermitteln dürfen. Um diese Vorgabe zu erfüllen, bekommen die Kassen einen Versichertendatensatz und einen Leistungsdatensatz, die nur in den in der Vereinbarung aufgeführten Fällen zusammengeführt werden dürfen. Es liegt auf der Hand, daß in beiden Datensätzen vorkommende identische Daten das Risiko des Zusammenführens erhöhen. Es war daher mein vordringliches Anliegen, den Umfang der zu übermittelnden Daten auf das erforderliche Maß zu beschränken sowie eine solche Auswertungsmöglichkeit zu verhindern.

Hierbei konnte ich gemeinsam mit den Datenschutzbeauftragten der Länder erreichen, daß im Versichertendatensatz die Angaben „Zahnarztnummer/Zahnarztname" und der „Fallwert in Punkten und DM" entfallen. Bei einigen Daten (z. B. Zahnbezug, Tag der Behandlung) ist die Erforderlichkeit für Zwecke der Abrechnung noch nicht hinreichend belegt. Die Kassenseite hat hierzu erklärt, daß genauere Begründungen für die Erforderlichkeit dieser Daten erst gegeben werden könnten, wenn das DV-Projekt für das Abrechnungsverfahren auf Kassenseite hinreichend entwickelt sei. Im Rahmen dieser Überlegungen habe ich die Kassen um Prüfung gebeten, ob eine teilweise Löschung des Versichertendatensatzes vor der Übermittlung des Leistungsdatensatzes möglich ist, um das Risiko des Zusammenführens dieser Datensätze weiter zu senken. Eine Antwort hierzu steht noch aus.

Der Verband der Angestellten-Krankenkassen e.V. (VdAK) stimmte als einziger Spitzenverband der Vereinbarung über einen reduzierten Datensatz zunächst nicht zu (s. hierzu die Entschließung der 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder **Anlage 20**). Mittlerweile haben sich KZBV und VdAK jedoch geeinigt und die Vereinbarung unterzeichnet.

21.1.2 Abrechnung und Wirtschaftlichkeitsprüfung für ärztliche Leistungen

Die Vereinbarungen über die Übermittlung von Leistungsdaten sind im ärztlichen – im Gegensatz zum zahnärztlichen (s. o. Nr. 21.1.1) – Bereich weiter fortgeschritten: Sowohl für die Übermittlung für Abrechnungszwecke als auch für Wirtschaftlichkeitsprüfungen liegt eine Vereinbarung der Spitzenverbände der Krankenkassen mit der Kassenärztlichen Bundesvereinigung (KBV) vor.

Zwar sind derzeit die technischen Voraussetzungen für eine durchgehend automatisierte Datenweitergabe noch nicht in vollem Umfang vorhanden, so daß die Kassenärztlichen Vereinigungen den Krankenkassen nach wie vor auch Papierausdrucke zuleiten, aus denen diese entgegen § 295 Abs. 2 SGB V erkennen können, welcher Versicherte welche Leistung aufgrund welcher Diagnose erhalten hat. Es ist jedoch anzunehmen, daß die vertraglichen Vorgaben rasch umgesetzt werden. In diesem Zusammenhang begrüße ich besonders die Zusage beider Vertragsparteien, in datenschutzrechtlich relevanten Fällen eine Vertragsanpassung vorzunehmen.

21.1.3 Abrechnung der Krankenhäuser

In der zwischen den Spitzenverbänden der Krankenkassen und der Deutschen Krankenhausgesellschaft abgeschlossenen Vereinbarung über Form und Inhalt der nach § 301 SGB V zwischen Krankenhäusern und Kassen vorgesehenen Datenübermittlung war zunächst unter den zu nennenden Gründen für die Aufnahme ins Krankenhaus vorgesehen, die Schlüssel 04 „Hinweis auf Mord/Totschlag/Raufhändel" sowie 05 „Hinweis auf Selbstmord/Selbstschädigung" zu übermitteln.

Hierfür gibt es jedoch keine Rechtsgrundlage in § 301 SGB V. Insbesondere handelt es sich bei diesen Bezeichnungen nicht um medizinisch definierte Aufnahmegründe, sondern um eine erste rechtliche Bewertung. Nach Erörterung mit den Vertragsparteien stellte sich heraus, daß die Kassen einen Anhaltspunkt dafür benötigen, ob sie ggf. für ihre Aufwendungen Regreß bei einem Dritten nehmen können.

Einen Hinweis darauf, daß ein solcher Anspruch im Einzelfall bestehen kann, halte ich für zulässig, da anderenfalls die Kasse bei jedem Krankenhausaufenthalt gezwungen wäre, den Versicherten zu befragen, ob ein Anspruch gegen Dritte vorliegen kann. Der Schlüssel 04 lautet nunmehr „Hinweis auf Einwirkungen von äußerer Gewalt", der Schlüssel 05 wurde ersatzlos gestrichen.

21.1.4 Abrechnung der sonstigen Leistungserbringer

Nach § 302 Abs. 1 i.V. m. § 303 Abs. 3 SGB V sind die Leistungserbringer im Bereich der Heil- und Hilfsmittel und die weiteren Leistungserbringer verpflichtet, maschinenlesbar oder auf maschinell verwertbaren Datenträgern folgende Angaben weiterzugeben:

- Erbrachte Leistungen nach Art, Menge und Preis,
- Tag der Leistungserbringung,
- Arztnummer des verordnenden Arztes und
- die Angaben, die sich nach § 291 Abs. 2 Nr. 1 bis 6 SGB V auf der Krankenversichertenkarte befinden.

Die entsprechenden Richtlinien der Spitzenverbände der Krankenkassen sehen aber auch die Mitteilung von Diagnosen und Befunden an die Krankenkassen vor. In einer von mir erbetenen Stellungnahme der Spitzenverbände, der sich das BMG angeschlossen hat, wird darauf hingewiesen, daß die Kassen Leistungen nur dann bewilligen dürften, wenn sie ausreichend, zweckmäßig und wirtschaftlich seien (§§ 2, 12 Abs. 1 SGB V). Auch werde in einigen Fällen die ärztliche Verordnung ohnehin durch den Versicherten selbst seiner Kasse zur Beantragung von

Leistungen vorgelegt. In den anderen Fällen sei eine Übermittlung ebenfalls zulässig (§ 69 SGB X).

Diese Ausführungen haben mich nicht überzeugt. Die zu übermittelnden Daten der sonstigen Leistungserbringer sind zum Teil – etwa im Falle der Masseure – vom Arztgeheimnis umfaßt. Für eine Durchbrechung des Arztgeheimnisses sind eindeutige gesetzliche Regelungen erforderlich. Im Hinblick auf die Sensibilität der Diagnosen hat der Gesetzgeber im Abrechnungsgeschehen diesem verfassungsrechtlichen Gebot im SGB V Rechnung getragen (siehe §§ 295 Abs. 1, 297 Abs. 2 Nr. 4 sowie § 301 Abs. 1 Nr. 3 SGB V). Der Vorschrift des § 302 SGB V läßt sich eine entsprechend eindeutige Übermittlungsbefugnis nicht entnehmen; ein Rückgriff auf § 69 SGB X muß ausscheiden, da § 302 SGB V die Abrechnung der sonstigen Leistungserbringer abschließend regelt.

Ich habe nach wie vor Zweifel, inwieweit sich die Angabe von Diagnosen und Befunden in allen Fällen auf eine wirtschaftliche und zweckmäßige Leistungserbringung auswirken kann. Wenn es solche Gründe gibt, ist eine Gesetzesergänzung zwingend.

21.1.5 Diagnosenverschlüsselung nach dem ICD-10

Um die Jahreswende 1995/96 sorgte die Abkürzung „ICD-10" für Diskussionen bei Ärzten und Patienten sowie im Gesundheitsausschuß des Deutschen Bundestages, bei dem BMG und mir. Mit der Automatisierung der Datenübermittlung zu Abrechnungszwecken verpflichtete der Gesetzgeber Ärzte und Krankenhäuser zur Codierung der zu übermittelnden leistungsbegründenden Diagnosen nach dem ICD-10-Schlüssel (s. Abb. 11). Der angeordnete Schlüssel, den die Weltgesundheitsorganisation für globale Statistik- und Forschungszwecke entwickelt hatte, enthält weit ausdifferenzierte Diagnosen von Krankheiten und ist damit gut zur statistischen Beschreibung des Gesundheitszustandes von großen Gruppen geeignet. Seine Verwendbarkeit zur Begründung der Notwendigkeit ärztlicher Leistungen ist in einigen Fällen jedoch mangelhaft:

- In der ärztlichen Praxis werden Leistungen nicht nur aufgrund einer präzise festgestellten Krankheit erbracht, sondern es finden auch Vorsorge- und Beratungsleistungen, z. B. bei Schwangerschaften statt. Da Schwangerschaft aber keine Krankheit ist, enthält der ICD-10 folgerichtig nur Schlüssel für Schwangerschaftskomplikationen, die als Krankheit angesehen werden können. Zu derartigen Vorsorge- und Beratungsleistungen kann also keine Diagnose nach ICD-10 angegeben werden.
- Diagnostische Leistungen werden oft erbracht, um zu klären, welche Krankheit die beobachteten Symptome verursacht, wobei es gelegentlich auch darum geht, bestimmte Möglichkeiten auszuschließen. Die am Ende festgestellte Diagnose ist also nicht geeignet, die Leistungen zu begründen. Dafür müßten Symptomatiken beschrieben werden, für die im ICD-10 keine Schlüsselwerte bestehen, oder „Verdacht auf..." bzw. „Ausschluß von..." angegeben werden.
- Der Differenzierungsgrad des 4stelligen Schlüssels ist gelegentlich feiner, als es zur Leistungsbegründung erforderlich wäre, in einigen Fällen nach Meinung von Ärzten sogar feiner, als es zur Behandlung nötig wäre. Deshalb sehen die Empfehlungen des Zentralinstituts für die kassenärztliche Versorgung in der Bundesrepublik Deutschland für die an der vertragsärztlichen Versorgung teilnehmenden Ärzte häufig denjenigen vierstelligen Schlüssel vor, der den dreistelligen Schlüssel für die Kategorie durch Hinzufügen von „nicht näher bezeichnet" lediglich formal auf vier Stellen verlängert, ohne dem Sinn nach mehr als die dreistellige geschlüsselte Kategorie zu beschreiben. Mit dieser sinnvollen Lösung würde die Vorschrift des § 295 Abs. 1 Satz 2 SGB V „Die Diagnosen... sind nach dem vierstelligen Schlüssel ... zu verschlüsseln" allenfalls dem Wortlaut nach befolgt. Dagegen wären die bei sinngemäßer Anwendung gebotenen weitergehenden Differenzierungen, von der Sache her beurteilt, überflüssig fein und deshalb datenschutzrechtlich bedenklich.

Meine Kritik an der Pflicht zur Verwendung des vierstelligen ICD-10 Schlüssel richtet sich somit nicht gegen die Pflicht, Leistungen in angemessenem Umfang zu begründen, sondern vielmehr gegen die Eignung des Schlüsselkataloges für diesen Zweck.

Diese Kritik ist – wenn auch mit teilweise unterschiedlichen Bewertungen – im Grundsatz vom Gesundheitsausschuß des Deutschen Bundestages, dem BMG, den Spitzenverbänden der Krankenkassen, der Kassenärztlichen Bundesvereinigung und der Deutschen Krankenhausgesellschaft geteilt worden, so daß sehr schnell eine Rahmenvereinbarung zur Lösung des Problems zwischen den drei letztgenannten Stellen abgeschlossen werden konnte.

Danach ist vorgesehen, daß ein Arbeitsausschuß auf der Grundlage des ICD-10 unter strikter Beachtung der datenschutzrechtlichen Bestimmungen eine praktikable Fassung eines Diagnoseschlüssels für Zweck der Leistungsabrechnung erarbeitet. Vor der verbindlichen Einführung des ICD-10 zum 1. Januar 1998 soll es zudem eine Erprobungsphase geben.

Die weitere Entwicklung werde ich sorgfältig beobachten.

21.1.6 Wahrnehmung von Übermittlungsfunktionen durch private Stelle

Die Mehrheit der Bevölkerung – ca. 72 Millionen – ist gesetzlich krankenversichert. Weit über 200 000 Leistungserbringer und eine Vielzahl von Krankenkassen gewährleisten die Versorgung der Versicherten. So verwundert nicht die – auch öffentlich geführte – intensive Diskussion eines Projekts, dessen Ziel die Koordination der zahlreichen Datenflüsse zu den Kassen war.

Dazu beauftragten die Spitzenverbände der Krankenkassen die debis-Systemhaus Network Services GmbH, die Datenflüsse von den Kassen(zahn)ärztlichen Vereinigungen, Krankenhäusern, Apothekern und den sonstigen Leistungserbringern an die Kran-

Abbildung 11

Auszug aus ICD-10

O64 Geburtshindernis durch Lage-, Haltungs- und Einstellungsanomalien des Feten

O64.0 Geburtshindernis durch unvollständige Drehung des kindlichen Kopfes
Geburtshindernis durch persistierende Kindslage:
- hintere Hinterhauptslage
- okzipitoillakal
- okzipitosakral
- okzipitotransversal

Tiefer Querstand

O64.1 Geburtshindernis durch Beckenendlage

O64.2 Geburtshindernis durch Gesichtslage
Geburtshindernis durch Kinnlage

O64.3 Geburtshindernis durch Stirnlage

O64.4 Geburtshindernis durch Querlage
Armvorfall
Exkl.: Eingekeilte Schulter (O66.0)
Schulterdystokie (O66.0)

O64.5 Geburtshindernis durch kombinierte Einstellungsanomalien

O64.8 Geburtshindernis durch sonstige Lage-, Haltungs- und Einstellungsanomalien

O64.9 Geburtshindernis durch Lage-, Haltungs- und Einstellungsanomalien, nicht näher bezeichnet

O65 Geburtshindernis durch Anomalie des mütterlichen Beckens

O65.0 Geburtshindernis durch Beckendeformität

O65.1 Geburtshindernis durch allgemein verengtes Becken

O65.2 Geburtshindernis durch Beckeneingangsverengung

O65.3 Geburtshindernis durch Beckenausgangsverengung und Verengung in Beckenmitte

O65.4 Geburtshindernis durch Mißverhältnis zwischen Fet und Becken, nicht näher bezeichnet
Exkl.: Dystokie durch Anomalie des Feten (O66.2-O66.3)

O65.5 Geburtshindernis durch Anomalie der mütterlichen Beckenorgane
Geburtshindernis durch Zustände, die unter O34.- aufgeführt sind

O65.8 Geburtshindernis durch sonstige Anomalie des mütterlichen Beckens

O65.9 Geburtshindernis durch Anomalie des mütterlichen Beckens, nicht näher bezeichnet

O66 Sonstiges Geburtshindernis

O66.0 Geburtshindernis durch Schulterdystokie
Eingekeilte Schultern

O66.1 Geburtshindernis durch verhakte Zwillinge

O66.2 Geburtshindernis durch ungewöhnliche großen Feten

O66.3 Geburtshindernis durch sonstige Anomalien des Feten
Dystokie durch:
- Doppelfehlbildung [zusammengewachsene Zwillinge]
- fetal:
  - Aszites
  - Hydrops
  - Myelomeningozele
  - Steißteratom
  - Tumor
  - Hydrozephalus beim Feten

O66.4 Mißlungener Versuch der Geburtsbeendigung, nicht näher bezeichnet
Mißlungener Versuch der Geburtsbeendigung mit nachfolgender Schnittentbindung

O66.5 Mißlungener Versuch einer Vakuum- oder Zangenextraktion, nicht näher bezeichnet
Mißlungene Anwendung von Vakuumextraktor oder Zange mit nachfolgender Zangen- oder Schnittentbindung

O66.8 Sonstiges näher bezeichnetes Geburtshindernis

O66.9 Geburtshindernis, nicht näher bezeichnet
Dystokie:
- durch fetale Ursachen o.n.A.
- durch mütterliche Ursachen o.n.A.
- o.n.A.

kenkassen zu bündeln und zu koordinieren. Die Abrechnungsdaten sollten dem Systemhaus debis über öffentliche Leitungswege oder durch Übersenden maschinenlesbarer Datenträger zugeleitet, von ihr den einzelnen Krankenkassen zugeordnet und dann an diese weitergeleitet werden.

Bei diesem Vorhaben kommen verschiedene Faktoren zusammen, die hohe Anforderungen an die einzusetzenden Sicherheitsmaßnahmen stellen: die Sensibilität und Menge der Daten, die leichte Auswertbarkeit maschinell verfügbarer Daten, die Nutzung öffentlicher Leitungswege sowie die Weitergabe der Daten über eine zentrale Stelle. Ich habe daher wiederholt deutlich gemacht, daß für eine ausreichende Sicherung der zu übermittelnden Daten gegen unbefugte Kenntnisnahme eine kryptographische Verschlüsselung unerläßlich ist. Der Inhalt der Vereinbarungen zwischen den Verbänden der gesetzlichen Krankenkassen und dem Systemhaus debis ist von mir auch dahingehend verstanden worden, daß debis nur die Verbindungsdaten, also keine Dateninhalte, lesen kann. Diese Einschätzung wird von der Bundesregierung (BT-Drs. 13/3001 vom 14. November 1995) geteilt.

Trotz zahlreicher Besprechungen mit den Beteiligten kommt das Projekt offenbar nicht voran, von dem sich die Bundesregierung eine Kostenersparnis verspricht. Die Schuld an diesen Verzögerungen wird immer wieder „gern" mir angelastet. Meine Forderungen nach einer kryptographischen Verschlüsselung sind jedoch seit Anfang 1995 bekannt. Ich kann nur vermuten, daß die Beteiligten sich über die Konsequenzen – technisch und organisatorisch als auch hinsichtlich der Kosten – kein ausreichend präzises Bild verschafft haben.

Unter diesen mir bekannten tatsächlichen und vertraglichen Bedingungen halte ich die Wahrnehmung einer Übermittlungsfunktion durch eine private Stelle aus datenschutzrechtlicher Sicht für nicht vertretbar. Ich habe daher den meiner Kontrolle unterliegenden Stellen gem. § 81 Abs. 2 SGB X i.V. m. § 25 BDSG eine Beanstandung angekündigt, falls bei der Durchführung des Datenträgeraustausches eine Einsichtsmöglichkeit durch das Systemhaus debis nicht ausgeschlossen ist.

21.2 Umfangreiche Datenerhebung im Psychotherapieverfahren

Eine Leistungspflicht der Krankenkasse ist nach den Psychotherapie-Richtlinien und der Psychotherapie-Vereinbarung – beispielsweise für tiefenpsychologisch fundierte Psychotherapie oder Verhaltenstherapie – nur dann gegeben, wenn im sog. „Gutachterverfahren" die vorgeschlagene Therapie positiv beurteilt wurde. Dieses läuft im wesentlichen so ab, daß der behandelnde Therapeut bei der Krankenkasse eine Begutachtung des Patienten beantragt und hierzu eine umfangreiche Befragung des Patienten durchführt. Diese mündet in einen mehrseitigen Bericht, den ein Gutachter über die Krankenkasse erhält. Für die Krankenkassenmitarbeiter ist dabei eine Einsichtnahme nicht möglich, da der Bericht in einem verschlossenen Umschlag weitergeleitet wird. Aufgrund des Berichtes befürwortet der Gutachter die Therapie oder lehnt sie ab.

Einige Therapeuten haben sich an mich gewandt, weil sie meinen, daß beim Patienten zu viele Daten erhoben werden.

Aus meiner Sicht birgt dieses Verfahren strukturell die Gefahr einer zu umfangreichen, nicht an den Grundsätzen der Erforderlichkeit orientierten Datenerhebung. Denn die beantragenden Therapeuten versuchen oftmals durch umfassende Angaben zu vermeiden, daß ihr Antrag abgelehnt wird. Nach der Rechtsprechung des Bundesverfassungsgerichts (NJW 1993, S. 2365) stehen psychologische Befunde dem unantastbaren Bereich privater Lebensgestaltung noch näher als rein medizinische Feststellungen, so daß bei der Erhebung psychologischer Befunde in besonderem Maße der Grundsatz der Verhältnismäßigkeit und Minimierung von Datenerhebungen zu berücksichtigen ist.

Inwieweit die Datenerhebung beim Patienten reduziert werden kann, werde ich mit den zuständigen Stellen ebenso weiter erörtern wie die Frage nach Maßnahmen der Qualitätssicherung, etwa im Hinblick auf die Erstellung von regelmäßigen Dokumentationen; Ergebnisse sind in diesem wichtigen, aber auch empfindlichen Bereich nicht leicht zu erreichen.

21.3 Werbemaßnahmen der Kassen

Im Berichtszeitraum habe ich mich erneut mit datenschutzrechtlichen Aspekten der Mitgliederwerbung der Krankenkassen auseinandersetzen müssen; sowohl von Versicherten- als auch von Kassenseite bin ich auf (vermeintliche) Werbemaßnahmen hingewiesen worden.

Bisher wurde das Beschaffen von Namen und Anschriften zum Zwecke der Werbung neuer Mitglieder durch die Kassen als unzulässig bewertet, da es an einer Datenerhebungsbefugnis hierfür im abschließenden Datenerhebungskatalog des § 284 Abs. 1 SGB V fehlt. Aufgrund des Gesundheitsstrukturgesetzes vom 21. Dezember 1992 haben sich die rechtlichen Rahmenbedingungen jedoch erheblich verändert. Seit dem 1. Oktober 1996 können die Mitglieder der gesetzlichen Krankenkassen frei wählen, welcher Kasse sie angehören wollen.

Dementsprechend sind die Krankenkassen nunmehr auf eine aktive Mitgliederwerbung angewiesen. Dies erfordert auch eine neue datenschutzrechtliche Bewertung. Dabei ist zu beachten, daß die bei personenbezogenen Werbemaßnahmen in der Regel verwendeten Adreßdaten keine Aussage in bezug auf ein bestehendes oder künftiges Versicherungsverhältnis enthalten. Es sind vielmehr „Allerweltsdaten", die im Grundsatz auch jedem zugänglich sind. Ob es zu einem sozialrechtlichen Verhältnis (Krankenversicherung) kommt, ist im Zeitpunkt der Werbung noch offen. Dementsprechend neige ich zu der Auffassung, daß der strenge Schutz des Sozialgeheimnisses erst dann anzuwen-

den ist, wenn ein Betroffener sein Interesse an einer Mitgliedschaft bekundet und die Voraussetzungen für ein Versicherungsverhältnis dadurch schafft, daß er schutzbedürftige Sozialdaten zu diesem Zweck mitteilt.

Das BMG hat sich in dieser Angelegenheit noch nicht abschließend festgelegt.

21.4 Neue Wege in Prävention und Behandlung: Managed Care

Eine Krankenkasse hatte sich wegen der beabsichtigten Einführung von Managed Care-Strukturen an mich gewandt. Managed Care ist ein Sammelbegriff für alle Verfahren, die die Betreuung der Patienten durch Ärzte und andere Leistungserbringer optimieren sollen. Ein Teilaspekt von Managed Care ist die von den Krankenkassen koordinierte Beratung von Patienten und Ärzten über die Versorgungsstrukturen, was z. B. auch Einfluß auf die Auswahl der Leistungserbringer durch den Patienten haben kann. Weiter geht es um die zweckmäßige Behandlung insbesondere von chronischen Krankheiten. Dazu müssen für die Verträge zwischen den Krankenkassen und den verschiedenen, zusammenwirkenden Leistungserbringern neue Wege begangen werden, die z. B. die speziellen Anforderungen einer Krankheit berücksichtigen, für deren Behandlung Managed Care genutzt werden soll.

Die Konzeption von Managed Care im einzelnen steht noch nicht fest. Es ist aber zu erwarten, daß die Krankenkassen zur Betreuung der Versicherten weitere Sozialdaten erheben, verarbeiten oder vorhandene Daten unter Zweckänderung nutzen müssen. Nur für die Pflegekassen ist bereits eindeutig festgelegt, daß sie für Zwecke der Pflegeversicherung Daten erheben, verarbeiten und nutzen dürfen, soweit dies für die Beratung über Maßnahmen der Prävention und Rehabilitation sowie über die Leistungen und Hilfen zur Pflege erforderlich ist (§ 94 Abs. 1 Nr. 7 SGB XI). Insgesamt wird auch zu prüfen sein, in welchem Maße Managed Care überhaupt den Umgang mit personenbezogenen Daten bei den Kassen erfordert.

Neu an diesen Überlegungen ist, daß nicht der Versicherte selbst, sondern die Kasse initiativ wird und den Patienten etwa auf die Betreuungsmöglichkeit in einer Erfahrungsaustauschgruppe hinweist. Ein solches Vorgehen muß für den Versicherten transparent gestaltet werden und ihn weitestgehend aktiv einbinden, damit er sich nicht – unzulässig – überwacht fühlt.

21.5 Chance zur Verbesserung des Datenschutzes bei der Neustrukturierung der Bahnbetriebskrankenkasse konsequent nutzen

Unmittelbar vor der Vereinigung mit der Bundesbahnbetriebskrankenkasse (BBKK) zur Bahnbetriebskrankenkasse (Bahn-BKK) habe ich die Reichsbahnbetriebskrankenkasse (RBKK) beraten und kontrolliert.

Insgesamt mußte ich feststellen, daß die nach der Vereinigung weitgehend von der Bundesbahnbetriebskrankenkasse übernommenen datenschutzrechtlichen Regelungen, die ihrerseits schon nicht der aktuellen Gesetzgebung entsprachen, nicht umgesetzt waren. Über Verlauf und Ergebnis der Kontrolle sind mit Blick auf die Neustrukturierung der zum 1. Januar 1996 gebildeten Bahn-BKK u. a. Mängel im Leistungswesen und in der Organisation des Datenschutzes von allgemeiner Bedeutung:

Mit Blick auf die Zusammenführung der RBKK und der BBKK zur Bahn-BKK und der damit verbundenen Neustrukturierung habe ich die zahlreichen Mängel in meinem Kontrollbericht detailliert beschrieben und von einer Beanstandung zunächst abgesehen. Die Beseitigung der festgestellten Mängel wurde mir zugesagt. Ich hoffe, daß die Chance genutzt wird, mit der Neustrukturierung der Bahnbetriebskrankenkasse die datenschutzrechtliche Situation dem gesetzlichen Standard anzupassen.

Zum Leistungswesen:

Jeder Sachbearbeiter in der Leistungsabteilung verfügt über eine Liste mit sog. „betriebsgefährdenden Erkrankungen" (z. B. Blutarmut, Schilddrüsenerkrankung, Bluthoch- und -unterdruck). Falls der Verdacht auf eine solche Krankheit vorliegt, wird eine entsprechende Anfrage an den Bahnarzt als Betriebsarzt der Deutschen Bahn AG gegeben. Umgekehrt informiert der Bahnarzt den zuständigen Sachbearbeiter, wenn er, z. B. als Betriebsarzt im Rahmen einer Tauglichkeitsuntersuchung, vom Vorliegen einer betriebsgefährdenden Krankheit ausgeht. Beide Übermittlungen erfolgen in der Regel ohne Information des Betroffenen. Diese Verfahren sind bei Mitarbeitern der Bahn, die in anderen gesetzlichen Krankenkassen versichert sind, grundsätzlich nicht möglich. In diesem Zusammenhang ist bemerkenswert, daß der Bahnarzt gleichzeitig die Aufgaben des Medizinischen Dienstes (MdK) für die Bereiche der Bahnbetriebskrankenkasse und der Betriebskrankenkasse des Bundesverkehrsministeriums wahrnimmt. Im vorliegenden Fall habe ich vor allem im Hinblick auf den Transparenzgrundsatz wegen fehlender Information des Betroffenen über die damit zusammenhängenden Datenverarbeitungen und -nutzungen Bedenken.

Das in der Satzung geregelte Verfahren über die Auskunftserteilung an Versicherte ist an die Neufassung des SGB X (§§ 83 und 25 SGB X) ebenso wenig angepaßt worden wie Auskunftsansprüche über in Anspruch genommene Leistungen der gesetzlichen Krankenversicherung nach § 305 SGB V.

Die meisten von der Betriebskrankenkasse benutzten Vordrucke für Datenerhebungen, Einverständniserklärungen etc. entsprechen ebenfalls nicht den üblichen datenschutzrechtlichen Anforderungen. Es fehlen insbesondere die gesetzlich vorgesehenen Hinweise für die Betroffenen (§§ 66 SGB I und 67a Abs. 3 und 4 sowie 67b SGB X), wie z. B. auf die Folgen fehlender Mitwirkung, den Zweck von Datenerhebungen und deren Rechtsgrundlage oder die Freiwilligkeit von Angaben.

Zur Organisation des Datenschutzes:

Satzung und Geschäftsordnung der RBKK entsprachen in bezug auf die Datenschutzorganisation nicht den Vorgaben der aktuellen Gesetzgebung.

Der Leiter einer Bezirksleitung der RBKK besaß keinerlei Zugriffsrechte auf Dateien der eingesetzten PC-Netze, während der Leiter einer anderen Bezirksleitung mit vielfachen Zugriffsberechtigungen ausgestattet war. Die Erforderlichkeit dieser Festlegung konnte nicht erklärt werden. Die starke Diskrepanz bei der Zugriffsberechtigung macht Regelungen über den Einsatz von Personalcomputern dringend erforderlich.

Der Stellenwert des internen gesetzlichen Datenschutzbeauftragten (§ 81 Abs. 4 SGB X i.V. m. §§ 36, 37 Abs. 1 BDSG) entsprach nicht den gesetzlichen Vorgaben. Er war auf dem Gebiet des Datenschutzes nicht der Leitung der RBKK unmittelbar unterstellt. Eine Beteiligung bei datenschutzrelevanten Vorgängen wurde ebenso wenig praktiziert wie seine Mitwirkung bei der Auswahl der bei der Verarbeitung personenbezogener Daten tätigen Personen (§ 37 Abs. 1 Nr. 3 BDSG).

Vorschläge des Bundesversicherungsamtes (BVA) zur Verbesserung der datenschutzrechtlichen Situation anläßlich einer Prüfung im Jahre 1994, die weitgehend mit meinen Feststellungen übereinstimmen, waren zum Kontrollzeitpunkt Ende 1995 trotz entsprechender Zusagen noch immer nicht umgesetzt.

21.6 Versichertendaten für alle Geschäftsstellen?

Bei landesweiten oder überregionalen gesetzlichen Krankenkassen wurde im Berichtszeitraum die Frage diskutiert, ob alle Geschäftsstellen umfassend auf alle Versichertendaten zugreifen dürfen.

Rechtlicher Ausgangspunkt ist die Vorschrift zum Sozialgeheimnis (§ 35 SGB I). Danach gehört zur Wahrung des Sozialgeheimnisses auch die Verpflichtung, innerhalb des Leistungsträgers sicherzustellen, daß die Sozialdaten nur Befugten zugänglich sind oder nur an diese weitergegeben werden. Daneben sind Maßnahmen der Speicher-, Zugriffs- und Organisationskontrolle vorzusehen (Anlage zu § 78a SGB X). Im Hinblick auf diese rechtlichen Vorgaben haben die Datenschutzbeauftragten des Bundes und der Länder auf der 49. Konferenz am 9./10. März 1995 die Entschließung „Eingeschränkter Zugriff auf Versichertendaten bei landesweiten oder überregionalen gesetzlichen Krankenkassen" gefaßt **(s. Anlage 9)** und den Kassen zur Umsetzung empfohlen.

Eine Nachfrage bei den Ersatzkassen zur Umsetzung der Entschließung ergab folgendes: Zum Teil wird bereits entsprechend verfahren; es wurde allerdings auch mitgeteilt, daß insbesondere unter Servicegesichtspunkten eine der Entschließung entsprechende Verfahrensweise schwerlich umsetzbar ist.

Auch vor dem Hintergrund der Regelung des § 17 Abs. 1 Nr. 1 und 3 SGB I, wonach die Leistungsträger verpflichtet sind, Sozialleistungen in zeitgemäßer Weise, umfassend und schnell zu erbringen bzw. den Zugang zu den Sozialleistungen möglichst einfach zu gestalten, sind die von Kassenseite vorgebrachten Argumente sicherlich nicht von der Hand zu weisen. Ich bin allerdings der Auffassung, daß sich Service für den Versicherten und eingeschränkte Zugriffe nicht ausschließen. Ein Lösungsweg, der sowohl dem Service gegenüber dem Versicherten als auch dessen Recht auf informationelle Selbstbestimmung gerecht würde, wäre allerdings die Einholung einer Einwilligung.

21.7 Datenschutzrechtlich problematische Ausgestaltung der Modellvorhaben

Der gemeinsame Gesetzentwurf der Fraktionen von CDU/CSU und F.D.P. zur Neuordnung von Selbstverwaltung und Eigenverantwortung in der gesetzlichen Krankenversicherung (2. GKV-Neuordnungsgesetz) sieht in § 63 Abs. 5 und Abs. 6 vor, daß die Krankenkassen und die Kassenärztlichen Vereinigungen die für die Durchführung eines Modellvorhabens erforderlichen personenbezogenen Daten erheben, verarbeiten und nutzen können. Durch Modellvorhaben sollen beispielsweise Erkenntnisse zur Verbesserung der Qualität und Wirtschaftlichkeit der Versorgung gewonnen werden.

Der Bundestags-Ausschuß für Gesundheit hatte in seiner Beschlußempfehlung vom 22. Mai 1996 (BT-Drucksache 13/4691 S. 13) zum GKV-Weiterentwicklungsgesetz die Einbindung des Versicherten in die Modellvorhaben zu Recht von dessen Einwilligung abhängig gemacht und ihn damit in den Mittelpunkt des Verfahrens gestellt. Diese Vorgabe berücksichtigt der Gesetzentwurf leider nicht. Nur die in der Einwilligung zum Ausdruck kommende Freiwilligkeit der Teilnahme, die Aufklärung über den Zweck der Speicherung und die vorgesehenen Übermittlungen sowie auch die – ursprünglich vorgesehene – Anonymisierung nach Jahresfrist bewirken, daß die Modellvorhaben für die Versicherten transparent und damit auch von ihnen akzeptiert werden.

21.8 Beanstandung einer Kasse wegen unzulässiger Ermittlungen im Rahmen von Regreßverfahren nach § 116 SGB X

Eine Kasse hatte sich an das Ordnungsamt der Stadt Heidelberg im Wege eines Amtshilfeersuchens gewandt. Darin teilte sie der Stadt mit, daß sie nach § 116 SGB X einen Ersatzanspruch gegen einen Versicherten habe. Da der Ersatzanspruch bis zum damaligen Zeitpunkt nicht beglichen war, bat die Kasse um folgende Angaben: Geburtsdatum, ausgeübter Beruf, Einkommens- und Vermögensverhältnisse, familiäre Verhältnisse (Familienstand, Kinder, Rentner etc.), ob der Betroffene noch gemeldet bzw. ortsansässig sei, wovon er seinen Lebensunterhalt bestreite und bei welchem Arbeitgeber ein Beschäftigungsverhältnis bestehe. Der Betroffene wollte von mir wissen, ob die Kasse rechtens gehandelt habe.

Grundsätzlich steht einer Kasse das Recht zu, im Rahmen von Regreßverfahren nach § 116 SGB X Datenerhebungen durchzuführen. In diesem Fall ist

jedoch gleich mehrfach gegen datenschutzrechtliche Vorschriften verstoßen worden:

Die Kasse konnte mir nicht nachvollziehbar darlegen, daß die Kenntnis der einzelnen Antworten auf die im Schreiben an das Ordnungsamt der Stadt Heidelberg gestellten Fragen für ihre Aufgabenerfüllung nach § 67a Abs. 1 SGB X erforderlich war.

Des weiteren hat die Kasse durch ihr Ermittlungsersuchen in dem speziellen Fall gegen den Ersterhebungsgrundsatz verstoßen, wonach Daten beim Betroffenen zu erheben sind (§ 67a Abs. 2 Satz 1 SGB X). Eine zulässige Ausnahme vom Ersterhebungsgrundsatz, wie etwa diejenige, daß die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordert und damit eine Erhebung bei anderen Stellen gerechtfertigt hätte, hat mir die Kasse auf den Einzelfall bezogen nicht dargelegt.

Schließlich wurden dem Betroffenen gegenüber weder durch das Ordnungsamt der Stadt Heidelberg noch durch die Kasse die Hinweis- und Aufklärungspflichten nach § 67a Abs. 3 SGB X erfüllt. Diese Hinweis- und Aufklärungspflichten sind jedoch unabdingbare Voraussetzung dafür, daß der Betroffene erkennen kann, ob er seine Daten preisgeben muß. Dieses Unterlassen muß sich die Kasse als anfragende Stelle und damit Herrin des Verfahrens zurechnen lassen.

Die dargestellten Verstöße habe ich nach § 81 Abs. 2 SGB X i.V.m. § 25 Abs. 1 SGB X beanstandet.

21.9 Schutz des Persönlichkeitsrechts der Frauen im Rahmen von Leistungen nach dem Schwangeren- und Familienhilfeänderungsgesetz

Seit dem 1. Januar 1996 haben Frauen Anspruch auf Leistungen bei Vornahme eines nicht rechtswidrigen oder unter den Voraussetzungen von § 218a Abs. 1 StGB vorgenommenen Abbruchs einer Schwangerschaft (vgl. Art. 5 SFHÄndG und § 24b Abs. 4 SGB V). Ich habe die Umsetzung dieser Vorschriften bei der Hamburg-Münchener Ersatzkasse kontrolliert.

Der von den Spitzenverbänden miterarbeitete und von der Hamburg-Münchener Ersatzkasse verwendete Antragsvordruck war zu zwei Punkten verbesserungsbedürftig: Die Erhebung der Angabe „Familienstand" war nicht erforderlich. Zudem fehlten die Hinweise nach § 67a Abs. 3 SGB X auf die Rechte der Antragstellerin, wie z. B. der Hinweis auf eine Rechtsvorschrift, die zur Auskunft verpflichtet, oder die Folgen der Auskunftsverweigerung. Es wurde mir zugesagt, die Vordrucke entsprechend zu ändern.

Die Abrechnung erfolgt im ambulanten Bereich zum Teil in der Form der direkten Einzelabrechnung der Ärzte mit den Krankenkassen, aber auch über die Kassenärztlichen Vereinigungen. Im Hinblick auf den eindeutigen Wortlaut des Art. 5 § 3 Abs. 4 Satz 1 SFHÄndG (*„Der Arzt oder die Einrichtung rechnet Leistungen nach § 2 mit der Krankenkasse ab ..."*) halte ich die Abrechnung über die Kassenärztlichen Vereinigungen aus datenschutzrechtlicher Sicht weiterhin für klärungsbedürftig, da über diesen Abrechnungsweg besonders schützenswerte Daten der betroffenen Frauen auch an nicht ausdrücklich im Gesetz genannte Stellen übermittelt werden.

Darüber hinaus bin ich der Auffassung, daß die bis jetzt personenbezogene Kostenerstattung durch die Länder fallbezogen durchgeführt werden muß. Unbestritten muß die zuständige Landesbehörde aufgrund der Angaben der Kassen in der Lage sein, die sachliche und rechnerische Richtigkeit der Kostenerstattung zu prüfen. Wenn jedoch die Kasse bei der Geltendmachung der Kostenerstattung erklärt, daß es sich bei der Antragstellerin um eine nach Art. 1 § 1 SFHÄndG berechtigte Person handelt, ist es für die Prüfung der Kostenerstattung nicht notwendig, deren Namen zu kennen. Durch eine numerische Kennzeichnung kann sichergestellt werden, daß eventuelle Einwände gegen die Richtigkeit der Erstattung dem konkreten Einzelfall zugeordnet werden können. Eine personenbezogene Übermittlung an die Landesstellen ist damit nicht erforderlich.

Im Hinblick auf die Sensibilität der Daten und die gesetzliche Forderung, im gesamten Verfahren das Persönlichkeitsrecht der Frau unter Berücksichtigung der besonderen Situation der Schwangerschaft zu achten (Art. 5 § 3 Abs. 5 SFHÄndG), halte ich eine fallbezogene Übermittlung an die Landesstellen für zwingend.

Ich werde mich beim BMG und den Spitzenverbänden für ein datenschutzgerechtes Verfahren einsetzen.

22 Rentenversicherung

22.1 Datenstelle der Rentenversicherungsträger beim VDR

Der Verband Deutscher Rentenversicherungsträger (VDR) unterhält eine sog. „Stammsatzdatei", die für die Zwecke der gesetzlichen Rentenversicherung eingerichtet wurde. Sie enthält Grunddaten („Stammsatz") aller gesetzlich Rentenversicherten, das sind über 50 Millionen Bürger. Mit der Datei soll die Vergabe der Rentenversicherungsnummern gesteuert und der reibungslose Datenaustausch unter den Rentenversicherungsträgern ermöglicht werden, um eine effiziente Durchführung der gesetzlichen Rentenversicherung zu sichern. In § 150 Abs. 1 SGB VI hat der Gesetzgeber die zulässigen Zwecke, für die die Stammsatzdatei verwendet werden darf, abschließend aufgeführt. Ihr Umfang macht die Stammsatzdatei allerdings auch für Zwecke außerhalb der gesetzlichen Rentenversicherung interessant. Gleichwohl hat sich bisher bei differenzierter Befassung stets eine andere effiziente Lösung aufzeigen lassen.

22.1.1 Online-Abrufe durch die Hauptzollämter

Arbeitgeber sind gesetzlich verpflichtet, sich von ihren Beschäftigten den Sozialversicherungsausweis vorlegen zu lassen und sie der Einzugsstelle für den

Gesamtsozialversicherungsbeitrag zu melden. Damit soll illegale Beschäftigung vermieden und das Aufkommen der Beiträge zur gesetzlichen Sozialversicherung gesichert werden. Die Prüfung, daß die Arbeitgeber diesen Pflichten nachkommen, obliegt der Bundesanstalt für Arbeit und den Hauptzollämtern. Diese führen örtliche Kontrollen bei Arbeitgebern und an Arbeitsstätten durch, beispielsweise auf Baustellen. Zur Überprüfung festgestellter Unregelmäßigkeiten im Meldeverfahren benötigen die Hauptzollämter Auskünfte aus Dateien des VDR, unter anderem aus der Stammsatzdatei. Diese Auskünfte wurden bisher schriftlich erteilt. Das hatte vor allem den Nachteil, daß die erforderlichen Auskünfte erst mit entsprechenden Verzögerungen, die in der Regel mehrere Tage in Anspruch nahmen, vorlagen. Zwischen dem VDR und den Hauptzollämtern wird daher die Einrichtung eines Online-Abrufverfahrens vorbereitet, was nach § 150 Abs. 4 SGB VI grundsätzlich zulässig ist.

Im Rahmen meiner Zuständigkeit habe ich die Genehmigungsbehörden beraten. Dabei kam es mir vor allem darauf an, daß die Zulässigkeit des einzelnen Abrufs nachvollziehbar bleibt und ein Verfahren zur regelmäßigen internen Stichprobenprüfung vorgesehen wird. Der Schutz der Vertraulichkeit abgerufener Daten auf dem Übertragungswege muß, etwa durch Verschlüsselung, sichergestellt sein. Bei den Hauptzollämtern ist die Zweckbindung für das Prüfverfahren nach § 107 SGB IV einzuhalten und die Löschung der Sozialdaten nach Abschluß des Verfahrens, oder wenn sie dafür nicht mehr benötigt werden, vorzunehmen. Meine Hinweise hat das BMA als Genehmigungsbehörde für den VDR berücksichtigt.

22.1.2 Kein Abgleich mit Sozialhilfedaten

Erhebliche Bedenken bestünden gegen einen Datenabgleich etwa von Sozialhilfedaten mit der Stammsatzdatei des VDR. Derartige Erwägungen hatte es im Zusammenhang mit dem Entwurf eines Gesetzes zur Reform der Sozialhilfe gegeben. Ich habe hierzu entsprechend Stellung genommen, woraufhin davon abgesehen wurde, diese Überlegungen weiter zu verfolgen (s. o. Nr. 19.4).

22.1.3 Umfassendes Sozialdatenprofil wäre verfassungsrechtlich höchst problematisch

Überlegungen gab es für ein Konzept, wonach die Datenstelle des VDR Aufgaben einer Auskunftsstelle sowie einer (zentralen) Vermittlungsstelle hätte übernehmen sollen. Zurecht ist dem das BMA mit Entschiedenheit entgegengetreten, weil es eine wie auch immer geartete Sammlung von Daten anderer Sozialleistungsbereiche durch die Rentenversicherungsträger oder deren Verband für nicht zulässig hält. Auch ich bin der Auffassung, daß es nicht Aufgabe der Rentenversicherungsträger ist, Daten für Sozialhilfezwecke zu sammeln und damit eine diesen Trägern obliegende Aufgabe zu übernehmen. Denn ein solcher Ausbau der Datenstelle des VDR über den Bereich der Rentenversicherung hinaus wäre unvereinbar mit geltendem Recht. Das BMJ hat diese Position bekräftigt und betont, daß eine über die ohnehin zulässige Übermittlung von Sozialdaten zwischen verschiedenen Sozialleistungsträgern hinausgehende Zusammenführung aller Sozialdaten beim VDR dazu führen würde, daß hinsichtlich einer einzelnen Person ein umfassendes Sozialdatenprofil entstehen würde. Eine umfassende Sozialdatensammlung würde aber einen unverhältnismäßigen Grundrechtseingriff darstellen. Ich teile diese Beurteilung des BMJ, das zurecht seine Bedenken auch damit begründet hat, daß der jeweilige Sozialleistungsträger bei Einrichtung einer solchen Datenzentrale nicht mehr die Verantwortung für die Zulässigkeit der Übermittlung „seiner" Daten tragen könnte.

22.1.4 Expertenkommission „Alternative Steuer-Transfer-Systeme"

Die vom BMF eingesetzte Expertenkommission „Alternative Steuer-Transfer-Systeme" hat im Juni 1996 ein Gutachten zu den Möglichkeiten einer Integration von Einkommensbesteuerung und steuerfinanzierten Sozialleistungen veröffentlicht. Die Expertenkommission hatte mich zuvor zu den von ihr untersuchten Modellen um Stellungnahme gebeten.

Das sogenannte „Bürgergeldmodell" hätte die Konzentration personenbezogener Steuer- und Sozialdaten in einem zentralen Datenbestand bei einer Behörde bedeutet. Zu den oben (Nr. 22.1.3) dargestellten verfassungsrechtlichen Bedenken gegen einen umfassenden „Sozialdatenpool" wäre hinzugekommen, daß Daten zusammengeführt würden, die jeweils besonderen Amtsgeheimnissen unterliegen, nämlich Steuerdaten, für die das Steuergeheimnis (§ 30 AO) gilt, und Sozialdaten, die dem Schutz des Sozialgeheimnisses (§ 35 SGB I) unterliegen. Eine derart umfassende zentrale Datensammlung hätte zur Folge gehabt, daß über jeden unter steuerlichen oder sozialen Gesichtspunkten „erfaßten" Bürger ein umfassendes Datenprofil entstanden wäre. In ihrem Gutachten hat die Expertenkommission das „Bürgergeldmodell" nicht empfohlen.

Auch das von der Expertenkommission untersuchte sog. „Kooperationsmodell" und das von ihr empfohlene „Sozialtransferamts-Modell" weisen einige Probleme auf, die jedoch nicht annähernd so gravierend waren, wie beim „Bürgergeldmodell".

22.2 Anspruchs- und Anwartschaftsüberführungsgesetz

Das Anspruchs- und Anwartschaftsüberführungsgesetz (AAÜG) regelt die Überführung von Ansprüchen und Anwartschaften aus den Zusatz- und Sonderversorgungssystemen der ehemaligen DDR. Das Gesetz sieht eine Begrenzung des berücksichtigungsfähigen Arbeitsentgelts oder -einkommens bei Zugehörigkeit zu bestimmten Versorgungssystemen vor (§§ 6 und 7 AAÜG). Die frühere Fassung von § 6 Abs. 3 erstreckte diese Begrenzung auf Zeiten „systemnaher" Beschäftigung oder Tätigkeit. Dazu zählten auch ehrenamtliche Berufungs- oder Wahlfunktionen im Staatsapparat oder in einer Partei oberhalb der Kreisebene. Diese Vorschriften wurden aufgrund ihrer Wirkungen für die Betroffenen verbreitet als „Rentenstrafrecht" bezeichnet.

Für die Überführung der Ansprüche und Anwartschaften nach dem AAÜG ist die BfA zuständig. Der von ihr verwandte Fragebogen an die Betroffenen enthielt unter Nr. 4.5 einen differenzierten Katalog mit Fragen nach allen Wahl- und Berufungsfunktionen sowie Beschäftigungen, für die das Gesetz eine Begrenzung des berücksichtigungsfähigen Entgelts vorsah. Viele der Betroffenen empfanden sich hierdurch zu ihrer politischen Vergangenheit ausgefragt, ohne daß ihnen ein Bezug der Antworten für die Rentenberechnung erkennbar gewesen wäre.

Auf meine Bitte hat die BfA in dem Formular bei den einzelnen Fragen einen Hinweis auf die jeweils zugrundeliegende Rechtsvorschrift aufgenommen. Ferner versendet sie mit dem Formular ein Merkblatt, das über das AAÜG informiert.

Die betroffenen Versorgungsträger müssen der BfA die erforderlichen Auskünfte mitteilen, damit sie die neuen versicherungsrechtlichen Ansprüche und Leistungen aus der Rentenversicherung feststellen kann. Da das Gesetz einen früheren Verlust der Anwartschaften (z. B. durch Rückzahlung der Beiträge) als nicht eingetreten fingiert und ein Verzicht des Betroffenen auf die Überführung von Ansprüchen und Anwartschaften aus Sonder- und Zusatzversorgungssystemen als nicht möglich gilt, finden diese Datenübermittlungen auch gegen den Willen des Betroffenen statt.

Versorgungsträger für die „freiwillige zusätzliche Altersversorgung für hauptamtliche Mitarbeiter der SED/PDS" ist die Partei des Demokratischen Sozialismus (PDS). Für Angehörige dieses Zusatzversorgungssystems muß die BfA daher Daten über Beschäftigungszeiten und Arbeitsentgelte von der PDS erheben. Dies haben Betroffene z. T. mit Verwunderung zur Kenntnis genommen, was sie mir gegenüber äußerten.

Das Unbehagen vieler Betroffener kann ich – auch angesichts der breiten Spanne der betroffenen Funktionen und Beschäftigungen – gut nachvollziehen. Hingegen waren der Fragebogen der BfA und die Auskünfte zwischen den Versorgungsträgern und der BfA datenschutzrechtlich nicht zu beanstanden, da sie der geltenden Rechtslage entsprachen.

Durch die inzwischen erfolgte Änderung des AAÜG wird nur noch für einen engen Kernbereich von Spitzenfunktionären das berücksichtigungsfähige Entgelt begrenzt. Dadurch ist der Kreis der Betroffenen nunmehr erheblich eingeschränkt.

22.3 Dialogverfahren der Rentenversicherungsträger

Die einmal begründete Zuständigkeit einer Landesversicherungsanstalt bleibt grundsätzlich auch nach dem Umzug eines Versicherten in ein anderes Bundesland erhalten (vgl. § 126 Abs. 1 und 2 SGB VI). Selbst für einfache Auskünfte mußte sich bisher der Versicherte dann an die entfernte Rentenversicherung wenden. Um die Zusammenarbeit bei der Versichertenbetreuung zu verbessern, haben die gesetzlichen Rentenversicherungsträger die Einrichtung eines „Dialogverfahrens" vereinbart. Das Verfahren ermöglicht es dem Versicherten, die gewünschten Informationen über sein Versicherungsverhältnis und über erworbene Anwartschaften auch bei anderen als dem zuständigen Rentenversicherungsträger erhalten zu können. Dazu fordert der an sich unzuständige Rentenversicherungsträger die erbetene Auskunft automatisiert an. Die Antwort kann er dem Versicherten dann ausdrucken und erläutern.

In einer zweiten Stufe des Dialogverfahrens kann dann das gesamte Versicherungskonto übermittelt werden. Der befragte Rentenversicherungsträger hat somit die Möglichkeit, die gewünschte Auskunft unmittelbar zu geben und z. B. auch Modellrechnungen mit fiktiven zusätzlichen Versicherungszeiten durchzuführen.

Die Einrichtung und Durchführung dieses Dialogverfahrens ist rechtlich zulässig. Es stellte sich allerdings die Frage, ob das Dialogverfahren als „Datenverarbeitung im Auftrag" (§ 80 SGB X) oder als „Abrufverfahren" (§ 79 SGB X) einzuordnen war. Während im ersten Fall die Anzeige an die Aufsichtsbehörde genügt, ist für die Einrichtung automatischer Abrufverfahren deren Genehmigung erforderlich. Ich habe das Dialogverfahren als Datenverarbeitung im Auftrag bewertet.

Zugleich habe ich in meiner Stellungnahme besondere Maßnahmen zur technischen und organisatorischen Sicherung für das Dialogverfahren gefordert, weil es einen bundesweiten Zugriff auf Rentenversicherungskonten eröffnet. So halte ich die Protokollierung der Zugriffe und deren stichprobenmäßige Kontrolle für unverzichtbar. Der auskunftsuchende Versicherte sollte seine Identität z. B. mit dem Personalausweis nachweisen müssen und seinen Wunsch auf Auskunftserteilung unter Nutzung des Dialogverfahrens schriftlich dokumentieren. Dies gibt dem Versicherten die Gewißheit, daß andere Personen das Dialogverfahren nicht mißbrauchen können, um unbefugt Rentenauskünfte über ihn zu erlangen.

Die BfA, die an dem Dialogverfahren anfangs nicht teilgenommen hatte, hat mich inzwischen über den Abschluß entsprechender Verwaltungsvereinbarungen mit anderen Rentenversicherungsträgern unterrichtet.

23 Unfallversicherung

23.1 Unfallversicherungsrecht kodifiziert

Am 1. Januar 1997 ist das Gesetz zur Einordnung des Rechts der gesetzlichen Unfallversicherung in das Sozialgesetzbuch – SGB VII – in Kraft getreten. Die Vorbereitung dieses auch unter Datenschutzgesichtspunkten wichtigen Gesetzes habe ich von Anfang an mit großer Intensität und in guter Zusammenarbeit mit dem BMA begleitet.

Anknüpfend an die in meinem 15. Tätigkeitsbericht (Nr. 14.1) im einzelnen dargestellten Grundsatzprobleme der gesetzlichen Unfallversicherung war es mein vorrangiges Ziel, den Versicherten so weit wie möglich in das Feststellungsverfahren einzubeziehen und die einzelnen Verfahrensschritte für ihn transpa-

rent zu gestalten, sowie die Datenerhebung, -verarbeitung und -nutzung im einzelnen – orientiert am Maßstab der Verhältnismäßigkeit – normenklar festzulegen.

Insgesamt kann ich eine befriedigende Bilanz meiner Bemühungen ziehen:

- In den Fällen, in denen ein Unfallversicherungsträger bei einem anderen Sozialleistungsträger (z. B. einer Krankenkasse) besonders schutzwürdige Sozialdaten im Sinne des § 76 SGB X anfordert, ging die in § 76 Abs. 2 Nr. 1 SGB X normierte Hinweispflicht auf sein Widerspruchsrecht gegen die Übermittlung ins Leere, weil bei der übermittelnden Stelle – der Krankenkasse – kein Verwaltungsverfahren anhängig ist. Diese Lücke wird nunmehr durch § 200 Abs. 1 SGB VII geschlossen. Danach ist der Unfallversicherungsträger verpflichtet, auch auf ein gegenüber einem anderen Sozialleistungsträger bestehendes Widerspruchsrecht hinzuweisen, wenn dieser nicht selbst zu einem Hinweis nach § 76 Abs. 2 Nr. 1 SGB X verpflichtet ist. Ein entsprechendes Verfahren wird bereits seit längerem von der BfA und der BA praktiziert (vgl. meinen 15. TB Nr. 10.8.3).

- Das Verfahren der Erteilung eines Gutachtenauftrages wurde ebenfalls gesetzlich geregelt, was damit die Rechte der Versicherten stärkt. Wegen des durch jede Untersuchung erfolgenden erheblichen Eingriffs in die Grundrechte der Versicherten, der besonderen Sensibilität der erhobenen medizinischen Daten sowie der in diesem Zusammenhang häufig befürchteten und mitunter auch beklagten Interessengebundenheit von Gutachtern war es mir ein wesentliches Anliegen, eine umfassende Mitwirkung des Versicherten sicherzustellen. Dies ist mit der Vorschrift des § 200 Abs. 2 SGB X gelungen.

  Aufgrund der Bedeutung dieser Vorschrift gebe ich den Bericht des Ausschusses für Arbeit und Sozialordnung (BT-Drs. 13/4853 vom 12. Juni 1996 S. 22 und S. 13), der eindrucksvoll die parlamentarischen Überlegungen zum „Gutachterwesen" zum Ausdruck bringt, im Wortlaut wieder:

  „Die Vorschrift begründet bei der Bestellung von Gutachtern ein Auswahlrecht für den Versicherten und dient damit der Transparenz des Verfahrens. Das Auswahlrecht setzt voraus, daß der Unfallversicherungsträger dem Versicherten mehrere geeignete Gutachter vorschlägt; auch der Versicherte hat das Recht, einen oder mehrere Gutachter vorzuschlagen. In bestimmten Fällen (insbesondere dann, wenn zu einem Kausalzusammenhang noch keine breiten medizinisch-wissenschaftlichen Erkenntnisse vorliegen) wird allerdings nur eine sehr geringe Zahl von Gutachtern zur Verfügung stehen, so daß der Unfallversicherungsträger dem Versicherten lediglich zwei oder auch nur einen Gutachter vorschlagen kann. Der Gesetzgeber geht aber davon aus, daß es sich dabei nur um Ausnahmesituationen handeln kann. Mit der Neuregelung verbindet der Gesetzgeber ferner die nachdrückliche Erwartung, daß die Unfallversicherungsträger dafür Sorge tragen, daß eine ausreichende Anzahl von Gutachtern zur Verfügung steht und der für die Erstattung der Gutachten benötigte Zeitraum deutlich verringert wird. ... Es bestand auch Übereinstimmung, daß sich die im Ausschuß neu beschlossene Regelung des Artikels 1 § 200 Abs. 2 auch auf die Vergabe von Gutachten nach Aktenlage erstreckt."

- In der Vergangenheit habe ich oftmals kritisiert, daß zahlreiche Unfallversicherungsträger Informationen über sämtliche Vorerkrankungen und auch nicht-medizinische Daten – zum Teil auch mehrfach – erhoben haben. Nunmehr sind Zweck und Umfang der Datenerhebung durch Unfallversicherungsträger bei Krankenkassen, früher behandelnden Ärzten sowie Durchgangsärzten und vergleichbaren, nach dem sog. Ärzteabkommen für bestimmte Verletzungsarten vorgesehenen Ärzten hinreichend normiert:

  - Nach § 188 SGB VII können die Unfallversicherungsträger von den Krankenkassen Auskunft über die Behandlung, den Zustand sowie über Erkrankungen und frühere Erkrankungen des Versicherten verlangen, soweit dies für die Feststellung des Versicherungsfalles erforderlich ist. Sie sollen dabei ihr Auskunftsverlangen auf solche Erkrankungen oder auf solche Bereiche von Erkrankungen beschränken, die mit dem Versicherungsfall in einem ursächlichen Zusammenhang stehen können.
  - Ärzte und Zahnärzte, die nicht an einer Heilbehandlung nach § 34 beteiligt sind, sind verpflichtet, dem Unfallversicherungsträger auf Verlangen Auskunft über die Behandlung, den Zustand sowie über Erkrankungen und frühere Erkrankungen des Versicherten zu erteilen, soweit dies für die Heilbehandlung und die Erbringung sonstiger Leistungen erforderlich ist. Der Unfallversicherungsträger soll Auskunftsverlangen zur Feststellung des Versicherungsfalls auf solche Erkrankungen oder auf solche Bereiche von Erkrankungen beschränken, die mit dem Versicherungsfall in einem ursächlichen Zusammenhang stehen können (vgl. § 203 SGB VII).
  - Durchgangsärzte und vergleichbare, nach dem sog. Ärzteabkommen für bestimmte Verletzungsarten vorgesehene Ärzte erheben, speichern und übermitteln an die Unfallversicherungsträger Daten über die Behandlung und den Zustand des Versicherten sowie andere personenbezogene Daten, soweit dies für Zwecke der Heilbehandlung und die Erbringung sonstiger Leistungen erforderlich ist. Ferner erheben, speichern und übermitteln sie die Daten, die für ihre Entscheidung, eine Heilbehandlung nach § 34 durchzuführen, maßgeblich waren (vgl. § 201 SGB VII).

- Das verfassungsrechtliche Transparenzgebot ist nunmehr ebenfalls in ausreichendem Maße berücksichtigt:

  - Nach der Regelung des § 103 Abs. 2 SGB VII ist der Versicherte berechtigt, an der Unter-

suchung eines Versicherungsfalles, die am Arbeitsplatz oder am Unfallort durchgeführt wird, teilzunehmen. Sofern aufgrund des Versicherungsfalles Ansprüche entstehen können, gilt entsprechendes für die Hinterbliebenen.

- Der Unfallversicherungsträger hat den Versicherten auf das Recht hinzuweisen, auf Verlangen über die von den Krankenkassen übermittelten Daten unterrichtet zu werden (§ 188 Satz 4 SGB VII).
- Der Versicherte kann vom Unternehmer verlangen, daß ihm eine Kopie der Unfall- oder Berufskrankheitenanzeige überlassen wird (§ 193 Abs. 4 Satz 2 SGB VII).
- Nach § 201 Abs. 1 Satz 5 SGB VII bestehen für die Durchgangsärzte und für die nach § 34 SGB VII vergleichbaren Ärzte Unterrichtungspflichten u. a. über den Erhebungszweck.
- In den Fällen, in denen Unfallversicherungsträger bei früher behandelnden Ärzten Daten erheben, haben die Träger den Versicherten auf ein solches Auskunftsverlangen sowie auf das Recht, auf Verlangen über die von den Ärzten übermittelten Daten unterrichtet zu werden, rechtzeitig hinzuweisen (§ 203 Abs. 2 SGB VII).
- Sofern eine Datei für mehrere Unfallversicherungsträger errichtet wird, ist der Versicherte vor der erstmaligen Speicherung über die Art der gespeicherten Daten, die speichernde Stelle und den Zweck der Datei durch den Unfallversicherungsträger schriftlich zu unterrichten (§ 204 Abs. 7 SGB VII).
- Werden Daten für die Forschung zur Bekämpfung von Berufskrankheiten an die Unfallversicherungsträger oder deren Verbände übermittelt, haben diese den Versicherten oder den früher Versicherten schriftlich über die übermittelten Daten und über den Zweck der Übermittlung zu unterrichten (§ 206 Abs. 1 Satz 2 SGB VII).

– Eine am Maßstab der Verhältnismäßigkeit orientierte Reduzierung der Datenerhebung über den Versicherten konnte ich dadurch erreichen, daß ich ein gestuftes Erhebungsverfahren angeregt habe, das nunmehr in § 199 Abs. 3 SGB VII normiert ist: Der Unfallversicherungsträger soll Auskünfte über Erkrankungen und frühere Erkrankungen des Betroffenen von anderen Stellen oder Personen erst einholen, wenn hinreichende Anhaltspunkte für den ursächlichen Zusammenhang zwischen der versicherten Tätigkeit und dem schädigenden Ereignis oder der schädigenden Einwirkung vorliegen.

– Schließlich ist die Errichtung einer Datei für mehrere Unfallversicherungsträger bei einem von ihnen oder bei einem Verband der Unfallversicherungsträger auf eine normenklare Grundlage gestellt worden, da § 204 SGB VII nunmehr im einzelnen festlegt, welche Daten für welche Zwecke erhoben, verarbeitet oder genutzt werden dürfen.

Zu meinem Bedauern hat der HVBG unmittelbar nach Verkündung des SGB VII dieses in einer mit mir nicht abgestimmten „Erstkommentierung" allen Unfallversicherungsträgern zur Verfügung gestellt und darin die relevanten Neuregelungen teilweise im Sinne der bisherigen unzureichenden Verwaltungspraxis kommentiert. Für die Erarbeitung einer Dienstanweisung zum Datenschutz für die Praxis der Berufsgenossenschaften werde ich nun intensive Gespräche mit dem HVBG führen. Ich erwarte hierzu zufriedenstellende Ergebnisse, weil meine Kontrollen bei der Südwestlichen Bau-Berufsgenossenschaft und der Großhandels- und Lagerei-Berufsgenossenschaft ausgesprochen erfreuliche Ergebnisse erbracht haben (s. u. Nr. 23.5). Die Gespräche im Rahmen dieser Kontrollen haben gezeigt, daß Datenschutz als Unternehmensziel einer Berufsgenossenschaft akzeptiert wird und daß Datenschutz – richtig verstanden und umgesetzt – auch dazu beitragen kann, Verfahren zu verkürzen und Kosten zu senken. Beispiele sind das sogenannte abgestufte Erhebungsverfahren (§ 199 Abs. 3 SGB VII) und die Regelung, nach der es unzulässig ist, gleichzeitige Mehrfacherhebungen bei verschiedenen Stellen und mehrfache zeitversetzte Angaben des Versicherten zur Krankheitsgeschichte und zum Hergang des Unfalls parallel zur Unfallanzeige vorzunehmen (§ 201 SGB VII i.V. m. § 67 a Abs. 1 SGB X).

23.2 Abschottungsprobleme bei arbeitsmedizinischen Vorsorgeuntersuchungen

Zu den Anforderungen an die datenschutzgerechte Organisation des Arbeitsmedizinischen Dienstes (AMD) gehört dessen hinreichende Abschottung von seinen jeweiligen Trägern. Dies gebietet eine möglichst organisatorische, zumindest aber funktionale und personelle Trennung mit der Folge, daß dem Unfallversicherungsträger nur die Dienstaufsicht, nicht aber auch die Fachaufsicht über den AMD zukommt.

Das Problem der Abschottung kann erhebliche praktische Bedeutung haben. So hatte der Arzt eines AMD die Vorlage von Patientengutachten an die Leiterin des AMD mit der Begründung abgelehnt, infolge nicht hinreichender Abschottung des AMD sei nicht gewährleistet, daß das Gutachten sodann nicht auch der Berufsgenossenschaft zur Kenntnis kommen könnte.

Nach bisherigem Recht war das Abschottungsgebot nicht ausdrücklich gesetzlich normiert. Rechtsgrundlage und Ausmaß der gebotenen Abschottung waren streitig. In das inzwischen in Kraft getretene SGB VII ist das Abschottungsgebot aufgenommen worden (§ 24 SGB VII). Die neue Vorschrift enthält jedoch zugleich eine Einwilligungsklausel, die die Übermittlung von Sozialdaten vom AMD an den Unfallversicherungsträger mit Einwilligung des Versicherten zuläßt. Wie sich diese praktisch auswirkt, werde ich sorgfältig beobachten.

Mit dem Hauptverband der gewerblichen Berufsgenossenschaften (HVBG) habe ich inzwischen Ge-

spräche zur Umsetzung der gesetzlichen Neuregelung auf die Organisation der AMD aufgenommen.

23.3 Vorlage des ehemaligen DDR-Sozialversicherungsausweises

Ein Petent machte mich darauf aufmerksam, daß Berufsgenossenschaften zur Ermittlung von Vorerkrankungen, die für die Beurteilung von Berufskrankheiten und Arbeitsunfällen von Bedeutung sein können, von Versicherten aus den neuen Bundesländern oft die Vorlage des vollständigen Sozialversicherungsausweises verlangen. Im Falle des Petenten waren Diagnosen der letzten 30 Jahre darin aufgeführt.

Durch die Unfallanzeige des Arbeitgebers erfuhr die Süddeutsche Metallberufsgenossenschaft (SMBG), daß sich der Petent während der Arbeit am rechten Arm verletzt haben soll. Aufgrund der in der Unfallanzeige genannten Diagnose – einer Verletzung, bei deren Entstehung häufig Vorschäden mitwirken – habe die SMBG den Petenten u. a. um Zusendung seines Sozialversicherungsausweises der ehemaligen DDR gebeten. Da zu diesem Zeitpunkt die exakte Diagnose noch nicht feststand und auch kein Arztbericht vorlag, stimmte die SMBG mit mir überein, daß es nach § 67a SGB X nicht erforderlich war, Informationen über sämtliche Vorerkrankungen zu erheben.

Im Rahmen eines Beratungsbesuches bei einer anderen Berufsgenossenschaft ergab sich zur Praxis der Anforderung des Sozialversicherungsausweises folgendes Bild:

Der Sozialversicherungsausweis wird dann nicht angefordert, wenn die Berufskrankheit in der DDR bereits anerkannt und dies der Berufsgenossenschaft bekannt ist. Er wird hingegen bei den Arbeitsunfällen benötigt, bei denen sich einschlägige Vorerkrankungen nicht ermitteln lassen.

Auch bei den sog. „Altfällen", die jetzt erst gemeldet werden, und bei Berufskrankheiten kommt dem Sozialversicherungsausweis eine wesentliche Rolle zu. In diesen Fällen wird der Sozialversicherungsausweis dann angefordert, wenn ein Unfallereignis oder das Vorliegen einer Berufskrankheit fraglich ist. Ohne die Vorlage des Sozialversicherungsausweises als amtliches Schriftstück wäre in vielen Fällen nur die Ablehnung eines Anspruchs aus Beweisgründen möglich.

Im Ergebnis dürfte die Anforderung des kompletten Sozialversicherungsausweises oftmals unverhältnismäßig sein. Im Interesse der Betroffenen sollten aber praktikable Lösungen gefunden werden. So wäre z. B. eine individuelle Auflistung der Vorerkrankungen durch den Versicherten selbst und eine anschließende Nachfrage bei den vorbehandelnden Ärzten unter den Voraussetzungen des § 203 SGB VII denkbar. Auch eine Aufforderung des Versicherten, durch den Arzt seines Vertrauens die für die Feststellung relevanten (Vor)erkrankungen anhand des Sozialversicherungsausweises auswerten und benennen zu lassen, kommt in Betracht.

23.4 Kontrollen von Berufsgenossenschaften

Im Berichtszeitraum habe ich die Verwaltungs-Berufsgenossenschaft (VBG) und die Bergbau-Berufsgenossenschaft (BBG) kontrolliert, um aus deren Verwaltungspraxis, insbesondere zum Feststellungsverfahren von Berufskrankheiten Hinweise auf einen Regelungsbedarf für das parallel verlaufende Gesetzgebungsverfahren SGB VII gewinnen zu können. Außerdem habe ich die Großhandels- und Lagereisowie die Südwestliche Bau-Berufsgenossenschaft beraten und kontrolliert.

23.4.1 Kontrolle der Verwaltungs-Berufsgenossenschaft

Die VBG setzt im Rahmen des Verwaltungsverfahrens zur Feststellung von Berufskrankheiten Vordrucke sowie frei formulierte Texte ein, die die notwendigen datenschutzrechtlichen Hinweise und Erläuterungen entweder gar nicht, nur unvollständig oder in unzutreffender Weise enthalten.

Einige der eingesehenen Berufskrankheitenakten enthielten vorgefertigte Einwilligungsformulare für Versicherte, die insgesamt als unwirksam anzusehen waren: Soweit sich die Einwilligungserklärungen darauf beziehen, daß die Berufsgenossenschaft zur Feststellung von Leistungen insbesondere Krankengeschichten und Akten anderer Versicherungen und Behörden benötigt, ist dies unzulässig. Denn es verleitet den Versicherten dazu, in die Übermittlung nicht erforderlicher, vor allem medizinischer Informationen einzuwilligen. Soweit die Erklärung auf Auskünfte über bestehende und frühere Erkrankungen abstellt, bezieht sie in die erbetene Einwilligung auch solche Auskünfte ein, die von behandelnden Ärzten nach Maßgabe des § 100 SGB X i.V. m. § 1543d RVO und von Krankenkassen gem. § 1502 RVO auf Grund gesetzlicher Verpflichtung erteilt werden müssen. Auf diese Weise entsteht für den Versicherten der unzutreffende Eindruck, die Zulässigkeit auch der kraft Gesetzes zu übermittelnden Angaben hänge von seiner Einwilligung ab. Soweit die Einwilligung auf die Übermittlung von Sozialdaten des Versicherten an „andere, insbesondere Ärzte, Arbeitgeber und Behörden" bezogen ist, ist dies mit der Regelung des § 76 Abs. 2 SGB X unvereinbar. Mit einer derartigen, auf keinen konkreten Dateninhalt und Übermittlungszweck bezogenen Einwilligung wird dem Betroffenen die Möglichkeit genommen, einer solchen Übermittlung im Einzelfall gem. § 76 Abs. 2 SGB X zu widersprechen.

Insgesamt vermittelte die Kontrolle der Einzelvorgänge den Eindruck, daß die VBG im Berufskrankheiten-Verfahren Auskünfte bei Ärzten, Krankenkassen und Arbeitgebern ausschließlich auf der Grundlage von Einwilligungserklärungen einholt und sich dabei nicht auf die Auskunftspflichten nach Maßgabe der §§ 1502, 1543 c und 1543 d RVO i.V. m. § 100 SGB X bezieht. Im Ergebnis erhält die VBG auf diese Weise erheblich mehr medizinische und nicht-medizinische Informationen über den Versicherten als ihr auf Grund dieser Vorschriften zustehen.

Die VBG hat mir zugesagt, die entsprechenden Einwilligungserklärungen, Hinweise und Erläuterungen in Vordrucken, Formschreiben und Textbausteinen sowie die Arbeitsregeln für frei formulierte Schreiben entsprechend zu überarbeiten. Zielvorgabe dafür ist, daß der Versicherte über Inhalt, Umfang und Zweck der benötigten Informationen so umfassend aufgeklärt wird, daß er seine Entscheidung auf der Grundlage einer möglichst vollständigen Transparenz des Verfahrens treffen kann. Inzwischen hat die VBG in enger Zusammenarbeit mit mir den Entwurf einer Dienstanweisung für den Datenschutz erstellt, der den Belangen des Datenschutzes weitgehend entspricht.

23.4.2 Kontrolle der Bergbau-Berufsgenossenschaft

Bereits in meinem 15. Tätigkeitsbericht (Nr. 14.4) habe ich über das Verfahren der Ersterhebung bei der Bergbau-Berufsgenossenschaft (BBG) berichtet: Nach Darstellung der BBG versendet sie einen Vordruck mit den wesentlichen Einzelfragen zur Klärung der arbeitstechnischen und gesundheitlichen Voraussetzungen an den Versicherten mit der Bitte, diesen innerhalb von zwei Wochen zurückzuschicken. Erst nach Ablauf einer zusätzlichen Frist von einer Woche für die Postlaufzeit richtet sie gezielt Anfragen an andere Sozialleistungsträger und weitere Stellen.

Bei der Überprüfung dieses Verfahrens anhand von zwei Einzelfällen sind allerdings Zweifel aufgetaucht, ob die zeitlichen Vorgaben regelmäßig so eingehalten werden. Die BBG hat mir daher eine entsprechende Überarbeitung der Arbeitshandbücher zugesagt. Darüber hinaus wird die BBG auf meine Anregung hin den Ersterhebungsbogen um den Hinweis ergänzen, daß sie für das Feststellungsverfahren wesentliche Angaben, die vom Versicherten nicht, unvollständig oder widersprüchlich beantwortet worden sind, gegebenenfalls bei Ärzten bzw. Krankenhäusern, Arbeitgebern oder anderen Sozialleistungsträgern nach Maßgabe der entsprechenden gesetzlichen Vorschriften erheben wird.

Auch habe ich ein zufriedenstellendes Ergebnis im Hinblick auf den Umfang der Übermittlung von angeforderten ärztlichen Entlassungsberichten nach Rehabilitationsmaßnahmen erreicht. Da die BBG nicht den kompletten Entlassungsbericht, sondern lediglich Informationen zum Aufnahmebefund, zur Therapie (u. U. auch über die Mitwirkung des Versicherten), zum Entlassungsbefund und zu Behandlungsvorschlägen benötigt, werden die Behandlungsaufträge um einen entsprechenden Hinweis ergänzt, um zu gewährleisten, daß lediglich diese Daten übermittelt werden.

23.4.3 Kontrolle der Südwestlichen Bau-Berufsgenossenschaft

Die Südwestliche Bau-Berufsgenossenschaft ist als Sozialleistungsträger nach § 81 Abs. 4 Satz 1 SGB X i.V. m. § 36 Abs. 1 Satz 1 BDSG verpflichtet, einen internen Datenschutzbeauftragten zu bestellen. Diese Funktion ist seit einiger Zeit vakant. Mit der Hauptgeschäftsführung wurden folgende Möglichkeiten zur Lösung besprochen:

- Zusammenfassung von Innenrevision und Datenschutz in Personalunion und
- Bestellung eines gemeinsamen Datenschutzbeauftragten zusammen mit einem anderen kleineren Sozialleistungsträger.

Gegen eine Zusammenfassung von Innenrevision und Datenschutzbeauftragten habe ich keine grundsätzlichen Bedenken. Allerdings muß sichergestellt werden, daß die unterschiedliche Zwecksetzung von Prüfungen der Finanzkontrolle und des Datenschutzes nicht zu Lasten der Aufgabenwahrnehmung des Datenschutzbeauftragten geht. Wird ein gemeinsamer Datenschutzbeauftragter bestellt, sollte dieser dem größeren Sozialleistungsträger zugeordnet werden, hier also der Südwestlichen Bau-Berufsgenossenschaft. Für den kleineren Sozialleistungsträger ist der Datenschutzbeauftragte dann ein sogenannter externer Datenschutzbeauftragter (s. auch Nr. 19.1).

Darüber hinaus habe ich noch Aspekte des Akteneinsichtsrechts, im Feststellungsverfahren von der Leistungsabteilung verwandte Formulare und Textbausteine und die Abschottung der Beihilfestelle erörtert:

- Zum Akteneinsichtsrecht wurde Übereinstimmung erzielt, daß der Versicherte ein uneingeschränktes Einsichtsrecht in ihn betreffende ärztliche Gutachten hat. Bei der Entscheidung über die Akteneinsicht des Versicherten in die Begehungsberichte des Technischen Aufsichtsdienstes (z. B. über Arbeitsplatzmessungen) oder in den Unfalluntersuchungsbericht kommt es mit Rücksicht auf Betriebs- und Geschäftsgeheimnisse des Unternehmers auf eine Güterabwägung an. Hinsichtlich der die Arbeitssituation des Versicherten betreffenden Informationen, die für das Verfahren erforderlich sind, geht das Einsichtsrecht des Versicherten regelmäßig vor. Denn das Einsichtsrecht nach § 25 SGB X ist als Ausfluß des informationellen Selbstbestimmungsrechts im Lichte des § 83 SGB X zu sehen.

  Mein Einsichts- und Auskunftsrecht nach § 24 Abs. 4 BDSG erkennt die Südwestliche Bau-Berufsgenossenschaft uneingeschränkt an.
- Zu den Formularen und Textbausteinen habe ich einige Hinweise gegeben, die im Rahmen der zum Inkrafttreten des SGB VII gebotenen Überarbeitung Berücksichtigung finden können.
- Die bei einer früheren Kontrolle als notwendig erkannte Abschottung der Beihilfestelle war inzwischen vollzogen und hat sich bewährt. Mit der Beihilfebearbeitung sind ausschließlich der Abschnittsleiter Beihilfe und zwei Halbtagsbeschäftigte befaßt. Weitere Personen erhalten von den Vorgängen keine Kenntnis. Als beispielhaft ist hervorzuheben, daß Schreiben der Beihilfestelle mit dem Zusatz „Beihilfestelle" auf dem Briefkopf und mit einem Hinweis an den Empfänger, daß Schreiben in Beihilfeangelegenheiten bereits in der Adresse einen Zusatz „Beihilfestelle" tragen sollen, versehen sind. Diese organisatorischen

Maßnahmen schaffen die Voraussetzungen dafür, daß die Eingangspost in Beihilfeangelegenheiten von der Poststelle unmittelbar dem Abschnittsleiter Beihilfe zugeleitet werden.

23.4.4 Kontrolle der Großhandels- und Lagerei-Berufsgenossenschaft

Bei der Großhandels- und Lagerei-Berufsgenossenschaft habe ich vor allem die Gutachterdatei für Berufskrankheiten kontrolliert. Die Datei ist eine Arbeitshilfe für die Mitarbeiter der Berufskrankheiten-Abteilung und dient der Ermittlung eines für die Begutachtung bestimmter Berufskrankheiten kompetenten und möglichst ortsnahen Gutachters. In der Datei waren zu einigen Gutachtern Merkmale enthalten, die sich auf die Bearbeitungsdauer oder Verwertbarkeit des Gutachtens (Schlüssigkeit der Begründung, Erfahrungswerte über die Akzeptanz bei Gerichten, Auffassung des Gutachters zu wissenschaftlich streitigen Fachfragen) bezogen. Obwohl gegen die Erforderlichkeit einer solchen Datei keine grundsätzlichen Bedenken bestehen, habe ich in Übereinstimmung mit der Großhandels- und Lagerei-Berufsgenossenschaft festgestellt, daß die Gutachterdatei u. a. wegen der darin enthaltenen Daten und ihrer Konzeption so nicht zulässig und somit änderungsbedürftig ist. Inzwischen hat mir die Großhandels- und Lagerei-Berufsgenossenschaft mitgeteilt, daß sie die Gutachterdatei entsprechend meinen Empfehlungen überarbeitet hat und die betroffenen Gutachter über die Speicherung ihrer Daten informiert werden.

23.5 Kontrolle beim Hauptverband der gewerblichen Berufsgenossenschaften

Bei der Kontrolle einzelner Berufsgenossenschaften habe ich im Jahre 1995 festgestellt, daß diese noch bis Ende 1994 auf den Meldeformularen für die BK-DOK – einer Datei, die Daten über Verwaltungsverfahren und Entscheidungen über Berufskrankheiten enthält – die Rentenversicherungsnummer (RV-Nr.) der Versicherten angegeben hatten. Nach Angaben der kontrollierten Berufsgenossenschaften beruhte diese Angabe auf entsprechenden Vorgaben des HVBG im Handbuch zur Verschlüsselung der BK-DOK und wurde erst aufgrund des HVBG-Rundschreibens vom 14. November 1994 eingestellt. Mir gegenüber hatten die Vertreter des HVBG während meines Kontrollbesuches im August 1993 mehrfach versichert, daß die Meldung der RV-Nr. im Rahmen der BK-DOK erst ab 1. April 1994 geplant sei und nach ausführlicher Erörterung zugesagt, dieses Vorhaben bis zu einer eindeutigen rechtlichen Klärung aufzuschieben.

Nach § 81 Abs. 2 SGB X i. V.m. § 25 BDSG habe ich beim HVBG beanstandet,

- daß die Erhebung und Nutzung der Rentenversicherungsnummer im Rahmen der BK-DOK gegen § 35 SGB I (Sozialgeheimnis) i.V. m. §§ 67a Abs. 1 (Datenerhebung), 67b Abs. 1 (Zulässigkeit der Datenverarbeitung und -nutzung), 78a (Technische und organisatorische Maßnahmen), 96 Abs. 3 Satz 1 SGB X (Bildung einer Zentraldatei) und § 18 f Abs. 1 Satz 1 SGB IV (Versicherungsnummer) und
- die seit 1993 wiederholten Fehlinformationen über die angeblich erst ab April 1994 geplante Erhebung und Nutzung der RV-Nr. und die Nichteinhaltung der Zusage, hierauf bis zu einer eindeutigen rechtlichen Klärung verzichten zu wollen, gegen § 24 Abs. 4 BDSG (Verpflichtung, den BfD zu unterstützen) verstößt.

Inzwischen besteht nach § 204 Abs. 1 Nr. 4 i.V. m. Abs. 2 Satz 2 SGB VII (Errichtung einer Datei für mehrere Unfallversicherungsträger) Rechtsklarheit: Die BK-DOK darf die RV-Nr. nicht enthalten.

Außerdem habe ich beim HVBG die Zentraldatei nach § 551 Abs. 2 RVO kontrolliert. In diesem Zusammenhang hatte ich den Berufsgenossenschaften empfohlen, anstelle des Vor- und Nachnamens, des Geburtsdatums und der Staatsangehörigkeit des betroffenen Versicherten dem HVBG lediglich das Geburtsjahr und das Aktenzeichen der Betriebskrankenkasse zwecks Datenaustausches mit der Zentraldatei zu melden. Nach meiner Kenntnis wird seit Anfang 1994 auch so verfahren. Gleichwohl mußte ich feststellen, daß zu Versicherten aus den Jahren 1963 bis 1993 auf den Bildschirmmasken der Übersichten zu bestimmten Erkrankungen der Vor- und Nachname sowie deren Geburtsdaten angezeigt wurden.

Der HVBG hat mir mitgeteilt, daß er es bedauere, daß die Daten nicht gelöscht worden seien. Dies sei aber unmittelbar nach meiner Kontrolle geschehen.

Ferner haben im Berichtszeitraum der HVBG und ich unterschiedliche Positionen zu den Kompetenzen des Hauptverbandes gegenüber seinen Mitgliedern vertreten. Aus verschiedenen Regelungen seiner Satzung ergibt sich, daß der HVBG, falls und soweit er gegenüber seinen Mitglieds-Berufsgenossenschaften zu datenschutzrechtlichen Problemen Stellung nimmt, nicht lediglich beratend tätig wird, sondern aus seiner „Führungsfunktion" (Grundsatz Nr. 4 der Satzung) heraus seinen Mitgliedern Handlungsleitlinien gibt. An diese fühlen sich seine Mitglieder im Sinne der satzungsmäßigen Verbandsdisziplin gebunden, so z. B. bei der Auslegung des § 1543 d RVO (Auskunftspflicht des behandelnden Arztes, jetzt in § 203 SGB VII neu geregelt). Der HVBG hat aber auch nach Auffassung des BMA lediglich koordinierende und unterstützende Funktion und darf in die Rechtsbeziehungen zwischen den Berufsgenossenschaften und ihren Versicherten nicht eingreifen. Dasselbe gilt hinsichtlich der zwischen den Berufsgenossenschaften und mir bestehenden Rechtsbeziehungen. Der Hauptgeschäftsführer des HVBG hatte auf der Hauptgeschäftsführerkonferenz vom 30. November 1995 moniert, daß ich anläßlich von Kontrollen einzelner Berufsgenossenschaften mit diesen eigene Datenschutzlösungen ohne vorherige Absprachen mit dem HVBG entwickelt hatte. Da die Mitglieds-Berufsgenossenschaften nach dem Datenschutzrecht jedoch selbständige und eigenverantwortlich handelnde Stellen sind, halte ich dies für legitim. Um für die Zukunft Unstimmigkeiten und Irritationen auszuschließen, wurde u. a. vereinbart,

datenschutzrechtliche Probleme im Bereich der gesetzlichen Unfallversicherung so frühzeitig und umfassend wie möglich einvernehmlich zu lösen.

24 Pflegeversicherung

24.1 Gemeinsame Verarbeitung und Nutzung personenbezogener Daten durch Kranken- und Pflegekassen

Die gesetzliche Krankenversicherung und die gesetzliche Pflegeversicherung bilden einerseits zwei eigenständige Zweige der Sozialversicherung. Andererseits aber sind die Aufgaben von Kranken- und Pflegekassen derart eng miteinander verwoben, daß eine gemeinsame Verarbeitung und Nutzung personenbezogener Daten, insbesondere auch zur Vermeidung von Doppelleistungen, geboten ist. Die Rahmenbedingungen hierfür legt § 96 SGB XI fest, wonach die Daten, die gemeinsam verarbeitet und genutzt werden sollen, abschließend unter meiner Beteiligung und der des BMA festzulegen sind.

Eine Festlegung der in diesem Zusammenhang erforderlichen Daten hat sich als schwierig erwiesen. Dies liegt zum einen daran, daß die Kassen unterschiedliche Programme und Systeme zur Datenverarbeitung einsetzen und hieraus unterschiedliche Bezeichnungen für ein und denselben Sachverhalt resultieren, wie z. B. „Lohnstufe" und „Lohneinstufung". Zum anderen werden Daten erhoben, wie etwa für die Beitragsbemessung freiwilliger Mitglieder, deren Einzelheiten sich aus der Satzung der jeweiligen Kasse ergeben und die gegebenenfalls durch die Rechtsprechung konkretisiert sind bzw. werden, so daß eine verbindliche Festlegung – z. B. „Berücksichtigung von Mieteinnahmen" – als ein äußerst schwieriger Weg erscheint.

Die Diskussion über den Datenkatalog muß jedoch fortgeführt werden. Ich werde dabei – im Rahmen meiner im SGB XI festgelegten Aufgaben – auf eine weitestmögliche Präzisierung hinwirken.

24.2 Gestaltung des Formulars „Nachweis über einen Pflegeeinsatz nach § 37 Abs. 3 Satz 5 SGB XI"

Das Sozialgesetzbuch XI – Soziale Pflegeversicherung – sieht in § 37 vor, daß Pflegebedürftige anstelle der häuslichen Pflegehilfe ein Pflegegeld beantragen können. Dieser Anspruch setzt voraus, daß der Pflegebedürftige mit dem Pflegegeld seine erforderliche Grundpflege und hauswirtschaftliche Versorgung durch eine Pflegeperson in geeigneter Weise selbst sicherstellt. Damit bei Bezug von Pflegegeld die Qualität der häuslichen Pflege gesichert bleibt, Defizite frühzeitig erkannt und ihnen entgegengewirkt werden kann, sind die Pflegebedürftigen verpflichtet, in regelmäßigen Abständen einen Pflichteinsatz durch die Pflegeeinrichtung abzurufen, mit der die Pflegekasse einen Versorgungsvertrag geschlossen hat.

Um eine datenschutzgerechte Verfahrensweise zu gewährleisten, sieht das Erste SGB XI-Änderungsgesetz vor, daß eine Mitteilung der bei dem Pflichteinsatz gewonnenen Erkenntnisse nur mit Einverständnis des Pflegebedürftigen an die Pflegekasse zulässig ist und daß er eine Durchschrift der Mitteilung erhält.

Das für die Mitteilung notwendige Formular ist unter Beteiligung des BMA und meines Hauses zu erstellen (§ 106 Abs. 1 Satz 2 SGB XI). Im Rahmen meiner Beteiligung habe ich insbesondere auf das Erfordernis einer eigenhändigen Unterschrift des Pflegebedürftigen hingewiesen und darauf hingewirkt, daß der Versicherte nach § 67a Abs. 3 SGB X über seine Rechtsposition, insbesondere den Zweck der Datenerhebung und auf die Folgen einer evtl. Verweigerung der Auskunft, informiert wird.

24.3 Pflegerichtlinien weiterhin erörterungsbedürftig

Die Pflegebedürftigkeitsrichtlinien vom 7. November 1994 in der geänderten Fassung vom 21. Dezember 1995 bestimmen die Merkmale der Pflegebedürftigkeit und der Pflegestufen sowie das Verfahren zu deren Feststellung.

Problematisch erscheint mir dabei der mehrseitige Vordruck für ein Gutachten (ein Auszug ist als Abbildung 12 wiedergegeben), das vom Medizinischen Dienst ausgefüllt und an die Pflegekassen übermittelt wird.

Nach § 18 Abs. 5 Satz 1 SGB XI hat der Medizinische Dienst der Pflegekasse das Ergebnis seiner Prüfung mitzuteilen und Maßnahmen zur Rehabilitation, die Art und den Umfang von Pflegeleistungen sowie einen individuellen Pflegeplan zu empfehlen.

Gegenüber dem BMA und den Spitzenverbänden der gesetzlichen Pflegekassen habe ich die Frage des zulässigen Umfangs der Mitteilung des Ergebnisses aufgeworfen. Von diesen Stellen wird hierzu insbesondere die Gesetzesbegründung angeführt und darauf verwiesen, daß die Pflegekassen in der Lage sein müssen, die gesamte Begutachtung durch den Medizinischen Dienst auf seine Rechtmäßigkeit prüfen zu können. Daneben seien die Informationen auch deshalb für die Pflegekasse erforderlich, um eine Änderung der Pflegestufe zu beurteilen und die Versorgung mit Pflegehilfsmitteln umfassend und bedarfsgerecht regeln zu können sowie den Versicherten ggf. auf eine mögliche Verbesserung der Pflegeumstände, z. B. einer Wohnumfeldverbesserung, hinweisen zu können.

Nach meiner Auffassung erscheint die Zulässigkeit der Übermittlung des gesamten Gutachtens im Hinblick auf die Aufgabenverteilung zwischen Medizinischem Dienst und Pflegekasse zweifelhaft. Hierfür spricht auch der Vergleich von § 18 Abs. 5 SGB XI mit § 277 Abs. 1 Satz 1 SGB V. Nach dieser Vorschrift erhält die Krankenkasse das „Ergebnis der Begutachtung" und „die erforderlichen Angaben über den Befund". Nach § 18 Abs. 5 SGB XI erhält die Pflegekasse vom MDK dagegen lediglich „das Ergebnis seiner Prüfung". Es ist daher notwendig, bei der Begutachtung durch den MDK das „Ergebnis" und den „Befund" zu trennen.

Abbildung 12

Gutachten zur Feststellung der Pflegebedürftigkeit gemäß SGB XI

Medizinischer Dienst der Krankenversicherung

MDK-Beratungsstelle Gutachten vom:

Versicherter: Geb.Datum:

4.3.3	**Für Sicherheit sorgen können**	☐ selbständig	☐ bedingt selbständig	teilweise unselbständig	☐ unselbständig
4.3.4	**Sich bewegen können**	☐ selbständig	☐ bedingt selbständig	☐ teilweise unselbständig	☐ unselbständig
4.3.5	**Sich sauberhalten und kleiden können**	☐ selbständig	☐ bedingt selbständig	☐ teilweise unselbständig	☐ unselbständig
4.3.6	**Essen und trinken können**	☐ selbständig	☐ bedingt selbständig	☐ teilweise unselbständig	☐ unselbständig
4.3.7	**Ausscheiden können**	☐ selbständig	☐ bedingt selbständig	☐ teilweise unselbständig	☐ unselbständig
4.3.8	**Sich beschäftigen können**	☐ selbständig	☐ bedingt selbständig	☐ teilweise unselbständig	☐ unselbständig
4.3.9	**Kommunizieren können**	☐ selbständig	☐ bedingt selbständig	☐ teilweise unselbständig	☐ unselbständig
4.3.10	**Ruhen und schlafen können**	☐ selbständig	☐ bedingt selbständig	☐ teilweise unselbständig	☐ unselbständig

ambulante Pflege

vollstationäre Pflege

Die Gutachten sind in der Regel so detailliert und minutiös, daß sie weit über die für die Pflegekassen erforderlichen Informationen hinausgehen. Es ist sicherlich schwierig, den Umfang des Gutachtens festzulegen, zumal nach meinem Verständnis die Untersuchung nicht von vornherein auf ein Krankheitsbild festgelegt ist, sondern vielmehr bei gleichem Krankheitsbild sich individuell unterschiedliche Pflegeleistungen als notwendig herausstellen können. Gleichwohl halte ich eine weitere Diskussion zu diesem wichtigen Thema für zwingend.

24.4 Führung von Pflegetagebüchern

Pflegetagebücher werden nach Auskunft einer Kasse längstens für sieben Tage in den Fällen eingesetzt, in denen die Einstufung des Pflegebedürftigen streitig ist bzw. der Gutachter bei der Beurteilung der Pflegebedürftigkeit unterstützt werden soll. Ein Auszug, der den Zeitraum von einem Tag betrifft, ist als Abbildung 13 wiedergegeben.

Die Pflegetagebücher sind aus datenschutzrechtlicher Sicht problematisch:

- Als Rechtsgrundlage für die Datenerhebung durch die Pflegekasse kann § 94 Abs. 1 Nr. 3 SGB XI in Betracht kommen. Die Angaben im Pflegetagebuch sind jedoch zumindest teilweise mit denjenigen identisch, die gem. § 18 SGB XI durch den Medizinischen Dienst bzw. gem. § 37 SGB XI durch die Pflegedienste erhoben werden. Eine Folge können unzulässige Mehrfacherhebungen bzw. -übermittlungen sein.
- Das Pflegetagebuch enthält keinen Hinweis auf die Rechtsgrundlage bzw. den Zweck der Datenerhebung gem. § 67 a Abs. 3 SGB X.
- Es ist weder eine Unterschrift des Pflegebedürftigen noch der Pflegeperson, die das Pflegetagebuch führt, vorgesehen. Damit kann im Ergebnis unklar sein, über welche Person das Pflegetagebuch geführt wird und von wem die Angaben herrühren.

Die Erörterungen im Hinblick auf die mit dem Pflegetagebuch verbundenen Fragen dauern noch an.

25 Gesundheitswesen

25.1 Ärztliche Schweigepflicht gegen Wissenschaft und Fortschritt ?

Mit der Novellierung des BDSG im Jahre 1990 wurden auch die Voraussetzungen zur Übermittlung personenbezogener Daten für Forschungszwecke derart erweitert, daß in vielen praktischen Fällen ein angemessener Ausgleich zwischen den Forschungsinteressen und den Interessen der Betroffenen am Schutz ihrer Daten möglich ist. Das Finden akzeptabler Lösungen wird zusätzlich dadurch erleichtert, daß in § 40 Abs. 1 BDSG für die Verarbeitung und Nutzung personenbezogener Daten durch Forschungseinrichtungen eine sehr enge Zweckbindung vorgeschrieben ist, was den Interessen der Betroffenen Rechnung trägt.

Wenn trotzdem gelegentlich aus Kreisen der Wissenschaft herbe Kritik an angeblich forschungsfeindlichen Datenschutzvorschriften geübt wird, so liegt das zu einem gewissen Teil an einer Überbewertung der Mitwirkungspflichten und Unterstützungsmöglichkeiten der Stellen, die Daten für ein Forschungsvorhaben liefern sollen. Im Konflikt mit den Forschern benutzen diese Stellen dann manchmal „Datenschutz" als Argument dafür, daß sie die gewünschten Daten nicht liefern. Ein wesentliches und derzeit kaum zu beseitigendes Forschungshindernis, das sich besonders bei medizinischen Forschungsvorhaben auswirkt, liegt darin, daß die im BDSG enthaltenen Übermittlungsbefugnisse u. a. auch die Berufsgeheimnisse unberührt lassen, die nicht auf gesetzlichen Vorschriften beruhen (§ 1 Abs. 4 Satz 2 BDSG). Einschlägig ist hier das ärztliche Berufsrecht. Dort heißt es in § 3 Abs. 7 der Musterberufsordnung für die deutschen Ärzte zur Schweigepflicht: *„Zum Zwecke der wissenschaftlichen Forschung und Lehre dürfen der Schweigepflicht unterliegende Tatsachen grundsätzlich nur soweit mitgeteilt werden, als dabei die Anonymität des Patienten gesichert ist oder dieser ausdrücklich zustimmt."* Damit wird die lange und gute ärztliche Tradition fortgesetzt, in erster Linie dem Patienten und seinen Interessen zu dienen. Der Zugang der medizinischen Forschung, etwa zu epidemiologischen Daten, ist aber nur schwer möglich, weil die Dokumentation von Patientendaten in der Regel personenbezogen erfolgt und nur mit viel Aufwand anonymisierte Auszüge erstellt werden können.

Mit dem zunehmenden Einsatz von automatisierten Verfahren zur medizinischen Dokumentation wird dieses Forschungshindernis zwar etwas abgebaut werden. Denn damit wird es erleichtert, aus einer patientenorientierten Dokumentation anonymisierte Auswertungen zu erstellen. Das wirkt sich aber nicht auf jene Forschungsvorhaben aus, bei denen zu den medizinischen Daten andere Angaben über die Patienten aus anderen Quellen hinzugefügt werden sollen, um den Zusammenhang mit Umwelteinflüssen oder den langfristigen Erfolg einer Behandlung, beispielsweise im Rahmen der Qualitätssicherung, zu untersuchen. Hier wird – ohne daß der Forscher ein Interesse an der Identifizierung des Patienten hat – der Personenbezug benötigt, um die Daten eines Falles zusammenzuführen. Erst wenn das erfolgt ist, wird eine Anonymisierung möglich. Zwar läge eine Lösung darin, die Einwilligung der Betroffenen einzuholen. Dies ist aber oft mit erheblichem Aufwand verbunden und dadurch erschwert, daß die Daten zwar nicht anonymisiert, die Betroffenen aber nur mit großer Mühe oder überhaupt nicht gefunden werden können.

Gleichwohl trifft eine Lockerung der ärztlichen Schweigepflicht zu Recht auf Bedenken. Denn mit der Weitergabe an eine Forschungseinrichtung erhält nicht nur eine weitere Stelle Kenntnis von diesen Daten. Sie sind dort auch rechtlich schwächer geschützt als beim Arzt oder im Gewahrsam einer Krankenanstalt. Das Zeugnisverweigerungsrecht der Strafprozeßordnung erstreckt sich für Ärzte nur auf *„das, was ihnen in dieser Eigenschaft anvertraut worden*

Abbildung 13

Samstag, den 31.08.96

Zeit/min	Morgendliche Hilfen; zum Beispiel beim Aufstehen, Toilettengang, Waschen, Ankleiden und Frühstück
	31.08.96
____	Noch im Bett liegend, Strümpfe u. Schuhe anziehen - aufnehmen
____	aus dem Bett - in Toilettenstuhl setzen, zur Toilette fahren. Gr. Urinbeutel abklemmen, entleeren, reinigen. Unten frei
40	machen u. auf Toilettenschüssel zum 1. Stuhlgang setzen. Zurück a.d.
____	Toilettenstuhl, zuvor Unterkleidung (Vorlage usw.) wieder
____	anziehen - an Waschtisch zur kleinen Morgentoilette (Gesicht,
____	Hände, Zähne, Haare) Morgenrock anziehen - in Rollstuhl
____	umsetzen, Urinbeutel verwahren - zum Frühstück rollen. Schürze anziehen.
30	Frühstück zubereiten u. verabreichen, Milchzucker i/Saft, Tabletten richten und eingeben.
	Begleitung, zum Beispiel zum Logopäden, Krankengymnast und zur Frühförderungsstelle zur Förderung des Erlernens der Verrichtungen des täglichen Lebens
20	Nach dem Frühstück 2. Gang zur Toilette, umsetzen
____	freimachen und anschließend wieder ordnen. Mit Mineralwasser versorgen.
40	Einkaufen, Hausarbeit
45	Große Körperpflege und ankleiden durch Pflegepersonal der DRK-Sozialstation
	Hilfe und pflegeunterstützende Leistungen im Laufe des Tages, zum Beispiel beim Umkleiden, Mittagessen, Toilettengang, Abklopfen von lungenkranken Kindern
40	Mittagessen zubereiten, servieren, die Mahlzeit in
____	mundgerechten Portionen auf einen Suppenlöffel häufen - heute zum Nachtisch Trauben: die Beeren vom Stengel pflücken u. auf einem kleinen Teller vorlegen.

Auszug aus einem Pflegetagebuch

noch Abbildung 13

20	Nach dem Essen auf der Toilette den Urinbeutel (am Knie mittels Netzstrumpf befestigt) entleeren, Auffanggefäß ausschütten und reinigen - Tabletten -
	Oberkleidung, Hose u. Schuhe ausziehen, zur Mittagsruhe ins Bett legen.
	anschl. Hausarbeit, Geschirr usw.
	Beschreibung von Anleitung und Beaufsichtigung bei der selbständigen Durchführung der täglichen Verrichtung durch den behinderten Menschen, wenn ihm die Fähigkeit fehlt, die Notwendigkeit der täglichen Verrichtung zu erkennen und in sinnvolles Handeln umzusetzen
20	Nach der Mittagsruhe - ca. 2 Stunden - aus dem Bett aufnehmen ankleiden - in den Rollstuhl setzen - a.d. Toilette
	Urinbeutel entleeren wie gehabt - frisieren.
20	Nachm-Kaffee zubereiten u. verabreichen danach Selbstbeschäftigung (Zeitschriften, Fernsehen)
	Hilfe- und Pflegeleistungen am Abend, zum Beispiel beim Abendessen, Auskleiden, Waschen, zu Bett bringen
30	Zubereitung des Abendessens u. verabreichen -
	Ohrspeicheldrüse li. ausdrücken - Tabletten
30	Auskleiden, Urinbeutel anschließen, Abendtoilette, zu Bett bringen durch Pflegerin des DRK
10	Wäschewechsel vorbereiten, neue Unterwäsche hinrichten
	Hilfe und Pflegeleistungen in der Nacht, zum Beipiel Beaufsichtigung, Beruhigen bei Erregungszuständen, Umbetten, Toilettengang, Wickeln
15	21.30 Uhr: 1. Umbetten, Mineralwasser reichen
15	01.30 Uhr: 2. Umbetten, Mineralwasser reichen
5	04.30 Uhr: Mineralwasser reichen
	insgesamt 3 bis 4 Flaschen pro Tag
380	gesamt

Auszug aus einem Pflegetagebuch

oder bekanntgeworden ist" (§ 53 Abs. 1 Nr. 3 StPO), und beschlagnahmefrei sind nur die Unterlagen *„im Gewahrsam der zur Verweigerung des Zeugnisses Berechtigten"* (§ 97 Abs. 2 StPO). Diese Schwäche könnte durch ein medizinisches Forschungsgeheimnis, das Patientendaten in einer Forschungseinrichtung so schützt „wie beim Arzt", beseitigt werden. Das könnte die Einwilligung der Patienten in die Nutzung ihrer Daten für Forschungszwecke zwar nicht generell ersetzen. Es würde aber eine Lockerung der sehr engen standesrechtlichen Regelung ermöglichen und darüber hinaus den Patienten auch die Einwilligung in den Fällen erleichtern, in denen sie nach wie vor erforderlich wäre.

Auch außerhalb der wissenschaftlichen Forschung gibt es dringenden Bedarf, Patientendaten so zu schützen, wie sie beim Arzt geschützt werden. So ist etwa im Zuge der fortschreitenden Automatisierung der Dokumentation damit zu rechnen, daß hierauf spezialisierte Unternehmen bestimmte Dokumentationsaufgaben besser und billiger erfüllen können, als dies von Krankenhäusern geleistet werden kann. Eine im Prinzip mögliche Übertragung dieser Aufgaben auf spezialisierte Unternehmen ist aber nicht zu verantworten, wenn damit zugleich der Schutz dieser Daten geschwächt würde. Ähnliche Probleme sind beim Einsatz von Chipkarten für Gesundheitsdaten (s. o. Nr. 9.2.4) und bei professioneller Unterstützung der ärztlichen Tätigkeit durch Multimedia-Netze zu lösen.

Kostensparende und deshalb sinnvolle Arbeitsteilung ist aber nicht nur eine Folgeerscheinung der modernen Informationstechnik. Auch im eher natürlichen Bereich der Ernährung bieten Unternehmen Leistungen für Krankenhäuser an. Wer für Patienten je nach medizinischer Anforderung unterschiedliches Essen zubereitet, portioniert und verteilt, der erfährt zwangsläufig einiges über „seine" Patienten, und deshalb sollte auch er deren Geheimnisse so wahren, wie die Ärzte und die anderen Mitarbeiter im Krankenhaus.

Diese Gründe legen es nahe, den traditionellen Schutz der Gesundheitsdaten auf diejenigen Bereiche auszudehnen, in denen diese Daten im Interesse der Patienten oder im Interesse der Allgemeinheit sinnvollerweise genutzt werden.

25.2 Transplantationsgesetz

Die insgesamt gute Zusammenarbeit mit dem BMG hat sich auch bei den Datenschutzregelungen des Entwurfs eines Gesetzes über die Spende, Entnahme und Übertragung von Organen (Transplantationsgesetz – TPG) bewährt. Der Entwurf wurde von den Fraktionen der CDU/CSU, SPD und FDP eingebracht (BT-Drucksache 13/4355), wobei das BMG die Fraktionen u. a. bei der Formulierung der Organisations- und Datenverarbeitungsvorschriften beraten hatte.

Ohne Zweifel stand und steht im Vordergrund der politischen Diskussion die Frage, unter welchen Bedingungen eine Transplantation erfolgen darf. Die Gewährleistung des Datenschutzes auf hohem Niveau wird aber vermutlich auf die Akzeptanz jeder Lösung einen gewissen Einfluß haben. So muß z. B. gesichert sein, daß schon die Existenz der in einem Organspenderegister hinterlegten Erklärungen über die Bereitschaft zur Organspende erst nach dem Tod des Betroffenen den zur Anfrage berechtigten Ärzten bekannt wird. Denn sonst könnte befürchtet werden, daß diese Erklärung vielleicht einen Einfluß auf die ärztliche Entscheidung hat. Dazu enthält der Entwurf sachgerechte und eindeutige Vorgaben für eine dieses näher regelnde Rechtsverordnung. Im Zusammenhang mit den Ergebnissen einer öffentlichen Anhörung hat das BMG eine ergänzende Formulierungshilfe erarbeitet, in der zur Sicherheit die Protokollierung aller Abrufe aus diesem Register festgelegt wird.

Die strikte Bindung einer Organentnahme an die Zustimmung des Betroffenen sichert am besten dessen Recht auf Selbstbestimmung in dieser wichtigen Frage (s. dazu auch die Entschließung der 51. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum Transplantationsgesetz, **Anlage 17**). Diskutiert wird aber auch eine erweiterte Zustimmungslösung, bei der dann, wenn keine Erklärung des Betroffenen vorliegt, die nächsten Angehörigen befragt werden sollen. Falls diese Erweiterung der Zustimmungslösung beschlossen wird, müssen die nächsten Angehörigen eines Verstorbenen, der für eine Organentnahme in Betracht kommt, dem Arzt benannt werden, der sie dazu befragen möchte. Nachdem ernsthafte Zweifel daran entstanden waren, ob die derzeitige Rechtslage das zuläßt, hat das BMG eine Formulierungshilfe für eine angemessene Lösung dieses Problems erarbeitet. Danach sollen u. a. die Ärzte, die einen Verstorbenen vor seinem Tode behandelt haben, einem Arzt, der bei dem Verstorbenen eine Organentnahme beabsichtigt, die entsprechenden Auskünfte erteilen und auch mitteilen, ob medizinische Gründe einer Transplantation entgegenstehen.

Die guten Erfahrungen aus den Beratungen mit dem BMG zu diesen und einigen weiteren datenschutzrechtlichen Details des Gesetzentwurfs lassen erwarten, daß – unabhängig vom Ergebnis der Diskussion der schwierigen ethischen Fragen der Organtransplantation – für die erforderliche Verarbeitung personenbezogener Daten datenschutzgerechte Regelungen gefunden werden.

26 Verteidigung

26.1 Beratung und Kontrolle der Teilstreitkräfte der Bundeswehr

Wegen der mir aus dem Einigungsvertrag erwachsenen Beratungs- und Kontrollaufgaben im Hinblick auf die datenschutzgerechte Behandlung von Personalunterlagen der ehemaligen Nationalen Volksarmee der DDR (NVA) und aufgrund vermehrter Eingaben aus dem Kreis ungedienter Wehrpflichtiger habe ich in den letzten Jahren die Wehrbereichsverwaltungen und Kreiswehrersatzämter öfters beraten und kontrolliert als die militärischen Dienststellen der Bundeswehr.

Seit 1995 kontrolliere ich wieder verstärkt militärische Dienststellen der drei Teilstreitkräfte. Neben drei Heereseinheiten habe ich zwei Marineeinheiten beraten und kontrolliert.

Die bisher gewonnenen Erfahrungen haben gezeigt, daß bei der Bundeswehr im Rahmen eines ausgeprägten militärischen Sicherheitsbewußtseins auch dem Datenschutz die erforderliche Achtung zuteil wird. So habe ich nur wenige Mängel beim Umgang mit personenbezogenen Daten von Soldaten vorgefunden.

26.2 Konsequente Löschung von Eintragungen in Disziplinarbüchern

Anläßlich einer Kontrolle bei einer Heereseinheit der Bundeswehr wurde ich auf ein Problem beim Führen der Disziplinarbücher aufmerksam gemacht. Für jeden Soldaten ist nach § 12 Wehrdisziplinarordnung (WDO) ein sogenanntes Disziplinarbuch zu führen, in das förmliche Anerkennungen sowie einfache und gerichtliche Disziplinarmaßnahmen und strafgerichtliche Strafen einzutragen sind. Einrichtung und Führung der Disziplinarbücher regelt eine Verwaltungsvorschrift. In Nummer 1 Abs. 2 dieser Vorschrift wird als Zweck dieser Bücher genannt:

„Das Disziplinarbuch soll den höheren Disziplinarvorgesetzten die Dienstaufsicht über die Ausübung der Disziplinargewalt erleichtern. Es dient gleichzeitig als Grundlage für die Tilgung von einfachen Disziplinarmaßnahmen und Gehaltskürzungen."

Aus der Art und Weise, wie die Disziplinarbücher geführt werden, kann der Disziplinarvorgesetzte auch nach erfolgter Tilgung einer Disziplinarmaßnahme erkennen, daß – mit großer Wahrscheinlichkeit – eine solche verhängt worden war. Das für den Betroffenen nachteilige Datum „Disziplinarmaßnahme" ist insofern trotz Beseitigung der Eintragung nicht vollständig „aus der Welt". Dies widerspricht dem Rehabilitationsgedanken der Tilgungsregelung des § 13 WDO, die einen Soldaten so stellt, als wäre niemals eine Disziplinarmaßnahme gegen ihn verhängt worden.

Das Disziplinarbuch besteht aus drei Teilen. Meine Bedenken richten sich gegen den ersten Teil, der in der Art eines Karteiblattes im Format DIN A 4 geführt wird. Das Blatt enthält auf der Vorderseite neben den Angaben von Namen, Rufnamen und Dienstgrad einige Daten über den Werdegang des Soldaten sowie Eintragungen über erteilte förmliche Anerkennungen. Auf der Rückseite des Blattes werden die Disziplinarmaßnahmen und die gerichtlichen Strafen eingetragen. Zu allen Maßnahmen wird auch das Datum der Erteilung oder Verhängung vermerkt. Abschließend werden die Einträge vom Disziplinarvorgesetzten mit Unterschrift, Dienstgrad und Datum bestätigt.

Sind Disziplinarmaßnahmen nach Ablauf der jeweiligen Frist zu tilgen, hat dies zur Folge, daß auch ein neues Karteiblatt angelegt wird. Eintragungen, die nicht zu löschen sind, wie z. B. förmliche Anerkennungen, werden wieder aufgenommen und vom Disziplinarvorgesetzten erneut mit Unterschrift, Dienstgrad und Datum dokumentiert. Aus der zeitlichen Differenz zwischen dem Datum der Erteilung der förmlichen Anerkennung und dem Datum der erneuten Dokumentation durch den Disziplinarvorgesetzten kann ein kundiger Leser schließen, daß ein neues Karteiblatt – bedingt durch die Tilgung einer Disziplinarmaßnahme – angelegt worden ist.

Ich habe dem Bundesministerium der Verteidigung deshalb empfohlen, durch eine Änderung des Verfahrens bei der Einrichtung und Führung der Disziplinarbücher dem Rehabilitationsgedanken künftig uneingeschränkt Rechnung zu tragen. Die Diskussion dauert noch an.

26.3 Im Interesse der Wehrpflichtigen mehr Daten an Musterungsärzte

Bei meiner Kontrolltätigkeit stoße ich häufig auf Fälle, in denen mehr Daten erhoben und verarbeitet werden, als für die Aufgabenerfüllung erforderlich sind. Sehr selten kommt es dagegen vor, daß einer Stelle – aus falsch verstandenem Bemühen um Datenschutz – personenbezogene Daten vorenthalten werden, die sie für eine sachgerechte Erfüllung ihrer Aufgaben benötigt. Ein solcher außergewöhnlicher Fall wurde mir durch die Kontrolle des Musterungsverfahrens in einem Kreiswehrersatzamt bekannt.

Das Musterungsverfahren beginnt regelmäßig mit der sogenannten Personalaufnahme, in der der Wehrpflichtige alle Angaben macht, die für die Durchführung der Musterung erforderlich sind. Diese mittels Vordrucks erhobenen Daten und die bereits im Schriftverkehr mit dem Kreiswehrersatzamt entstandenen Unterlagen werden in einer Personalakte zusammengefaßt. Vor Weitergabe dieser Akte an den Musterungsarzt werden alle Unterlagen und Anträge entnommen, die nach Meinung des Sachbearbeiters für die Führung der Personalunterlagen der Wehrpflichtigen keine gesundheitsrelevanten Angaben über den Wehrpflichtigen enthalten. Diese Unterlagen werden direkt an den Musterungsbeamten weitergeleitet, der nach der ärztlichen Untersuchung dem Wehrpflichtigen das Musterungsergebnis bekanntgibt.

Nach Auffassung der Hauptmusterungsärztin des kontrollierten Kreiswehrersatzamtes können aber die aus der Personalakte entfernten Unterlagen für das Ergebnis der ärztlichen Untersuchung von großer Bedeutung sein. So etwa bei einer aktenkundigen Terminverschiebung der Musterung wegen des Todes eines nahen Angehörigen des Wehrpflichtigen, die Rückschlüsse auf die psychische Konstitution des Wehrpflichtigen zulassen kann.

Ich habe die Argumentation der Musterungsärztin gegenüber dem Bundesministerium der Verteidigung aufgegriffen und darauf hingewiesen, daß der Sachbearbeiter mit der Beantwortung der Frage, ob Unterlagen für die Aufgabenerfüllung der Musterungsärzte von Bedeutung sein können und deshalb in der Personalakte verbleiben müßten, in der Regel überfordert sein dürfte.

Im Interesse der Wehrpflichtigen an einem Musterungsergebnis, das auch ihren Gesundheitsbelastun-

gen aufgrund persönlicher Lebensumstände in vollem Umfange Rechnung trägt, habe ich dem BMVg empfohlen, die bisherige Regelung, die den Musterungsärzten den Zugang zu den vollständigen Personalakten der Wehrpflichtigen verwehrt, zu überprüfen.

Das BMVg hat das Verfahren inzwischen entsprechend meinem Vorschlag geändert.

26.4 Unzulässiges Fotografieren von Demonstranten vor Kaserne

Wenig Gespür für die Persönlichkeitsrechte von Bürgern ließ ein Kasernenkommandant erkennen, als er befahl, Teilnehmer einer Mahnwache vor seiner Kaserne zu fotografieren. Bei den Demonstranten handelte es sich um Bürger, die sich für die Erhaltung des Bundeswehrstandortes in ihrem Ort einsetzten.

Ein kurzer Blick in das Bundesdatenschutzgesetz hätte den Kasernenkommandanten darüber informiert, daß das Erheben personenbezogener Daten, d. h. das Fotografieren, nur zulässig ist, wenn seine Aufgaben dies erfordern. Es gehört aber nicht zu den Aufgaben eines Kasernenkommandanten festzuhalten, welche Bürger außerhalb des Kasernenbereichs von ihrem Grundrecht auf Versammlungsfreiheit Gebrauch machen.

Einige Betroffene haben sich an mich und an das Bundesministerium der Verteidigung gewandt, um sich über das Verhalten des Kasernenkommandanten zu beschweren. Das Bundesministerium der Verteidigung, das meine Rechtsauffassung teilt, reagierte sofort und sagte zu, die Fotografien und die zugehörigen Negative nach Abschluß des inzwischen vor dem Wehrdienstsenat des Bundesverwaltungsgerichts laufenden gerichtlichen Verfahrens gegen den Kasernenkommandanten zu vernichten.

27 Zivildienst

– Entwurf einer Verordnung über die Führung der Personalakten im Zivildienst –

Mit § 36 Zivildienstgesetz (ZDG) wurde eine bereichsspezifische Regelung für den Umgang mit den Personalakten von Zivildienstpflichtigen und Zivildienstleistenden geschaffen. Zu einem datenschutzrechtlich bedeutsamen Aspekt dieser Vorschrift, nämlich der Übermittlung von Diagnosedaten erkrankter Zivildienstleistender, habe ich mich bereits im 14. Tätigkeitsbericht geäußert (s. 14. TB Nr. 16.1).

Die Vorschrift enthält für das BMFSFJ die Ermächtigung, Einzelheiten des Umgangs mit den Personalakten durch Rechtsverordnung zu regeln. Eine solche liegt nunmehr im Entwurf vor. Im Beratungsverfahren hatte ich Gelegenheit, meine Vorstellungen gegenüber dem BMFSFJ darzulegen. Es gelang mir dabei, eine Reihe von datenschutzrechtlichen Verbesserungen zu erzielen, beispielsweise daß für bestimmte Übermittlungen von personenbezogenen Daten die Einwilligung des Zivildienstleistenden einzuholen ist. Meine im 14. TB geäußerten Bedenken gegen eine generelle Übermittlung von Diagnosedaten auch in Fällen kurzfristiger Erkrankung habe ich im Hinblick auf die Notwendigkeit einer angemessenen medizinischen Betreuung der Zivildienstleistenden aufgegeben.

Änderungsbedarf sehe ich noch zu § 3 Abs. 2 Satz 4 des Verordnungsentwurfs. Dort ist vorgesehen, daß im Falle eines Rechtsstreits, bei dem die Tauglichkeitsakte beigezogen werden muß, auch das Prozeßreferat des Bundesamtes für den Zivildienst (BAZ) diese Akte einsehen darf. Diese Regelung widerspricht der insoweit eindeutigen Bestimmung des § 36 Abs. 1 Satz 3 ZDG, wonach Zugang zu den ärztlichen Unterlagen **nur** der ärztliche Dienst und das für die Heilfürsorge zuständige Referat des BAZ haben. In meiner Stellungnahme zum Verordnungsentwurf habe ich darauf hingewiesen, daß dem berechtigten Interesse des Prozeßreferates an der Kenntnis der für die Führung von Verwaltungsprozessen erforderlichen Informationen durch Gutachten oder Zeugenaussagen des ärztlichen Dienstes entsprochen werden kann. Eine Einsichtnahme in die Tauglichkeitsakte selbst ist insofern nicht erforderlich.

Ich werde die Angelegenheit beratend weiterverfolgen und gemeinsam mit dem BMFSFJ nach einer Lösung suchen, die sowohl dem Schutz besonders sensibler Daten der Zivildienstpflichtigen als auch dem berechtigten Interesse des Prozeßreferates Rechnung trägt.

28 Verkehrswesen

28.1 Autobahnmaut – abgeschlossener Feldversuch

In meinem 15. TB (Nr. 18.1) habe ich über den unter der Verantwortung des BMV durchgeführten Feldversuch berichtet und darauf hingewiesen, daß eine europäisch abgestimmte Lösung gefunden werden muß, die schon von vornherein datenschutzgerechte Vorgaben erfüllt. Dies wurde durch die Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder im März 1995 **(s. Anlage 10)** bekräftigt. Zur näheren Erläuterung der Entschließung habe ich dem BMV eine Zusammenstellung der Anforderungen übermittelt, die an die technische Gestaltung von Systemen für eine automatische Gebührenerhebung zu stellen sind **(s. Anlage 25)**. Diese Zusammenstellung beruhte auf dem Ergebnis der mit allen Beteiligten (BMV, die den Versuch durchführende Arbeitsgemeinschaft, Anbieter der Systeme) sehr kooperativ geführten Diskussionen.

Nach Abschluß des Feldversuchs stellte Bundesminister Wissmann im November 1995 die Ergebnisse und die daraus gewonnenen Schlußfolgerungen vor. Aus meiner Sicht sind folgende Erkenntnisse hervorzuheben:

- Im Feldversuch wurden weltweit zum ersten Mal Systeme zur Automatischen Gebührenerhebung (AGE) unter Bedingungen betrieben, wie sie für Autobahnen in Deutschland typisch sind. Die zehn am Feldversuch beteiligten AGE-Systeme internationaler Hersteller umfaßten alle heute bekannten

Grundtechnologien für eine automatische Gebührenerhebung, wie Selbstortung des Fahrzeugs durch Aufnahme von Satellitensignalen, Mobilfunk im D-Netz, Lokalkommunikation über Funk oder Mikrowellen, optische Fahrzeugerkennung und -klassifizierung.

- Es wurde nachgewiesen, daß von den untersuchten Systemen mindestens ein Vertreter jeder Grundtechnologie die Teilaufgabe Erhebung lösen und die darin gestellten anwendungsspezifischen Anforderungen erfüllen kann.

- Die Anforderungen an die Kontrolle, wie eindeutige Identifizierung, Trennung von Zahlungs- und Nutzungsdaten und Transparenz der Erhebungs- und Kontrollvorgänge, wurden von keinem System vollständig erfüllt. Ein wesentlicher Grund dafür war, daß entsprechende Anforderungen für diese Anwendungen vor Beginn des Feldversuchs nicht formuliert worden waren und die Notwendigkeit für den Einsatz geeigneter Verfahren – wie z. B. kontinuierliche Dokumentation von fehlerhaften Systemzuständen und manipulationssichere Erhebung, Übermittlung und Verarbeitung der Nutzungsdaten – erst während des Feldversuchs und in der begleitenden Systemanalyse erkannt wurde. Trotz Einführung entsprechender Verfahren bei einer vollautomatischen Kontrolle würde ein Risiko bestehen bleiben, das sich aus dem heute nicht abschätzbaren Verhalten zukünftiger Nutzer und aus den derzeit noch bestehenden Problemen der sicheren Fahrzeugerkennung und der Beweissicherung ergibt.

- Es wurde festgestellt, daß die Anforderungen des Datenschutzes erfüllt werden können, wenn für die Gebührenerhebung ein anonymes Zahlungsverfahren eingesetzt wird, die Vorgänge der Erhebung und Kontrolle für den Nutzer transparent gemacht werden und wenn durch die Kontrolle sichergestellt werden kann, daß kein Zahlungswilliger und kein Nutzer, der nicht gebührenpflichtig ist, als Falsch- oder Nichtzahler registriert wird. Systeme, die keine Speicherung von Abbuchungsdaten für den Zahlungsnachweis im Fahrzeuggerät gestatten, erfüllen nicht diese Anforderungen des Datenschutzes.

- Technische Einrichtungen wie AGE-Systeme können ausfallen, gestört oder durch Fremdeinwirkung beeinträchtigt werden. Damit Fehler der Erhebungs- und Kontrolleinrichtungen nicht zu Lasten der Beteiligten gehen, sind technische und organisatorische Maßnahmen vorzusehen, die einen wirksamen Schutz gegen solche Einwirkungen darstellen. Die grundlegenden Anforderungen an die Datensicherheit können durch die Kriterien Integrität, Verfügbarkeit, Authentisierung, Rücknahmefestigkeit (keine Systemänderung zu Lasten des Datenschutzes) und Zugangskontrolle zusammengefaßt werden. Die Ergebnisse der Analysen haben gezeigt, daß die implementierten Maßnahmen zur Datensicherheit bei den untersuchten Systemen unterschiedlich ausgeprägt waren und die vorstehend genannten Kriterien der Datensicherheit von keinem System voll erfüllt wurden.

- Die Ergebnisse des Feldversuchs haben aus technischer Sicht keine eindeutige Präferenz für eine Systementscheidung zugunsten eines Systems oder einer Technologie ergeben. Aus diesem Grunde und wegen der noch offenen Anforderungen hinsichtlich der Interoperabilität mit anderen AGE- und Telematik-Anwendungen sollte eine mögliche Technologieentscheidung erst nach Klärung dieser Fragen in einem Wettbewerb der Technologien auf der Basis einer für alle Systeme verbindlichen Wirkvorschrift erfolgen.

Die Probleme mit der Kontrolle automatisierter Verfahren waren entscheidend dafür, die Einführung der Autobahnmaut für Pkw zunächst zurückzustellen. Das schließt nicht aus, daß dieses Verfahren später bei der Erhebung von Autobahnbenutzungsgebühren für Lkw eingesetzt werden könnte, um weitere Erfahrungen mit diesem System zu gewinnen. Denn für Lkw könnten die notwendigen Mautkontrollen auch aus Anlaß der ohnehin häufiger durchgeführten Verkehrskontrollen erfolgen.

Durch die erfreulich kooperative Einbindung meiner Dienststelle und der Landesbeauftragten für den Datenschutz in die Entscheidungsfindung über die Anforderungen, die an die Einführung eines Systems zur automatischen Gebührenerhebung auf Autobahnen zu stellen sind, wurde erneut deutlich, daß der Datenschutz nicht technikfeindlich ist, sondern dazu beitragen kann, fehlerhafte Entscheidungen zu vermeiden, die nicht nur viel Geld kosten, sondern auch über Gebühr in die Freiheitsrechte der Bürger eingreifen können.

28.2 Kraftfahrt-Bundesamt – KBA –

Den Schwerpunkt einer Kontrolle beim KBA bildete eine Diskussion mit den Fachleuten für die Registerführung darüber, ob die geplanten neuen registerrechtlichen Vorschriften (s. u. Nr. 28.3) unter fachlichen Gesichtspunkten erforderlich und umsetzbar sind. Dabei vertrete ich zu den nachstehend aufgeführten Problemen folgende Auffassung:

- Meine Bedenken gegen die Einführung eines **Zentralen Fahrerlaubnisregisters** hatte ich unter anderem unter der Voraussetzung zurückgestellt, daß die örtlichen Fahrerlaubnisregister neben dem zentralen Register nur noch für den Übergangszeitraum bestehen bleiben, der für die technischen Vorkehrungen ohnehin benötigt wird. Der gesetzlich vorgesehene Zeitpunkt für den Wegfall der örtlichen Fahrerlaubnisregister und die Übernahme dieser Funktion durch das Zentrale Fahrerlaubnisregister beim KBA sollte sich aus der Sicht des Bundes an der technischen Umsetzbarkeit durch das KBA orientieren. Sofern die Länder einen längeren Umstellungszeitraum benötigen, müßte dies besonders begründet werden.

- Das KBA muß nach der Übernahme des gesamten Datenbestandes der örtlichen Fahrerlaubnisregister Vorkehrungen für eine ausreichende Notfallvorsorge treffen, damit die Arbeitsfähigkeit der Führerscheinstellen weiterhin gewährleistet ist.

- Bei den Verfahren zur Erteilung von Auskünften, in denen erst die Anfrage im automatisierten Verfahren gestellt und zeitversetzt später die Antwort erteilt wird (z. B. mittels Filetransfer, Telefax oder Datex-P), handelt es sich entsprechend dem technischen Ablauf um **Abrufe im automatisierten Verfahren**. Die für alle automatisierten Abrufverfahren vorgeschriebenen besonderen Sicherungsvorkehrungen (z. B. Feststellung des Abrufgrundes und der verantwortlichen Person) sind daher unter Berücksichtigung der jeweils eingesetzten technischen Verfahren auch für diese Auskunftsarten vorzusehen und entsprechend gesetzlich zu regeln.
- Das KBA erteilte Auskünfte aus dem **Verkehrszentralregister** bisher grundsätzlich als Vollauskunft. Die nur für einen kleinen Bereich praktizierte Teilauskunftsregelung soll – wie ich bereits seit vielen Jahren fordere (vgl. zuletzt 15. TB Nr. 18.2.2) – nunmehr auf sämtliche Auskunftsfälle ausgedehnt werden, in denen eine Teilauskunft genügt. Durch die jetzt vorgesehene Ergänzung der Registerzwecke um den Zweck „Beurteilung der Zuverlässigkeit von Personen" und aufgrund der damit verbundenen Erweiterung der Übermittlungsbefugnisse wird es allerdings schwieriger, diese ansonsten begrüßenswerte Regelung umzusetzen. Konzepte hierzu sind im KBA noch nicht entwickelt worden.

28.3 Neue straßenverkehrsrechtliche Regelungen

Der von der Bundesregierung vorgelegte Gesetzentwurf zur Änderung des Straßenverkehrsgesetzes und anderer Gesetze enthält neben neuen Regeln für die Erfassung, Speicherung und Übermittlung von Daten im und aus dem Verkehrszentralregister (VZR) aus datenschutzrechtlicher Sicht folgende bedeutende Änderungen:

- Errichtung eines Zentralen Fahrerlaubnisregisters,
- Ausweitung der Online-Abrufe,
- Entgeltfreiheit für Selbstauskünfte nach dem BDSG,
- zweckfremde Nutzung von Protokolldaten.

Bei der Erarbeitung des Gesetzentwurfs bin ich umfassend beteiligt worden. Die zahlreichen Gespräche sowie meine Stellungnahmen gegenüber dem BMV, die unter Beteiligung der Landesbeauftragten für den Datenschutz zustande kamen, haben bewirkt, daß mehrere von mir seit Jahren erhobene Forderungen so umgesetzt wurden, daß sie aus datenschutzrechtlicher Sicht gute Lösungen darstellen.

Gegen die Errichtung eines **Zentralen Fahrerlaubnisregisters** hatte ich früher Bedenken erhoben (vgl. 15. TB Nr. 18.3.3). Nachdem das BMV von seinem ursprünglichen Konzept abgewichen ist und im Einvernehmen mit den Ländern nunmehr die örtlichen Fahrerlaubnisregister nach einer Übergangsfrist aufgelöst und gleichwohl die aktuellen Anschriften der Fahrerlaubnisinhaber im zentralen Register nicht gespeichert werden sollen, habe ich gegen die entsprechenden gesetzlichen Regelungen keine grundsätzlichen Bedenken mehr. Obwohl meiner Meinung nach auch andere technische Verfahren einen Informationsaustausch mit den Mitgliedstaaten der Europäischen Union entsprechend der Zweiten EU-Führerscheinrichtlinie 91/439/EWG ermöglicht hätten, habe ich mich den Argumenten, die wegen der Gewährleistung der Richtigkeit und Vollständigkeit der Informationen für eine zentrale Speicherung sprachen, nicht verschlossen. Dies gilt umso mehr, als die Fahrerlaubnisdaten künftig auch im automatisierten Verfahren jederzeit sofort abrufbar sein sollen.

Die gesetzlich vorgesehene Erweiterung der **Online-Abrufe** aus sämtlichen beim KBA geführten Registern – also auch aus dem Verkehrszentralregister – und den örtlichen Registern ermöglicht die konsequente Nutzung der heute kostengünstig verfügbaren Technik. Sie ist datenschutzrechtlich akzeptabel, weil

- die Nutzungszwecke eindeutig definiert sind,
- die Abrufmöglichkeiten aus dem Ausland sich auf die Mitgliedstaaten der Europäischen Union und die anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum beschränken,
- der Umfang der Abrufe durch ausländische Stellen aus dem VZR auf die negativen Fahrerlaubnisdaten, wie z. B. Versagung, Entziehung, Widerruf, beschränkt wird,
- die Abrufmöglichkeit nur geschaffen wird, wenn der Empfängerstaat die EU-Datenschutzrichtlinie vom 24. Oktober 1995 anwendet, und
- sowohl bei Abrufen aus den örtlichen als auch aus den zentralen Registern unter bestimmten Voraussetzungen eine Zusatzprotokollierung hinsichtlich des Abrufzwecks und der hierfür verantwortlichen Person erfolgt.

Aufgrund meiner beharrlichen Mahnungen (vgl. zuletzt 15. TB Nr. 18.3.1), Eigenauskünfte aus dem VZR entsprechend der Regelung des BDSG entgeltfrei zu erteilen, sieht der Gesetzentwurf nunmehr die **Entgeltfreiheit** für die Auskunft an die Betroffenen bei allen Registern vor.

In meinem 15. TB (Nr. 18.3.2) hatte ich darauf hingewiesen, daß eine Öffnung der engen **Zweckbindung von Protokolldaten** für Fahndungszwecke allenfalls unter besonderen Bedingungen im Einzelfall infrage käme. Der Gesetzentwurf trägt diesem Grundsatz bei allen Registern durch die Formulierung Rechnung:

„Liegen Anhaltspunkte dafür vor, daß ohne ihre Verwendung die Verhinderung oder Verfolgung einer schwerwiegenden Straftat gegen Leib, Leben oder Freiheit einer Person aussichtslos oder wesentlich erschwert wäre, dürfen die Daten auch für diesen Zweck verwendet werden, sofern das Ersuchen der Strafverfolgungsbehörde unter Verwendung von Halterdaten einer bestimmten Person oder von Fahrzeugdaten eines bestimmten Fahrzeugs (oder unter Verwendung von Personendaten einer bestimmten Person) gestellt wird."

Die genannten Regelungen bedürfen teilweise – wie auch die Einführung des EU-Führerscheins im

Scheckkarten-Format – der Umsetzung durch Rechtsverordnungen. Ich gehe davon aus, daß ich an der Beratung der Verordnungsentwürfe so beteiligt werde, wie dies mit guten Ergebnissen im Gesetzgebungsverfahren der Fall war.

28.4 Luftverkehr

28.4.1 Offenstehende Regelungen

Auf die seit Jahren bestehenden datenschutzrechtlichen Defizite im Luftverkehrsrecht habe ich in meinem 15. TB (Nr. 18.6) hingewiesen. Nach einigen Anlaufschwierigkeiten wurden im November 1996 endlich Gespräche mit dem BMV über einen Gesetzentwurf geführt, der Regelungen für folgende Register der Luftfahrt enthält:

- Luftfahrzeugregister (Datei der Verkehrszulassungen),
- Zentrale Luftfahrerdatei (Datei der erteilten Erlaubnisse und Berechtigungen),
- Luftfahrer-Eignungsdatei (Datei der negativen Entscheidungen zu den erteilten Erlaubnissen und Berechtigungen sowie luftverkehrsrechtlich relevante Entscheidungen der Gerichte),
- Deliktsregister (Ordnungswidrigkeiten oder sonstige negative Entscheidungen über das Personal oder die verantwortlichen Personen von Unternehmen der Luftfahrt).

Die bisher konstruktiv verlaufenen Gespräche über die Notwendigkeit der Erhebung, Speicherung und Übermittlung personenbezogener Daten durch die Luftfahrtverwaltung sollen fortgesetzt werden. Ich hoffe, daß diese zu einem positiven Abschluß gebracht werden können und die Bundesregierung bald dem Beschluß des Deutschen Bundestages vom 22. Juni 1995 nachkommen kann, einen Gesetzentwurf mit bereichsspezifischen Datenschutzregelungen für die Erhebung, Verarbeitung und Veröffentlichung von personenbezogenen Daten im Zusammenhang mit der Vorbereitung und Abwicklung des Flugverkehrs vorzulegen.

28.4.2 Beratung und Kontrolle beim Luftfahrt-Bundesamt

Das Fehlen von rechtlichen Vorgaben und die dadurch fortbestehenden Unsicherheiten veranlaßten mich, im Berichtszeitraum erneut das Luftfahrt-Bundesamt (LBA) in Braunschweig zu beraten und zu kontrollieren.

So gab es mangels gesetzlicher Vorgaben und Richtlinien beim Beantworten von Anfragen Dritter eine gewisse Unsicherheit unter den Mitarbeitern. Ich traf sowohl auf die vorbildliche Methode, Auskünfte nur auf schriftliche Anforderung (einschließlich Fax) zu erteilen, als auch auf eine eher großzügige Handhabung der Datenweitergabe, wie z. B. Anschriften von Luftfahrzeughaltern ohne Identifizierung des Anfragenden herauszugeben. Das LBA wurde auf den dringenden Regelungsbedarf hingewiesen, um dem Datenschutz im Interesse der jeweils Betroffenen gerecht zu werden.

Ein schwieriges Thema ist weiterhin die Übermittlung personenbezogener Daten der Luftfahrzeugeigentümer, die im Rahmen der Verkehrszulassung erhoben und in die Luftfahrzeugrolle eingetragen sind. Wie zuletzt in meinem 15. TB (Nr. 18.6) festgestellt, fehlt es auch heute noch an einer ausreichenden Rechtsgrundlage für die Übermittlung dieser Daten zur Veröffentlichung in den Nachrichten für Luftfahrer und im Registre Aéronautique International. Trotzdem übermittelt das Amt diese Zulassungsdaten ohne Einwilligung der Luftfahrzeugeigentümer zur Veröffentlichung und auch, ohne den Eigentümern Gelegenheit zum Widerspruch dagegen einzuräumen. Deshalb mußte ich erneut eine Beanstandung aussprechen. Inzwischen stellte sich heraus, daß eine Veröffentlichung dieser Daten für Verwaltungsmaßnahmen auf dem Gebiet des Luftverkehrs nicht erforderlich ist, da für diese Zwecke in der Regel nicht die Daten der Eigentümer, sondern die der Halter benötigt werden. Ich muß daher feststellen, daß das Bundesministerium für Verkehr durch die Veröffentlichung personenbezogener Daten aus der Luftfahrzeugrolle einen fortgesetzten Verstoß gegen datenschutzrechtliche Grundsätze nicht nur geduldet hat, sondern auch Verantwortung dafür trägt, daß trotz meiner Beanstandungen nicht geprüft wurde, ob die Veröffentlichung dieser Daten für die Aufgabenerfüllung überhaupt sachdienlich ist.

In einigen Arbeitsbereichen des Amtes – u. a. beim Führen der Luftfahrerdatei – werden erhobene Daten trotz interner Vorgaben für Aufbewahrungsfristen unbefristet gespeichert. Technische Möglichkeiten zum programmgesteuerten, regelmäßigen Löschen werden nicht genutzt. Neben der Behebung dieser organisatorischen Mängel ist auch die Erforderlichkeit der Datenvorhaltung je nach den Speicherungszwecken zu prüfen. Hier besteht ebenfalls Handlungsbedarf seitens des LBA.

Alle festgestellten Defizite sind zwar auch auf die Schwachstellen in der Organisation des Luftfahrt-Bundesamtes zurückzuführen. In erster Linie gründen sie aber auf dem Fehlen der notwendigen gesetzlichen Regelungen. Inzwischen hat mir das BMV mitgeteilt, daß einige der von mir festgestellten Mängel bereits behoben seien. Durch weitere Maßnahmen des LBA (z. B. Schulungskonzept, interne Verfahrensregelungen) sowie durch die bevorstehende Änderung des Luftverkehrsrechts soll künftig dem Datenschutz Rechnung getragen werden.

29 Postdienst

29.1 Datenschutz begleitet die Post-Liberalisierung

Im Rahmen der Postreform III wird das Postwesen völlig neu gestaltet; die Liberalisierung erfaßt nun auch die Postdienstleistungen. Anstelle des Monopolbereiches (unter dem sogenannten Beförderungsvorbehalt) der Deutschen Post AG entsteht ein Bereich, in dem die Regulierungsbehörde Lizenzen an geeignete Unternehmen erteilen kann. Damit erhalten auch andere private Beförderungsunternehmen Zugang zum Markt der Postdienstleistungen. Für

einige Segmente der bisherigen Dienstleistungen hat das BMPT durch Postbefreiungs-Verordnungen den Lizenzierungsvorbehalt bereits aufgehoben. Das betrifft bisher das Befördern von Katalogen und von Briefen über 1 000 g, Sendungen mit einem Mindestpreis von 10 DM und den sogenannten Dokumentenaustauschdienst. Nach dem Inkrafttreten dieser Verordnungen kann grundsätzlich jedermann derartige Postdienste anbieten. Andererseits ist im Entwurf des neuen Postgesetzes für den Marktführer eine noch bis zum 31. Dezember 2002 befristete Exklusivlizenz für Briefsendungen unter 100 g vorgesehen.

Für den Datenschutz ergeben sich Probleme bei der Liberalisierung des Postdienstes insbesondere daraus, daß die bisherigen öffentlichen Aufgaben der Post von Privaten wahrgenommen werden sollen, und zwar – entsprechend der parlamentarischen Vorgabe – unter Beibehaltung des bisherigen Schutzniveaus für die Bürger als Vertragspartner der Post (Postkunden) und als am Postverkehr Beteiligte (Empfänger). Gleichzeitig sollen aber auch die Befugnisse staatlicher Stellen zu Eingriffen in den Postverkehr im bisherigen Umfang erhalten bleiben. Weiterhin sind Ungleichheiten für alle am Wettbewerb Teilnehmenden auszuschließen oder zumindest zu mildern, soweit sie Folgen des früheren Monopols sind.

Die neue Postdienstunternehmen-Datenschutzverordnung (PDSV) vom 4. November 1996 sorgt für gleiche Datenschutz-Vorgaben bei allen Anbietern von Postdienstleistungen. Sie löste die alte – nur für die Bundespost und deren Nachfolger Deutsche Post AG gültige – Postdienst-Datenschutzverordnung (PD-DSV) vom 24. Juni 1991 ab. Das BMPT hat mich von Anfang an beteiligt, so daß ich meine Auffassungen einbringen konnte und nunmehr ein auch aus datenschutzrechtlicher Sicht akzeptables Ergebnis vorliegt:

Die Verarbeitung und Nutzung von Kundendaten für Werbung, Beratung und Marktforschung ist danach nur zulässig, wenn der Postkunde auf sein Widerspruchsrecht dagegen ausdrücklich hingewiesen wurde und er davon nicht Gebrauch gemacht hat. An die Stelle der nach der früheren Praxis nicht immer wirksamen Widerspruchsregelung zur Anschriftenübermittlung an Dritte ist die Einwilligung durch den Betroffenen getreten.

Nach dem Post- und Telekommunikations-Regulierungsgesetz (PTRegG) gilt das derzeitige Postgesetz längstens bis zum 31. Dezember 1997 und ist bis dahin zu ersetzen. Im Rahmen der Ressortabstimmung habe ich mich an der Diskussion des vom BMPT dazu vorgelegten Entwurfs beteiligt. Meine Anregungen sind in mehreren Punkten berücksichtigt worden. Bedenken habe ich aber noch immer insoweit, als eine Verpflichtung der Postdienstunternehmen zur Übermittlung von Vertragsdaten über Postdienstleistungen an die Verfassungsschutzbehörden des Bundes und der Länder, den BND, den MAD und das Zollkriminalamt sowie an Polizei- und Ordnungswidrigkeitenbehörden vorgesehen ist, die zudem keinerlei Abstufung danach enthält, ob es sich um Bagatellfälle oder Schwerkriminalität handelt.

29.2 Neue Verfahren im Postdienst

Die Deutsche Post AG hat ihre Logistik im Fracht- und Briefdienst wesentlich verändert. Am markantesten zeigen sich die Veränderungen in dem Aufbau von bundesweit 33 Frachtpostzentren und 83 Briefverteilzentren. Für den Normalverbraucher war das Einrichten von ca. 1 400 Postagenturen in Einzelhandelsgeschäften, Lotto-Annahmestellen, Tankstellen usw. besonders augenfällig.

Die mir gegenüber geäußerten Befürchtungen der Bürger, daß von den Agenturbetreibern das Postgeheimnis nicht so gewahrt würde wie von Postbediensteten, konnte ich nicht bestätigen. Das Postgeheimnis gilt gleichermaßen für die Beamten und Angestellten der Deutschen Post AG wie für die in Postagenturen Beschäftigten oder für postdienstliche Leistungen verrichtende Mitarbeiter der Deutschen Bahn AG, von Luftverkehrsgesellschaften und Reedereien. Ich habe keine Anzeichen dafür, daß es in einer dieser Gruppen weniger gut gewahrt würde.

Mit neuen Konzepten im Paketdienst bilden sich auch neue Informationsbeziehungen bei der Annahme, Verteilungssteuerung, Transportüberwachung, Auslieferung und zuletzt beim Zustellen oder Abholen der Sendungen. Die Trennung der elektronischen Information von der körperlichen Fracht- oder Briefsendung schafft ein Abbild, einen Datenschatten, der auch unabhängig von der realen Sendung verarbeitet und genutzt werden kann. Durch den Abgleich von realer Sendung und Datenbild an bestimmten Durchlaufpunkten werden die Laufweg- und Laufzeitverfolgung zur Kontrolle oder zu Nachweiszwecken für den Postkunden möglich. Im Frachtdienst spricht man vom „Tracking and Tracing", kurz „T & T", was nichts anderes als „Verfolgen und Auffinden" bedeutet.

Eine Voraussetzung für derartige Paketverfolgungssysteme sind auf dem Paket angebrachte Aufkleber (Labels) mit maschinenlesbaren Angaben über Empfänger und Absender. Die Absender-Labels ersetzen die bisherigen Paketnummernzettel und werden mit dem Paketschein auf die Sendung geklebt, was für den Einzelkunden in der Postannahmestelle geschieht oder vom Großkunden selbst vorgenommen werden kann. Ein Absender-Label enthält als Strichcode die Nummer des Abgangs-Frachtpostzentrums, eine Kennzahl zur Absendung (Postfiliale, Großkunde oder Selbstbucher), die individuelle Einlieferungsnummer des Paketes und eine Prüfziffer. Bei der Einlieferung in das Frachtpostzentrum werden die Pakete mit einem weiteren Aufkleber versehen, der den Leitcode mit Postleitzahl, Straße und Hausnummer des Empfängers sowie Paketart und eine Prüfziffer enthält. Personenbezogene Daten sind wie bisher die Absender- und Empfängeradressen auf dem Paketschein, die nicht in das T & T-Informationssystem eingehen. Die Identifizierung der Sendung ist nur mit der Einlieferungsnummer möglich.

Am Zielort werden aus den Leitcode-Labels die Listen für die Auslieferung gedruckt, und hier wird erstmals der Empfängername vom Paket erfaßt, und zwar wird er manuell in die Auslieferungsliste über-

tragen. Die Zustellung/Auslieferung bestätigt der Empfänger mit seiner Unterschrift in dieser Liste – genauso wie bisher. Für das T & T-System wird die Liste mit der Empfangsbestätigung maschinell gelesen, die Aktualität ist damit gewährleistet. Aufbewahrungsdauer (maximal 1½ Jahre) und Verwendung (zu Nachweiszwecken) der Absender- und Empfängerdaten unterliegen denselben datenschutzrechtlichen Regelungen wie bisher. Gegen diese Modernisierung im Paketdienst habe ich keine Bedenken.

Für den Briefdienst ist ein ähnliches Briefverfolgungssystem denkbar, was besonders bei den Zusatzleistungen Eilbrief, Wertbrief, Nachnahme oder Einschreiben sinnvoll wäre. Die in den Briefverteilzentren eingesetzten neuen Sortier- und Verteilmaschinen arbeiten aber noch nach dem alten Verfahren, bei dem auf dem Briefumschlag ein fluoreszierender Strichcode mit der Postleitzahl und dem Bestimmungsort gedruckt wird.

Ein weiteres neues System erprobt die Post für die Nach- und Rücksendungen, mit dem alle Nachsendeanträge in einer zentralen Datei erfaßt und verarbeitet werden. In vier Nachsendestationen (München, Karlsruhe, Köln und Magdeburg) sollen die Briefsendungen mit den geänderten Adressen als Aufkleber versehen und versendet werden. Das gleiche geschieht mit den Rücksendungen; die aufgeklebte Adresse ist dann die des Absenders.

Auch wenn bisher alles dafür spricht, daß die vorgesehenen Änderungen weder die Datenschutzrechte der Absender noch die der Empfänger verletzen, so wird den neuen Verfahren und hierbei besonders der Adressenverarbeitung vorsorglich auch weiterhin meine Aufmerksamkeit gehören.

29.3 Umzugsadressen und Werbung

Aktuelle Anschriften potentieller Kunden sind für die Direktwerbung von entscheidender Bedeutung. Daher versucht die Werbebranche – auch mit Hilfe der Post – möglichst aktuelle Anschriften zu führen. Eine sinnvolle Maßnahme dazu ist, eine durch Umzug veraltete Adresse durch die neue zu ersetzen:

Haben umziehende Bürger bei der Post einen Nachsendeantrag gestellt und in den Adressentausch „neu gegen alt" auch für Dritte eingewilligt, erhält die Firma „Deutsche PostAdress GmbH" die alten und die neuen Anschriften. (Einen stark vereinfachten Überblick über die Datenflüsse zeigt Abbildung 14). Mit diesem Bestand können Versender – und auch Adreßhändler – ihr jeweiliges Adressenmaterial aktualisieren, wobei die erstmalige Aufnahme von Kundenanschriften in diesem Zusammenhang unzulässig ist (s. 15. TB Nr. 20.3.2). Die Anschriften dürfen von der PostAdress nicht für andere Zwecke genutzt werden, weil die ausdrückliche Einwilligung des Antragstellers dies nicht umfaßt. Sie sind nach Ablauf des Nachsendezeitraumes von 6 Monaten zu löschen; eine einmalige Verlängerung für weitere 6 Monate ist mit erneutem Antrag des Betroffenen möglich.

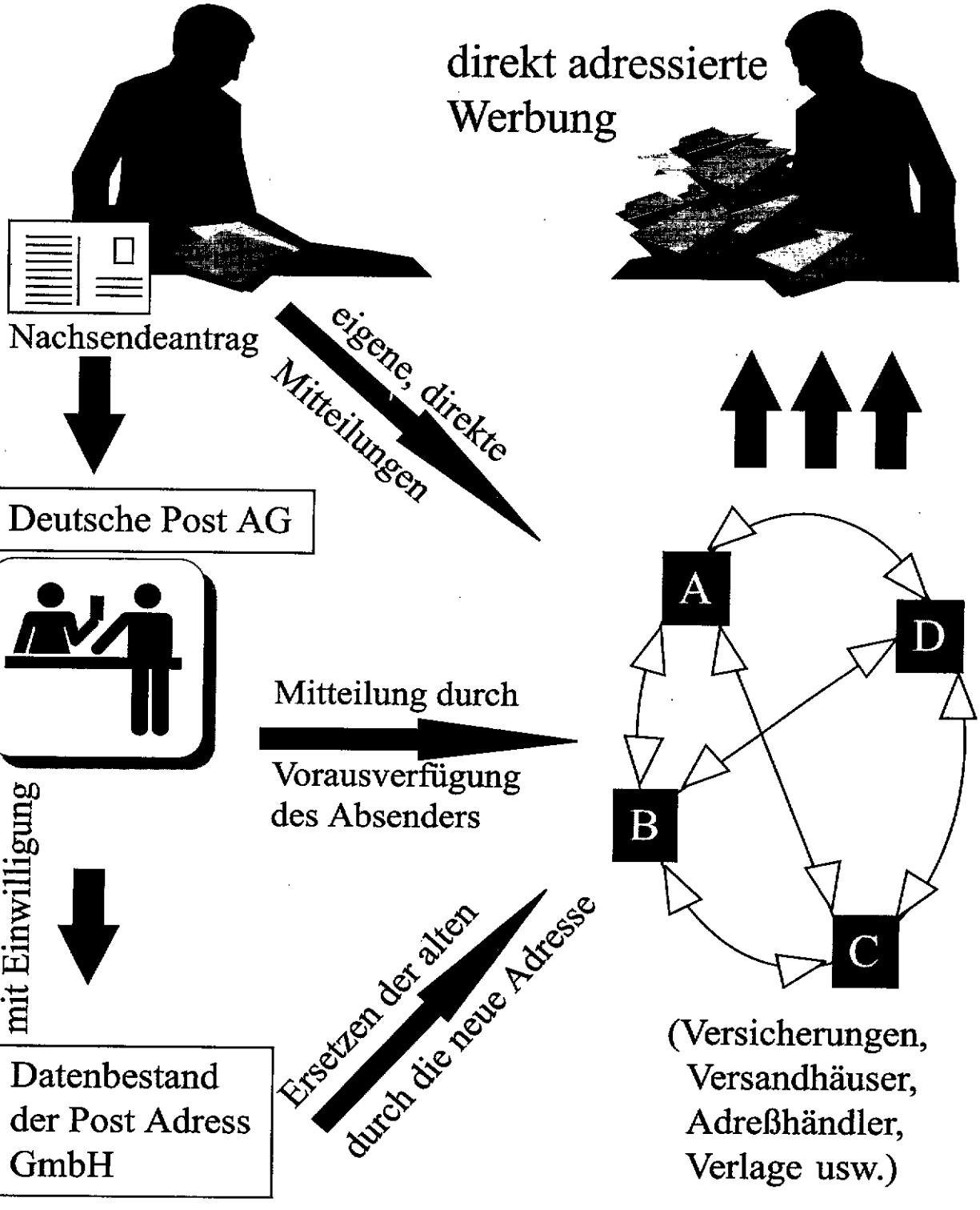
Die PostAdress hat sich daran nicht gehalten und die Anschriften nach Ablauf des Nachsendezeitraumes im sog. Listbroking vermarktet. Dabei werden die Anschriften nicht an andere Firmen übermittelt, sondern lediglich zum Adressieren einzelner Werbesendungen dieser Firmen genutzt. Viele Betroffene wandten sich daraufhin an mich, da sie Werbung von Firmen erhalten hatten, mit denen sie bisher noch nie in Verbindung standen. Diese Zweckentfremdung ist weder Bestandteil des Vertrages zur Anschriftenübermittlung von der Deutschen Post AG an die PostAdress, noch ist sie aus anderen Gründen datenschutzrechtlich zulässig. Auf meine Intervention hin wurde gemeinsam mit der Generaldirektion der Post die zwischen der Deutschen Post AG und mir übereinstimmende Rechtsauffassung gegenüber der PostAdress durchgesetzt mit dem Ergebnis, daß diese Nutzung der Anschriften eingestellt wurde. Seitdem werden die Umzugsdaten wieder planmäßig nach Ablauf des Nachsendezeitraums gelöscht.

Mit Hilfe eines neuen Verfahrens wird – durch bloßes Teiladressieren der Werbesendungen – das schwierige Bezeichnen jedes einzelnen Adressaten mit dessen Namen und Anschrift umgangen. Bei diesem Verfahren, das auch unabhängig von Umzügen ist, werfen die Briefträger teiladressierte Werbesendungen (z. B. „An die Bewohner des Hauses Holzgasse 9") in die Briefkästen des genannten Hauses. Verschont werden davon normalerweise nur die Bürger, deren Briefkästen Aufkleber wie „Keine Werbung einwerfen" tragen. Die ausgewählten Teiladressen stammen aus der Datenbank eines privaten Adressenhändlers, in der ca. 14 Millionen Gebäude in Deutschland mit unterschiedlichsten kaufkraft- und interessenbezogenen Indikatoren, wie z. B. Art, Größe und Zustand des Hauses, Art der Wohngegend sowie gegebenenfalls Angaben zum Garten, klassifiziert sind. Auf dieser Basis können die Zielgruppen produktspezifisch ausgewählt und die Werbesendungen nur an potentielle Kunden, z. B. in Einfamilienhäusern mit Garten oder an junge Familien in Neubausiedlungen, gesendet werden, was dem Erfolg der Werbemaßnahme zugute kommt.

Eine datenschutzrechtliche Beurteilung ist insoweit problematisch, als die Datei des privaten Adressenhändlers primär nicht personenbezogen ist. Wird seine Datei jedoch mit den Anschriften von Personen aus Adressenbeständen Dritter zusammengeführt, entstehen Daten über persönliche oder sachliche Verhältnisse dieser Personen. Eine solche Sammlung besteht nach meiner Kenntnis oft nur für kurze Zeit, z. B. für eine Mailing-Aktion, also nur, um die Adressen der gewünschten Zielgruppe für eine Werbemaßnahme herauszufinden und die Werbesendungen mit diesen Adressen zu versehen. Danach müßte die Verknüpfung von Gebäudemerkmalen und Anschriften von Personen sofort wieder aufgehoben werden. Ob und wie derartige Probleme der Anwendbarkeit des Datenschutzrechts im Rahmen der Novellierung des BDSG gelöst werden können, ist derzeit noch offen (s. auch Nr. 2.1.5).

Abbildung 14

Mögliche Adressenwanderungen beim Umzug



29.4 Mißglückte Datenerhebung per Postwurfsendung

In einer Großaktion wollte die Deutsche Post AG von allen ca. 36,5 Millionen Haushalten in Deutschland die aktuellen Anschriften der in einem Haushalt lebenden oder unter der Anschrift zu erreichenden Personen erhalten. Dazu verteilte sie – zunächst in den östlichen und südlichen Bundesländern – als Postwurfsendung Antwortkarten mit dem Aufruf „Ihr Postzusteller bittet um Ihre Hilfe".

Unmittelbar nach dem Start der Aktion erhielt ich am 17. Oktober 1996 und an den darauffolgenden Tagen viele Anrufe und Schreiben von Bürgern, von privaten und öffentlichen Stellen. In teilweise empörten Äußerungen wie „Ausforschungsaktion", „... was geht das die Post an, wer bei mir wohnt ...", „bundesweites Post-Melderegister" wurde die Prüfung und Einstellung dieser Aktion gefordert. Für einige Postbenutzer war es der Anlaß, die Löschung aller ihrer bisher bei der Post gespeicherten Daten zu fordern.

Die Aktion erfolgte zu einem Zeitpunkt, an dem noch die alte Postdienst-Datenschutzverordnung galt. Die neue Datenschutzverordnung für Postdienstunternehmen (s. o. Nr. 29.1) war aber bereits am 27. September 1996 vom Bundesrat verabschiedet worden, und bis zum Inkrafttreten stand lediglich noch die Veröffentlichung im Bundesgesetzblatt aus. Doch weder die alte noch die neue Verordnung gaben der Post das Recht, eine derartige Datenerhebung durchzuführen. Zwar hätte sie jede Anschrift und die Einwilligung in deren weitere Verwendung erbitten dürfen. Sie hätte aber klar und deutlich auf die Zwecke der Speicherung und auf die vorgesehenen Übermittlungen hinweisen müssen. Das verklausulierte Anbieten eines Widerspruchs gegen Übermittlungen erfüllte diese Bedingungen nicht, und ohne weitere Erläuterungen durfte die Post auch nicht einen beliebigen Empfänger über die Angaben aller Mitbewohner verfügen lassen.

Nach einer ersten Prüfung habe ich mich sofort an den Vorstand der Deutschen Post AG gewandt und die Einstellung dieser Aktion gefordert. Hierbei habe ich auf die Mängel dieser Datenerhebung aufmerksam gemacht und gefordert, daß niemandem bei Nichtabsendung der Karte Nachteile entstehen. Die Post hat mir daraufhin umgehend mitgeteilt und in der Öffentlichkeit erklärt, daß sie diese Anschriftenerhebung unverzüglich einstellt und die eingegangenen Rückantworten vernichtet.

Ich verkenne nicht, daß das Interesse der Post an der Reduzierung der jährlich etwa 76 Millionen Fehlsendungen infolge veralteter oder aus anderen Gründen unrichtiger Anschriften legitim und wirtschaftlich sinnvoll ist und im überwiegenden Allgemeininteresse liegt. Dazu kann eine möglichst große Sammlung solcher Anschriften hilfreich sein, an die eine Zustellung mit hoher Wahrscheinlichkeit möglich ist. Ich habe daher meine Beratung für eine unbedenkliche Adressenerhebung angeboten. Erste Gespräche dazu fanden bereits statt.

30 Statistik

30.1 Neuordnung der amtlichen Statistik

Dem Ziel, öffentliche Ausgaben zu verringern und die Wirtschaft von überflüssigen administrativen Verpflichtungen zu entlasten, dienen auch die Bemühungen um Verringerungen und Einsparungen bei der amtlichen Statistik. Mit dem Ziel, die Statistik auf das absolut notwendige Maß zu reduzieren, hat der Statistische Beirat, der nach dem Bundesstatistikgesetz berufen ist, das Statistische Bundesamt in Grundsatzfragen zu beraten, die Arbeitsgruppe „Zukunftsperspektiven der amtlichen Statistik" gebildet. In dieser Arbeitsgruppe, an deren Sitzungen ich ebenfalls mitgewirkt habe, waren Vertreter der Befragten, der Nutzer und der Produzenten der amtlichen Statistik vertreten. Die von der Arbeitsgruppe erstellten und vom Statistischen Beirat abschließend beratenen Vorschläge für ein Rahmenkonzept zur „Neuordnung der amtlichen Statistik" bilden einen konstruktiven Beitrag zum Thema „Schlanker Staat und amtliche Statistik".

Bei den Beratungen wurden jedoch auch Begehrlichkeiten und Wunschvorstellungen deutlich, die zu einer Erosion des Datenschutzes im Bereich der Statistik führen könnten. Es geht dabei um Pläne und Vorhaben, statistische Daten multifunktional zu nutzen, Datenpools zu bilden, beliebigen Zugang zu Verwaltungsdaten zu ermöglichen und statistische Daten für Verwaltungszwecke nutzbar zu machen.

Die Statistik ist jedoch gut beraten, bei der Wahl ihrer Mittel sorgfältig vorzugehen. Denn um eine langfristige Perspektive zu sichern, sind der Erhalt des Vertrauens der Auskunftgebenden und die damit einhergehende Sicherung der Repräsentativität entscheidende Kriterien. Schließlich werden die Ergebnisse von Befragungen immer eine wichtige Grundlage statistischer Analysen sein, und deren Qualität hängt wesentlich von der Auskunftsbereitschaft der Bürger und Unternehmen ab. Daher muß die Statistik sich darum bemühen, dieses Vertrauen zu erhalten und durch Gewährleistung datenschutzrechtlicher Maßnahmen immer wieder neu zu bilden. Staatlicher Zwang kann auch hier nur begrenzt wirksam werden, und ein die Interessen der Auskunftgebenden überspielendes staatliches Handeln würde allenfalls kurzfristig vorteilhaft sein. Auf Dauer würden sich der Umfang und die Genauigkeit der Information verringern.

Die Statistik muß sich auch davor hüten, Datenlieferungen aus den Verwaltungen durch die einzelfallbezogene Preisgabe ihrer Erkenntnisse an die jeweilige Fachverwaltung zu honorieren. Die Statistik erbringt ihre „Gegenleistung", indem sie die Entscheidungsträger in Politik, Wirtschaft und Gesellschaft dabei unterstützt, vorausschauend zu planen und sachlich fundiert zu entscheiden. Dazu gehört auch eine für die Bürger klar erkennbare Distanz zur Verwaltung. Die Auskunftgebenden müssen darauf vertrauen können, daß die zu rein statistischen Zwecken gemachten Angaben nicht auch den Verwaltungen bekannt oder sogar für Einzelmaßnahmen genutzt werden.

Es gilt daher, allen Tendenzen entgegenzuwirken, daß infolge der notwendigen Einsparmaßnahmen der Datenschutz – als vermeintlicher Kostenverursacher – auf die Streichliste gerät. Insbesondere mit Blick auf Vorhaben wie multifunktionale Nutzung und Aufbau eines gemeinsamen Datenpools für statistische Daten ist es bedenklich, wenn den statistischen Stellen ein beliebiger Zugang zu Verwaltungsdaten eröffnet wird. Dem betroffenen Bürger wäre es dann nicht mehr möglich zu überschauen, wer was wann und bei welcher Gelegenheit über ihn weiß und zu welchen statistischen Zwecken die über ihn vorhandenen Daten verwendet werden können. Auch im abgeschotteten Bereich der Statistik ist eine Abbildung der Persönlichkeit durch unbeschränkte Verknüpfung der erreichbaren Daten nicht hinnehmbar.

Auch wenn die bedenklichen Wunschvorstellungen noch davon entfernt sind, zur statistischen Rechtswirklichkeit zu werden, sind erste in diese Richtung weisende Vorstöße nicht zu übersehen. In den Unterlagen für die Sitzung des Ausschusses für das Statistische Programm der Europäischen Union, einem durch Ratsbeschluß einberufenen Gremium der Leiter der nationalen statistischen Ämter unter Vorsitz der statistischen Gemeinschaftsdienststelle EUROSTAT, findet sich die Ausführung, es sei *„... wenig wahrscheinlich, daß die Achtung vor dem Privatleben als sozialem und ethischem Wert ein ausreichend starkes Gegengewicht darstellt, um die sich abzeichnende Entwicklung in bezug auf die Nutzung von Verwaltungsdateien für statistische Zwecke aufhalten zu können. [...] die statistischen Ämter, für die der Zugang zu den in ihren Ländern bestehenden Verwaltungsdateien mit Schwierigkeiten verbunden ist, (sehen sich) gezwungen, die Unterstützung von Eurostat zu erbitten."* Es wäre nicht hinnehmbar, wenn als störend empfundene nationale Datenschutzvorschriften durch europäische Rechtsakte ausgehebelt würden. Dadurch entstünde ein nicht wieder gut zu machender Schaden sowohl für die Statistik als auch für unser Verhältnis zu Europa.

30.2 Statistikverordnung der Europäischen Union

Die Beratungen zum Verordnungsvorschlag des Rates über die Tätigkeit der Gemeinschaft im Bereich der Statistik befinden sich in der abschließenden Phase. Meine Bedenken gegen die Vorentwürfe, die ich in den zurückliegenden Tätigkeitsberichten dargestellt habe (s. zuletzt 15. TB Nr. 22.1.1), sind im wesentlichen berücksichtigt worden. Die Einwände einzelner Mitgliedstaaten, etwa gegen den vorbehaltlosen Zugang der statistischen Ämter und der statistischen Gemeinschaftsdienststelle – EUROSTAT – zu Verwaltungsdaten, sind – aufgrund des in den Mitgliedstaaten unterschiedlich entwickelten Statistikrechts – für mich nachvollziehbar. Die Verordnung des Rates über die Gemeinschaftsstatistik in ihrer derzeitigen Fassung würde das in Deutschland bewährte Niveau des Datenschutzes in der Statistik nicht absenken.

Die Absicht der Gemeinschaft, allgemeine Regelungen für die Gemeinschaftsstatistik zu treffen, die bereichsspezifische Regelungen zum Datenschutz enthalten, ist zu begrüßen. Das positive Bild wird jedoch dadurch getrübt, daß die allgemeinen Defizite des Datenschutzes auf europäischer Ebene nach wie vor bestehen. Zwar müssen nach den Erwägungsgründen der geplanten Statistikverordnung die für die Erstellung von Gemeinschaftsstatistiken zu erhebenden vertraulichen Daten geschützt werden, um das Vertrauen der Auskunftspflichtigen zu gewinnen und zu erhalten. Auch soll in allen Mitgliedstaaten die Geheimhaltung der statistischen Daten den gleichen Grundsätzen entsprechen. Andererseits fehlt es aber an einer allgemeinen, umfassenden und rechtsverbindlichen Datenschutzregelung für die Organe und Einrichtungen von Europäischer Gemeinschaft und Union. Erst die Umsetzung der von den Datenschutzbeauftragten der Europäischen Union aufgestellten Forderungen nach einem europäischen Grundrecht auf Datenschutz, verbindlichen Datenverarbeitungsregelungen für die Organe und Einrichtungen der Gemeinschaft sowie die Einrichtung einer unabhängigen europäischen Datenschutzkontrollinstanz (vgl. Kopenhagener Resolution der Konferenz der Datenschutzbeauftragten der Europäischen Union vom 8. September 1995, s. o. Nr. 2.2 und Anlage 4) wird das Vertrauen der Gemeinschaftsbürger in die Statistik fördern und sich auf die Erfüllung statistischer Aufgaben positiv auswirken.

30.3 Statistikregistergesetz

Die EG-Unternehmensregisterverordnung Nr. 2186/93 vom 22. Juli 1993 verpflichtet die statistischen Ämter von Bund und Ländern, nach Maßgabe des nationalen Rechts ein Statistikregister aufzubauen und zu führen (vgl. 15. TB Nr. 22.1.2). Die Aufgaben sind unter den statistischen Ämtern aufgeteilt. Während die statistischen Landesämter für den Aufbau des Registers in ihrem Bereich zuständig sind, ist das Statistische Bundesamt für das Gesamtregister und insbesondere für die Koordinierung verantwortlich. Da die für das Unternehmensregister benötigten Informationen nicht in ausreichendem Maße aus vorhandenem statistischen Datenmaterial übernommen werden können, sind Rechtsvorschriften erforderlich, um die Lieferung von Daten aus administrativen Registern und Dateien zur Aufnahme in das Unternehmensregister zu ermöglichen. Der vom BMWi erarbeitete Entwurf eines Statistikregistergesetzes regelt daher im wesentlichen die Übermittlung von Informationen aus den Dateien der obersten Finanzbehörden der Länder, der Bundesanstalt für Arbeit, der Industrie- und Handelskammern sowie der Handwerkskammern an die statistischen Ämter.

Neben den Namen und Adressen von Unternehmen und ihren Betrieben sind in das Statistikregister insbesondere Angaben über Umsatz, Zahl der Beschäftigten, Rechtsform, Beginn und Ende der wirtschaftlichen Tätigkeit sowie den Wirtschaftszweig aufzunehmen und jährlich zu aktualisieren. Der zugrunde gelegte Unternehmensbegriff ist hierbei sehr weit und umfaßt juristische Personen ebenso wie natürliche Personen aller Wirtschaftszweige und Berufe, soweit sie zum Bruttosozialprodukt infolge ihrer selbständigen wirtschaftlichen Tätigkeit beitragen. Im Unternehmensregister werden daher Angehörige der freien

Berufe und Selbständige gleichermaßen erfaßt wie Handwerker und Einzelhändler. Ausgenommen sind nur private Haushalte und landwirtschaftliche Betriebe. Das Register, dessen Gesamtzahl der nachzuweisenden Einheiten auf etwa 3,5 Millionen geschätzt wird, bildet u. a. die Basis für gesamt- und regionalwirtschaftliche Strukturanalysen sowie den Hochrechnungsrahmen und die Auswahlgrundlage für Stichprobenerhebungen.

Um die aus den verschiedenen Dateien gelieferten Angaben im Unternehmensregister zusammenzuführen, war zunächst daran gedacht, eine von den statistischen Ämtern zu vergebende einheitliche Unternehmenskennummer als gemeinsames Ordnungsmerkmal für die Dateien bei den oben genannten Stellen einzuführen. Dieser Verfahrensweise haben die beteiligten Ressorts unter Hinweis auf den unverhältnismäßig hohen Kostenaufwand widersprochen. Meine Bedenken bezogen sich darauf, daß dieses einheitliche Kennzeichen die Wirkungen eines Personenkennzeichens für Unternehmer entfalten könnte, wenn es über den abgeschotteten Statistikbereich hinaus auch in den administrativen Registern und Dateien verwendet wird.

Das Statistikregister soll nun in der Weise aufgebaut werden, daß die statistischen Ämter von den Unternehmen die jeweiligen bereichsspezifisch vergebenen Kennungen, wie z. B. die Steuernummer, erfragen und mit den erfragten Kennungen die Meldungen aus den verschiedenen Bereichen zusammenführen. Dieses Verfahren verursacht bei den Auskunftspflichtigen lediglich eine geringe Belastung und führt im Vergleich zu der Alternative, einen statistikinternen Datenabgleich durchzuführen, zu geringen Kosten und schnell zu einer guten Qualität der Daten. Die Arbeiten am Entwurf für ein Statistikregistergesetz dauern noch an.

Der Sachverständigenrat „Schlanker Staat" hat aus Gründen der Rationalisierung und Kostenersparnis vorgeschlagen, ein einheitliches Kennzeichen für Unternehmen, losgelöst vom Aufbau und der Führung des Statistikregisters, einzuführen. Dieser Vorschlag, der die vor vielen Jahren geführte – und wegen des damals nicht zu bewältigenden Verwaltungsaufwandes abgebrochene – Diskussion um ein Institutionenkennzeichen wieder aufnimmt, wird vom Statistischen Beirat unterstützt. Unter der Voraussetzung, daß ein einheitliches Kennzeichen für Unternehmen notwendig ist und nicht zu einem Personenkennzeichen für Selbständige und Angehörige freier Berufe wird, bin ich gern bereit, die Verwirklichung mit begleitenden Sicherheitsmaßnahmen für den Schutz der Privatsphäre zu unterstützen.

30.4 Mikrozensusgesetz

Das am 17. Januar 1996 in Kraft getretene Mikrozensusgesetz und Gesetz zur Änderung des Bundesstatistikgesetzes sieht eine Fortführung der Repräsentativerhebung über die Bevölkerung und den Arbeitsmarkt für weitere neun Jahre vor. Daneben wurde entsprechend meiner bereits vor längerer Zeit erhobenen Forderung (vgl. 14. TB Nr. 23.7) die erforderliche Rechtsgrundlage für den Einsatz computergestützter Verfahren bei statistischen Erhebungen durch Aufnahme einer klaren Regelung in das Bundesstatistikgesetz geschaffen.

Das Mikrozensusgesetz berücksichtigt insbesondere meine Bedenken gegen die Erweiterung des Erhebungsprogramms und die Einschränkung der Freiwilligkeit von Antworten (vgl. 15. TB Nr. 22.2). Allerdings ließen sich die am Gesetzgebungsverfahren beteiligten Ressorts nur schwer davon überzeugen, daß auch bei Beibehaltung der Freiwilligkeit von Antworten die erforderliche Repräsentativität der Befragungen gegeben ist und geringe Einbußen im Interesse der befragten Bürger hinnehmbar sind.

Nachdem bisher zwei Erhebungsbögen verwendet wurden – einer für Fragen mit Auskunftspflicht und ein weiterer für freiwillige Angaben, werden die Fragen jetzt, nach Sachgebieten geordnet, in einem Erhebungsbogen zusammengefaßt. Hierdurch können die im sachlichen Zusammenhang stehenden Fragen mit weniger Aufwand beantwortet werden. Um dem gesetzgeberischen Willen Geltung zu verschaffen, habe ich bei der Gestaltung des einheitlichen Erhebungsbogens auf einem deutlich wahrnehmbaren Hinweis auf die Freiwilligkeit bestanden. Das Statistische Bundesamt ist dem mit geeigneten Maßnahmen sowohl für die schriftliche als auch für die mündliche Befragung nachgekommen.

30.5 Hochbaustatistikgesetz

Das Zweite Gesetz über die Durchführung von Statistiken der Bautätigkeit und die Fortschreibung des Gebäudebestandes vom 27. Juli 1978 (2. BauStatG) bedarf dringend der Anpassung an die vom Bundesverfassungsgericht im Volkszählungsurteil von 1983 aufgestellten Grundsätze zur informationellen Selbstbestimmung. In der Neufassung sind außerdem die vereinfachten Verfahren im Bauordnungsrecht sowie die Kürzungsvorschläge des erweiterten Abteilungsleiterausschusses Statistik bezüglich des Erhebungsprogramms berücksichtigt. Um klarzustellen, worauf sich die Statistik der Bautätigkeit bezieht, lautet der Titel des Gesetzentwurfs nunmehr „Gesetz über die Statistik der Bautätigkeit im Hochbau und die Fortschreibung des Wohnungsbestandes". Der Entwurf des BMBau sieht die erforderlichen Regelungen für die Verwendung bestimmter Erhebungsmerkmale für Zwecke der Mieten- und Baupreisestatistik sowie als Grundlage für künftige Gebäude-, Wohnungs- und Bevölkerungsstichproben vor und schließt damit datenschutzrechtliche Lücken des 2. BauStatG.

Dem von den Gemeinden und Gemeindeverbänden geäußerten Wunsch, mit Hilfe der Bautätigkeitsstatistik die kommunalen Gebäudebestandsverzeichnisse fortzuschreiben, konnte ich nicht folgen, weil er die Verwendung der zu übermittelnden Angaben für nicht-statistische Zwecke offen ließ. Meine Besorgnis habe ich dem BMBau frühzeitig mitgeteilt. Der Entwurf stellt in seiner derzeitigen Fassung sicher, daß die Übermittlungen auf diejenigen Erhebungsmerkmale begrenzt bleiben, die auf Verwaltungsdaten beruhen, und daß deren Nutzung an ausschließlich statistische Zwecke gebunden ist.

30.6 Agrarstatistik – InVeKoS

Bei den derzeitigen Reformbemühungen der amtlichen Statistik spielt die Nutzung von Verwaltungsdaten eine wichtige Rolle. Es liegt im allgemeinen Interesse, die Auskunftspflichtigen durch praktikable Lösungen insbesondere durch Vermeidung unnötiger Doppel- und Mehrfachbefragungen zu entlasten. Aus meiner Sicht sind gesetzliche Regelungen vertretbar, mit denen die Informationsbedürfnisse der Statistik – soweit möglich – mit Angaben aus vorhandenen Verwaltungsdateien zu erfüllen sind.

Nicht akzeptabel ist es jedoch, wenn die Verwaltung für Zwecke der Statistik ihren vorgeblich eigenen Bedarf an bestimmten Daten tendenziell über das erforderliche Maß ausdehnt und sich auf diese Weise ihr nicht zustehende Kenntnisse über den Betroffenen verschafft.

Dem Vorschlag, die bei der Durchführung gemeinschaftlicher Beihilferegelungen im Integrierten Verwaltungs- und Kontrollsystem (InVeKoS) gespeicherten Angaben der Landwirtschaftsbetriebe für die Agrarstatistik zu nutzen und eine ergänzende Regelung in das Agrarstatistikgesetz aufzunehmen, habe ich daher mit der Einschränkung zugestimmt, daß weder die Angaben, die nur für die Agrarstatistik bestimmt sind, den Verwaltungen zur Kenntnis gelangen, noch Ergebnisse von erforderlichen Plausibilitätskontrollen der agrarstatistischen Daten einzelfallbezogen in die Verwaltung zurückfließen dürfen.

30.7 Energiestatistik

Für energiepolitische Entscheidungen im Hinblick auf eine sichere, wirtschaftliche und umweltschonende Energieversorgung hat das BMWi den Entwurf eines Gesetzes über Energiestatistiken vorgelegt. Damit soll ein energiestatistischer Rahmen geschaffen werden, der eine zusammenhängende Erfassung des Aufkommens, der Umwandlung und der Verwendung von Energiearten ermöglicht. Soweit statistische Erhebungen in bestimmten Energieträger- und Verwendungsbereichen, wie beispielsweise für private Haushalte, erforderlich sind, sollen hier die gesetzlichen Grundlagen geschaffen werden. Noch ungeklärt ist in diesem Zusammenhang die Frage der zusätzlichen Belastung der zu Befragenden und damit der finanziellen Auswirkungen dieses Vorhabens.

Die Regelungen für die Erhebung bei privaten Haushalten, die Aufschlüsse über den Verbrauch der hauptsächlich für Heizzwecke, zur Warmwasserbereitung sowie für die private PKW-Nutzung eingesetzten Energieträger geben soll, sahen zunächst als ein Erhebungsmerkmal „Ausstattung der Wohnung mit elektrischen Geräten" vor. Obwohl die Begründung zu dem Gesetzentwurf ausführte, daß es sich hierbei nur um stromintensive Geräte entsprechend einer noch zu erstellenden Liste handeln sollte, war das Merkmal nicht ausreichend begrenzt. Ich habe darauf hingewiesen, daß das unter Auskunftspflicht zu erfragende Merkmal zum Einfallstor für Lebensstilerforschung zweckentfremdet werden könnte. Das BMWi hat daraufhin in der jetzigen Entwurfsfassung vorgesehen, daß neben der Erwähnung „stromintensive Geräte" eine beispielhafte Aufzählung derartiger Geräte folgt. Insofern konnte ich der Auskunftspflicht, die aus fachlicher Sicht angesichts der mit ca. 0,03% ziemlich kleinen Stichprobe notwendig ist, zustimmen.

30.8 „Volkszählung 2001"

Die Europäische Union beabsichtigt, im Jahre 2001 eine unionsweite Volks- und Wohnungszählung durchzuführen. Für dieses Vorhaben hat die EU-Kommission einen ersten Vorschlag für eine Verordnung erarbeitet. Das vorgeschlagene Erhebungsprogramm ist in einigen Teilen umfangreicher als das der nationalen Volks-, Berufs- und Wohnungszählung 1987. So soll beispielsweise das Geburtsdatum mit Tag, Monat und Jahr erfaßt werden. Während der Ausschuß für das Statistische Programm, in dem die Leiter der nationalen statistischen Ämter vertreten sind, sich positiv zu dem Vorschlag geäußert hat, ist dieser bei der deutschen Regierung wegen des hohen Kostenaufwandes und der hier geltenden Vorgabe, Statistiken nur im absolut erforderlichen Umfang durchzuführen, auf Widerstand gestoßen. Da die Kommission an dem Statistikvorhaben „Volkszählung 2001" festhält und auch die anderen Mitgliedstaaten gegenüber einer Volkszählung grundsätzlich positiv eingestellt sind, wird nach Alternativen zur bisherigen Volkszählung in Form von kostenträchtigen Befragungen der Haushalte gesucht.

Als Lösungsweg bietet sich an, die in den Melderegistern vorhandenen Daten durch Registerauswertung für eine Volkszählung zu nutzen. Schwierigkeiten bereitet dabei, daß der Katalog der Meldedaten entsprechend den Meldezwecken begrenzt ist. Gegenüber der Volkszählung fehlen Angaben zum Erwerbsstatus, zu formalen Bildungsabschlüssen, zur Berufstätigkeit sowie zum Pendlerverhalten. Ferner lassen sich die Haushaltszusammenhänge nur ungenau aus den Meldedaten ableiten. Um hohe Kosten verursachende Vollerhebungen zu vermeiden, wird von deutscher statistischer Seite angestrebt, das Erhebungsprogramm eines europaweiten Zensus mit Blick auf die Belange der Bundesstatistik erheblich einzuschränken und den noch offenen Informationsbedarf durch repräsentative Erfassung einzelner Merkmale zu decken.

Eine wesentliche Rolle spielt die noch nicht ausdiskutierte Frage, wie präzise die Melderegister tatsächlich sind bzw. mit welcher durchschnittlichen Fehlerquote zu rechnen ist. Solche Fehler entstehen insbesondere durch nicht registrierte Zuzüge und Wegzüge von Einwohnern. Insofern ist eine Untersuchung der Registerqualität – mit akzeptablen Ergebnissen – unabdingbare Voraussetzung für das Ersetzen der Befragung durch die Auswertung der Melderegister.

Als Alternative zur Volkszählung durch Befragen böte die Registerauswertung beachtliche Vorteile. Sie wäre beispielsweise zu jedem beliebigen Zeitpunkt möglich, würde eine wesentlich frühere Bereitstellung der Ergebnisse erlauben und den Bürger nicht mit auskunftspflichtigen Befragungen belasten.

Nachteilig aus der Sicht der Statistik wäre aber die Beschränkung der auf diese Weise verfügbaren Daten auf den Inhalt der Melderegister.

Den Katalog der gesetzlich festgelegten Meldedaten zu erweitern, nur um nationale oder europäische Statistikanforderungen erfüllen zu können, halte ich für unzulässig. Dies habe ich auch für die Landesbeauftragten für den Datenschutz im Rahmen einer Sondersitzung des Unterausschusses „Melde-, Paß- und Personalausweiswesen" des Arbeitskreises I der Ständigen Konferenz der Innenminister der Länder vertreten; dem wurde nicht widersprochen.

31 Nicht-öffentlicher Bereich

31.1 Tendenzen in der Diskussion zur BDSG-Novellierung

Seit 24. Oktober 1995 läuft die Dreijahresfrist für die Umsetzung der EG-Datenschutzrichtlinie (s. auch Nr. 2.1.5). Die damit verbundene Diskussion, wie und wo das deutsche Datenschutzrecht novelliert werden muß, begann aber schon früher. Auch im Düsseldorfer Kreis, dem Gremium der Datenschutzaufsichtsbehörden der Länder für den privaten Bereich, zeigte sich bei den Erörterungen zur Novellierung des BDSG ein starkes Reformineresse. Die Aufsichtsbehörden halten es ebenfalls für erforderlich, die Umsetzung der Datenschutzrichtlinie zum Anlaß zu nehmen, die Bestimmungen für den privaten Bereich im ganzen zu aktualisieren. Für die anstehende Novellierung des BDSG zeichneten sich im wesentlichen folgende Tendenzen und Zielvorstellungen ab:

- **Kontrollbefugnis**

  Die Richtlinie gibt nunmehr vor, die Anlaßaufsicht durch eine umfassende Kontrollbefugnis, die der meinigen vergleichbar ist, zu ersetzen. Damit wird der Weg frei für eine effektive Datenschutzkontrolle.

- **Anwendungsbereich**

  Die Bestimmungen für den privaten Bereich sind grundsätzlich auch auf die Datenverarbeitung in Akten zu erstrecken, damit diese nicht, wie bisher, kontrollfrei bleibt. Die Richtlinie steht dem nicht entgegen. Sie gilt zwar nur für personenbezogene Daten in Dateien, jedoch geht ihr Dateibegriff über den des BDSG hinaus. Zudem können die Mitgliedstaaten die Kriterien zur Bestimmung einer strukturierten Sammlung – und damit einer Datei – festlegen (Erwägungsgrund 27). Dies legt eine für beide Bereiche zumindest in den Grundzügen einheitliche Bestimmung des Anwendungsbereichs nahe.

- **Registermeldung/betrieblicher Datenschutzbeauftragter**

  Die Datenschutzrichtlinie sieht dann Ausnahmen von der Pflicht, bei den Aufsichtsbehörden die Aufnahme und Beendigung einer Verarbeitung anzumelden und hierfür bestimmte Angaben zu machen, vor, wenn der für die Verarbeitung Verantwortliche einen internen Datenschutzbeauftragten bestellt und damit die unabhängige Überwachung des Datenschutzes sicherstellt. Da in Deutschland betriebliche Datenschutzbeauftragte von Gesetzes wegen zu bestellen sind, soll die Meldepflicht in möglichst weitem Umfang aufgehoben werden. Damit ließe sich künftig ein beträchtlicher, nach den Erfahrungen seit Inkrafttreten des BDSG im Jahre 1978 aber wenig nutzbringender Aufwand vermeiden. Teilweise wird befürwortet, bei den privaten Stellen, die weder einen Datenschutzbeauftragten zu bestellen haben noch der Meldepflicht unterliegen, die Transparenz der innerbetrieblichen Datenverarbeitung dadurch herzustellen, daß diese Stellen auf Anfrage jedermann in geeigneter Weise „meldungsrelevante" Angaben verfügbar machen.

- **Zulässigkeit der Datenverarbeitung**

  Die Vorschriften über die Datenverarbeitung für eigene Zwecke und die geschäftsmäßige Datenspeicherung für Zwecke der Übermittlung (§§ 28, 29 BDSG) sind überarbeitungsbedürftig. Es sollen Bestimmungen geschaffen werden, die mit der erforderlichen Regelungstiefe aufzeigen, unter welchen Voraussetzungen die Verarbeitung personenbezogener Daten zulässig ist. Die geltenden Regelungen haben – auch aufgrund der hierzu nur spärlich ergangenen Rechtsprechung – keine deutlichen Konturen angenommen. Der Umsetzungsbedarf wird zu einem Teil durch die Vorgaben der Richtlinie zur Verarbeitung besonders schützenswerter Daten (Artikel 8) aufgezeigt. Ebenfalls regelungsbedürftig im privaten Bereich ist die Bindung der Datenverarbeitung an bestimmte Zwecke, die nach der Richtlinie bereits bei der Datenerhebung festzulegen sind (Erwägungsgrund 28).

- **Grenzüberschreitender Datenverkehr**

  Für den grenzüberschreitenden Datenverkehr in Drittländer, die kein angemessenes Datenschutzniveau aufweisen, besteht Regelungsbedarf.

- **Videoüberwachung**

  Moderne Videotechnik wird zunehmend genutzt, um Geschäftsräume, Verkehrseinrichtungen, Grundstücke, Arbeitsplätze und Geldautomaten zu überwachen. Dort, wo die Technik sichtbar ist oder wo auf sie hingewiesen wird, schafft sie nach den meisten Erfahrungen mehr Sicherheit. Auch hilft sie, in Verdachtsfällen Abläufe und Geschehnisse zu rekonstruieren. Die Regelungen des derzeit geltenden BDSG sind aber nur anwendbar, wenn öffentliche Stellen Videotechnik nutzen. Für den privaten Bereich werden damit wichtige Fragen wie nach der Transparenz für den Betroffen, der Zulässigkeit, dem Umfang und dem Zeitpunkt der Löschung von Videoaufzeichnungen nicht beantwortet. Auch die gesetzlichen Regelungen und

die Rechtsprechung zum Recht am eigenen Bild helfen hier nicht weiter. Ich halte es daher für erforderlich, das BDSG hierzu entsprechend zu ergänzen.

- **Chipkarten**

  Der Einsatz von Chipkarten bereitet rechtliche Schwierigkeiten. Der Fall, daß der Betroffene seine Daten in seinem Herrschaftsbereich mit sich führt und allein oder im Zusammenwirken mit verschiedenen Stellen ganz unterschiedliche Verarbeitungen auslöst, ist im bisherigen Modell des BDSG nicht adäquat zu erfassen. Es ist daher durch eine spezielle Regelung für Chipkarten klarzustellen, wer die datenschutzrechtliche Verantwortung wofür trägt, und sicherzustellen, daß der Betroffene vor Einwilligung ausreichend Kenntnis von den Verantwortlichkeiten, Abläufen und Risiken erlangt (s. auch Nrn. 2.1.5 sowie u. a. 9.2.4 und 9.3).

- **Private Sicherheitsunternehmen**

  Das Geschäftsfeld privater Sicherheitsdienste hat enorm zugenommen. Bei der Überwachung von Personal und Kunden, aber auch beim Einsatz in U-Bahnen, gibt es enge Kontakte mit dem Publikum und eine intensive Verarbeitung personenbezogener Daten. Die Regelungen des BDSG sind zu allgemein, um die Rechte der Betroffenen angesichts der besonderen Risiken dieser Branche sicherzustellen. Es gilt zu regeln, welche Daten „private Hilfssheriffs" erheben dürfen, unter welchen Voraussetzungen und zu welchem Zweck dies möglich sein soll, an wen die Daten weitergegeben werden dürfen und wann sie zu löschen sind.

31.2 Wesentliche Einzelprobleme

31.2.1 Datenschutzbeauftragter

Bei den Verhandlungen in Brüssel zur EG-Datenschutzrichtlinie (vgl. 15. TB Nr. 33.1.4.7 und oben Nr. 2.1) war es mir ein großes Anliegen, das Modell des betrieblichen Datenschutzbeauftragten europaweit bekanntzumachen. In der verabschiedeten Fassung sieht die Datenschutzrichtlinie als Alternative zur Meldepflicht vor, daß der für die Verarbeitung Verantwortliche eine „unabhängige Überwachung" des Datenschutzes durch einen Datenschutzbeauftragten sicherstellt (Artikel 18 Abs. 2). Es ist daher anzunehmen, daß es schon bald betriebliche Datenschutzbeauftragte in anderen Mitgliedstaaten geben wird.

In Deutschland besteht im nicht-öffentlichen Bereich seit jeher die gesetzliche Pflicht, einen betrieblichen Datenschutzbeauftragten zu bestellen. Meine Erfahrungen mit dem Modell des betrieblichen Datenschutzbeauftragten, die – aufgrund der Zuständigkeiten – nicht aus Kontrollen, sondern aus vielen Besprechungen, Vorträgen und Informationsbesuchen resultieren, sind im wesentlichen positiv. Allerdings weisen zwei Untersuchungen zum betrieblichen Datenschutzbeauftragten (Fachhochschule Ulm und Gesellschaft für Datenschutz und Datensicherheit) auf einige Probleme hin, z. B. hinsichtlich der Ausbildung oder der für die Aufgabenerfüllung zur Verfügung gestellten Arbeitszeit. Ich verspreche mir jedoch von der Einführung einer anlaßfreien Kontrolle der Aufsichtsbehörden eine Beseitigung solcher Defizite, insbesondere weil diejenigen Unternehmen, die den Datenschutz als eine vernachlässigenswerte Größe behandeln, spüren werden, wie wichtig ein gut ausgebildeter, informierter und im Unternehmen voll eingebundener und akzeptierter Datenschutzbeauftragter ist. Ferner ist eine Art Betriebsgarantie für guten Datenschutz nicht nur nach meinen Erfahrungen mittlerweile ein Marketingargument und darüber hinaus auch noch imagefördernd.

31.2.2 Datenerhebung im Wertpapierhandel und durch Kopie von Ausweisdokumenten

Das seit dem 1. Januar 1995 geltende Wertpapierhandelsgesetz (WpHG) haben Kreditinstitute zum Anlaß genommen, im Rahmen der Anlageberatung mit Hilfe von Fragebögen umfangreiche Daten über ihre Kunden zu erheben. Nach Privatkonten, der Höhe des Verfügungskredits, dem Sparverhalten, dem Eigenvermögen wurde ebenso gefragt wie nach Versicherungsverträgen, Erbschaften oder dem Namen des Steuerberaters. Durch die Gestaltung der Fragebögen und des Erhebungsverfahrens wurde bei den Kunden der Anschein erweckt, sie seien zur Auskunft verpflichtet. Tatsächlich sind die Kreditinstitute zwar nach dem WpHG verpflichtet, Angaben zu verlangen, soweit dies zur Wahrung der Interessen ihrer Kunden und im Hinblick auf Art und Umfang der beabsichtigen Geschäfte erforderlich ist. Diese Anforderungen dienen jedoch dem Kundeninteresse an einer sachgerechten und individuellen Beratung und sind daher absolut freiwillig. Eine entsprechende Aufklärung ist aber fast durchweg unterblieben, vielleicht weil die Institute auch ein Eigeninteresse an den Angaben haben.

Die Aufsichtsbehörden haben diese Bedenken gegenüber den Kreditinstituten zum Ausdruck gebracht und entsprechende Änderungen angemahnt. Dem Bundesaufsichtsamt für den Wertpapierhandel, das für die Überwachung der Verhaltenspflichten nach dem WpHG zuständig ist und hierfür von den Kreditinstituten zu beachtende Richtlinien erstellt, habe ich im Einvernehmen mit den Aufsichtsbehörden mitgeteilt, in welcher Weise Datenschutzbelange eingehalten werden sollen. Danach haben Kreditinstitute ihre Kunden auf die Freiwilligkeit der Angaben hinzuweisen und müssen sich jeweils auf die Angaben beschränken, die für eine anleger- und anlagegerechte Beratung erforderlich sind. Wenn nicht der Anlageberater den Kunden persönlich anspricht, sollten Fragebögen verwendet werden, die es gestatten, optional Angaben zu machen.

Probleme bei Form und Inhalt von Datenerhebungen zeigten sich auch bei der Identifizierung von Bankkunden durch Kreditinstitute. Unter Berufung auf Vorschriften des Geldwäschegesetzes und der Abgabenordnung fertigten Kreditinstitute bei einer Konto- oder Depoteröffnung generell Kopien der vorgelegten Ausweisdokumente. Tatsächlich ist die Kopie des Ausweisdokumentes jedoch nur in bestimmten, nach

dem Geldwäschegesetz identifizierungspflichtigen Vorgängen gesetzlich vorgesehen. Damit wird es den Banken erleichtert, ihren Identifizierungspflichten nachzukommen. Für die Kreditinstitute lag es nahe, aus praktischen Erwägungen diese Verfahrensweise schon bei Kontoeröffnung anzuwenden. Die Abgabenordnung erfordert bei Kontoeröffnung jedoch nur Aufzeichnungen aus Ausweisdokumenten, um die Identität des Kunden eindeutig zu bestimmen. In der Regel reichen hierfür Name, Anschrift und Geburtsdatum, ggf. Nummer des Dokuments sowie Ausstellungsbehörde aus. Keinesfalls sind die weiteren aus einer Ausweiskopie ersichtlichen Informationen erforderlich. Für die Speicherung von Augenfarbe, Größe, Geburtsort oder Aussehen (Lichtbild) lag regelmäßig auch eine Einwilligung nicht vor. Die Erhebung erfolgte insofern ohne rechtliche Legitimation und quasi auf Vorrat. Auch gegen diese unzulässige Praxis sind Aufsichtsbehörden vorgegangen, wenngleich einige sich durch den fraglichen Dateibezug bei einer nur aktenmäßigen Ablage der Kopien in ihrer Kontrollbefugnis eingeschränkt sahen.

31.2.3 Scoring-Verfahren am Beispiel der SCHUFA

Die SCHUFA beabsichtigt, für ihre Vertragspartner künftig einen sog. Scorewert (score = Punktzahl) über Betroffene zu ermitteln und zu beauskunften. Im Bereich des Versandhandels sowie bei Handels- und Wirtschaftsauskunfteien ist der Einsatz von Scoring-Verfahren bereits weit verbreitet. Bei diesen Verfahren wird aus einem Datenbestand mittels mathematisch-statistischer Verfahren ein Scorewert erstellt, der die Wahrscheinlichkeit für den Eintritt eines bestimmten Ereignisses wiedergibt. Dem Empfänger dieser Information bleibt es überlassen festzulegen, wie diese Risikoprognose in bezug auf sein Geschäftsinteresse zu bewerten ist. Die SCHUFA hat vor, ihren gesamten Datenbestand zu nutzen, um Scorewerte zu bilden. Aus ihrer Verfahrensbeschreibung läßt sich derzeit noch nicht klar erkennen, inwieweit auch soziodemographische Annahmen und Erfahrungswerte, wie beispielsweise Alter, Wohngegend oder Familienstand mit einfließen werden. Der auf Verlangen eines Vertragspartners gebildete Wert soll weitergegeben, jedoch nicht dauerhaft im SCHUFA-Datenbestand gespeichert werden.

Ich teile nicht die bei den Aufsichtsbehörden vorherrschende Meinung, daß eine Beeinträchtigung schutzwürdiger Belange nicht zu erwarten sei. Denn die SCHUFA fügt durch die Bildung eines Scorewertes den Daten des Betroffenen einen zusätzlichen Wert hinzu, der diesen Daten einen bestimmten Stellenwert im Gesamtfeld der SCHUFA-Datei zuweist und den Charakter einer Bewertung hat. Meine Bedenken habe ich den Aufsichtsbehörden mitgeteilt und darauf hingewiesen, daß – unabhängig von der Frage, ob eine Speicherung des Scorewertes im Rechtssinne erfolgt – die von den Vertragspartnern jederzeit abrufbare Information auch dem Betroffenen mitgeteilt werden müsse, wenn er eine Auskunft verlangt. Der Umfang des Auskunftsanspruchs nach dem BDSG sollte die Regelungen der EG-Datenschutzrichtlinie zu automatisierten Einzelentscheidungen (Artikel 12 i. V. m. Artikel 15) berücksichtigen und den durch die Datenverarbeitung gewonnenen Wert mit umfassen. Denn es ist nicht auszuschließen, daß dieser Scorewert für die Einschätzung der Kreditwürdigkeit wesentliche Bedeutung erlangt. Für mich ist auch fraglich, ob die SCHUFA im Falle des Scorewerts tatsächlich „nur objektive Daten" übermittelt, wie es in der SCHUFA-Klausel festgelegt ist. Der Düsseldorfer Kreis hat sich hingegen darauf beschränkt, der SCHUFA zu empfehlen, einen Hinweis auf das Scoring-Verfahren in das Merkblatt zur SCHUFA-Klausel aufzunehmen und darüber hinaus sicherzustellen, daß die Vertragspartner, die an Privatpersonen Warenkredite vergeben, den Scorewert nur zu deren Gunsten nutzen und im Falle eines Auskunftsbegehrens das Scoring-Verfahren allgemein erläutern. Mir ist diese Position nicht recht verständlich, da eine Nichtberücksichtigung des Scorewertes für den Empfänger eben doch die Bedeutung hat, daß der – grundsätzlich in Betracht zu ziehende – Scorewert ungünstig sein muß.

31.2.4 Allfinanzklauseln

Die Versicherungswirtschaft nutzt seit längerer Zeit Einwilligungsklauseln für die Datenweitergabe für Kundenwerbung im Rahmen von Allfinanzkonzepten, die mit den Aufsichtsbehörden abgestimmt sind (s. 15. TB Nr. 32.2). Eine entsprechende Abstimmung wird auch zwischen der Kreditwirtschaft und den obersten Aufsichtsbehörden angestrebt. Die Einwilligung ermöglicht es, den Kunden umfassend zu beraten und ihm alle Dienstleistungen der Unternehmen des gleichen „Allfinanzverbundes" (im Verbund bzw. Konzern kooperiende Unternehmen aus dem Banken-, Versicherungs- und Bausparkassenbereich) anzubieten, ohne im Einzelfall die Zustimmung für die Beiziehung der Daten aus bestehenden Verträgen erbitten zu müssen. Übermittelt werden dabei nicht nur allgemeine Angaben, wie etwa „Bausparvertrag 1994 abgeschlossen", sondern umfangreiche, mitunter besonders schützenswerte Daten, wie z. B. Kontostände, Einlagen, Kredite und Verwahrungsgeschäfte, jeweils mit weiteren Spezifikationen. Empfänger der Daten sind neben den Unternehmen auch deren Vermittler und Vertreter, die meist im regionalen Umfeld ihre Kunden beraten.

Die konkrete Ausgestaltung der Klauseln bereitet Schwierigkeiten. Die Kreditwirtschaft hält es für angemessen, die Einwilligungserklärung drucktechnisch hervorzuheben und mit dem Hinweis zu verbinden, daß die Erklärung ohne Folgen für den Vertrag gestrichen oder jederzeit widerrufen werden kann. Ich halte das für nicht ausreichend. Da die Erklärung meist Teil umfangreicher allgemeiner Geschäftsbedingungen sein wird, besteht die Gefahr, daß sie vom Kunden gar nicht zur Kenntnis genommen wird. Aus meiner Sicht muß daher sichergestellt sein, daß der Kunde tatsächlich eine Auswahlentscheidung trifft. Dies könnte etwa durch gesonderte Unterschrift oder durch Ankreuzen erfolgen. Damit würde auch den Anforderungen der EG-Datenschutzrichtlinie (s. o. Nr. 2.1) entsprochen, welche vorsieht, daß der Betroffene „in Kenntnis der Sachlage" (Artikel 2 lit. h)) und „ohne jeden Zweifel" (Artikel 7 lit. a)) einwilligt.

32 Europa und Internationales

32.1 Europarat

Für das „Übereinkommen zum Schutz des Menschens bei der automatischen Verarbeitung personenbezogener Daten" (Europaratskonvention 108) fand sich im Berichtszeitraum kein neuer Signatarstaat. Von Griechenland wurde die Konvention am 11. August 1995, als mittlerweile 17. Mitgliedstaat, ratifiziert. Hierbei ist anzumerken, daß Griechenland trotz Ratifizierung – und Inkraftsetzung am 1. Dezember 1995 – als letzter der Mitgliedstaaten der Europäischen Union noch nicht über ein eigenes Datenschutzgesetz verfügt (s. u. Nr. 32.3.1).

Der Schweizerische Bundesrat verabschiedete 1995 eine Botschaft mit dem Ziel der Ratifikation der Konvention 108. Nachdem die Kantone im Rahmen des Anhörungsverfahren im vergangenen Jahr im wesentlichen Zustimmung signalisiert haben, wird mit den weiteren parlamentarischen Beratungen für das laufende Jahr 1997 gerechnet.

Die von der Projektgruppe Datenschutz des Europäischen Ausschusses für rechtliche Zusammenarbeit (CJ-PD) ausgearbeitete „Empfehlung Nr. R (95) 4 des Ministerkomitees an die Mitgliedstaaten zum Schutz personenbezogener Daten auf dem Gebiet der Telekommunikationsdienste, unter besonderer Bezugnahme auf Telefondienste" wurde am 7. Februar 1995 vom Ministerkomitee angenommen. Die Empfehlung enthält insbesondere Bestimmungen, die auf Abonnentenverzeichnisse, die Verwendung von Daten zu Zwecken des Direktmarketings, die detaillierte Rechnungsstellung, interne Telefonzentralen, die Identifizierung der Rufnummer, die Um- oder Weiterleitung von Anrufen und die Verwendung von Mobiltelefonen Anwendung finden.

Eine Empfehlung zum Schutz medizinischer Daten war Gegenstand einer intensiven Koordinierungstätigkeit der Mitgliedstaaten der Europäischen Union im Hinblick auf die Frage der Vereinbarkeit der Empfehlung mit der EG-Datenschutzrichtlinie (s. o. Nr. 2.1). Die Empfehlung wurde vom Lenkungsausschuß für rechtliche Zusammenarbeit (CDCJ) im November 1996 abschließend beraten und soll im ersten Halbjahr 1997 dem Ministerkomitee zur Annahme vorgelegt werden.

Auch der Empfehlungsentwurf zum Schutz personenbezogener Daten, die für statistische Zwecke erhoben und verarbeitet werden, war Gegenstand der Koordinierungstätigkeit der EU-Mitgliedstaaten hinsichtlich ihrer Vereinbarkeit mit der Datenschutzrichtlinie. Die im November 1996 von der Projektgruppe Datenschutz (CJ-PD) einstimmig angenommene Empfehlung soll im März 1997 im Lenkungsausschuß für rechtliche Zusammenarbeit (CDCJ) beraten und anschließend dem Minsterkomitee zur Annahme vorgelegt werden.

Noch im Entwurfsstadium befindet sich eine Empfehlung zum Schutz personenbezogener Daten bei der Erhebung und Verarbeitung für Versicherungszwecke. In den Beratungen wurde bisher vorrangig der Inhalt der Einwilligungsklausel behandelt und die Frage erörtert, ob es sinnvoll sei, die den Finanzbereich betreffenden Daten den besonders schützenswerten Daten zuzuordnen.

Im Rahmen der neueingerichteten Arbeitsgruppe 15 (Neue Technologien) wurden als Schwerpunkte der künftigen Arbeit die Bereiche Datenautobahnen, Chipkarten und Verkehrskontrollsysteme bestimmt. In diesem Jahr wird entschieden, ob eine weitere Arbeitsgruppe (als AG 16) eingerichtet werden soll, die sich speziell und ausschließlich mit einem der vorstehenden Themen befaßt.

32.2 Internationale Zusammenarbeit der Datenschutzkontrollinstanzen

32.2.1 Die Konferenz der Datenschutzbeauftragten der Europäischen Union

Auf ihrer Konferenz in Lissabon am 6./7. April 1995 hoben die Datenschutzbeauftragten der Mitgliedstaaten der Europäischen Union die Notwendigkeit eines hohen gemeinsamen Datenschutzniveaus in der entstehenden europäischen Informationsgesellschaft hervor. Sie unterstrichen die Bedeutung der zum damaligen Zeitpunkt vom Rat beschlossenen und gerade vom Europäischen Parlament in zweiter Lesung beratenen allgemeinen Datenschutzrichtlinie und mahnten ihre umgehende Verabschiedung an (s. o. Nr. 2.1.1). Die Konferenz verabschiedete auf Vorschlag der Arbeitsgruppe Telekommunikation unter dem Vorsitz des Berliner Datenschutzbeauftragten eine Entschließung zur Telekommunikation und zur Informationsgesellschaft. Unter dem Motto „Datenautobahnen nur mit Leitplanken für den Datenschutz" wiesen sie besonders auf die Notwendigkeit eines hohen gemeinsamen Datenschutzniveaus in der entstehenden europäischen Informationsgesellschaft hin. In Anbetracht der bevorstehenden Annäherung des Fernmelde- und Rundfunkwesens (Multimedia-Anwendungen) seien ein hohes Datenschutzniveau und die Wahlfreiheit des Einzelnen Vorbedingungen für die öffentliche Akzeptanz, ohne die die Informationsgesellschaft nicht Realität werden könne. Die Konferenz setzte sich ferner für die Verbesserung des Entwurfs einer Richtlinie für den Datenschutz in digitalen Netzen (ISDN-Richtlinie) ein, zu der mittlerweile ein gemeinsamer Standpunkt beschlossen wurde, der dem Europäischen Parlament in zweiter Lesung vorliegt (s. o. Nr. 10.3). Darüber hinaus befaßte sich die Konferenz mit dem Entwurf einer Konvention für die europäische Polizeibehörde EUROPOL, der am 26. Juli 1995 von den Mitgliedstaaten der EU gezeichnet wurde und dessen Ratifizierung derzeit in den nationalen Parlamenten beraten wird (s. o. Nr. 11.5.1).

Die Konferenz vom 24. und 25. April 1996 in Manchester befaßte sich mit den Themenschwerpunkten EG-Datenschutzrichtlinie und mangelhafter Datenschutz bei Datenverarbeitungen und -übermittlungen an und durch europäische Dienststellen. Unter Hinweis auf die Forderungen der Kopenhagener Resolution vom 8. September 1995 über die Verankerung eines europäischen Grundrechts auf Datenschutz in einer künftigen Unionsverfassung, die Schaffung verbindlicher Datenschutzregelungen für

die Organe und Einrichtungen von Gemeinschaft und Union und die Einrichtung einer unabhängigen europäischen Datenschutzkontrollinstanz (s. o. Nr. 2.2 und Anlage 4) wandten sich die Datenschutzbeauftragten erneut an die Europäische Kommission, den Ministerrat und die Mitgliedstaaten und mahnten die dringende Umsetzung der Kopenhagener Forderungen an.

32.2.2 Die Internationale Datenschutzkonferenz

Die europäische Datenschutzrichtlinie bildete auch einen Themenschwerpunkt der 17. Internationalen Konferenz vom 6. und 7. September 1995 in Kopenhagen. In einem Redebeitrag habe ich meine Eindrücke und Erfahrungen als Vorsitzender der Arbeitsgruppe „Wirtschaftsfragen/Datenschutz" während der deutschen Ratspräsidentschaft in der EU (s. 15. TB Nr. 33.1) geschildert und eine erste Einschätzung der Richtlinie und ihres voraussichtlichen Umsetzungsbedarfs in das nationale Recht gegeben (s. o. Nr. 2.1.5). Weitere Themen bildeten der Arbeitnehmerdatenschutz, die Erhebung und Verarbeitung personenbezogener Daten in wissenschaftlicher Forschung und Statistik sowie der Schutz des Individuums angesichts der technischen Entwicklungen an der Schwelle zum Informationszeitalter.

Die 18. Internationale Datenschutzkonferenz am 18. und 19. September 1996 in Ottawa stand unter dem Thema „Privacy Beyond Borders". Die Mehrzahl der Referate und Beiträge befaßte sich mit den beiden Hauptthemen der derzeit in den meisten Industrieländern geführten Debatte um die Zukunft des Datenschutzes, nämlich mit den Auswirkungen der europäischen Datenschutzrichtlinie auf die Rechtsordnungen in den Staaten außerhalb der Gemeinschaft, den sog. Drittstaaten (s. o. Nr. 2.1.4) und mit den Fragen nach Stand und Perspektiven der Allianz von Technik und Datenschutz.

Stand und Chancen von „Privacy Enhancing Technologies" bildeten das Zentrum des zweiten Hauptthemas der Tagung. Die Beiträge hierzu befaßten sich mit Datenschutzfragen bei Multimedia, Internet und Verschlüsselungsfragen sowie den spezifischen Risiken und sozialethischen Implikationen der Speicherung und Auswertung genetischer Informationen. In einem Gesprächskreis zum Thema „Data Protection Law and Genetics" hatte ich Gelegenheit, aus Sicht des Datenschutzes und vor dem Hintergrund der Gesetzgebung und Rechtsprechung in der Bundesrepublik Deutschland zu der ebenso interessanten wie umstrittenen Thematik der Genomanalyse im Strafverfahren Stellung zu nehmen (s. o. Nr. 6.2).

32.3 Entwicklung des Datenschutzes im Ausland

Bei den weltweiten Bestrebungen des Datenschutzrechts sind Mitte der neunziger Jahre im wesentlichen vier Entwicklungslinien festzustellen, die sich in ihrem regionalen Bezug wie folgt unterscheiden lassen:

- die mit der Umsetzung der EG-Richtlinie befaßten Mitgliedstaaten der Europäischen Union (s. u. Nr. 32.3.1),
- die mittel- und osteuropäischen (MOE-)Staaten, in denen erste Datenschutzgesetze vorliegen (s. u. Nr. 32.3.2),
- Länder der westlichen Hemisphäre außerhalb der EU (Australien, Kanada und Neuseeland), die schon bisher über eine ausgeprägte Datenschutzkultur verfügten (s. u. Nr. 32.3.3) und
- exportorientierte Staaten wie Hongkong und Taiwan, die sich den rechtlichen Anforderungen ihrer Handelspartner stellen (s. u. Nr. 32.3.4).

32.3.1 Die Mitgliedstaaten der Europäischen Union

32.3.1.1 Umsetzung der EG-Datenschutzrichtlinie

Mit den Beratungen der Vorschläge für eine europäische Datenschutzrichtlinie aus den Jahren 1990 und 1992 waren zehn Ratspräsidentschaften befaßt, die alle engagiert das vorgegebene Ziel einer europaweiten Harmonisierung des Datenschutzrechts zur Förderung des freien Verkehrs personenbezogener Daten unter gleichzeitiger Stärkung des Rechts der Unionsbürger auf Achtung ihrer Persönlichkeitsrechte und insbesondere ihrer Privatsphäre verfolgt haben (zur deutschen Präsidentschaft in der 2. Jahreshälfte 1994 vgl. 15. TB Nr. 33.1.1). Zur Zeit der Brüsseler Beratungen gab es mit Blick auf das innerstaatliche Recht der Mitgliedstaaten drei verschiedene Konstellationen hinsichtlich des Standes der Gesetzgebung auf dem Gebiet des Datenschutzrechts.

Da gab es die Mitgliedstaaten, die schon lange vor den Kommissionsvorschlägen der neunziger Jahre über ein eigenes Datenschutzrecht verfügten, und deren rechtliche Vorstellungen zum Teil Eingang in die Richtlinie gefunden haben. So finden sich in der Richtlinie eine ganze Reihe von kombinierten Regelungselementen aus den Datenschutzsystemen der Mitgliedstaaten, wie z. B.

- die Dateienregistrierung nach französisch/britisch/skandinavischem Muster,
- der Sonderschutz für sensitive Daten, der in Frankreich und Irland eine besondere Rolle spielt,
- Ausnahmen zugunsten der wissenschaftlichen Forschung nach dänischem Vorbild,
- eine Unterstützung der branchen- oder berufsorientierten Selbstregulierung in Anlehnung an das niederländische Modell sowie
- die Verbots-Erlaubnis-Mechanik des deutschen Datenschutzrechts.

Eine zweite Gruppe bildeten diejenigen Mitgliedstaaten, die im Laufe der Brüsseler Beratungen nationale Rechtsvorschriften zum Schutz personenbezogener Daten geschaffen haben (Portugal 1991, Belgien und Spanien 1992). Naturgemäß folgen diese Gesetze in vielerlei Hinsicht der Richtlinie.

Griechenland und Italien dagegen verfügten auch bei Verabschiedung der Richtlinie am 24. Oktober 1995 noch nicht über nationale Datenschutzgesetze.

In allen Ländern der Gemeinschaft sind mittlerweile die entsprechenden Gremien mit der Anpassung des

nationalen Datenschutzrechts befaßt, sei es im Vorfeld parlamentarischer Überlegungen wie z. B. in Großbritannien, wo der Data Protection Registrar die öffentliche Debatte mit einer detaillierten Stellungnahme angeregt hat, sei es in Fachkommissionen wie in Dänemark, Luxemburg oder Österreich, oder sei es, daß bereits ein Regierungsentwurf vorgelegt wurde, wie kürzlich in den Niederlanden. In Italien ist zu Beginn des Jahres 1997 das Datenschutzgesetz in Kraft getreten, welches in enger Anlehnung an die Vorgaben der Richtlinie im übrigen eine Trennung zwischen öffentlichem und privatem Bereich vorsieht und u. a. Regelungen über das Meldeverfahren, die Datenschutzkontrolle, die Datensicherheit und die Übermittlung von Daten in Drittländer enthält. In Griechenland hat es in der Vergangenheit seit dem Jahr 1985 mehrere Entwürfe für ein Datenschutzgesetz gegeben. Der neueste Gesetzentwurf wurde dem Parlament im Juni 1996 vorgelegt. Mit seiner Verabschiedung wird in der ersten Jahreshälfte 1997 gerechnet.

32.3.1.2 Aktuelle Rechtsentwicklungen in einzelnen Mitgliedstaaten

Das aus dem Jahre 1992 stammende **belgische** Datenschutzgesetz ist in seiner letzten Stufe am 1. Juni 1995 in Kraft getreten. Das Gesetz enthält einheitliche Vorschriften für den öffentlichen und den privaten Sektor und gilt für automatisierte und manuelle Dateien, für die es ein Meldesystem vorsieht. Eine Datenschutzkommission hat die Aufgabe, mittels Kontrollen über die Einhaltung und die korrekte Anwendung des Gesetzes zu wachen.

In **Frankreich** ist am 1. Juli 1994 das Gesetz über die Verarbeitung von Daten für Forschungszwecke in Kraft getreten, welches strenge Voraussetzungen für den Datenumgang im Bereich der medizinischen Forschung vorsieht. Es ergänzt das Datenschutzgesetz aus dem Jahre 1978, indem es für bestimmte Datenübermittlungen eine Lockerung oder Aufhebung des Arztgeheimnisses vorsieht, wobei es jedoch im Gegenzug die Befugnisse der französischen Datenschutzbehörde (Commission Nationale de l'Informatique et des Libertés – CNIL) erweitert. Dieser wurden im Hinblick auf die Verarbeitung und Nutzung personenbezogener medizinischer Daten für Forschungszwecke – im öffentlichen wie im nicht-öffentlichen Bereich – umfassende Genehmigungsbefugnisse eingeräumt. Zur Vorbereitung der Entscheidung der CNIL ist einem ihr vorgeschalteten beratenden Ausschuß jedes Forschungsprojekt, in dessen Verlauf personenbezogene Daten verarbeitet werden, im Hinblick auf die angewandten Methoden, die Notwendigkeit des geplanten Datenumgangs und seine Erheblichkeit hinsichtlich des Forschungsziels zur Prüfung vorzulegen. Im Falle eines positiven Bescheids auf der Grundlage des ihr unterbreiteten Vorschlags legt die CNIL dann u. a. den Kreis der Auskunftsberechtigten und der zu informierenden Personen fest, bestimmt die einzuhaltenden Vorkehrungen der Datensicherheit, regelt die Aufbewahrungsdauer der angefallenen Daten und genehmigt grenzüberschreitende Datenübermittlungen. Da dieses umfassende Verfahren ausnahmslos für alle Forschungsprojekte im Zusammenhang mit personenbezogenen Daten gilt, bleibt seine Bewährung in der Praxis abzuwarten.

Das **portugiesische** Datenschutzgesetz aus dem Jahre 1991 wurde im August 1994 um Regelungen über sensitive Daten und den grenzüberschreitenden Datenfluß erweitert. Ebenfalls im Jahre 1994 wurde die nationale Kontrollkommission zum Schutz automatisierter personenbezogener Daten eingerichtet.

Das **spanische** Datenschutzgesetz aus dem Jahre 1993 wurde im Juni 1994 durch ein königliches Dekret (Verordnung) ergänzt, welches detailliertere Vorschriften zum grenzüberschreitenden Datenverkehr, zu den Meldepflichten und zu den Rechten des Betroffenen enthält sowie einzelne Begriffe des Datenschutzgesetzes definiert und erläutert. Im Juli 1994 wurde eine unabhängige öffentliche Institution mit Kontroll- und Eingriffsbefugnissen als Datenschutzbehörde eingerichtet.

32.3.2 Die mittel- und osteuropäischen Staaten

In den Staaten Mittel- und Osteuropas (MOE-Staaten) zeigt sich im Zuge der Wandlung von staatlicher Bevormundung in vielen Lebensbereichen hin zu liberalen Gesellschaftsformen und parlamentarischem Demokratieverständnis auch ein Gespür für den notwendigen Schutz der Persönlichkeitsrechte des Individuums. Daher war es naheliegend, auch die Belange des einzelnen in der im Aufbau begriffenen Informationsgesellschaft in die gesellschaftpolitische und insbesondere in die verfassungsrechtliche Diskussion einzubeziehen.

Die begrüßenswerte Entwicklung bis hin zu konkreten datenschutzrechtlichen Vorstellungen in zahlreichen MOE-Ländern wird jedoch begleitet von bisweilen schwerfälligen Formalisierungen sowohl bei der Datenschutzkontrolle als auch beim Rechtsschutz des einzelnen. So fehlt es in der Regel an einer unabhängigen Kontroll- und Beschwerdeinstanz. Statt dessen wird der Betroffene regelmäßig auf ein gerichtliches Verfahren verwiesen.

Eine Ausnahme bildet insofern **Ungarn**, wo im Mai 1993 das erste Datenschutzgesetz eines MOE-Staates in Kraft getreten ist. Das Gesetz regelt in einer Kombination von Datenschutz- und Informationszugangsrechten u. a. die Datenerhebung, die es nur mit Einwilligung des Betroffenen oder aufgrund eines Gesetzes erlaubt, und sieht Regelungen für den Umgang mit sensitiven Daten sowie Schadensersatz- und Strafbestimmungen vor. Zwischenzeitliche Ergänzungen des Gesetzes enthalten Regelungen über Marktforschung, Direktwerbung und Statistik. Im Juli 1995 wurde der erste Datenschutzbeauftragte vom Parlament gewählt. Er wacht über die Einhaltung der Vorschriften des Datenschutzgesetzes, wobei er über – anlaßbedingte – Kontrollrechte verfügt, und führt ein Melderegister. Seine Unabhängigkeit ist verfassungsrechtlich abgesichert.

Das am 1. Juni 1992 in der damaligen tschechoslowakischen Republik in Kraft getretene Gesetz über den Schutz personenbezogener Daten in Informationssystem habe ich gemeinsam mit meiner schwedischen Kollegin und meinem niederländischen Kol-

legen als vom Europarat bestellte Experten im Frühjahr 1995 für das Parlament der **Tschechischen Republik** im Hinblick auf notwendige Änderungen und Ergänzungen begutachtet. Das derzeit geltende Gesetz bezieht sich auf natürliche Personen im öffentlichen wie im privaten Bereich und erstreckt sich ausschließlich auf automatisierte Dateien. Nur für sensitive Daten ist ein Meldesystem vorgesehen. Die Durchführung des Gesetzes obliegt einer besonderen „Regulierungsbehörde". Die Gewährung von Lizenzen für den grenzüberschreitenden Datenverkehr wird Gegenstand gesetzlicher Sonderregelungen sein.

Nach der Auflösung des tschechoslowakischen Staates gilt auch in der **Slowakei** vorerst das aus dem Jahre 1992 stammende Gesetz. Derzeit wird im Nationalrat der neueingebrachte Entwurf eines Datenschutzgesetzes beraten.

Der Entwurf eines **slowenischen** Datenschutzgesetzes wurde im April 1994 einem Expertengremium des Europarates unterbreitet und danach erneut im Parlament eingebracht, wo die Beratungen zur Zeit noch andauern. Er bezieht sich sowohl auf den öffentlichen als auch auf den privaten Bereich.

Ein **kroatischer** Entwurf für ein Datenschutzgesetz ist kurz vor der Fertigstellung und wird demnächst ebenfalls dem Europarat zur Begutachtung vorgelegt werden.

In der **Ukraine** sind seit 1992 ein Informationsgesetz und seit 1994 ein „Gesetz über den Schutz der Information in automatisierten Systemen" in Kraft, die sich jedoch nicht auf den Datenschutz im westlichen Sinne beziehen. Diesen sieht ein Gesetzentwurf vor, der die Grundsätze der Europaratskonvention 108 berücksichtigt.

Vertreter des **polnischen** Innenministeriums und der Staatsduma der **Russischen Föderation**, die mit mir einen intensiven Gedankenaustausch führten, zeigten sich zuversichtlich in bezug auf die Schaffung von Datenschutzgesetzen in ihren Heimatländern.

32.3.3 Entwicklungen in Übersee – Antworten auf die europäische Herausforderung

Die in der Richtlinie getroffenen Regelungen der Übermittlung personenbezogener Daten in Staaten außerhalb der Europäischen Union (sog. Drittstaaten, s. o. Nr. 2.1.4) ist in diesen Ländern nicht ohne Echo geblieben. Schon heute kann festgestellt werden, daß die Richtlinie bei den Handelspartnern der Gemeinschaft große Beachtung gefunden und jedenfalls weit mehr Reaktionen hervorgerufen hat, als die 1981 beschlossene, inzwischen von 17 Staaten ratifizierte und einer etwa gleich großen Zahl weiterer Staaten gezeichnete Datenschutzkonvention 108 des Europarats (s. o. Nr. 32.1). Die Verabschiedung eines Datenschutzgesetzes in **Hongkong** für den öffentlichen wie für den nicht-öffentlichen Bereich im Jahre 1995 (zum Entwurf s. 15. TB Nr. 33.3) und die Ankündigung der **kanadischen** (zum neuen Datenschutzgesetz der Provinz Québec aus dem Jahre 1993, das erstmals in Kanada auch im privaten Sektor gilt, s. 15. TB Nr. 33.3), der **australischen** und der **neuseeländischen** Regierungen, den Datenschutz auf den gesamten nicht-öffentlichen Bereich auszuweiten, sind eindeutig als Antworten auf die europäische Herausforderung zu verstehen.

Auch die **USA** scheinen sich inzwischen auf die durch die Richtlinie geschaffenen Tatsachen einzustellen. Gegenüber dem Befund, daß sie lediglich über einen fragmentarischen Datenschutz verfügen (der Privacy Act aus dem Jahre 1974 bezieht sich ausschließlich auf die Behörden der Bundesregierung), verweisen offizielle amerikanische Stellen zwar nach wie vor auf die Fülle von bundes- und einzelstaatlichen Regelungen für gesonderte Bereiche sowie auf die meist an den OECD-Leitlinien ausgerichtete branchen- und unternehmensbezogene Selbstregulierung (s. o. Nr. 2.1.4 zu der für die Europäische Kommission gefertigten Studie von Schwartz und Reidenberg zum Datenschutzrecht in den Vereinigten Staaten). Doch zeichnet sich neuerdings eine Bereitschaft ab, den europäischen Erwartungen entgegenzukommen, wobei die Überlegungen aber in erster Linie auf institutionelle und verfahrensmäßige Lösungen zu zielen scheinen, durch die die Kooperation mit den europäischen Datenschutzinstanzen verbessert werden könnte. Ich unterstütze die Kommission in dem Bemühen, die amerikanische Seite von der Nützlichkeit einer möglichst umfassenden Reaktion zu überzeugen.

32.3.4 Erstes Datenschutzgesetz in Taiwan – Reformbestrebungen in Israel

Abgesehen von der schubartigen Entwicklung in den MOE-Staaten (s. o. Nr. 32.3.2) ist im Berichtszeitraum auch weltweit die Anzahl der Länder mit datenschutzrechtlichen Regelungen weiter gestiegen.

So gibt es in der nationalchinesischen Republik **Taiwan** seit 1995 ein Datenschutzgesetz, dessen Regelungsziel der Schutz des Persönlichkeitsrechts bei der automatisierten Datenverarbeitung durch „vernünftigen Umgang" mit persönlichen Daten ist. Zu den Prinzipien des Gesetzes, das – ähnlich dem deutschen BDSG – zwischen der Datenverarbeitung durch öffentliche und nicht-öffentliche Einrichtungen unterscheidet, zählt insbesondere, daß die Erhebung persönlicher Daten oder ihre Verarbeitung nur aufgrund der schriftlichen Einwilligung des Betroffenen oder einer gesetzlichen Anordnung möglich ist. Das Datenschutzgesetz enthält Regelungen im Hinblick auf die Zweckbindung sowie Vorschriften zum Schadensersatz (Verschuldenshaftung im öffentlichen Bereich, Beweislastumkehr im nicht-öffentlichen Bereich, in beiden Fällen auch die Möglichkeit der Geltendmachung eines Nichtvermögensschadens) sowie detaillierte Strafbestimmungen. Der Grund für die umfassenden Schadensersatz- und Strafvorschriften – sie machen ein Drittel des gesamten Gesetzestextes aus – liegt im Fehlen einer Datenschutzkontrolle durch betriebliche/behördliche Datenschutzbeauftragte bzw. einer externen Kontrollstelle. Dem Betroffenen ist damit – ähnlich den Regelungen in den meisten MOE-Staaten (s. o. Nr. 32.3.2) – lediglich der Rechtsweg zu den Zivil- und Strafgerichten eröffnet.

In **Israel** wird derzeit der Entwurf für eine Novelle zum Datenschutzgesetz aus dem Jahre 1981 parlamentarisch beraten. Dieser sieht u. a. eine Einschränkung der Meldepflichten, die Einführung von Regelungen zum Direktmarketing und die Neufassung der Verantwortlichkeiten der datenverarbeitenden Stelle vor. Im Oktober 1995 ist das Computer-Gesetz vom Parlament verabschiedet worden, welches u. a. Schadensersatzregelungen für den Mißbrauch von Computerdaten und die Verwendung von Computerviren enthält.

33 Tips und Hinweise für eine ordnungsgemäße Datenverarbeitung

33.1 Namen von Behördenmitarbeitern weltweit verfügbar?

Sowohl innerhalb der Bundesverwaltung als auch zwischen der Bundesverwaltung und anderen Stellen wird künftig in noch stärkerem Maße über Datennetze, wie dem Internet/WWW, kommuniziert. Eine besondere Bedeutung kommt dabei der Einführung bzw. Intensivierung der elektronischen Post, der „E-Mail" zu; damit eine Adressierung der Nachrichten – Informationen, Briefe, Rundschreiben usw. – möglich ist, benötigen sowohl die Dienststellen selbst als auch ihre Mitarbeiter ein „elektronisches Postfach". Diese Postfächer müssen in öffentliche Adreßverzeichnisse eingetragen und so allen Nutzern des Netzes zugänglich gemacht werden. Darüber hinaus kann es zweckdienlich sein, auch die Organigramme von Behörden im Netz zur Verfügung zu stellen.

Einige Ministerien hatten mich um Prüfung der Frage gebeten, ob eine solche Veröffentlichung datenschutzrechtlich zulässig ist. Ich vertrete hierzu folgende Auffassung:

Gegen die Angabe der Namen und Dienst-/Amtsbezeichnungen der Referatsleiter bei der Veröffentlichung von **Organigrammen** im Internet/WWW bestehen aus Sicht des Datenschutzes keine Bedenken.

Hinsichtlich der Veröffentlichung von **E-Mail-Adressen** habe ich das zuständige Bundesministerium des Innern auf die Notwendigkeit der Schaffung einheitlicher Regelungen für alle Bundesbediensteten hingewiesen. Ich habe dem Ministerium mitgeteilt, daß ich die Veröffentlichung der E-Mail-Adressen der Referatsleiter als unbedenklich ansehe, eine Veröffentlichung der E-Mail-Adressen der anderen Mitarbeiter aber wohl nur mit deren Einwilligung erfolgen könne. Bei dieser Bewertung bin ich davon ausgegangen, daß – wie es die Konventionen des Informationsverbundes Bonn-Berlin (IVBB s. u. Nr. 34.2) vorsehen – Name und Vorname der Betroffenen Bestandteile der E-Mail-Adresse sind. Eine sogenannte X.400-E-Mail-Adresse sieht dann z. B. so aus: C = de; A = bund 400; P = bfd; S = mustermann; G = adam.

Auch sollten die Betroffenen vorher über die beabsichtigte Veröffentlichung informiert werden, um ihnen zu ermöglichen, den Sachverhalt zu verstehen sowie dessen Folgen für die dienstlichen Aufgaben einschätzen zu können.

33.2 Kontrolle von IT mit IT

Im Berichtszeitraum habe ich die technischen und organisatorischen Maßnahmen zur Gewährleistung der Systemsicherheit eines PC-Netzes unter dem Betriebssystem Novell kontrolliert. Dabei wurde erstmals eine sogenannte Audit-Software benutzt. Diese Software analysiert nach der Installation Systemzustände und erstellt auf Anforderung darüber Reports.

Die Analysemöglichkeiten sind außerordentlich vielfältig. Zum Beispiel können die im System verschlüsselt abgelegten Paßwörter der Benutzer analysiert werden, natürlich ohne daß der „menschliche Prüfer" dabei in deren Kenntnis gelangt. Zur Paßwortgestaltung – die von großer Bedeutung für die Sicherheit gegen unbefugte Nutzung ist – habe ich wiederholt Empfehlungen gegeben (vgl. 14. TB Anlage 13)

Zur Paßwortanalyse wird vom Prüfer eine „Negativdatei" mit unsicheren – weil leicht zu erratenden – Paßwörtern erstellt. Dazu gehören „Banalpaßwörter", wie z. B. Vornamen und auf der Tastatur nebeneinanderliegende Zeichen (asdfgh), aber auch andere häufig benutzte unsichere Paßwörter, wie etwa der rückwärts geschriebene Benutzername.

Die Software verschlüsselt diese Paßwörter, vergleicht das Ergebnis mit dem verschlüsselten Paßwort des Benutzers und nimmt den Benutzer gegebenenfalls in eine „Warnliste" auf, wenn sein Paßwort mit einem aus der Negativdatei übereinstimmt.

Ein anderes Beispiel ist die Kontrolle der sogenannten „Station Restrictions". Mit dieser Funktion können einem Benutzer bestimmte „Clients", also in ein IT-Netz integrierte PC, zugewiesen werden. Er kann sich dann ausschließlich von diesen festgelegten Clients aus am System anmelden. Beispiel: Beihilfebearbeiter können sich nur von den PC in der Beihilfestelle aus beim System anmelden. Die Funktion stellt sicher, daß ein möglicher Angreifer nicht mit einem ihm bekannten Benutzernamen von jeder beliebigen Station Eindringversuche starten kann. Die Pflege dieser Einträge erfordert aber einen gewissen Aufwand. Deshalb wird die Funktion in vielen Systemen nicht benutzt. Die Audit-Software hilft hier; mit ihr kann ein Report erstellt werden, der alle Benutzer mit den für sie zugelassenen Clients auflistet.

Zum Teil sind solche Kontrollen – wie die der Paßwörter – gar nicht, zum Teil wegen des sehr hohen Zeitaufwandes – unter Verwendung von Listen usw. – nur mit nicht vertretbarem Aufwand durchführbar. Die Audit-Software erledigt sie auch in größeren Systemen in nur wenigen Minuten. Der Prüfer wird somit in die Lage versetzt, den Sicherheitszustand eines Systems sehr viel gründlicher zu durchleuchten. Im vorliegenden Fall wurde eine Vielzahl zwar nur kleinerer Mängel festgestellt, die aber in ihrer Gesamtheit eine deutliche Sicherheitslücke darstellten.

Derartige Software wird nach meiner Einschätzung viel zu selten genutzt. Sie ist nicht nur für den externen Prüfer – wie hier den Mitarbeitern meiner Dienststelle – von hohem Wert, sondern auch für den internen IT-Revisor, den behördlichen Datenschutz-

beauftragten und nicht zuletzt für den Administrator des Systems selbst.

33.3 Datenschutzprobleme bei optischen digitalen Speichermedien

Beim Einsatz optischer digitaler Speichermedien (CD-ROM) muß zwischen Datenträgern unterschieden werden, die nur einmal beschreibbar, aber beliebig oft lesbar sind und Datenträgern, die mehrfach beschreibbar und lesbar sind.

Grundsätzlich können **wiederbeschreibbare optische Datenträger** wie Magnetplatten behandelt werden, d. h. die gespeicherten Daten können – auch teilweise – je nach Erforderlichkeit geändert oder gelöscht werden.

Beim Einsatz nur **einmal beschreibbarer Datenträger** kann es dagegen dann Probleme geben, wenn Teile der Daten – z. B. auf berechtigtes Verlangen der Betroffenen – geändert oder etwa wegen des Ablaufs der Speicherfrist gelöscht werden müssen.

Das BDSG und die meisten Landesdatenschutzgesetze definieren das Löschen als „Unkenntlichmachen der Daten". Unkenntlich gemacht sind Daten dann, wenn die Informationen nicht länger aus den ursprünglich gespeicherten Daten gewonnen werden können. Bei Datenträgern der genannten Art können die Daten nicht gelöscht werden. Lediglich die im Datenverwaltungssystem – im Indexsystem oder der Datenbank – vorhandenen Hinweise auf die Daten werden gelöscht.

Der Arbeitskreis „Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eine Orientierungshilfe „Datenschutzrechtliche Aspekte beim Einsatz optischer Datenspeicherung" **(s. Anlage 26)** entwickelt, in der diese Problematik ausführlich beschrieben und Verfahrensweisen vorgeschlagen werden.

33.4 Datenschutz auch im „Grundschutzhandbuch"

Das Bundesamt für Sicherheit in der Informationstechnik – BSI – gibt seit Jahren das IT-Grundschutzhandbuch heraus, ein Hilfsmittel für Verantwortliche im Bereich IT-Sicherheit. Ziel des Handbuches ist es, Hilfestellung beim Erkennen von Gefährdungen und dem Entwickeln von Gegenmaßnahmen zu leisten (vgl. 15. TB Nr. 30.8). Für IT-Systeme mit einem mittleren Schutzbedarf soll damit ein ausreichender Grundschutz erreicht werden; bei Systemen mit einem höheren Schutzbedarf ist stets eine Einzelfallanalyse erforderlich.

Das Grundschutzhandbuch wird auch auf CD-ROM vertrieben und nicht nur von IT-Sicherheitsbeauftragten, sondern auch besonders von Datenschutzbeauftragten und DV-Revisoren angewandt. Es liegt nahe, in einen solchen Leitfaden auch den Aspekt Datenschutz zu behandeln und ihn damit zum Standardwerk für alle, die im IT-Bereich Verantwortung für die Sicherheit tragen, weiterzuentwickeln. Eine Arbeitsgruppe des Arbeitskreises „Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, der auch ein Vertreter des BSI angehörte, hat daher einen Abschnitt „Datenschutz" für das Handbuch erarbeitet. In ihm werden die rechtlichen Grundlagen des Datenschutzes erläutert, die Gefährdungslage beschrieben und Maßnahmeempfehlungen gegeben. Das BSI wird den Beitrag noch mit der Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung abstimmen. Zeitgleich erfolgt die Beteiligung der Aufsichtsbehörden für den nicht-öffentlichen Bereich. Wie ich aus Kontrollen und Beratungen weiß, wird mit dieser Anleitung zur Umsetzung des Datenschutzes einem Bedürfnis der Praktiker in den IT-Bereichen Rechnung getragen.

34 Aus meiner Dienststelle

34.1 Auf- und Ausbau der Informationstechnik in der Dienststelle

Durch die weitere Ausstattung meiner Dienststelle mit Informationstechnik konnten einige Arbeitsabläufe im Hause effektiver gestaltet werden. Es gelang, das in den vergangenen Jahren stetig gestiegene Arbeitsaufkommen mit einer gleichbleibenden Anzahl von Mitarbeitern zu bewältigen. Hierzu trugen unter anderem bei:

- Die Einführung eines elektronischen Schriftgutverwaltungssystems in meiner Registratur, wodurch die Suche nach Schriftstücken vereinfacht und beschleunigt wurde.
- Durch die Ausdehnung der Textverarbeitung auf alle PC-Benutzer des Hauses werden jetzt Texte auch von den Bearbeitern selbst erstellt. Hierdurch wird der zentrale Schreibdienst entlastet und steht für zusätzliche Aufgaben zur Verfügung. So hat er an der Layoutgestaltung meiner Informationsbroschüren mitgewirkt. Auch die Bedienung der IVBB-Kopfstelle (s. u. Nr. 34.2) und meiner Mailbox (s. u. Nr. 34.3) wird vom Schreibdienst unterstützt.
- Die Bearbeitungszeit für Schriftstücke wurde im Durchschnitt reduziert.
- Allen PC-Benutzern ist es grundsätzlich möglich, Texte direkt vom Arbeitsplatz aus per Telefax zu versenden.
- Durch die Bereitstellung von Datenbanken im Rechnernetz stehen den Bearbeitern viele Informationen jetzt direkt am Arbeitsplatz zur Verfügung. So können z. B. Gesetzestexte abgerufen werden, was aufwendige Recherchen in der Bibliothek einspart.

Die überwiegende Zahl der Arbeitsplätze meines Hauses (rund 90 %) ist mit untereinander vernetzten Arbeitsplatzrechnern ausgestattet, was meinen Mitarbeitern auch bei Kontroll- und Beratungsaufgaben zugute kommt.

34.2 Einführung von „Elektronischer Post" in meiner Dienststelle

Die Umsetzung des Beschlusses des Deutschen Bundestages vom 20. Juni 1991 zur Vollendung der Einheit Deutschlands sowie die Beschlußfassung des Bundesrates führen zu einer weiträumigen Aufteilung der Verfassungsorgane mit den Hauptstandorten Berlin und Bonn. Eine Folge hiervon ist die Einführung des Informationsverbundes Berlin-Bonn (IVBB). Er soll die Kommunikation

- zwischen räumlich verteilten Bereichen der einzelnen Ressorts am jeweiligen Standort,
- der Ressorts untereinander innerhalb der Standorte und zwischen den Standorten Berlin und Bonn,
- zwischen den Ressorts und dem Deutschen Bundestag,
- zwischen den Ressorts und dem Bundesrat,
- zwischen den Ressorts und dem Bundespräsidialamt sowie
- mit weiteren Kommunikationspartnern, insbesondere Landesverwaltungen und Stellen der Europäischen Union,

übergreifend sicherstellen.

Einen wesentlichen Teil des IVBB bildet ein elektronisches Mitteilungssystem auf der Basis des X.400 Standards des Comité Consultatif International Télégraphique et Téléphonique (CCITT) bzw. der International Organization for Standardization (ISO), das dem elektronischen Austausch von Dokumenten – Informationen, Briefen, Rundschreiben usw. – der beteiligten Stellen dienen soll (s. o. Nr. 33.1). Ein Anschluß meines Hauses an dieses System ist wegen der häufigen Kommunikation mit vielen Stellen des Parlamentes und der Regierung unerläßlich.

Bereits jetzt ist jeder der PC-Arbeitsplätze meines Hauses über diesen elektronischen Postaustausch erreichbar. Die X.400-Adresse für an mich gerichtete Nachrichten lautet: C = de; A = bund 400; P = bfd; S = poststelle. Es kann aber auch jeder Mitarbeiter direkt adressiert werden. Eine entsprechende Liste können die IVBB-Stellen einem automatisierten „Bulletin Board" entnehmen.

34.3 Einrichtung eines Mailboxsystems für Bürger – Tätigkeitsbericht und Broschüren jetzt auch elektronisch verfügbar –

Wie immer hatten viele Bürger und Journalisten Informationswünsche an mich. Und zunehmend wurde erwartet, daß man automatisiert mit mir kommunizieren kann.

Neben der vorstehend beschriebenen IT-Ausstattung habe ich ergänzend im Frühjahr 1996 die „BfD-BOX" in Betrieb genommen, ein PC-gestütztes Mailboxsystem.

Die BfD-Box dient zum einen für

- Zwecke der Öffentlichkeitsarbeit (Bereitstellung von Informationsbroschüren, Pressemitteilungen, Tätigkeitsberichten – dieser Bericht wird der erste sein – und Kontaktadressen),

zum anderen für die

- Kommunikation mit den Landesbeauftragten für den Datenschutz (Übersenden von Konferenzbeschlüssen, Erarbeitung von Texten in den Arbeitskreisen usw.).

Ferner wird auch den Landesbeauftragten für den Datenschutz eine Plattform geboten, auf der sie sich – innerhalb der BfD-BOX – mit einer eigenen „Teil-Mailbox" präsentieren können.

Die BfD-BOX ist für alle Interessenten, die über einen PC mit Anschluß an das öffentliche Telefonnetz verfügen, unter der Telefonnummer 02 28/37 10 62 und über ISDN unter der Rufnummer 02 28/ 9 57 97 26 erreichbar. Die Mailboxsoftware beinhaltet ein Command Line User Interface (CLUI), so daß sie mit allen gängigen Terminalprogrammen kommunizieren kann.

Die angebotenen Informationen können – in einer entsprechend aufgearbeiteten Form – von der BfD-BOX heruntergeladen werden. Dies ermöglicht es dem Interessenten, am eigenen PC Recherchen darin durchzuführen oder Textpassagen daraus zu nutzen, ohne diese abschreiben zu müssen.

34.4 Information für Bürger und auch für die Verwaltung

Meine Informationsbroschüren wurden auch im Berichtszeitraum überwiegend von Bürgern, aber zunehmend auch von Schulen, Universitäten und Verbänden für Schulungszwecke angefordert:

- BfD-Info 1
  Bundesdatenschutzgesetz – Text und Erläuterung –

  Die Broschüre enthält neben dem Gesetzestext eine einführende Darstellung des Gesetzes, die den einzelnen über seine Rechte aufklärt und auch als Basisinformation für diejenigen geeignet ist, die beruflich mit personenbezogenen Daten umgehen.
- BfD-Info 2
  Der Bürger und seine Daten

  Die Broschüre gibt einen Überblick über die Stellen, die möglicherweise personenbezogene Daten von Bürgern erheben, verarbeiten und nutzen und bei denen dann die Datenschutzrechte geltend gemacht werden können.
- BfD-Info 3
  Schutz der Sozialdaten

  Die Broschüre stellt den besonderen Datenschutz im Bereich der Sozialversicherung – also der Kranken-, Unfall- und Rentenversicherung sowie der Arbeitslosen- und der Pflegeversicherung – dar und geht auch auf den Datenschutz anderer im Hinblick auf Sozialleistungen, wie z. B. die Sozialhilfe, nach dem Sozialgesetzbuch ein.

- BfD-Info 4
  Der behördliche Datenschutzbeauftragte

  Die Broschüre informiert über Bestellung, Befugnisse und Aufgaben des behördlichen Datenschutzbeauftragten.

Wie auch in den zurückliegenden Jahren hält sich die Anzahl der versandten Broschüren bei rund 100 000 Exemplaren jährlich.

Zunehmend werde ich aber auch gefragt, ob ich meine Informationsschriften sowie den Tätigkeitsbericht in digitalisierter Form zur Verfügung stellen kann. Dieser Tätigkeitsbericht ist der erste, der sowohl als Diskette (entweder im HTML, RTF, Winword Version 2.0 oder 6.0 – oder ASC II-Format) als auch in Form einer CD-ROM (Formate auf der CD-ROM: HTML, RTF, Winword 2.0, Winword 6.0, ASC II) vorgelegt wird. Auf der CD-ROM stelle ich gleichzeitig die BfD-Info 1 mit zur Verfügung. Damit wird es möglich, mit Hilfe eines Browsers auf die jeweils genannten Vorschriften des BDSG zuzugreifen. Mit dieser Aufbereitung seiner Informationen sammelt mein Haus damit erstmals eigene Erfahrungen zur Nutzung von CD-ROM; dies gilt sowohl für die Akzeptanz dieser Informationsmittel als auch für den Aufwand, der erforderlich ist, um insbesondere die CD-ROM sinnvoll für eine automatisierte Nutzung aufzubereiten (s. auch Bestellformular am Ende des Berichtes).

35 Am Schluß noch einiges Wichtige aus zurückliegenden Tätigkeitsberichten

1. In meinem 15. TB (Nr. 2) hatte ich berichtet, daß ein Entwurf für eine **Datenschutzordnung des Deutschen Bundestages** vorbereitet, aber in der 12. Wahlperiode nicht mehr verabschiedet worden war. Auch bisher ist eine solche nicht erlassen worden. In der Zwischenzeit hat die Konferenz der Präsidentinnen und Präsidenten der deutschen Landesparlamente „Thesen zum parlamentsspezifischen Datenschutzrecht" mit einem Musterentwurf für eine Datenschutzordnung verabschiedet. Sie enthalten außerdem eine Empfehlung für eine – in die Datenschutzgesetze aufzunehmende – „Parlamentsklausel", die den Geltungsbereich des jeweiligen Datenschutzgesetzes gegenüber dem parlamentarischen Bereich abgrenzt und vorsieht, daß das Parlament eine Datenschutzordnung erläßt. In Hessen und Rheinland-Pfalz sind bereits Datenschutzordnungen verabschiedet worden. In diesen und in einigen weiteren Ländern enthalten die Datenschutzgesetze auch „Parlamentsklauseln", die zum Teil nur die Geltung des Datenschutzgesetzes behandeln, zum Teil aber auch ausdrücklich den Erlaß einer Datenschutzordnung vorsehen.

   Ich würde es begrüßen, wenn der Deutsche Bundestag seine Datenschutzordnung noch in dieser Legislaturperiode beschließt.

2. Das BMJ hat den angekündigten Entwurf einer **„Verordnung zur Änderung des Grundbucheinsichtsrechts"** (vgl. 15. TB Nr. 4.7.1) noch nicht vorgestellt. Es hat mich jedoch darüber unterrichtet, daß seiner Hausleitung ein Vorschlag zur Neuregelung des Grundbucheinsichtsrechts zur Entscheidung vorliegt. Ich hoffe, daß eine datenschutzgerechte Lösung bald gefunden wird.

3. Meine Bedenken dagegen, daß nach der im Entwurf der **Zweiten Zwangsvollstreckungsnovelle** vorgesehenen Regelung bei einer Mehrzahl von Drittschuldnern deren Namen und Anschriften grundsätzlich in einem einheitlichen Pfändungs- und Überweisungsbeschluß aufgeführt werden sollen, habe ich zuletzt in meinem 15. TB dargestellt (vgl. dort Nr. 4.11). Inzwischen habe ich meine Bedenken dem Rechtsausschuß des Deutschen Bundestages, dem der Gesetzentwurf zur Beratung vorliegt, vorgetragen. Ich werde mich im Rahmen des Gesetzgebungsverfahrens weiterhin für eine angemessene datenschutzgerechte Lösung des Problems einsetzen.

4. Die Neufassung der EG-Amtshilfe-Verordnung für den Zollbereich, auf deren Grundlage das **EG-Zollinformationssystem – EG-ZIS –** eingerichtet werden soll (vgl. 15. TB Nr. 5.6), konnte nach Auskunft des BMF bislang nicht verabschiedet werden, weil die Stellungnahme des Europäischen Parlaments noch nicht vorliegt. Inzwischen war die zuständige Arbeitsgruppe des Rates mit redaktionellen Anpassungen des Verordnungsentwurfs an die EG-Datenschutzrichtlinie befaßt. Das BMF hat mich hieran beteiligt. Eine endgültige Textfassung lag bis Redaktionsschluß noch nicht vor.

5. Über die datenschutzrechtlich bedenkliche Übersendung vollständiger **Abschriften von Urkunden** durch Gerichte, Notare und Behörden an Finanzbehörden habe ich zuletzt in meinem 15. TB (Nr. 5.8) informiert. Nach Erörterung der im wesentlichen Grundstückskaufverträge und Testamente betreffenden Problematik mit den Landesbeauftragten für den Datenschutz habe ich die Angelegenheit gegenüber dem BMF erneut aufgegriffen. In seiner Antwort hält das BMF seine Ablehnung gegenüber meinem Vorschlag für eine datenschutzgerechte Lösung, die in einer bloßen Anzeige des Sachverhalts gegenüber den Finanzbehörden besteht, aufrecht. Das BMF teilte mit, daß die obersten Finanzbehörden der Länder seine Auffassung teilen. Das weitere Vorgehen in dieser Angelegenheit werde ich mit den Landesbeauftragten für den Datenschutz abstimmen.

6. Die ablehnende Haltung der **Stiftung Preußischer Kulturbesitz** gegen die von mir geforderte Berufung eines **internen Datenschutzbeauftragten** habe ich in meinem 15. TB (Nr. 9.10) dargestellt. Das BMI hat aufgrund meiner Berichterstattung den Präsidenten der Stiftung gebeten, die Angelegenheit auf die Tagesordnung der Referentenkommission zu setzen und auch den Stiftungsrat damit zu befassen. In der Sitzung des Stiftungsrates im Dezember 1995 wurde von den Vertretern der Stiftung erneut die Bestellung eines internen Datenschutzbeauftragten mit der Begründung abgelehnt, daß die Stiftung sich in

einer Umbruchssituation befinde und eine Neuorganisation zur Diskussion stehe; ein stiftungsinterner Datenschutzbeauftragter sei in der gegenwärtigen Situation nicht erforderlich und könne wegen personeller Schwierigkeiten auch nicht bestellt werden.

Im Stiftungsrat wird Unverständnis über die Haltung der Stiftung geäußert, die Bestellung eines internen Datenschutzbeauftragten abzulehnen, da auch ohne gesetzliche Verpflichtung der Vorschlag des BfD für sinnvoll gehalten wird. Der Vorsitzende des Stiftungsrates hat daraufhin um weitere Berichterstattung in angemessener Zeit gebeten.

Aufgrund einer Nachfrage aus dem parlamentarischen Raum mußte ich feststellen, daß sich an dem oben dargestellten Sachstand bis heute nichts geändert hat.

7. Im 15. TB (Nr. 16.1) habe ich darüber berichtet, daß zwischen dem Beauftragten für Datenschutz der Evangelischen Landeskirche in Württemberg und mir unterschiedliche Rechtsansichten über mein **Kontrollrecht** gegenüber einer kirchlichen Einrichtung, die Zivildienstaufgaben des Bundes wahrnimmt, bestehen. Mittlerweile ist meine Kontrollzuständigkeit bundesweit im Rahmen der Verträge mit den Trägern der Freien Wohlfahrtspflege ausdrücklich festgelegt worden.

8. In meinem 15. TB (Nr. 20.2.7) hatte ich von Problemen berichtet, die dadurch entstehen, daß die Deutsche Telekom AG bislang als Kennzeichen eines Telefonanschlusses dessen sog. **Fernmeldekontonummer – FKTO –** benutzt; das ist die Telefonnummer in besonderer Schreibweise. Dadurch wird auch eine **„Geheimnummer"** Menschen und Stellen bekannt, denen der Kunde sie nicht zur Verfügung stellen will. Meiner dringenden Bitte, als Kennzeichen anstelle der Telefonnummer etwa die neu eingeführte Kundennummer zu verwenden, will die Telekom ab 1997 zwar entsprechen, zunächst allerdings nur mit ISDN-Anschlüssen beginnen, die bislang von Privatkunden kaum genutzt werden. Hier will ich versuchen, bei der Telekom noch eine „Kursänderung" zugunsten der üblichen Anschlüsse der Privatkunden zu erreichen.

9. Die Notwendigkeit, klare Regeln für den Umgang mit z. B. an den Weihnachtsmann gerichteten Kinderbriefen in den **Weihnachtspostämtern** zu schaffen, hatte ich begründet (s. 15. TB Nr. 20.3.3). Die von der Post daraufhin getroffenen Maßnahmen habe ich in einem dieser Postämter überprüft. Dabei zeigten sich noch Lücken in den Regelungen für die sichere Aufbewahrung und die anschließende Vernichtung, die rechtzeitig vor dem Weihnachtsfest 1996 geschlossen wurden.

10. Im 15. TB (Nr. 22.3) hatte ich angeregt, die in der letzten Legislaturperiode begonnene Novellierung des **Bevölkerungsstatistikgesetzes** fortzusetzen. Wegen ausstehender Änderungen im Personenstandsrecht wird mit den Arbeiten an dem Entwurf, der eine kostengünstige, zugleich aber auch eine datenschutzgerechte Lösung darstellen soll, derzeit noch abgewartet.

11. Auf die datenschutzrechtliche Problematik von **Ehescheidungsverbundurteilen** wegen der darin enthaltenen Zusammenfassung anderer Entscheidungen (Zugewinnausgleich, Unterhaltsansprüche und Sorgerecht für Kinder u. a.) habe ich zuletzt in meinem 15. Tätigkeitsbericht hingewiesen (vgl. dort Nr. 35 unter 3.). Reicht ein geschiedener Ehegatte ein solches Urteil bei einer Stelle (z. B. Meldebehörde, Standesamt, Finanzamt, Arbeitgeber) ein, so erhält diese neben den für die Erfüllung ihrer Aufgaben erforderlichen Angaben zwangsläufig eine Vielzahl anderer zum Teil sehr sensibler Informationen, die sie nicht benötigt. Da die Parteien eines Eherechtsstreits in der Regel keine Kenntnis davon haben, daß in den meisten Fällen, in denen ein Urteil vorzulegen ist, Auszüge aus dem Urteilstenor ausreichen und auch für die Zwangsvollstrekkung regelmäßig vollstreckbare Ausfertigungen ohne Tatbestand und Entscheidungsgründe genügen, hatte ich dem BMJ gegenüber vorgeschlagen, den Ehescheidungsverbundurteilen ein Merkblatt zur Unterrichtung beizufügen oder die Urteilsausfertigung mit einem entsprechenden Stempelaufdruck zu versehen.

Das BMJ hat die Landesjustizverwaltungen um Stellungnahme zu meinem Vorschlag gebeten. Bedauerlicherweise haben sich die Justizministerien unter Hinweis auf den damit verbundenen Verwaltungsaufwand mehrheitlich dagegen ausgesprochen, den Ehescheidungsverbundurteilen ein Merkblatt beizufügen. Ich habe mich daher an die Landesbeauftragten für den Datenschutz gewandt und ihnen vorgeschlagen, sich unmittelbar mit dem jeweiligen Justizressort um eine datenschutzgerechte Lösung zu bemühen. Dies führte zwar dazu, daß in einem Land ein Oberlandesgericht mit der Umsetzung eines entsprechenden Vorschlages beauftragt worden ist. Jedoch stieß der Versuch, eine datenschutzgerechte Lösung zu finden, bisher im übrigen auf Ablehnung.

Möglicherweise wird aber durch den zunehmenden Einsatz automatisierter Textverarbeitung in den Gerichten mittelfristig Abhilfe geschaffen werden können, da dann die Unterrichtung der Betroffenen ohne großen Verwaltungsaufwand mit Hilfe von Textbausteinen erfolgen kann. Ich hoffe jedenfalls, daß die Bemühungen der Landesbeauftragten langfristig noch in einem größeren Umfang zum Erfolg führen werden.

12. Das BMVg hat die **Personalaktenverordnung** nach § 29 Abs. 9 Soldatengesetz inzwischen erlassen (vgl. 15. TB Nr. 35 unter 9.). Mit der Verordnung – in das Beratungsverfahren war ich einbezogen und meine Anregungen wurden größtenteils berücksichtigt – ist ein erfreulicher datenschutzrechtlicher Standard für das Personalaktenrecht der Soldaten erreicht worden.

Anlage 1 (zu Nr. 1.13)

Hinweis für die Ausschüsse des Deutschen Bundestages

Nachfolgend habe ich dargestellt, welche Kapitel dieses Berichts für welchen Ausschuß von *besonderem Interesse* sein könnten:

Ausschuß für Wahlprüfung, Immunität und Geschäftsordnung	35 unter 1.
Auswärtiger Ausschuß	1.3; 2; 4; 32
Innenausschuß	1; 2; 4.2.2; 5; 6.1; 6.2; 6.4; 6.5; 6.6; 6.9; 7.6; 8.1.1; 8.2.3; 8.2.4; 9.1 bis 9.3; 10.1.5; 10.4.1; 10.4.13 bis 10.4.15; 11; 12; 13.2; 14; 16; 17.1; 17.5; 18; 19.4 bis 19.6; 28.3; 28.4.1; 29.1; 31; 32; 33
Rechtsausschuß	2; 5.3.2; 5.5; 5.7; 5.9.1; 5.11; 6; 10.2.2; 31
Finanzausschuß	7; 8.3; 13.2 bis 13.6; 34
Ausschuß für Wirtschaft	8.1.1; 8.2.3; 8.2.4; 9.3; 10.1.4; 13.1; 17.3; 17.4; 30.3; 30.7; 31
Ausschuß für Ernährung, Landwirtschaft und Forsten	8.4; 30.6
Ausschuß für Arbeit und Sozialordnung	7.10; 19 bis 24
Verteidigungsausschuß	15; 26; 35 unter 12.
Ausschuß für Familie, Senioren, Frauen und Jugend	10.1.4; 10.4.11; 19.4 bis 19.6; 21.9; 24; 27
Ausschuß für Gesundheit	9.1; 9.2; 13.2; 19; 21 bis 24; 25
Ausschuß für Verkehr	17.2; 28
Ausschuß für Post und Telekommunikation	1.12; 8.4; 10; 29
Ausschuß für Raumordnung, Bauwesen und Städtebau	30.5
Ausschuß für Bildung, Wissenschaft, Forschung, Technologie und Technikfolgenabschätzung	1.5; 8.1; 8.2; 9; 25.1
Ausschuß für die Angelegenheiten der Europäischen Union	1.3; 2; 10.3; 30.2; 30.3; 32 insb. 32.2 und 32.3.1

Anlage 2 (zu Nr. 1.12)

Übersicht über die durchgeführten Kontrollen, Beratungen und Informationsbesuche

Deutscher Bundestag
- Verwaltung

Bundeskanzleramt
- Bundesnachrichtendienst

Auswärtiges Amt
- 3 Botschaften
- ein Generalkonsulat

Bundesministerium des Innern
- Statistisches Bundesamt
- Bundesamt für die Anerkennung ausländischer Flüchtlinge – Zentrale Nürnberg und Außenstelle Zirndorf
- Bundesbeauftragter für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR – Zentrale Berlin und 2 Außenstellen
- Bundesverwaltungsamt Ausländerzentralregister und Staatsangehörigkeitsdatei
- Bundesgrenzschutz
- Grenzschutzamt Frankfurt/Flughafen
- Grenzschutzdirektion
- eine Bahnpolizeiwache
- Bundeskriminalamt
- Nationales SIRENE-Büro
- Deutsche Verbindungsbeamte bei EUROPOL/EDE
- Bundesamt für Verfassungsschutz
- Bundesdruckerei

Bundesministerium der Justiz
- Deutsches Patentamt

Bundesministerium der Finanzen
- Bundesschuldenverwaltung
- Bundesaufsichtsamt für das Versicherungswesen
- Zollkriminalamt
- 7 Oberfinanzdirektionen
- 13 Hauptzollämter
- 2 Zollfahndungsämter
- 3 Zollfahndungszweigstellen
- Treuhand Liegenschaftsgesellschaft

Bundesministerium für Wirtschaft

Bundesministerium für Arbeit und Soziales
- Bundesversicherungsamt
- Bundesanstalt für Arbeit
- 6 Arbeitsämter

Bundesministerium der Verteidigung
- 3 Bundeswehreinheiten (Heer)
- 3 Bundeswehreinheiten (Marine)
- 1 Kreiswehrersatzamt

Bundesministerium für Familie, Senioren, Frauen und Jugend
- Bundesamt für den Zivildienst
- 3 Verwaltungsstellen Zivildienst

Bundesministerium für Gesundheit

Bundesministerium für Verkehr
- Luftfahrt-Bundesamt
- Kraftfahrt-Bundesamt
- Bundesamt für Güterverkehr

Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit
- Bundesamt für Strahlenschutz
- Umweltbundesamt

Bundesverfassungsgericht

Deutsche Post AG
- Generaldirektion
- 2 Niederlassungen
- eine Filiale

Deutsche Telekom AG
- 5 Niederlassungen

Sonstige
- Schweizer Bundesamt für Flüchtlinge in Bern
- Bundesknappschaft
- Barmer Ersatzkasse – eine Außenstelle
- Reichsbahn-Betriebskrankenkasse
- Hanseatische Krankenkasse
- Hamburg-Münchener-Ersatzkasse, Hauptverwaltung und einer Außenstelle
- Institut für Arbeitsmarkt- und Berufsforschung
- Hauptverband der gewerblichen Berufsgenossenschaften
- 5 Berufsgenossenschaften
- Bundesversicherungsanstalt für Angestellte
- eine Privatfirma als Auftragsverarbeiter nach § 11 BDSG
- 2 Wirtschaftsunternehmen

Anlage 3 (zu Nr. 1.12)

Übersicht über Beanstandungen nach § 25 BDSG

Auswärtiges Amt

- Verstoß gegen § 4 Abs.1 BDSG i.V. mit § 8 Abs. 1 AsylVfG durch unzulässige Übermittlung personenbezogener Daten von Visumantragstellern an das Bundesamt für die Anerkennung ausländischer Flüchtlinge (s. Nr. 4.2.2)

Bundesministerium der Finanzen

- Verstoß gegen § 18 Abs.1 und 2 Satz 3 BDSG durch Betreiben des Automatisierten Vollstrekkungsverfahrens (AVS) bei Hauptzollämtern ohne ausreichende Datenschutzregelungen (s. Nr. 5.6)

Luftfahrt-Bundesamt

- Verstoß gegen § 4 BDSG wegen unzulässiger Übermittlung personenbezogener Daten von Luftfahrzeugeigentümern zur Veröffentlichung ohne entsprechende Rechtsgrundlage und ohne Einwilligung der Betroffenen (s. Nr. 28.4.2).

Vorstand der Deutschen Telekom AG

- Unzulässiges Mithören von Telefonaten durch die Auslandsvermittlung; Verstoß gegen § 10 FAG (s. Nr. 10.4.2).

Hauptverband der gewerblichen Berufsgenossenschaften (HVBG)

- Verstoß gegen §§ 35 SGB I i.V.m. 67 a Abs. 1, 67 b Abs. 1, 78 a, 96 Abs. 3 Satz 1 SGB X, 18 f Abs. 1 Satz 1 SGB IV wegen unzulässiger Erhebung und Nutzung der Rentenversicherungsnummer (siehe Nr. 23.6).
- Verstoß gegen § 24 Abs. 4 BDSG wegen mangelnder Unterstützung (siehe Nr. 23.6).

Gesetzliche Krankenkasse

- Verstoß gegen §§ 35 SGB I i.V. m. 67 a Abs. 1, 67 a Abs. 2 Satz 1 und 67 a Abs. 3 SGB X wegen unzulässiger Ermittlungen im Rahmen von Regreßverfahren nach § 116 SGB X (siehe Nr. 21.8).

Anlage 4 (zu Nrn. 2.2, 32.2.1)

Kopenhagener Resolution der Konferenz der Datenschutzbeauftragten der Europäischen Union vom 8. September 1995

(1) Der Vertrag über die Europäische Union nimmt an zwei Stellen (Artikel F Abs. 2 und Artikel K.2 Abs. 1) ausdrücklich auf die Europäische Konvention zum Schutz der Menschenrechte und Grundfreiheiten Bezug und garantiert darin die Achtung der in der Konvention festgeschriebenen Grundrechte. Damit ist auch Artikel 8 der EMRK – Gebot der Achtung der privaten Sphäre – von der Garantie des Unionsvertrages mitumfaßt.

Die Konferenz nimmt die für 1996 geplante Regierungskonferenz zum Anlaß, im Hinblick auf den europäischen Grundrechtsschutz im allgemeinen und auf das Recht des einzelnen auf Datenschutz im besonderen eine weitergehende Änderung bzw. Ergänzung der Unions- und Gemeinschaftsverträge zu fordern. Sie unterstützt dabei die Bestrebungen zur Schaffung eines verbindlichen europäischen Grundrechtskatalogs und plädiert darüber hinaus für die Aufnahme eines europäischen Grundrechts auf Datenschutz in diesen Katalog, wodurch die Unionsorgane wie die nationalen Stellen gebunden werden und der Datenschutz den Bürgern in einklagbarer Form gewährt wird.

(2) Gemeinschaftsrechtliche Regelungen verpflichten die Mitgliedstaaten in immer größerem Maße zur Erhebung und Verarbeitung personenbezogener Daten, und gleichzeitig führen die europäischen Einrichtungen selbst zunehmend personenbezogene Datenbanken. Diese Einrichtungen sind jedoch nicht an die Grundsätze des Datenschutzes gebunden, insbesondere unterliegen sie keinem Datenschutzgesetz. Da der Datenschutz aber nicht mehr länger aus dem Wirken der Gemeinschafts- und Unionsorgane ausgeklammert bleiben kann, mahnt die Konferenz die Schaffung gemeinschaftsbezogener Datenschutzregelungen an.

Zwar war in dem von der Europäischen Kommission am 13. September 1990 vorgelegten Datenschutzpaket eine „Erklärung der Kommission betreffend die Anwendung der Grundsätze der Richtlinie zum Schutz von Personen bei der Verarbeitung personenbezogener Daten auf die Organe und Einrichtungen der EG" enthalten, die auf die Anwendung der Datenschutzrichtlinie auf EG-Institutionen abzielte. Dieses Vorhaben muß weiterverfolgt werden. Die am 24. Juli 1995 verabschiedete Datenschutzrichtlinie richtet sich nur an die nationalen Gesetzgeber als Adressaten.

(3) Um künftig sicherzustellen, daß den vielfältigen und umfangreichen Aktivitäten der Gemeinschaft die rechtzeitige und systematische Prüfung der datenschutzrechtlichen Auswirkungen zuteil wird, fordert die Konferenz für die Gewährleistung des Datenschutzes durch Gemeinschaftsorgane und -einrichtungen die Schaffung rechtsverbindlicher Regelungen. Sie erinnert in diesem Zusammenhang an die Zusatzerklärung der Datenschutzbeauftragten der EG-Länder zur Berliner Resolution der Internationalen Konferenz der Datenschutzbeauftragten vom 30. August 1989 und ihren Vorschlag, wonach die Grundsätze der Europaratskonvention 108 durch entsprechende Rechtsakte der Europäischen Gemeinschaft für alle Mitgliedstaaten ebenso wie für die Institutionen der EG selbst verbindlich gemacht werden sollten.

(4) Während die Datenschutzregelungen der Mitgliedstaaten unabhängige Kontrollinstanzen zur Sicherung der gesetzlichen Rechte des Betroffenen vorsehen, fehlt es nach wie vor an einer unabhängigen und effektiven Datenschutzkontrollinstanz, an die sich jeder wenden kann, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch Organe oder Einrichtungen der Gemeinschaft in seinen Rechten verletzt zu sein. Die Konferenz verweist auch in diesem Zusammenhang auf die Zusatzerklärung der Datenschutzbeauftragten der EG-Länder zur Berliner Resolution aus dem Jahre 1989 und ihren Vorschlag betreffend die Einrichtung einer unabhängigen Datenschutzkontrollinstanz. Diese sollte nicht nur Eingaben von Betroffenen entgegennehmen, sondern auch die Verarbeitung personenbezogener Daten innerhalb der Gemeinschaftsorgane und -einrichtungen – nicht nur anlaßbezogen – kontrollieren, die Organe und Einrichtungen der Gemeinschaft in allen Datenschutzfragen beraten sowie mit den nationalen Datenschutzorganen zusammenarbeiten.

Es ist daher notwendig und dringend geboten, in den Unions- und Gemeinschaftsverträgen die Schaffung einer unabhängigen Kontrollinstanz für die Verarbeitung personenbezogener Daten durch Gemeinschaftsorgane und einrichtungen vorzusehen. Die Mitgliedstaaten sollten einen derartigen Vorschlag unterbreiten und einem geeigneten Text im Rahmen der Internationalen Konferenz zur Überprüfung der Verträge in 1996 zustimmen.

Copenhagen Resolution of the Conference of Data Protection Commissioners of the European Union of 8 September 1995

(1) The Treaty on European Union twice explicitly refers to the European Convention for the Protection of Human Rights and Fundamental Freedoms (Artikel F, paragraph 2 and Artikel K.2, paragraph 1) and guarantees therein the respect for the basic rights enshrined in the Convention. Thus, also Article 8 of the ECHR – obligation to respect privacy – is included in the guarantee by the Treaty on European Union.

In light of the Intergovernmental Conference scheduled for 1996 the Conference calls for a comprehensive amendment to the Union and Community Treaties as regards the European protection of basic rights in general and the right of the individual to data protection in particular. In so doing, it supports efforts to set up a binding European catalogue of basic rights and furthermore advocates the inclusion of a European basic right to data protection in such catalogue, which would bind the organs of the Union and national bodies and grant the citizens data protection in an actionable manner.

(2) Member States are under an increasing obligation under Community provisions to collect and process personal data, and at the same time more and more European institutions themselves hold personal data banks. However, these institutions are not bound by data protection principles and, above all, are not subject to any act governing data protection. As data protection may no longer be excluded from action by Community and Union organs, the Conference urges the creation of Community-related data protection provisions.

It is true that the data protection package submitted by the European Commission on 13 September 1990 included a "Commission Declaration Concerning the Application of the Principles Contained in the Directive on the Protection of Individuals With Regard to the Processing of Personal Data to EC Organs and Institutions", which was intended to apply the Data Protection Directive to EC institutions. However, this issue must be pursued further. The Data Protection Directive adopted on 24 July 1995 is merely addressed to national legislators.

(3) So as to ensure in future that the manifold and far-reaching activities of the Community are timely and systematically examined from a data protection aspect, the Conference calls for the creation of legally binding provisions so that data protection by Community institutions and bodies is guaranteed. In this context, it draws attention to the Additional Declaration of the Data Protection Commissioners of the EC Countries to the Berlin Resolution of the International Conference of Data Protection Commissioners of 30 August 1989 and to its proposal to make the principles of the Convention 108 of the Council of Europe legally binding for all Member States as well as for the EC institutions themselves through legal acts of the European Community to this effect.

(4) Whereas the regulations governing data protection in the various Member States are providing for independent control authorities to ensure the data subject's staturory rights there is still no independent and effective data protection control body which an individual may turn to if he feels that Community institutions or bodies infringed on his rights by processing his personal data. In this context, too, the Conference draws attention to the Additional Declaration of the Data Protection Commissioners of the EC Countries to the 1989 Berlin Resolution and to its proposal to set up an independent data protection control body. This body should receive complaints by data subjects, control the processing of personal data within Community institutions and bodies – not only if this is called for by particular events – and advise Community institutions and bodies on all data protection issues and co-operate with national data protection authorities.

It is therefore necessary and urgent to provide in the Union and Community Treaties for the creation of an independent control authority for the processing of personal data by Community institutions and bodies. Member States should make such proposal and agree to an appropriate text in the context of the Intergovernmental Conference for the Revision of the Treaties in 1996.

Anlage 5 (zu Nr. 5.13)

Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1995 zum Datenschutz bei Wahlen

Bei der Durchführung von Wahlen haben sich Probleme bei der Verarbeitung personenbezogener Daten ergeben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat hierzu die folgende Entschließung *) gefaßt:

1. Durchführung von Wahlstatistiken

Diejenigen Wahlberechtigten, in deren Wahlbezirk eine repräsentative Wahlstatistik durchgeführt werden soll, sind bereits mit der Wahlbenachrichtigung hierüber zu informieren. In allgemeiner Form ist auch im Wahllokal ein gut sichtbarer Hinweis auf die Einbeziehung in die Wahlstatistik anzubringen.

Die Statistik sollte nur in solchen Wahlbezirken durchgeführt werden, in denen jede Geschlechts- und Altersgruppe wenigstens so viele Wahlberechtigte aufweist, daß das Wahlgeheimnis mit Sicherheit gewahrt bleibt. Das Kriterium ist vom Landeswahlleiter vor der Festlegung der Auswahlbezirke zu prüfen. Gegebenenfalls sind ungeeignete Wahlbezirke auszutauschen.

Die Auszählung der Wahlberechtigten und der Wahlbeteiligung auf der Grundlage der Wählerverzeichnisse sollte durch den Wahlvorstand erfolgen, während die statistische Auszählung der Stimmzettel durch die jeweils für die Durchführung der Statistik zuständige Stelle vorzunehmen ist.

Untersuchungen, bei denen Angaben über die Wahlbeteiligung oder die Stimmabgabe aus verschiedenen Wahlen einzelfall- und personenbezogen zusammengeführt werden, gefährden das Wahlgeheimnis und sind daher unzulässig.

2. Auslegung von Wählerverzeichnissen

Durch die Einsicht in das Wählerverzeichnis besteht nach der jetzigen Rechtslage die Gefahr, daß Daten sowohl von Bürgern, über die in Melderegistern eine Auskunftssperre eingetragen ist, als auch von Bürgern, die in einer speziellen sozialen Situation leben (z. B. Justizvollzugsanstalten, Frauenhäuser, psychiatrische Kliniken, Obdachlose), offenbart werden.

Um einerseits die Kontrollmöglichkeit durch die Öffentlichkeit im Vorfeld einer Wahl weiterhin zu gewährleisten, andererseits die datenschutzrechtlichen Belange der genannten Betroffenen zu wahren und dem Mißbrauch einer Adreßrecherche vorzubeugen, fordern die Datenschutzbeauftragten des Bundes und der Länder, daß bei allen Wahlen

- entweder in den öffentlich ausliegenden Wählerverzeichnissen nur Name, Vorname und Geburtsdatum der Wahlberechtigten aufgeführt werden
- oder aber bei Wiedergabe der Adressen im Wählerverzeichnis nur Auskünfte zu bestimmten Personen an den Auskunftssuchenden erteilt werden, wenn er vorher die Adresse dieser Person aufgegeben hat.

Im übrigen sind Daten von Bürgern, für die in Melderegistern eine Auskunftssperre eingetragen ist, im Wählerverzeichnis nicht zu veröffentlichen.

3. Gewinnung von Wahlhelfern

Bei der Gewinnung von Wahlhelfern sind folgende Grundsätze zu beachten:

Es dürfen nur die zur Bestellung erforderlichen Daten, wie Name, Vorname und Wohnanschrift, erhoben werden. Die Betroffenen sind über den Zweck der Datenerhebung und die weitere Datenverarbeitung umfassend zu unterrichten.

Über die Abwicklung der jeweiligen Wahl hinaus dürfen die Daten der Wahlhelfer, soweit sie nicht ausdrücklich widersprochen haben, in einer Wahlhelferdatei nur gespeichert werden, wenn sie dieser Speicherung nicht widersprochen haben. Die Wahlhelfer sind auf ihr Widerspruchsrecht hinzuweisen.

Beschäftigtendaten dürfen nur auf freiwilliger Basis übermittelt werden, sofern nicht eine besondere Rechtsvorschrift die Übermittlung zuläßt. Im Falle der Freiwilligkeit muß es den Beschäftigten möglich sein, selbst die Meldung unmittelbar gegenüber der Wahlbehörde abzugeben. Nach Gründen, die einer Übernahme des Ehrenamtes entgegenstehen, darf erst im förmlichen Verfahren durch die Wahlbehörde gefragt werden.

4. Erteilung von Wahlscheinen

Die in den Wahlordnungen des Bundes und der Länder enthaltene Regelung, nach der die Antragstellung für die Erteilung eines Wahlscheines auf einem Vordruck zu begründen ist und der Grund gegenüber der Gemeinde glaubhaft gemacht werden muß, ist aus datenschutzrechtlicher Sicht unverhältnismäßig. Da sich aus der geforderten Differenzierung der Begründung keine unterschiedlichen Rechtsfolgen ableiten, ist diese entbehrlich. Es genügt in der Antragstellung eine Erklärung des Wahlberechtigten, daß er am Tag der Wahl aus wichtigem Grund das für ihn zuständige Wahllokal nicht aufsuchen kann.

*) Bei Gegenstimme von Baden-Württemberg zu Nr. 4

Anlage 6 (zu Nr. 6.14)

Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1995 zu Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich

Bisher ist der Gesetzgeber im Bereich der Justiz den verfassungsrechtlichen Forderungen nach ausreichenden normenklaren Regelungen über die Aufbewahrung von Akten und die Speicherung personenbezogener Daten in Dateien nicht nachgekommen. So enthalten z. B. die bislang bekanntgewordenen Entwürfe zu einem Strafverfahrensänderungsgesetz nur unzureichende Generalklauseln. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder *) erklärt deshalb:

1. Aufbewahrung, Aussonderung und Vernichtung der Akten und die Speicherung personenbezogener Daten in Dateien im Bereich der Justiz müssen nach den Grundsätzen des Bundesverfassungsgerichts im Volkszählungsurteil für die Gerichte, Staatsanwaltschaften und Strafvollzugsbehörden gesetzlich geregelt werden, wobei sich die Aufbewahrungsdauer am Recht auf informationelle Selbstbestimmung und am Zweck der Speicherung zu orientieren hat.

   Hierbei hat der Gesetzgeber die grundlegenden Entscheidungen zur Aufbewahrungsdauer selbst zu treffen. Aufgrund einer hinreichend konkreten Verordnungsermächtigung können die Einzelheiten durch Rechtsverordnung bestimmt werden.

2. Die derzeit bestehenden Aufbewahrungsfristen sind konsequent zu vereinfachen und zu verkürzen. Soweit geboten sind Verkürzungen vorzunehmen.

3. Die derzeit geltende generelle 30jährige Aufbewahrungsfrist für Strafurteile und Strafbefehle mit der Folge der umfassenden Verfügbarkeit der darin enthaltenen Informationen ist nicht angemessen. Bei der Bemessung der Aufbewahrungsfrist von Strafurteilen und Strafbefehlen sowie für die Bestimmung des Zeitpunkts der Einschränkung der Verfügbarkeit ist vielmehr nach Art und Maß der verhängten Sanktionen zu differenzieren.

   Bei der Festlegung des Beginns der Aufbewahrungsfrist sollte – abweichend von der bisherigen Praxis, nach der es auf die Weglegung der Akte ankommt – regelmäßig auf den Zeitpunkt des Eintritts der Rechtskraft der ergangenen gerichtlichen Entscheidung abgestellt werden.

   Ergeht keine rechtskraftfähige Entscheidung, so sollte die Aufbewahrungsfrist mit dem Erlaß der Abschlußverfügung beginnen.

4. Wird der Akteninhalt auf Bild- oder Datenträgern, die an die Stelle der Urschrift treten, aufbewahrt, so sind gleichwohl unterschiedliche Löschungsfristen für einzelne Aktenteile zu beachten. Aus datenschutzrechtlicher Sicht sind Datenträger zu wählen, die eine differenzierte Löschung gewährleisten. Ist bei Altbeständen eine teilweise Aussonderung technisch nicht möglich oder nur mit unverhältnismäßigem Aufwand zu bewerkstelligen, so hat eine Sperrung der an sich auszusondernden Teile zu erfolgen.

5. Sind in einer Akte Daten mehrerer beteiligter Personen gespeichert, so ist eine Sperre hinsichtlich solcher Aktenteile, die einzelne beteiligte Personen betreffen, vorzusehen, wenn diese Aktenteile eigentlich ausgesondert werden müßten, aus praktischen Gründen aber keine Vernichtung erfolgen kann.

6. Bei Freisprüchen und Einstellungen des Verfahrens wegen Wegfalls des Tatverdachts ist dafür Sorge zu tragen, daß ein Zugriff auf die automatisiert gespeicherten Daten nur noch zu Zwecken der Aktenverwaltung erfolgen kann.

7. Für die Daten von Nebenbeteiligten (z. B. Anzeigeerstatter, Geschädigte) ist eine vorzeitige Löschung vorzusehen. Hinsichtlich der Hauptbeteiligten sollte eine Teillöschung der Personen- und Verfahrensdaten stattfinden, sobald die vollständigen Daten zur Durchführung des Verfahrens nicht mehr erforderlich sind.

8. Soweit Daten verschiedener Gerichtszweige oder verschiedener speichernder Stellen in gemeinsamen Systemen verarbeitet werden, ist durch rechtliche, technische und organisatorische Maßnahmen sicherzustellen, daß die Zweckbindung der gespeicherten Daten beachtet wird.

*) Bei Stimmenthaltung von Hamburg

Anlage 7 (zu Nr. 11.2)

Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1995 zur Rechtstatsachensammlung zur Überprüfung polizeilicher Befugnisse

Die Datenschutzbeauftragten des Bundes und der Länder hatten in ihrer 48. Konferenz am 26./27. September 1994 Vorschläge zur Überprüfung der Erforderlichkeit polizeilicher Befugnisse und deren Auswirkungen für die Rechte der Betroffenen erarbeitet.

Ziel dieser Vorschläge war es, die Diskussion über die Erforderlichkeit der bestehenden Instrumente zur polizeilichen Datenverarbeitung und deren Ausweitung auf Erkenntnisse zu stützen, die stärker als bisher gesichert sind.

Auch von seiten der Polizei, insbesondere des Bundeskriminalamtes, sind Vorschläge für eine umfassende Rechtstatsachensammlung über die Anzahl besonderer Erhebungsmethoden, den Erfolg dieser Maßnahmen und Durchführungsschwierigkeiten unterbreitet worden. Sie sind jedoch bisher von der Mehrzahl der Landespolizeien abgelehnt worden. Statt dessen soll eine Bund/Länder-Fallsammlung eingerichtet werden. Hierzu stellen die Datenschutzbeauftragten des Bundes und der Länder fest:

Die Einrichtung einer Rechtstatsachensammlung als objektives Instrument zur Bewertung polizeilicher Eingriffsbefugnisse wäre auch aus datenschutzrechtlicher Sicht zu begrüßen. Diese Sammlung darf jedoch nicht einseitig das Ziel verfolgen, Forderungen der Polizei zur Einführung zusätzlicher Befugnisse argumentativ zu unterstützen. Das Vorhaben geht in die falsche Richtung, wenn es von vornherein aufgrund des angelieferten Datenmaterials auf bestimmte Ergebnisse festgelegt ist. Vielmehr muß die Sammlung ohne rechtspolitische Vorgaben angelegt werden. Sie soll eine objektive Beurteilung des Einsatzes und der Ergebnisse besonderer Methoden zur Datenerhebung ermöglichen.

Das Bundesverfassungsgericht hat im Volkszählungsurteil gefordert, daß der Gesetzgeber ungewissen Auswirkungen eines Gesetzes dadurch Rechnung tragen muß, daß er die ihm zugänglichen Erkenntnisquellen ausschöpft, um die Auswirkungen so zuverlässig wie möglich abschätzen zu können; bei einer sich später zeigenden Fehlprognose ist er zur Korrektur verpflichtet. Der Gesetzgeber kann aufgrund veränderter Umstände zur Nachbesserung einer ursprünglich verfassungsgemäßen Regelung gehalten sein.

Die Datenschutzbeauftragten halten daher ihren Vorschlag einer ergebnisoffenen Überprüfung der bestehenden Befugnisse aufrecht. Sie erwarten, daß sich die Polizeien der Diskussion über die Erforderlichkeit und Angemessenheit weitreichender Befugnisse zu Eingriffen in das Persönlichkeitsrecht nicht entziehen werden. In Betracht kommt auch eine unabhängige Überprüfung der bestehenden polizeilichen Eingriffsbefugnisse durch das kriminalistische Institut beim BKA in enger Kooperation mit einem fachlich qualifizierten unabhängigen Forschungsinstitut.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Innenministerkonferenz auf, die Überlegungen für eine offene und aussagekräftige Rechtstatsachensammlung weiterzuverfolgen und die Datenschutzbeauftragten zu beteiligen.

Anlage 8 (zu Nr. 17.5)

Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1995: Maßhalten beim vorbeugenden personellen Sabotageschutz

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, bei Sicherheitsüberprüfungen zum personellen Sabotageschutz Augenmaß zu bewahren. Bei diesen Sicherheitsüberprüfungen werden sensible Daten, z. B. über politische Anschauungen oder Alkoholkonsum, vorbeugend erhoben, also ohne daß der Betroffene dazu Anlaß geboten hätte. Polizei und Verfassungsschutz sind routinemäßig beteiligt. Schon wenn der Betroffene im Verlauf der Überprüfung auch nur in den Verdacht der Unzuverlässigkeit gerät, kann dies bereits erheblichen Einfluß zumindest auf das berufliche Fortkommen nehmen.

Gegenwärtig sind solche Überprüfungen spezialgesetzlich für den Atombereich und für Flughäfen vorgesehen. Das Bundesministerium des Innern will jetzt klären, inwieweit Beschäftigte in anderen Einrichtungen überprüft werden sollen.

Unstreitig können solche Überprüfungen unbescholtener Bürger nur zum Schutz von „lebens- und verteidigungswichtigen Einrichtungen" angemessen sein und nur Personen betreffen, die dort an „sicherheitsempfindlichen Stellen" tätig sind. Als „lebenswichtig" sehen die Innenminister und -senatoren aber bereits Stellen an, „die für das Funktionieren des Gemeinwesens unverzichtbar sind". Damit könnten Beschäftigte in weiten Bereichen des öffentlichen Dienstes und der Wirtschaft mit Sicherheitsüberprüfungen überzogen werden.

Die Datenschutzbeauftragten meinen, daß das Persönlichkeitsrecht hier größere Zurückhaltung gebietet. Die Sicherheitsüberprüfungen müssen auf Bereiche beschränkt bleiben, in denen einer erheblichen Bedrohung für das Leben zahlreicher Menschen vorgebeugt werden muß.

Soweit in solchen Bereichen Sicherheitsüberprüfungen durchgeführt werden sollen, bedarf es einer ebenso klaren gesetzlichen Grundlage, wie bisher im Atomgesetz und im Luftverkehrsgesetz. Die zu schützenden Arten lebens- und verteidigungswichtiger Einrichtungen müssen durch Rechtsvorschrift abschließend festgelegt sein. Dabei sind für die jeweiligen Bereiche angemessene Regelungen zu treffen, die mit Rücksicht auf die Interessen Betroffener folgende allgemeine Grundsätze beachten:

- möglichst klare Vorgaben zur „Sicherheitsempfindlichkeit" in der Vorschrift und exakte Festlegung dieser Stellen durch die zuständige Behörde nach Anhörung der Personalvertretung der einzelnen Einrichtung,
- Zustimmung des Betroffenen als Verfahrensvoraussetzung,
- abschließender Katalog der regelmäßig durchzuführenden Maßnahmen, dabei Beschränkung auf vorhandene Erkenntnisse, keine Ausforschungsermittlungen,
- strenge Zweckbindung und angemessene organisatorische Vorkehrungen zu deren Gewährleistung, insbesondere Trennung von Personalakte,
- eigene Verfahrensrechte des Betroffenen, insbesondere rechtliches Gehör vor ablehnender Entscheidung und aktenkundige Gegendarstellung,
- angemessener Auskunftsanspruch, einschließlich Akteneinsicht,
- effektive Datenschutzkontrolle, auch zur Datenverarbeitung in Akten bei nicht-öffentlichen Stellen.

Im Regelfall muß zusätzlich gelten:

- Überprüfung durch die zuständige Aufsichtsbehörde selbst, nicht durch Verfassungsschutzbehörden,
- keine Einbeziehung weiterer Personen (wie Ehegatten usw.).

Ausnahmetatbestände wären – auch zum Verfahren – präzise zu fassen.

Die Praxis der Sicherheitsüberprüfungen zum personellen Sabotageschutz steht in Bund und Ländern vor einer wichtigen Weichenstellung. Sie muß klar und angemessen sein.

Anlage 9 (zu Nr. 21.6)

Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1995 zu: Eingeschränkter Zugriff auf Versichertendaten bei landesweiten oder überregionalen gesetzlichen Krankenkassen

Die gesetzlichen Krankenkassen schließen sich zunehmend zu landesweiten oder überregionalen gesetzlichen Krankenkassen zusammen. Es stellt sich daher verstärkt die Frage, welche bzw. wieviele Geschäftsstellen solcher Krankenkassen umfassend auf alle gespeicherten Daten eines Versicherten zugreifen können.

Die Datenschutzbeauftragten halten nur folgendes für vertretbar:

1. Geschäftsstellen einer Krankenkasse können ohne schriftliches Einverständnis des Versicherten nur auf einen „Stammdatensatz" zugreifen. Dieser „Stammdatensatz" darf nur den Namen, das Geburtsdatum, die Anschrift, die Krankenversichertennummer und die betreuende Geschäftsstelle des Versicherten umfassen.
2. Lediglich eine Geschäftsstelle kann umfassend auf den Datensatz eines Versicherten zugreifen, sofern der Versicherte nicht ausdrücklich und eindeutig schriftlich in derartige Zugriffsmöglichkeiten durch weitere Geschäftsstellen eingewilligt hat.
3. Vor der Einwilligung ist der Betroffene umfassend aufzuklären. Die Daten dürfen nur zweckgebunden verwendet werden.

Anlage 10 (zu Nr. 28.1)

Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1995 zu: Automatische Erhebung von Straßennutzungsgebühren

Gegenwärtig werden Systeme zur automatischen Erhebung von Straßenbenutzungsgebühren in mehreren Versuchsfeldern erprobt. Sie können im Rahmen der weiteren Entwicklung zu zentralen Komponenten umfassender Verkehrstelematiksysteme (z. B. Verkehrsinformation und -leitung) werden.

Mit der Einführung derartiger Verkehrstelematiksysteme besteht die Gefahr, daß personenbezogene Daten über den Aufenthaltsort von Millionen Verkehrsteilnehmern, erhoben und verarbeitet werden. Exakte Bewegungsprofile können dadurch erstellt werden. Damit wären technische Voraussetzungen geschaffen, daß Systembetreiber und andere nachvollziehen können, wer wann wohin gefahren ist. Derartige Datensammlungen wären aus datenschutzrechtlicher Sicht nicht hinnehmbar, weil das Grundrecht auf freie Entfaltung der Persönlichkeit auch das Recht umfaßt, sich möglichst frei und unbeobachtet zu bewegen. Vor diesem Hintergrund ist es besonders wichtig, elektronische Mautsysteme datenschutzgerecht auszugestalten. Bei den anstehenden Entscheidungen sind andere Verfahren wie z. B. die Vignette einzubeziehen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, daß der Grundsatz der datenschutzgerechten Ausgestaltung von Systemen zur automatischen Erhebung von Straßenbenutzungsgebühren von allen Beteiligten am Feldversuch auf der BAB A 555 akzeptiert wird. Zur Umsetzung dieses Grundsatzes fordern die Datenschutzbeauftragten:

- Der Grundsatz der „datenfreien Fahrt" muß auch künftig gewährleistet sein. Über Verkehrsteilnehmer, die ordnungsgemäß bezahlen, dürfen keine Daten erhoben oder verarbeitet werden, die die Herstellung eines Personenbezugs ermöglichen. Es sind ausschließlich solche Zahlungsverfahren anzuwenden, bei denen die Abrechnungsdaten nur dezentral beim Verkehrsteilnehmer gespeichert werden. Die Verkehrsteilnehmer dürfen jedoch nicht gezwungen werden, einen lückenlosen Nachweis über ihre Bewegungen zu führen.
- Die Überwachung der Gebührenzahlung darf nur stichprobenweise erfolgen. Die Möglichkeit einer flächendeckenden Kontrolle ist von vornherein technisch und rechtlich auszuschließen. Die Gebührenkontrolle ist so zu gestalten, daß die Identität des Verkehrsteilnehmers nur dann aufgedeckt wird, wenn tatsächliche Anhaltspunkte dafür bestehen, daß die Gebühren nicht entrichtet worden sind.
- Die Verfahren der Gebührenerhebung und -kontrolle müssen für die Verkehrsteilnehmer durchschaubar sein. Der Verkehrsteilnehmer muß jederzeit über sein Guthaben, die Abbuchung und den eventuellen Kontrollvorgang informiert sein.
- Alle datenschutzrelevanten Systemkomponenten sind so auszugestalten, daß sie weder vom Betreiber noch von anderer Seite beeinträchtigt oder zurückgenommen werden können.

Die hierbei anzuwendenden Verfahren wären gesetzlich abschließend vorzugeben. Dabei ist sicherzustellen, daß anfallende personenbezogene Daten von allen beteiligten Stellen vertraulich behandelt werden und einer strikten Zweckbindung unterliegen. Ferner ist zu gewährleisten, daß Betreiber derartiger Systeme – unabhängig von ihrer Rechtsform – einer Datenschutzkontrolle nach einheitlichen Kriterien unterliegen. Die Bundesregierung wird aufgefordert, bei der anstehenden internationalen Normierung elektronischer Mautsysteme die datenschutzrechtlichen Anforderungen durchzusetzen.

Anlage 11 (zu Nr. 9.3.2)

Entschließung der Datenschutzbeauftragten des Bundes und der Länder zum Datenschutz bei elektronischen Geldbörsen und anderen kartengestützten Zahlungssystemen vom 13. Oktober 1995

Die Datenschutzbeauftragten das Bundes und der Länder halten es für dringend erforderlich, daß bei kartengestützten Zahlungssystemen, die zunehmend in Konkurrenz zum Bargeld treten, datenschutzfreundliche Verfahren eingesetzt werden. Dabei bietet es sich an, vor allem Guthabenkarten zu verwenden. Es sollten nur solche Clearingverfahren eingesetzt werden, die weder eine individuelle Kartennummer benutzen noch einen anderen Bezug zum Karteninhaber herstellen.

Sowohl im öffentlichen Personennahverkehr als auch bei der Deutschen Bahn AG können Fahrscheine bargeldlos erworben werden. Auch Autofahrer können auf Bargeld verzichten: Beim Parken, beim Tanken, künftig auch bei der Benutzung von Autobahnen wird verstärkt auf elektronisches Bezahlen zurückgegriffen. Immer mehr Telefonate und Warenautomaten werden auf bargeldlose Zahlungsverfahren umgestellt, so daß viele Artikel des täglichen Bedarfs elektronisch bezahlt werden können. Von Kreditinstituten wird die Kombination verschiedener Anwendungen auf einer Karte angestrebt, z. B. mit einer Kombination der Bezahlung für den öffentlichen Nahverkehr, Parkgebühren und Benutzungsentgelte für öffentliche Einrichtungen.

Zum elektronischen Bezahlen werden entweder Kreditkarten, Debitkarten oder Guthabenkarten eingesetzt. Bei Kredit- und Debitkarten werden sämtliche Zahlungsbeträge verbucht, dem Käufer in Rechnung gestellt, auf den Kontoauszügen ausgedruckt und für mindestens 6 Jahre gespeichert. Dagegen wird bei Guthabenkarten im voraus ein Guthaben eingezahlt und bei jeder einzelnen Zahlung das Guthaben entsprechend herabgesetzt; die Zahlungsbeträge müssen keinem Käufer zugeordnet werden.

Beim elektronischen Bezahlen entstehen sehr unterschiedliche Datenschutzrisiken. Bei Kredit- und Debitkarten besteht die Gefahr, daß die aus Abrechnungsgründen gespeicherten personenbezogenen Daten ausgewertet und zweckentfremdet genutzt werden: Informationen über den Kauf von Fahrscheinen oder über die Nutzung von Autobahnen können zu Bewegungsprofilen verdichtet werden. Das Konsumverhalten des einzelnen wird bis ins Detail nachvollziehbar, falls auch Kleineinkäufe am Kiosk nachträglich abgerechnet werden. Durch den Datenverkauf für Werbung und Marketing können sich weitere Risiken ergeben. Demgegenüber kann bei der Verwendung von Guthabenkarten auf das Speichern personen- oder kartenbezogener Daten aus erfolgten Zahlungen verzichtet werden.

Vor allem im Kleingeldbereich ist die Nutzung von Debit- und Kreditkarten entbehrlich, da fälschungssichere Guthabenkarten auf der Basis von Chipkarten mit integriertem Verschlüsselungsbaustein zur Verfügung stehen. Falls größere Geldbeträge nachträglich per Kredit- oder Debitkarte bezahlt werden, ist darauf zu achten, daß die Abrechnung zunächst über Konten erfolgt, deren Inhaber dem Zahlungsempfänger nicht namhaft gemacht wird. Erst bei Zahlungsunregelmäßigkeiten ist es notwendig, den Bezug zum Kontoinhaber herzustellen.

Angesichts der Risiken, aber auch der von Chipkarten ausgehenden Chancen, fordern die Datenschutzbeauftragten die Kartenherausgeber und die Kreditwirtschaft dazu auf, kartengestützte Zahlungssysteme zu entwickeln, die möglichst ohne personenbezogene Daten auskommen, und deren Anwendung so zu gestalten, daß ein karten- und damit personenbezogenes Clearing nicht erfolgt. Der Gesetzgeber muß sicherstellen, daß auch in Zukunft die Möglichkeit besteht, im wirtschaftlichen Leben im gleichen Umfang wie bisher anonym zu bleiben.

Anlage 12 (zu Nr. 2.2)

Entschließung der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. November 1995 zur Weiterentwicklung des Datenschutzes in der Europäischen Union

Die Konferenz der Datenschutzbeauftragten der Europäischen Union hat am 8. September 1995 in Kopenhagen in einer Resolution im Hinblick auf die für 1996 geplante Regierungskonferenz dafür plädiert, anläßlich der Überarbeitung der Unions- und Gemeinschaftsverträge in einen verbindlichen Grundrechtskatalog ein einklagbares europäisches Grundrecht auf Datenschutz aufzunehmen. Die Schaffung rechtsverbindlicher Datenschutzregelungen für die Organe und Einrichtungen der Union sowie die Schaffung einer unabhängigen und effektiven Datenschutzkontrollinstanz der EU werden angemahnt. Dieser Resolution schließt sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder an. Sie hält angesichts der fortschreitenden Integration und des zunehmenden Einsatzes von Informations- und Kommunikationstechnologien in der EU eine Weiterentwicklung des Datenschutzes im Rahmen der EU für geboten.

Sie fordert die zuständigen Politiker und insbesondere die Bundesregierung auf, dafür einzutreten, daß im EU-Vertragsrecht ein Grundrecht auf Datenschutz aufgenommen wird, die materiellen Datenschutzregelungen in der EU verbessert werden, das Amt eines Europäischen Datenschutzbeauftragten geschaffen wird sowie eine parlamentarische und richterliche Kontrolle der Datenverarbeitung der im EU-Vertrag vorgesehen Instanzen sichergestellt wird.

Grundrecht auf Datenschutz

Bei einer Weiterentwicklung der Europäischen Union ist es unabdingbar, daß dem Grundrechtsschutz eine angemessene Bedeutung beigemessen wird. Dies sollte dadurch geschehen, daß die Verträge zur Europäischen Union mit einem Grundrechtskatalog ergänzt werden. Mit einer Entschließung vom 10. Februar 1994 hat das Europäische Parlament einen Entwurf zur Verfassung der Europäischen Union zur Erörterung gestellt, der u. a. folgende Aussagen enthält: „Jeder hat das Recht auf Achtung und Schutz seiner Identität. Die Achtung der Privatsphäre und des Familienlebens, des Ansehens (. . .) wird gewährleistet."

Die Konferenz der Datenschutzbeauftragten ist mit ihrer Entschließung vom 28. April 1992 dafür eingetreten, daß in das Grundgesetz nach dem Vorbild anderer europäischer Verfassungen ein Grundrecht auf Datenschutz aufgenommen wird. Sie hat hierfür einen Formulierungsvorschlag gemacht. Auf ihren Konferenzen am 16./17. Februar 1993 und 9./10. März 1994 bekräftigten die Datenschutzbeauftragten des Bundes und der Länder ihre Position. Diese Forderung wurde aber wegen des Nichterreichens der notwendigen qualifizierten Mehrheit durch den Gesetzgeber nicht umgesetzt.

In Wirtschaft, Verwaltung und Gesellschaft der Staaten der EU erhält der Dienstleistungs- und Informationssektor eine zunehmende Bedeutung. Dies hat zur Folge, daß mit hochentwickelten Informationstechnologien von privaten wie von öffentlichen Stellen verstärkt personenbezogene Daten verarbeitet und auch grenzüberschreitend ausgetauscht werden. Diese Entwicklung wird gefördert durch die Privatisierung und den rasanten Ausbau transeuropäischer elektronischer Telekommunikations-Netze. Dadurch gerät das Grundrecht auf informationelle Selbstbestimmung in besonderem Maße auf der überstaatlichen Ebene in Gefahr. Dieser Gefahr kann dadurch entgegengetreten werden, daß in einen in den überarbeiteten EU-Vertrag aufzunehmenden Grundrechtskatalog das Grundrecht auf Datenschutz und zu dessen Konkretisierung ein Recht auf unbeobachtete Telekommunikation aufgenommen werden. Dies hätte folgende positive Auswirkungen:

- Anhand einer ausdrücklichen gemeinsamen Rechtsnorm kann sich eine einheitliche Rechtsprechung zum Datenschutz entwickeln, an die sowohl die EU-Organe wie auch die nationalen Stellen gebunden werden.
- Ein solches Grundrecht wäre die Basis für eine Vereinheitlichung des derzeit noch sehr unterschiedlichen nationalen Datenschutzrechts auf einem hohen Niveau.
- Den Bürgerinnen und Bürgern wird deutlich erkennbar, daß ihnen in einklagbarer Form der Datenschutz in gleicher Weise garantiert wird wie die traditionellen Grundrechte.
- Das grundlegende rechtsstaatliche Prinzip des Datenschutzes wird dauerhaft, auch bei Erweiterung der EU, gesichert.
- Mit der rechtlichen Konkretisierung eines Rechts auf unbeobachtete Telekommunikation würde der zunehmenden Registrierung des Verhaltens der Bürgerinnen und Bürger in der multimedialen Informationsgesellschaft entgegengewirkt und der Schutz des Fernmeldegeheimnisses auch nach dem Abbau der staatlichen Monopole im Sprachtelefondienst sichergestellt.

Materielle Datenschutzregelungen

Mit der kürzlich verabschiedeten EU-Datenschutzrichtlinie wird ein großer Fortschritt für den Datenschutz auf europäischer Ebene erreicht. Dies darf aber nicht den Blick dafür verstellen, daß in einzelnen Bereichen spezifische, dringend nötige Daten-

schutzregelungen fehlen. Insbesondere sind folgende Bereiche regelungsbedürftig:

- Es bedarf eines für die EU-Institutionen verbindlichen eigenen Datenschutzrechts. Die datenschutzrechtliche Verantwortung der Mitgliedstaaten einschließlich ihrer Datenschutzkontrolle der Übermittlung von Daten an EU-Institutionen bleibt dabei unberührt.
- Die geplante ISDN-Datenschutzrichtlinie darf weder einer völlig falsch verstandenen Subsidiarität zum Opfer fallen noch in unzureichender Form verabschiedet werden.
- Die im Bereich der Statistik bestehenden datenschutzrechtlichen Defizite sind abzubauen.
- Es soll eine Technikfolgenabschätzung bei der Förderung und Einführung neuer Informationstechniken mit Personenbezug durch die EU obligatorisch eingeführt werden.
- In den Bereichen Inneres und Justiz sind aufeinander abgestimmte verbindliche Regelungen mit hohem Datenschutzstandard, die die Datenverarbeitung in Akten und die Sicherung der Datenschutzkontrolle mit umfassen, zu schaffen.
- Es bedarf der Harmonisierung des Arbeitnehmerdatenschutzes auf hohem Niveau in den Staaten der EU.
- Für das Personal der EU-Organe ist der Arbeitnehmerdatenschutz sicherzustellen, was z. B. bei der Durchführung von Sicherheitsüberprüfungen insbesondere unter Beteiligung von Behörden der Heimatstaaten von großer Bedeutung ist.

Es ist zu prüfen, inwieweit Informationszugangsrechte in weiteren Bereichen eingeführt werden sollen.

Europäischer Datenschutzbeauftragter

Die Konferenz der EU-Datenschutzkontrollinstanzen (25./26. Mai 1994, 8. September 1995) und die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (25. August 1994) haben darauf hingewiesen, daß es an einer unabhängigen und effektiven Datenschutzkontrollinstanz fehlt, an die sich jeder wenden kann, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch Stellen der EU in seinen Rechten verletzt zu sein. Aufgabe eines Europäischen Datenschutzbeauftragten sollte die Behandlung aller Datenschutzbelange der EU sein. Dazu gehört nicht nur die Bearbeitung von Betroffeneneingaben, sondern auch die datenschutzrechtliche Beratung der EU-Organe und -Einrichtungen sowie deren anlaßunabhängige Kontrolle, die Begleitung informationstechnischer EU-Projekte und der entsprechenden EU-Normsetzung sowie die Zusammenarbeit mit den nationalen Kontrollinstanzen. Wegen der teilweise anders gelagerten Aufgaben sollen die Funktionen des Europäischen Datenschutzbeauftragten und des Bürgerbeauftragten nach den EG-Verträgen nicht vermengt werden. Die Bundesregierung sollte im Rahmen der Vorbereitung der Regierungskonferenz 1996 darauf hinwirken, daß ein unabhängiger Europäischer Datenschutzbeauftragter in den Verträgen über die Europäische Union institutionell abgesichert wird.

Parlamentarische und richterliche Kontrolle

Bei der Zusammenarbeit der EU-Staaten in den Bereichen Justiz und Inneres muß mit Besorgnis festgestellt werden, daß eine ausreichende parlamentarische und richterliche Kontrolle im EUV derzeit nicht gewährleistet ist. Die geplante Europol-Konvention ist hierfür ein Beispiel. Mit unbestimmten Formulierungen werden einem fast völlig freischwebenden Europäischen Polizeiamt informationelle Befugnisse eingeräumt, einem Amt, das keiner parlamentarischen Verantwortlichkeit und nur einer unzureichenden (teils nur nationalen) Rechtskontrolle unterworfen wird. Zur Wahrung des Datenschutzes bei der Umsetzung gemeinsamer Maßnahmen in den Bereichen Justiz und Inneres muß daher unbeschadet der Kontrolle durch die nationalen Datenschutzbehörden auch eine im Rahmen ihrer jeweiligen Zuständigkeiten lückenlose Kontrolle durch die nationalen Parlamente und Gerichte sowie durch das Europäische Parlament und den Europäischen Gerichtshof sichergestellt werden.

Anlage 13 (zu Nr. 6.5)

Entschließung der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. November 1995 zu Planungen eines Korruptionsbekämpfungsgesetzes

Derzeit gibt es Vorschläge, die Bekämpfung der Korruption durch Verschärfungen des Strafrechts und des Strafprozeßrechts mit weiteren Eingriffen in das Grundrecht auf informationelle Selbstbestimmung zu organisieren. Ein Beispiel dafür ist der Beschluß des Bundesrates vom 3. November 1995 zur Einbringung eines Korruptionsbekämpfungsgesetzes.

Nach dem vom Bundesrat beschlossenen Gesetzentwurf sollen Bestechlichkeit und Bestechung in den Kreis derjenigen Tatbestände aufgenommen werden, bei deren Verdacht die Überwachung des Fernmeldeverkehrs und der Einsatz technischer Mittel ohne Wissen des Betroffenen (§§ 100a, 100c StPO) angeordnet werden dürfen.

Die Datenschutzbeauftragten weisen demgegenüber darauf hin, daß es vorrangig um Prävention, nicht um Repression geht. Die Datenschutzbeauftragten treten für eine entschlossene und wirksame Bekämpfung der Korruption mit rechtsstaatlichen Mitteln unter strikter Beachtung der Freiheitsrechte ein.

Sie wenden sich zugleich gegen eine Rechtspolitik, welche noch bevor sie sich darüber im klaren ist, was die bisherigen Verschärfungen und Eingriffe an Vorteilen und an Nachteilen gebracht haben, auf weitere Verschärfungen und Eingriffe setzt.

Gerade gegenüber der Korruption gibt es Möglichkeiten, welche Effektivität versprechen und gleichwohl die Privatsphäre der unbeteiligten und unschuldigen Bürgerinnen und Bürger nicht antasten:

- Rotation derjenigen Mitarbeiterinnen und Mitarbeiter einer Behörde, deren Position und Aufgaben erfahrungsgemäß für Bestechungsversuche in Betracht kommen;
- Vier- und Sechsaugenprinzip bei bestimmten Entscheidungen;
- Trennung von Planung, Überwachung und Ausführung, von Ausschreibung und Vergabe;
- Prüfverfahren und Innenrevision;
- Codes of Conduct (formalisierte „Ethikprogramme") im Bereich der Wirtschaft;
- verbesserte Transparenz von Entscheidungsprozessen in der Verwaltung.

Die in den Gesetzentwürfen vorgesehene weitere Einschränkung von Grundrechten, die mit einer abermaligen Erweiterung der Telefonüberwachung verbunden wäre, ist nur vertretbar, wenn sie nach einer sorgfältigen Güter- und Risikoabwägung zusätzlich zu den o. g. Verfahrens- und Verhaltensmaßregeln als geeignet und unbedingt erforderlich anzusehen wäre.

Die Datenschutzbeauftragten verlangen, daß vor einer zusätzlichen Aufnahme von Straftatbeständen in den Katalog der Abhörvorschrift des § 100a StPO diese Abwägung durchgeführt wird.

Die Datenschutzbeauftragten fordern weiterhin, daß eine Erweiterung des genannten Straftatenkataloges nur befristet vorgenommen wird, damit sich vor einer Verlängerung die Notwendigkeit stellt, auf der Grundlage einer sorgfältigen Erfolgs- und Effektivitätskontrolle erneut die Erforderlichkeit und Verhältnismäßigkeit einer solchen Erweiterung des Grundrechtseingriffs zu überprüfen.

Die Datenschutzbeauftragten verlangen, daß der Gesetzgeber vor weiteren Eingriffen in Freiheitsrechte eine sorgfältige Güter- und Risikoabwägung vornimmt und dabei insbesondere verantwortlich prüft, ob sich die innenpolitischen Ziele mit Mitteln erreichen lassen, welche die informationelle Selbstbestimmung der Bürgerinnen und Bürger schonen.

Schließlich gibt die anstehende erneute Erweiterung des Katalogs von § 100a StPO Veranlassung, den Umfang der darin genannten Straftaten sobald wie möglich grundlegend zu überprüfen.

Anlage 14 (zu Nr. 9.2.2)

Entschließung der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. November 1995 zu: Datenschutzrechtliche Anforderungen an den Einsatz von Chipkarten im Gesundheitswesen

Die Datenschutzbeauftragten des Bundes und der Länder haben auf ihrer 47. Konferenz am 9./10. März 1994 kritisch zum Einsatz von Chipkarten im Gesundheitswesen Stellung genommen. In dem Beschluß wird die Nutzung von Patientenkarten von mehreren Voraussetzungen zur Sicherung des Persönlichkeitsrechts abhängig gemacht.

Seitdem werden in mehreren Ländern Modellversuche und Pilotprojekte durchgeführt. Die Bandbreite reicht

- von allgemeinen Patientenkarten, die an möglichst viele Patienten/Versicherte ausgegeben werden, eine Vielzahl von Krankheitsdaten enthalten und von einem unbestimmten Kreis von Personen und Institutionen des Gesundheitswesens zu vielfältigen Zwecken verwendet werden können (z. B. Vital-Card der AOK Leipzig, Persönliche Patientenkarte Neuwied, BKK-Patientenkarte Berlin)
- bis zu krankheitsspezifischen Karten für bestimmte Patientengruppen mit reduziertem Datensatz und einer Definition der Verwendung (z. B. Dialyse-Card, Diab-Card, Krebsnachsorgekarte, Defi-Card).

Datenschutzrechtlich stellen sich vor allem folgende Probleme:

- Die massenhafte Einführung der Karten erzeugt einen sozialen Druck auf die Betroffenen, sie mitzuführen und vorzuzeigen. Diesen Erwartungen wird sich der Betroffene vielfach nur unter Befremden des Arztes oder sogar der Gefahr, daß dieser die Behandlung ablehnt, verweigern können.
- Die Verwendung von allgemeinen Patientenkarten bringt die Gefahr einer pauschalen Offenbarung von medizinischen Daten mit sich.
- Dem Patienten wird die Last aufgebürdet, für die Sicherheit seiner medizinischen Daten selbst zu sorgen.

Die Datenschutzbeauftragten fordern alle für Kartenprojekte im Gesundheitswesen Verantwortlichen in Politik, Industrie, Ärzteschaft, Wissenschaft und in den Krankenversicherungen auf, das Recht auf informationelle Selbstbestimmung der betroffenen Patienten bzw. Versicherten zu gewährleisten. Die 50. Konferenz hält folgende Voraussetzungen für elementar:

1. Besondere Schutzwürdigkeit medizinischer Daten

Medizinische Daten sind besonders schutzwürdig, unabhängig davon, welche Technologien eingesetzt werden, ob die Patientendaten beim Arzt gespeichert und versandt oder über ein Netz abgerufen werden oder ob der Patient die Daten auf einer Chipkarte bei sich hat. Es handelt sich oftmals um belastende, schicksalhafte Daten. Zudem geht es nicht nur um Daten des Patienten, sondern auch um fremde Einblicke in die ärztliche Tätigkeit.

2. Wirksame Entscheidung der Betroffenen über die Verwendung einer Karte

Die freie Entscheidung der Betroffenen (Patienten/Versicherten), eine Chipkarte zu verwenden, muß gewährleistet sein. Dies umfaßt die Entscheidung,

- ob Daten auf einer Chipkarte gespeichert werden,
- welche der Gesundheitsdaten auf die Karte aufgenommen werden,
- welche Daten auf der Karte wieder gelöscht werden,
- ob die Karte bei einem Arztbesuch bzw. einem Apothekenbesuch vorgelegt wird und
- welche Daten im Einzelfall zugänglich gemacht werden.

Ein Widerruf der Entscheidung muß ohne Nachteile für die Betroffenen möglich sein. Die gleiche Freiheit der Entscheidung für oder gegen die Verwendung der Chipkarte muß für Ärzte und Apotheker gewährleistet sein. Eine wirksame Entscheidung für oder gegen die Verwendung einer Chipkarte setzt eine schriftliche, objektive, vollständige und nachvollziehbare Information über Zweck, Art, Umfang und Beteiligte der Chipkarten-Kommunikation voraus. Das Gesamtkonzept des Chipkarteneinsatzes und der damit verbundenen Datenverarbeitung muß für die Betroffenen überschaubar sein.

Auf der Karte darf nicht der Datensatz der Krankenversichertenkarte nach § 291 Abs. 2 SGB V, insbesondere nicht die Krankenversicherung und die Krankenversicherungs-Nr., gespeichert werden, da andernfalls – zumal bei allgemeinen Patientenkarten mit hohem Verbreitungsgrad – die Krankenversichertenkarte verdrängt und deren Nutzungsbeschränkungen umgangen werden.

3. Freiheit der Entscheidung

Die uneingeschränkte Freiheit der Entscheidung der Betroffenen für oder gegen die Verwendung einer Chipkarte muß gewährleistet sein, denn der Einsatz von Chipkarten im Gesundheitswesen führt keineswegs zwangsläufig zu größerer Autonomie der Patienten. Neue Technologien können sich auch als Verführung erweisen, deren Preis erst langfristig erkennbar wird. Die individuelle Entscheidung des Bürgers über die Verarbeitung seiner Daten war und bleibt ein zentrales Recht gegenüber Eingriffen

in seine Freiheitssphäre. Mit der Chipkarte können sich jedoch Situationen ergeben, in denen wirkliche Freiheit, tatsächliche Wahlmöglichkeit der Betroffenen nicht mehr gewährleistet sind und durch technische und organisatorische, rechtliche und soziale Rahmenbedingungen wiederhergestellt werden müssen.

Dem Staat kommt hier eine veränderte Rolle zu: Freiheitsrechte nicht einzuschränken, sondern sie zu sichern, wo Entwicklungen des Marktes und der Technologien sowie Gruppeninteressen die Entscheidungsfreiheit des Bürgers bedrohen. Die Technologie selbst kann für die Sicherung der Freiheitsrechte ein wertvolles Hilfsmittel sein. Darüber hinaus kommt der Informiertheit der Betroffenen ein zentraler Stellenwert zu. Ihre Kompetenz zur Entscheidung und zum praktischen Umgang mit der Karte muß gestärkt werden, damit sie auch langfristig die größtmöglichen Chancen haben, ihre Interessen durchzusetzen.

Mit der Ausstellung der Karte dürfen nur die Vorteile verknüpft werden, die sich unmittelbar aus den Nutzungspraktiken der Karte selbst ergeben. Die freie Entscheidung der Betroffenen, eine Karte zu nutzen oder dies abzulehnen, darf nicht durch einen Nutzungszwang oder eine Bevorzugung von Karten-Nutzern (z. B. durch Bonuspunkte) bzw. von Karten-Verweigerern eingeschränkt werden.

4. Keine Verschlechterung der Situation der Betroffenen

Durch die Einführung von Kommunikationssystemen mit Chipkarten dürfen die Betroffenen nicht schlechter gestellt werden als im konventionellen Verfahren. Die medizinische Versorgung, der Schutz der Gesundheitsdaten und die Mitentscheidungsrechte der Betroffenen müssen in Umfang und Qualität erhalten bleiben.

Das therapeutische Verhältnis Arzt/Patient darf sich durch den Einsatz von Chipkarten nicht verschlechtern. Freiheit und Vertrauen innerhalb des Arzt-Patienten-Verhältnisses sowie der Grundsatz der Abschottung der dem Arzt anvertrauten Informationen und der ärztlichen Erkenntnisse nach außen, gegen die Kenntnisnahme durch Dritte, müssen erhalten bleiben. Insbesondere muß der Gesetzgeber sicherstellen, daß die auf der beim Patienten befindlichen Chipkarte gespeicherten medizinischen Daten ebenso gegen Beschlagnahme und unbefugte Kenntnisnahme geschützt sind wie die beim Arzt gespeicherten Daten. Eine Kommunikation unter Vorlage der Karte mit Personen oder Stellen außerhalb des Arzt-Patienten-Verhältnisses, z. B. Arbeitgebern oder Versicherungen, muß vom Gesetzgeber untersagt werden.

Das sich im Gespräch entwickelnde Vertrauensverhältnis zwischen Arzt und Patient darf nicht durch eine chipkartenvermittelte Kommunikation verdrängt werden. Verkürzte Darstellungen medizinischer Sachverhalte auf der Chipkarte – z. B. mit Hilfe von Schlüsselbegriffen – dürfen nicht zu einer Minderung der Qualität des therapeutischen Verhältnisses führen; das liegt auch im Interesse des Arztes. Der Patient muß auch weiterhin die Möglichkeit des individuellen Dialogs wählen können. Dies schließt insbesondere die Freiheit des Betroffenen ein, eine Chipkarte im Einzelfall nicht vorzulegen, auf der Chipkarte nur einen begrenzten Datensatz speichern zu lassen oder zu entscheiden, welchem Arzt welche Informationen oder Informationsbereiche offenbart werden. Der Patient darf durch die Ausgestaltung und den Verwendungszusammenhang der Chipkarte nicht zur pauschalen Offenbarung seiner Daten gezwungen sein. So sind Daten auf der Chipkarte so zu ordnen, daß z. B. beim Zahnarzt die gynäkologische Behandlung geheim bleiben kann.

Es darf keine „Einwilligung in Chipkarten und Chipkartensysteme mit verminderter Datensicherheit geben. Der Gesetzgeber muß die Patienten vor „billigen Gesundheitskarten" ohne ausreichende Sicherung vor einer Nutzung durch Dritte schützen.

5. Sicherstellung der Integrität und Authentizität der Daten

Zur Sicherstellung der Vertraulichkeit, Integrität und Authentizität der Daten auf Chipkarten im Gesundheitswesen und zur Differenzierung der Zugriffsmöglichkeiten nach dem Grundsatz der Erforderlichkeit in unterschiedlichen Situationen sind kryptographische Verfahren sowie geeignete Betriebssysteme zur Abschottung unterschiedlicher Anwendungsbereiche nach dem Stand der Technik in Chipkarten und Schreib-/Lese-Terminals zu implementieren. Eine Protokollierung der Lösch- und Schreibvorgänge auf der Karte ist unverzichtbar.

Darüber hinaus ist für das infrastrukturelle Kartenumfeld (Herstellung, Verteilung, Personalisierung, . . ., Rücknahme) sicherzustellen, daß ausreichende technische und organisatorische Maßnahmen Berücksichtigung finden. Für die zur Erstellung und Personalisierung von Gesundheits-Chipkarten dienenden Systeme sowie die informationstechnischen Systeme und Verfahren, mit denen Daten auf der Chipkarte gelesen, eingetragen, verändert, gelöscht oder verarbeitet werden, muß der gleiche hohe Sicherheitsstandard erreicht werden.

6. Keine neuen zentralen medizinischen Datensammlungen

Der Einsatz von Chipkarten im Gesundheitswesen darf nicht zur Entstehung neuer zentraler Dateien von Patientendaten bei Kassenärztlicher Vereinigung, Krankenkassen, Kartenherstellern oder sonstigen Stellen führen. Dies gilt auch für das Hinterlegen von Sicherungskopien der auf der Karte gespeicherten medizinischen Daten. Es steht in der freien Entscheidung der Betroffenen, ob sie dem Arzt ihres Vertrauens eine umfassende Pflege aller Chipkarten-Daten – einschließlich der Sicherungskopien – übertragen oder nicht.

7. Leserecht des Karteninhabers

Der Karteninhaber muß das Recht und die Möglichkeit haben, seine auf der Chipkarte gespeicherten Daten vollständig zu lesen.

8. Suche nach datenschutzfreundlichen Alternativen

Angesichts der aufgezeigten Gefährdungen der informationellen Selbstbestimmung im Gesundheitswesen muß die Suche nach datenschutzfreundlichen Alternativen zur Chipkarte fortgesetzt werden.

Vorstehende Kriterien sind der Maßstab für die datenschutzrechtliche Bewertung von Projekten für die Einführung von Chipkarten im Gesundheitswesen.

Die Datenschutzbeauftragten von Bund und Ländern fordern die Gesetzgeber auf, die dringend notwendigen Regelungen zur Sicherung der Rechte von Patienten und Ärzten zu schaffen. Ebenso ist durch die Gesetzgeber den Besonderheiten der Datenverarbeitung auf Chipkarten durch bereichsspezifische Regelungen Rechnung zu tragen.

Anlage 15 (zu Nr. 2.1.5)

Entschließung der 51. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 1996 zu: Modernisierung und europäische Harmonisierung des Datenschutzrechts

Die Datenschutzrichtlinie der Europäischen Union vom Oktober 1995 verpflichtet alle Mitgliedstaaten, ihr Datenschutzrecht binnen drei Jahren auf europäischer Ebene zu harmonisieren. Die Richtlinie geht zu Recht von einem hohen Datenschutzniveau aus und stellt fest: „Die Datenverarbeitungssysteme stehen im Dienste des Menschen".

Die Datenschutzbeauftragten begrüßen diesen wichtigen Schritt zu einem auch international wirksamen Datenschutz. Sie appellieren an den Gesetzgeber in Bund und Ländern, die Umsetzung der Richtlinie nicht nur als Beitrag zur europäischen Integration zu verstehen, sondern als Aufforderung und Chance, den Datenschutz fortzuentwickeln. Die Datenschutzbeauftragten sprechen sich für eine umfassende Modernisierung des deutschen Datenschutzrechts aus, damit der einzelne in der sich rapide verändernden Welt der Datenverarbeitung, der Medien und der Telekommunikation über den Umlauf und die Verwendung seiner persönlichen Daten soweit wie möglich selbst bestimmen kann.

Die wichtigsten Ziele sind:

1. Weitgehende Vereinheitlichung der Vorschriften für den öffentlichen und privaten Bereich mit dem Ziel eines hohen, gleichwertigen Schutzes der Betroffenen, bespielsweise bei der Datenerhebung und bei der Zweckbindung bis hin zur Verarbeitung in Akten.

2. Erweiterung der Rechte der Betroffenen auf Information durch die datenverarbeitenden Stellen über die Verwendung der Daten, auf Auskunft, auf Widerspruch und im Bereich der Einwilligung.

3. Verpflichtung zu Risikoanalyse, Vorabkontrolle, Technikfolgenabschätzung und zur Beteiligung der Datenschutzbeauftragten bei der Vorbereitung von Regelungen mit Auswirkungen auf den Datenschutz.

4. Verbesserung der Organisation und Stärkung der Befugnisse der Datenschutzkontrolle unter den Gesichtspunkten der Unabhängigkeit und der Effektivität.

5. Einrichtung und effiziente Ausgestaltung des Amtes eines internen Datenschutzbeauftragten in öffentlichen Stellen.

6. Weiterentwicklung der Vorschriften zur Datensicherheit, insbesondere im Hinblick auf Miniaturisierung und Vernetzung.

Darüber hinaus machen die Datenschutzbeauftragten folgende Vorschläge:

7. Erweiterung des Schutzbereichs bei Bild- und Tonaufzeichnungen und Regelung der Video-Überwachung.

8. Stärkere Einbeziehung von Presse und Rundfunk in den Datenschutz; Aufrechterhaltung von Sonderregelungen nur, soweit dies für die Sicherung der Meinungsfreiheit notwendig ist.

9. Sonderregelungen für besonders empfindliche Bereiche, wie den Umgang mit Arbeitnehmerdaten, Gesundheitsdaten und Informationen aus gerichtlichen Verfahren.

10. Sicherstellung der informationellen Selbstbestimmung bei Multimedia-Diensten und anderen elektronischen Dienstleistungen durch die Pflicht, auch anonyme Nutzungs- und Zahlungsformen anzubieten, durch den Schutz vor übereilter Einwilligung, z. B. durch ein Widerrufsrecht, und durch strenge Zweckbindung für die bei Verbindung, Aufbau und Nutzung anfallenden Daten.

11. Besondere Regelungen für Chipkarten-Anwendungen, um die datenschutzrechtliche Verantwortung aller Beteiligten festzulegen und den einzelnen vor unfreiwilliger Preisgabe seiner Daten zu schützen.

12. Schutz bei Persönlichkeitsbewertungen durch den Computer, insbesondere durch Beteiligung des Betroffenen und Nachvollziehbarkeit der Computerentscheidung.

13. Verstärkung des Schutzes gegenüber Adressenhandel und Direktmarketing.

14. Verbesserung des Datenschutzes bei grenzüberschreitender Datenverarbeitung; Datenübermittlung ins Ausland nur bei angemessenem Datenschutzniveau.

Anlage 16 (zu Nr. 6.1.2)

Entschließung der 51. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 1996 zu: Grundsätze für die öffentliche Fahndung im Strafverfahren

Bei den an die Öffentlichkeit gerichteten Fahndungsmaßnahmen nach Personen (Beschuldigten, Verurteilten, Strafgefangenen und Zeugen) wird stets das Recht des Betroffenen auf informationelle Selbstbestimmung eingeschränkt. Es bedarf daher nach den Grundsätzen des Bundesverfassungsgerichts im Volkszählungsurteil vom 15. Dezember 1983 für alle Maßnahmen der öffentlichen Fahndung nach Personen einer normenklaren und dem Grundsatz der Verhältnismäßigkeit entsprechenden gesetzlichen Regelung, die bisher fehlt.

1. Der Gesetzgeber hat zunächst die Voraussetzungen der öffentlichen Fahndung zu regeln und dabei einen sachgerechten Ausgleich zwischen dem öffentlichen Strafverfolgungsinteresse und dem Recht auf informationelle Selbstbestimmung des Betroffenen zu treffen.

   Die öffentliche Fahndung sollte nur bei Verfahren wegen Verletzung bestimmter vom Gesetzgeber zu bezeichnender Straftatbestände und bei Straftaten, die aufgrund der Art der Begehung oder des verursachten Schadens ein vergleichbares Gewicht haben, zugelassen werden.

   Sie soll nur stattfinden, wenn weniger intensive Fahndungsmaßnahmen keinen hinreichenden Erfolg versprechen.

   Der Grundsatz der Erforderlichkeit mit der gebotenen Beschränkung des Verbreitungsgebiets ist auch bei der Auswahl des Mediums zu berücksichtigen.

2. Bei der öffentlichen Fahndung nach unbekannten Tatverdächtigen, Beschuldigten, Angeschuldigten, Angeklagten einerseits und Zeugen andererseits erscheint es geboten, die Entscheidung, ob und in welcher Weise gefahndet werden darf, grundsätzlich dem Richter vorzubehalten; dies gilt nicht bei der öffentlichen Fahndung zum Zwecke der Straf- oder Maßregelvollstreckung gegenüber Erwachsenen.

   Bei Gefahr in Verzug kann eine Eilkompetenz der Staatsanwaltschaft vorgesehen werden; dies gilt nicht bei der öffentlichen Fahndung nach Zeugen. In diesem Falle ist unverzüglich die richterliche Bestätigung der Maßnahme einzuholen.

   Die öffentliche Fahndung nach Beschuldigten setzt voraus, daß ein Haftbefehl oder Unterbringungsbefehl vorliegt bzw. dessen Erlaß nicht ohne Gefährdung des Fahndungserfolges abgewartet werden kann.

3. Eine besonders eingehende Prüfung der Verhältnismäßigkeit hat bei der Fahndung nach Zeugen stattzufinden.

   Eine öffentliche Fahndung nach Zeugen darf nach Art und Umfang nicht außer Verhältnis zur Bedeutung der Zeugenaussage für die Aufklärung der Straftat stehen. Hat ein Zeuge bei früherer Vernehmung bereits von seinem gesetzlichen Zeugnis- oder Auskunftsverweigerungsrecht Gebrauch gemacht, so soll von Maßnahmen der öffentlichen Fahndung abgesehen werden.

4. In Unterbringungssachen darf eine öffentliche Fahndung mit Rücksicht auf den Grundsatz der Verhältnismäßigkeit nur unter angemessener Berücksichtigung des gesetzlichen Zwecks der freiheitsentziehenden Maßregel, insbesondere der Therapieaussichten und des Schutzes der Allgemeinheit angeordnet werden.

5. Die öffentliche Fahndung zur Sicherung der Strafvollstreckung sollte zur Voraussetzung haben, daß

   - eine Verurteilung wegen einer Straftat von erheblicher Bedeutung vorliegt und
   - der Verurteilte, der sich der Strafvollstreckung entzieht, (noch) eine Restfreiheitsstrafe von in der Regel mindestens einem Jahr zu verbüßen hat, oder ein besonderes öffentliches Interesse, etwa tatsächliche Anhaltspunkte für die Begehung weiterer Straftaten von erheblicher Bedeutung, an der alsbaldigen Ergreifung des Verurteilten besteht.

6. Besondere Zurückhaltung ist bei internationaler öffentlicher Fahndung geboten. Dies gilt sowohl für Ersuchen deutscher Stellen um Fahndung im Ausland als auch für Fahndung auf Ersuchen ausländischer Stellen im Inland.

7. Öffentliche Fahndung unter Beteiligung der Medien sollte in den Katalog anderer entschädigungspflichtiger Strafverfolgungsmaßnahmen des § 2 Abs. 2 StrEG aufgenommen werden.

   Durch Ergänzung des § 7 StrEG sollte in solchen Fällen auch der immaterielle Schaden als entschädigungspflichtig anerkannt werden.

   Der Gesetzgeber sollte vorsehen, daß auf Antrag des Betroffenen die Entscheidung über die Entschädigungspflicht öffentlich bekanntzumachen ist.

Anlage 17 (zu Nr. 25.2)

Entschließung der 51. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 1996 zu: Transplantationsgesetz

Bei der anstehenden gesetzlichen Regelung, unter welchen Voraussetzungen die Entnahme von Organen zur Transplantation zulässig sein soll, werden untrennbar mit der Ausformung des Rechts auf Selbstbestimmung auch Bedingungen des Rechts auf informationelle Selbstbestimmung festgelegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont hierzu, daß von den im Gesetzgebungsverfahren diskutierten Modellen die „enge Zustimmungslösung" – also eine ausdrückliche Zustimmung des Organspenders – den geringsten Eingriff in das Recht auf informationelle Selbstbestimmung beinhaltet. Sie zwingt niemanden, eine Ablehnung zu dokumentieren. Sie setzt auch kein Organspenderregister voraus.

Mit einer engen Zustimmungslösung ist auch vereinbar, daß der Organspender seine Entscheidung z. B. einem nahen Angehörigen überträgt.

Anlage 18 (zu Nr. 6.9)

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 9. Mai 1996 zu: Forderung zur sicheren Übertragung elektronisch gespeicherter personenbezogener Daten

Der Schutz personenbezogener Daten ist während der Übertragung oder anderer Formen des Transportes nicht immer gewährleistet. Elektronisch gespeicherte personenbezogene Daten können sowohl auf leitungsgebundenen oder drahtlosen Übertragungswegen als auch auf maschinell lesbaren Datenträgern weitergegeben werden. Oft sind die Eigenschaften des Transportweges dem Absender und dem Empfänger weder bekannt noch durch sie beeinflußbar. Vor allem die Vertraulichkeit, die Integrität (Unversehrtheit) und die Zurechenbarkeit der Daten (Authentizität) sind nicht sichergestellt, solange Manipulationen, unbefugte Kenntnisnahme und Fehler während des Transportes nicht ausgeschlossen werden können. Die Verletzung der Vertraulichkeit ist möglich, ohne daß Spuren hinterlassen werden.

Zahlreiche Rechtsvorschriften gebieten, das Grundrecht auf informationelle Selbstbestimmung auch während der automatisierten Verarbeitung personenbezogener Daten zu sichern (z. B. § 78a SGB X mit Anlage, § 10 Abs. 8 Btx-Staatsvertrag, § 9 BDSG nebst Anlage und entsprechende landesgesetzliche Regelungen).

Kryptographische Verfahren (z. B. symmetrische und asymmetrische Verschlüsselung, digitale Signatur) sind besonders geeignet, um Verletzungen des Datenschutzes beim Transport schutzwürdiger elektronisch gespeicherter Daten zu verhindern. Mit ihrer Hilfe lassen sich Manipulationen und Übertragungsfehler nachweisen und die unberechtigte Kenntnisnahme verhindern. Derartige Verfahren sind heute Stand der Technik und können in vielen Anwendungsfällen mit vertretbarem Aufwand eingesetzt werden.

Angesichts der beschriebenen Situation und der vorhandenen technischen Möglichkeiten fordern die Datenschutzbeauftragten des Bundes und der Länder, geeignete sichere kryptographische Verfahren beim Transport elektronisch gespeicherter personenbezogener Daten unter Berücksichtigung ihrer Schutzwürdigkeit anzuwenden.

Anlage 19 (zu Nr. 6.8)

Entschließung der 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22./23. Oktober 1996 über Eingriffsbefugnisse zur Strafverfolgung im Informations- und Telekommunikationsbereich

Die Entwicklung moderner Informations- und Telekommunikationstechniken führt zu einem grundlegend veränderten Kommunikationsverhalten der Bürger.

Die Privatisierung der Netze und die weite Verbreitung des Mobilfunks gehen einher mit einer weitreichenden Digitalisierung der Kommunikation. Mailboxen und das Internet prägen die Informationsgewinnung und -verbreitung von Privatleuten, von Unternehmen und öffentlichen Institutionen gleichermaßen.

Neue Dienste wie Tele-Working, Tele-Banking, Tele-Shopping, digitale Videodienste und Rundfunk im Internet sind einfach überwachbar, weil personenbezogene Daten der Nutzer in digitaler Form vorliegen. Die herkömmlichen Befugnisse zur Überwachung des Fernmeldeverkehrs erhalten eine neue Dimension; weil immer mehr personenbezogene Daten elektronisch übertragen und gespeichert werden, können sie mit geringem Aufwand kontrolliert und ausgewertet werden. Demgegenüber stehen jedoch auch Gefahren durch die Nutzung der neuen Technik zu kriminellen Zwecken. Die Datenschutzbeauftragten erkennen an, daß die Strafverfolgungsbehörden in die Lage versetzt werden müssen, solchen mißbräuchlichen Nutzungen der neuen Techniken zu kriminellen Zwecken wirksam zu begegnen.

Sie betonen jedoch, daß die herkömmlichen weitreichenden Eingriffsbefugnisse auch unter wesentlich veränderten Bedingungen nicht einfach auf die neuen Formen der Individual- und Massenkommunikation übertragen werden können. Die zum Schutz der Persönlichkeitsrechte des einzelnen gezogenen Grenzen müssen auch unter den geänderten tatsächlichen Bedingungen der Verwendung der modernen Informationstechnologien aufrechterhalten und gewährleistet werden. Eine Wahrheitsfindung um jeden Preis darf es auch insoweit nicht geben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat daher Thesen zur Bewältigung dieses Spannungsverhältnisses entwickelt.

Sie hebt insbesondere den Grundsatz der spurenlosen Kommunikation hervor. Kommunkationssysteme müssen mit personenbezogenen Daten möglichst sparsam umgehen. Daher verdienen solche Systeme und Technologien Vorrang, die keine oder möglichst wenige Daten zum Betrieb benötigen. Ein positives Beispiel ist die Telefonkarte, deren Nutzung keine personenbezogenen Daten hinterläßt und die deshalb für andere Bereiche als Vorbild angesehen werden kann. Daten allein zu dem Zweck einer künftig denkbaren Strafverfolgung bereitzuhalten, ist unzulässig.

Bei digitalen Kommunikationsformen läßt sich anhand der Bestands- und Verbindungsdaten nachvollziehen, wer wann mit wem kommuniziert hat, wer welches Medium genutzt hat und damit wer welchen weltanschaulichen, religiösen und sonstigen persönlichen Interessen und Neigungen nachgeht. Eine staatliche Überwachung dieser Vorgänge greift tief in das Persönlichkeitsrecht der Betroffenen ein und berührt auf empfindliche Weise die Informationsfreiheit und den Schutz besonderer Vertrauensverhältnisse (z. B. Arztgeheimnis, anwaltliches Vertrauensverhältnis). Die Datenschutzbeauftragten fordern daher, daß der Gesetzgeber diesen Gesichtspunkten Rechnung trägt.

Die Datenschutzbeauftragten wenden sich nachhaltig dagegen, daß den Nutzern die Verschlüsselung des Inhalts ihrer Nachrichten verboten wird. Die Möglichkeit für den Bürger, seine Kommunikation durch geeignete Maßnahmen vor unberechtigten Zugriffen zu schützen, ist ein traditionelles verfassungsrechtlich verbürgtes Recht.

Aus Sicht des Datenschutzes besteht andererseits durchaus Verständnis für das Interesse der Sicherheits- und Strafverfolgungsbehörden, sich rechtlich zulässige Zugriffsmöglichkeiten nicht dadurch versperren zu lassen, daß Verschlüsselungen verwendet werden, zu denen sie keinen Zugriff haben. Eine Reglementierung der Verschlüsselung, z. B. durch Schlüsselhinterlegung, erscheint aber aus derzeitiger technischer Sicht kaum durchsetzbar, da entsprechende staatliche Maßnahmen – insbesondere im weltweiten Datenverkehr – ohnehin leicht zu umgehen und kaum kontrollierbar wären.

Anlage 20 (zu Nr. 21.1.1)

Entschließung der 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22./23. Oktober 1996 zur automatisierten Übermittlung von Abrechnungsdaten durch Kassenzahnärztliche Vereinigungen an gesetzliche Krankenkassen

Der in dem Schiedsspruch vom 20. Februar 1995 für die Abrechnung festgelegte Umfang der Datenübermittlung zwischen Kassenzahnärztlichen Vereinigungen und gesetzlichen Krankenkassen erfüllt nicht die Anforderungen des Sozialgesetzbuches an diesen Datenaustausch. § 295 SGB V fordert, daß Daten nur im erforderlichen Umfang und nicht versichertenbezogen übermittelt werden dürfen.

Die Datenschutzbeauftragten begrüßen es deshalb, daß der größte Teil der gesetzlichen Krankenkassen in „Protokollnotizen" – Stand 22. März 1996 – den Umfang der zu übermittelnden Daten reduziert hat. Das Risiko der Identifizierbarkeit des Versicherten wurde dadurch deutlich verringert. Zum letztlich erforderlichen Umfang haben die Spitzenverbände der gesetzlichen Krankenkassen erklärt, daß genauere Begründungen für die Erforderlichkeit der Daten erst gegeben werden könnten, wenn das DV-Projekt für das Abrechnungsverfahren auf Kassenseite weit genug entwickelt sei.

Der Verband der Angestellten-Ersatzkassen (VdAK) hat bisher als einziger Spitzenverband der gesetzlichen Krankenkassen diese Datenreduzierungen nicht mitgetragen. Die Datenschutzbeauftragten fordern den VdAK auf, sich in der Frage der Datenübermittlung zwischen Kassenzahnärztlichen Vereinigungen und gesetzlichen Krankenkassen der einheitlichen Linie anzuschließen. Dies liegt im gesetzlich geschützten Interesse der Versicherten.

Die besonderen Vorgaben des Sozialgesetzbuches für die Prüfung der Wirtschaftlichkeit der ärztlichen Abrechnungen werden dadurch nicht berührt.

Anlage 21 (zu Nr. 8.2.3)

Arbeitskreis „Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder:

Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet

1. Dezember 1995

I. Einleitung

Seit einiger Zeit wächst in öffentlichen Stellen der Wunsch nach einem Zugang zu globalen Datennetzen, insbesondere zu dem Internet. Die Netzanbindung soll sowohl zur Informationsgewinnung als auch zur Bereitstellung eigener Informationen für andere dienen (zur Beschreibung des Internet und der wichtigsten Internetdienste vgl. Anlage 1).

Dabei ist der Anschluß an das Internet mit erheblichen Gefährdungen des Datenschutzes und der Datensicherheit verbunden. Die Risiken resultieren großenteils daraus, daß das Internet nicht unter Sicherheitsaspekten entwickelt wurde. Schwächen finden sich in den Protokollen für die Datenübertragung, in den Implementierungen und Installationen der Programme für die Internet-Dienste und in den angeschlossenen Rechnersystemen. So gibt es beispielsweise keine sicheren Mechanismen zur Identifikation und Authentisierung im Netz. Ohne besondere Schutzmaßnahmen kann sich ein Angreifer oft mit wenig Aufwand unter Ausnutzung der Sicherheitslücken unberechtigten Zugang zu fremden Rechnern verschaffen und dort Daten ausspähen oder sogar manipulieren oder zerstören. Dies ist besonders gravierend, weil angesichts von z. Zt. mehr als 40 Millionen Internet-Teilnehmern auch die Zahl der potentiellen Angreifer, die diese Sicherheitslücken ausnützen und somit die am Internet angeschlossenen Verwaltungsrechner bedrohen, sehr groß ist.

Die vorliegende Orientierungshilfe soll den für den Betrieb von Netzen der öffentlichen Verwaltung Verantwortlichen deutlich machen, mit welchen Risiken für die Sicherheit der „internen" Netze bei einem Anschluß an das Internet zu rechnen ist und wie diese Risiken begrenzt werden können. Die Frage, ob und ggf. unter welchen Bedingungen Verwaltungen personenbezogene Daten über das Internet austauschen dürfen, ist nicht Gegenstand der Orientierungshilfe und muß jeweils konkret untersucht werden.

Die hier entwickelten Strategien zur Risikobegrenzung bedürfen im Einzelfall einer weiteren Konkretisierung, wobei neben den beschriebenen Firewall-Architekturen ggf. weitere Maßnahmen zu ergreifen sind, um eine Gefährdung personenbezogener Daten zu vermeiden (etwa Einsatz von Verschlüsselungsverfahren). Angesichts einer sich ständig verändernden Gefährdungslage infolge der Entdeckung neuer unerwarteter Sicherheitsprobleme bleiben auch bei Einsatz von Firewall-Systemen erhebliche Restrisiken bestehen.

Der Anschluß an das Internet ist angesichts dieser Gefährdungslage aus Datenschutzsicht nur vertretbar, wenn zuvor eine eingehende Analyse und Bewertung der damit verbundenen Risiken erfolgt ist und die Gefahren durch technische und organisatorische Maßnahmen sicher beherrscht werden können. Die nachfolgenden Empfehlungen stellen ein Konzentrat aus den weiter unten angestellten eingehenderen Betrachtungen dar.

II. Empfehlungen

- Verwaltungsnetze dürfen an das Internet nur angeschlossen werden, wenn und soweit dies erforderlich ist. Die Kommunikationsmöglichkeiten haben sich am Kommunikationsbedarf zu orientieren. Dabei ist auch zu prüfen, inwieweit das Behördennetz in anschließbare, nicht anschließbare und bedingt anschließbare Teile segmentiert werden muß und ob die Aufgabe mit einem nicht in das Verwaltungsnetz eingebundenen Rechner erfüllt werden kann.

- Voraussetzung für die Anbindung eines Behördennetzes an das Internet ist das Vorliegen eines schlüssigen Sicherheitskonzepts und dessen konsequente Umsetzung. Die Internet-Anbindung darf nur erfolgen, wenn die Risiken durch technische und organisatorische Maßnahmen wirksam beherrscht werden können.

- Die Sicherheit des Verwaltungsnetzes und der Schutz von personenbezogenen Daten, die auf vernetzten Systemen verarbeitet werden, ist durch geeignete Firewall-Systeme sicherzustellen, die eine differenzierte Kommunikationssteuerung und Rechtevergabe unterstützen. Dabei sind die Anforderungen, die von den Firewall-Komponenten zu erfüllen sind, vorab zu definieren, wobei sich die Verwaltung ggf. auch externen Sachverstands bedienen sollte.

- Um der Gefahr von Maskeraden und der Ausforschung der Netzstrukturen des geschützten Netzes entgegenzuwirken, ist eine gesonderte interne Adreßstruktur zu verwenden. Die internen Adressen sind durch die zentrale Firewall auf externe Internet-Adressen umzusetzen.

- Der ausschließliche Einsatz einer zentralen Firewall-Lösung ist nur dann vertretbar, wenn eine Orientierung am höchsten Schutzbedarf erfolgt, auch wenn dies Nachteile für weniger sensible Bereiche mit sich bringt. Die Frage der Kontrolle interner Verbindungen bleibt bei einer solchen Lösung offen. Ferner ist eine ausschließlich zentrale Lösung mit der Maxime der lokalen Haltung und Verwaltung von sicherheitsrelevanten Daten (Pflege von Benutzerprofilen) schwer vereinbar. Werden solche Daten nicht durch diejenigen verwaltet, die den verwalteten Bereich direkt überschauen können, besteht die Gefahr erheblicher Differenzen zwischen Realität und sicherheitstechnischem Abbild.

- Das Konzept gestaffelter Firewalls kommt den Datenschutzanforderungen an Verwaltungsnetze entgegen, die aus einer Vielzahl verschiedener Teilnetze bestehen, in denen Daten unterschiedlicher Sensibilität von unterschiedlichen Stellen für unterschiedliche Aufgaben verarbeitet werden und in denen dementsprechend jeweils unterschiedliche Sicherheitsanforderungen bestehen. Die mit gesonderten Firewalls abgesicherten Subnetze sollten jeweils einen definierten Übergang zu dem Gesamtnetz erhalten. Die Anbindung des Gesamtnetzes an das Internet sollte stets über ein zentrales Gateway erfolgen, das durch eine Firewall geschützt wird.

- Der personelle und sachliche Aufwand für Firewall-Lösungen ist generell hoch. Es ist gleichwohl unverzichtbar, hochspezialisierte Kräfte einzusetzen, um gegen mindestens ebenso spezialisierte Angreifer gewappnet zu sein. Dieser Aufwand ist jedoch stets dann gerechtfertigt, wenn Verwaltungsnetze an das Internet angeschlossen werden sollen, in denen sensible personenbezogene Daten verarbeitet werden.

- Der Betrieb von Firewall-Systemen muß klaren Richtlinien folgen. Diese Richtlinien müssen neben Zuständigkeitsregelungen auch Vorgaben über die Protokollierung, die Behandlung von sicherheitsrelevanten Ereignissen und Sanktionen bei Sicherheitsverstößen enthalten.

- Auch bei Einsatz von Firewalls bleiben Restrisiken bestehen, denen anwendungsbezogen begegnet werden muß. So bleibt es auch beim Einsatz von Firewalls notwendig, sensible Daten nur verschlüsselt zu übertragen; hierzu gehören neben besonders sensiblen personenbezogenen Daten auch Paßwörter und sonstige Authentifikationsdaten.

- Bei einem unvertretbaren Restrisiko muß auf einen Anschluß des jeweiligen Netzes an das Internet verzichtet werden. Der Zugriff auf Internet-Dienste muß in diesem Fall auf nicht in das Verwaltungsnetz eingebundene Systeme beschränkt werden, auf denen ansonsten keine sensiblen Daten verarbeitet werden.

- Firewall-Konzepte entlasten die dezentralen Verwalter von vernetzten Systemen nicht von ihrer Verantwortung zur Gewährleistung des Datenschutzes; vielmehr erhöhen sich mit der Vernetzung die Anforderungen an die lokale Systemverwaltung, da Administrationsfehler ungleich schwerwiegendere Konsequenzen haben könnten als bei stand alone betriebenen Rechnern.

III. Sicherheitsrisiken im Internet

Die nachfolgend dargestellten Sicherheitsrisiken spiegeln lediglich einen kleinen Ausschnitt der möglichen Angriffe auf Rechnersysteme mit Internet-Anschluß wider. Selbst wenn Gegenmaßnahmen gegen die bekannten Gefährdungen getroffen werden, läßt sich ein hundertprozentiger Schutz ohne Verzicht auf die Netzanbindung nicht realisieren. Sobald ein Computer Zugang zu einem Datennetz hat, ist er von anderen angeschlossenen Rechnern aus erreichbar. Damit wird das eigene System der Gefahr eines unberechtigten Gebrauches ausgesetzt. Es gibt jedoch eine Reihe von Schutzvorkehrungen, um das Sicherheitsrisiko zu minimieren.

1. Protokollimmanente Sicherheitsrisiken

Sowohl die Nutzerkennung als auch das Paßwort werden bei den gängigen Diensten im Klartext über das lokale Netz (z. B. Ethernet) und über das Internet übertragen. Mit Programmen, die unter dem Namen Packet Sniffer bekannt sind, kann der Datenverkehr im Netz bzw. auf den Netzknoten belauscht und nach interessanten Informationen durchsucht werden. So können diese Abhörprogramme zahlreiche Nutzerkennungen mit den zugehörigen Paßworten ausspähen, mit deren Hilfe sich ein Angreifer einen unberechtigten Zugriff auf andere Rechner verschaffen kann.

Datenpakete können nicht nur abgehört, sondern auch manipuliert werden. Da bei vielen Internet-Diensten die Authentisierung der Rechner lediglich über die IP-Nummer des Nutzers erfolgt, kann sich dies ein Angreifer zunutze machen, indem er IP-Pakete mit gefälschten Absenderadressen ans fremde Rechnersystem schickt (IP-Spoofing). Sofern das System die IP-Adresse für vertrauenswürdig hält, wird dem Eindringling ein Zugang, unter Umständen sogar mit Administratorrechten, gewährt. Ferner kann der Übertragungsweg bei dynamischem Routing geändert werden. Pakete können abgefangen werden, so daß sie nicht an ihrem Ziel ankommen; ein Angreifer kann sie durch eigene Pakete ersetzen. Weiterhin läßt sich die Kommunikation eines authorisierten Nutzers mitschneiden und später wiedereinspielen, wodurch sich der Angreifer bei vielen Diensten die Rechte des Nutzers verschafft (z. B. beim Festplattenzugriff über NFS [Network File System]).

2. Dienstspezifische Sicherheitsrisiken

E-Mail und Usenet-News:

Private Nachrichten können mitgelesen werden, sofern sie nicht verschlüsselt sind. E-Mails und News-Artikel ohne eine digitale Signatur lassen sich leicht

verändern oder fälschen. Über den elektronischen Postweg können Programme und Textdokumente mit Viren ins System gelangen. Selbst ein automatisches Durchsuchen der Nachrichten nach Viren bietet keinen vollständigen Schutz.

Die Informationen über Datum und Uhrzeit der Erstellung einer Nachricht können zu einem Persönlichkeitsprofil des Absenders ausgewertet werden. Daneben forschen Adreßsammler nach E-Mail- und Post-Adressen, um unaufgefordert Werbung zuzuschicken.

Sendmail, das auf UNIX-Rechnern am häufigsten eingesetzte Programm zum Verschicken elektronischer Post, weist zudem eine ganze Reihe von sicherheitsrelevanten Fehlern auf, die zu einer Zugangsmöglichkeit mit Administratorrechten führen können.

Zudem ist nicht sicherzustellen, daß eine email den Empfänger überhaupt erreicht und daß der Absender einen Nachweis der Zustellung erhält.

Telnet:

Ist der Telnet-Dienst nicht eingeschränkt, sondern von beliebigen Adressen aus zu beliebigen Ports auf dem eigenen Rechner möglich, wird die Zugangskontrolle gefährdet. Auch ein Angreifer, dem es nicht gelingt, sich einen Zugang mit Administratorrechten zu verschaffen, hat häufig die Möglichkeit, einen nichtprivilegierten Account auf dem Rechner zu nutzen. Dieser Account kann dann als Ausgangsbasis für den Angriff auf weitere Rechner verwendet werden.

FTP:

Schlecht gewartete FTP-Server stellen ein Risiko dar, da in älteren Versionen des FTP-Server-Programms (ftpd) Sicherheitslücken existieren, die zur Erlangung von Administratorrechten führen können. Besondere Vorsicht ist geboten, da viele Beschreibungen zur Installation und Konfiguration von Anonymous-FTP-Servern sicherheitsbedenkliche Fehler enthalten. Bei Fehlkonfigurationen kann es einem Angreifer gelingen, die Datei mit den verschlüsselten Paßwörtern aller Benutzer auf seinen Rechner zu laden und dort in aller Ruhe zu entschlüsseln. Läßt man zu, daß Benutzer eines FTP-Servers eigene Dateien in Verzeichnissen ablegen können, wo andere sie sich holen können, kann sich der FTP-Server schnell zu einem Umschlagplatz von Raubkopien entwickeln.

WWW:

Gefährdungen entstehen bei WWW-Servern durch fehlerhafte Software oder Konfigurationen. Ohne den Einsatz von SSL (Secure Socket Layer) läßt sich die Kommunikation abhören. Außerdem weisen CGI (Common Gateway Interface)-Skripte häufig Sicherheitslücken auf. Zur Zeit sind WWW-Browser in der Entwicklung, die das Ablegen von Dateien auf dem Server erlauben. Dies kann zu weiteren Sicherheitsproblemen führen. Beim Nutzen des World Wide Web können zahlreiche Daten über den Anwender und sein Verhalten (was hat wer wann aufgerufen und wie lange gelesen?) protokolliert werden, so daß ein umfassendes Persönlichkeitsprofil erstellt werden kann.

Finger:

Die Daten, die der Finger-Dienst ausgibt, können einem Angreifer Informationen über die Nutzerkennungen auf dem System liefern, die gezielt für einen Angriff verwendet werden können. Berühmt geworden ist dieser Dienst 1988 durch den sogenannten Internet-Wurm. Dabei handelte es sich um ein Angriffsprogramm, das ausnutzte, daß die beim Aufruf von Finger übergebenen Parameter in einen Puffer fester Länge geschrieben wurden. Die Daten, die nicht mehr in den Puffer paßten, überschrieben den Stack im Arbeitsspeicher, wo sie als Programmcode behandelt und ausgeführt wurden. Bei geschickter Wahl der übergebenen Zeichenreihe kann so beliebiger Code zur Ausführung kommen. Ähnliche Programmfehler finden sich auch heute noch in vielen anderen Serverprogrammen. Zum Beispiel ist gerade Ende 1995 ein weiterer solcher Fehler im Programm Sendmail bekannt geworden. Der Protokollierbefehl Syslog und manche WWW-Browser (auch für MS-Windows) enthalten ebenfalls Fehler dieser Art.

IV. Kommunikationsanalyse

Bevor eine öffentliche Stelle Zugang zum Internet bekommt, muß sie eine Analyse des Kommunikationsbedarfs durchführen. Bei der Beurteilung der Erforderlichkeit eines Internet-Anschlusses ist ein strenger Maßstab anzulegen. Auch wenn die Erforderlichkeit bejaht wird, ist zu prüfen, ob der Verwendungszweck nicht schon durch den Anschluß eines isolierten Rechners erreicht werden kann.

Die Art des zu realisierenden Zugangs hängt wesentlich davon ab, welche Dienste des Internet genutzt werden sollen. Dabei ist zu unterscheiden zwischen Diensten, die von lokalen Benutzern im Internet abgerufen werden, und Diensten, die von lokalen Rechnern für Benutzer im Internet erbracht werden. Diese Kommunikationsanforderungen müssen auf Grund der unterschiedlichen Aufgaben sowohl für den zentralen Zugang zum Internet als auch für jeden einzelnen Rechner analysiert werden. Es dürfen nur die IP-Pakete weitergeleitet werden, die für den zu nutzenden Dienst bezogen auf den nutzungsberechtigten Rechner notwendig sind.

Wird bei der Analyse des Kommunikationsbedarfs festgestellt, daß die Anbindung an das Internet auf IP-Ebene notwendig ist, das TCP/IP-Protokoll also in seiner vollen Funktionalität genutzt wird, müssen weitere Sicherheitsbetrachtungen durchgeführt werden, die Voraussetzung für die Planung und Realisierung von Sicherheitskonzepten sind. Ausgangspunkte einer derartigen Risikoanalyse sind der Schutzbedarf der zu verarbeitenden Daten und die Sicherheitsziele der öffentlichen Stelle.

In Anlehnung an die Empfehlungen des BSI-Grundschutzhandbuches sind zur Feststellung des Schutzbedarfs folgende Fragen zu beantworten:

- Welche Datenpakete dürfen auf der Grundlage welchen Protokolls bis zu welchem Rechner im Netz weitergeleitet werden?
- Welche Informationen sollen nicht nach außen gelangen?
- Wie können z. B. die interne Netzstruktur und Benutzernamen nach außen unsichtbar gemacht werden?
- Welche Authentisierungsverfahren sollen benutzt werden; sind benutzerspezifische Authentisierungsverfahren notwendig?
- Welche Zugänge werden benötigt (z. B. nur über einen Internet-Service-Provider)?
- Welche Datenmengen werden voraussichtlich übertragen?
- Welche Rechner mit welchen Daten befinden sich im Netz, die geschützt werden müssen?
- Welche Nutzer gibt es im Netz, und welche Dienste sollen dem einzelnen Nutzer zur Verfügung gestellt werden?
- Welche Aktivitäten im Netz sollen protokolliert werden? (Dabei werden ggf. Fragen des Arbeitnehmerdatenschutzes tangiert)
- Welche Dienste sollen auf keinen Fall genutzt werden?
- Wird sichergestellt, daß nur die Dienste genutzt werden können, die ausdrücklich freigegeben worden sind (was nicht erlaubt ist, ist verboten)?
- Welcher Schaden kann im zu schützenden Netz verursacht werden, wenn Unberechtigte Zugang erhalten?
- Welche Restrisiken verbleiben, wenn die vorgesehenen Schutzmaßnahmen realisiert wurden?
- Welche Einschränkungen würden Benutzer durch den Einsatz von Schutzmaßnahmen akzeptieren?

Um im Rahmen der empfohlenen Kommunikationsanalyse beurteilen zu können, welche Dienste von welchem Nutzer an welchem Rechner tatsächlich benötigt werden, sollten die jeweiligen Stellen zunächst versuchen, genaue Kenntnisse über die Möglichkeiten und Gefährdungen der angebotenen Kommunikationsmöglichkeiten zu erlangen (etwa durch entsprechende Tests mit an das Internet angeschlossenen Einzelplatz-PC).

V. Firewalls

Soll ein Verwaltungsnetz an das Internet angeschlossen werden, so kann dies entweder durch einen zentralen Zugang oder durch mehrere dezentrale erfolgen. Aus Sicherheitsgründen ist ein zentraler Zugang vorzuziehen. Ist das Verwaltungsnetz erst einmal an das Internet angeschlossen, so lassen sich die durch die Anbindung hervorgerufenen Sicherheitsrisiken durch Einsatz einer Firewall reduzieren.

Unter einer Firewall (Brandschutzmauer) wird eine Schwelle zwischen zwei Netzen verstanden, die überwunden werden muß, um Systeme im jeweils anderen Netz zu erreichen. Die Hauptaufgabe einer Firewall besteht darin, zu erreichen, daß jeweils nur zugelassene netzübergreifende Aktivitäten möglich sind und daß Mißbrauchsversuche frühzeitig erkannt werden. Üblicherweise wird dabei davon ausgegangen, daß die Teilnehmer des internen Netzes (hier: des Verwaltungsnetzes) vertrauenswürdiger sind als die Teilnehmer des externen Netzes (hier: des Internet). Gleichwohl sind Firewall-Lösungen auch geeignet, die „grenzüberschreitenden" Aktivitäten der internen Nutzer, d.h. den Übergang zwischen verschiedenen Teilnetzen (z. B. Ressortnetze) innerhalb eines Verwaltungsnetzes zu begrenzen.

Firewalls weisen die folgenden Charakteristika auf:

- die Firewall ist die definierte und kontrollierte Schnittstelle zwischen dem zu schützenden und dem nicht vertrauenswürdigen Netz;
- im internen Netz besteht jeweils ein einheitliches Sicherheitsniveau; eine weitere Differenzierung nach Sicherheitsstufen geschieht – zumindest auf der Ebene des Netzes – nicht;
- die Firewall setzt eine definierte Sicherheitspolitik für das zu schützende Netz voraus; in diese müssen die Anforderungen aller vernetzten Stellen einfließen;
- es besteht die Notwendigkeit einer firewallbezogenen Benutzerverwaltung derjenigen internen Teilnehmer, die mit Rechnern in dem externen Netz kommunizieren dürfen.

Die Stärke der Firewall hängt wesentlich von der eingesetzten Technik und ihrer korrekten Administration ab; entscheidend für die Sicherheit sind jedoch auch die Staffelung und die organisatorische Einbindung von Firewalls in die IuK-Infrastruktur.

Von besonderer Relevanz ist der Aspekt, daß für den von einer Firewall geschützten Bereich das erforderliche Schutzniveau definiert wird. Diese Anforderung kann mit drei Lösungsvarianten erfüllt werden:

1. einheitlich hohes Schutzniveau im internen Netz, d. h. Orientierung am höchsten vorhandenen Schutzbedarf;
2. einheitlich niedriges Schutzniveau, d. h. Orientierung am niedrigsten vorhandenen oder einem insgesamt geringen oder mittleren Schutzbedarf;
3. einheitlich niedriges Schutzniveau sowie Durchführung zusätzlicher Maßnahmen zum Schutz von Netz-Komponenten mit höherem Schutzbedarf.

Die Varianten 1 und 2 entsprechen am ehesten zentralen Firewall-Lösungen, wobei angesichts der Sensibilität der in der Verwaltung verarbeiteten Daten allein Variante 1 mit den Anforderungen des Datenschutzrechts vereinbar sein dürfte. Variante 3 führt zur Lösung gestaffelter Firewalls, d.h. zu einer Konstellation, bei der neben einer zentralen, den mittleren Schutzbedarf abdeckenden Firewall (die u. a. die interne Netzstruktur nach außen sichert) bereichsbezogen und bedarfsorientiert Firewall-Anschlüsse mit

unterschiedlichem Sicherheitsniveau implementiert werden können. Allerdings können selbst bei einheitlich hohem Schutzniveau im Gesamtnetz gestaffelte Firewalls sinnvoll sein, um den möglichen Schaden, der mit Sicherheitsverletzungen verbunden ist, auf ein Netzsegment zu begrenzen. Dies gilt insbesondere auch für die Abwehr von internem Mißbrauch.

1. Zentrale Firewalls

Rein zentrale Firewall-Lösungen (vgl. Abb. 1) sind durch folgende Aspekte charakterisiert:

- die zentrale Firewall bildet die einzige Schnittstelle zwischen dem kompletten zu schützenden Verwaltungsnetz und dem übrigen Internet;
- innerhalb des Verwaltungsnetzes besteht ein einheitliches Sicherheitsniveau, eine weitere Differenzierung nach Sicherheitsstufen erfolgt nicht;
- eine Kontrolle der internen Verbindungen durch die Firewall ist nicht möglich;
- die zentrale Firewall setzt eine definierte Sicherheitspolitik für das gesamte Verwaltungsnetz voraus; abweichende Sicherheitspolitiken für besonders schützenswerte Bereiche sind auf Netzebene nicht durchsetzbar;
- es besteht die Notwendigkeit einer zentralen Benutzerverwaltung. Für jeden Teilnehmer muß sowohl auf Dienstebene als auch bezogen auf die zugelassenen Adressen die zulässige Kommunikation festgelegt werden.

Da eine zentrale Firewall eine Differenzierung nach Teilnetzen nicht unterstützt und dementsprechend ein einheitliches Sicherheitsniveau für das gesamte Verwaltungsnetz voraussetzt, muß sich der Grad des gewährleisteten Schutzes nach den sensibelsten Daten richten und ist dementsprechend hoch. Dies hat jedoch für Verwaltungsbereiche mit weniger sensiblen Daten den Nachteil, unnötig hohe Schranken zu errichten. Daraus ergibt sich die Gefahr, daß von diesen Stellen zusätzliche Internet-Zugänge mit geringeren Restriktionen geschaffen werden, wodurch der gesamte Zweck der Firewall ad absurdum geführt wird.

Ein weiterer Nachteil zentraler Firewalls besteht in dem – auch aus dem Großrechnerbereich bekannten – Problem, daß eine Benutzerverwaltung, die fernab von dem jeweiligen Fachbereich erfolgt, häufig zu Abweichungen zwischen der Realität von Benutzerrechten und deren Abbildung in Form von Accounts führt.

Da sich Firewall-Lösungen primär zum Schutz gegen Zugriffe von außen eignen, sekundär auch zum Schutz gegen Zugriffe von innen nach außen, jedoch nicht zur Kontrolle der rein internen Zugriffe, besteht bei rein zentralen Lösungen die Gefahr, daß das gesamte Verwaltungsnetz als eine Einheit betrachtet wird und insofern nur die Zugriffe von oder nach außen restringiert werden. Dieser Aspekt ist zwar nur mittelbar Teil des Themas „Internetanbindung", muß bei einer Gesamtbetrachtung von Netzwerksicherheit jedoch unbedingt einbezogen werden.

Der Einsatz einer alleinigen zentralen Firewall ist allenfalls dann vertretbar, wenn alle angeschlossenen Teilnetze über ein gleiches Sicherheitsbedürfnis bzw. -niveau verfügen und zudem nicht die Gefahr des internen Mißbrauchs besteht. Davon kann in behördenübergreifenden Verwaltungsnetzen mit einer Vielzahl angeschlossener Rechner jedoch nicht ausgegangen werden.

2. Gestaffelte Firewalls (Voraussetzungen, Einsatzmöglichkeiten, Forderungen)

Gestaffelte Firewall-Lösungen (vgl. Abb. 2) sind durch folgende Aspekte charakterisiert:

- es handelt sich um eine Kombination zentraler und dezentraler Komponenten, wobei durch eine zentrale Firewall ein Mindestschutz für das Gesamtnetz gegenüber dem Internet realisiert wird und dezentrale Firewalls in Subnetzen mit besonderem Schutzbedarf ein angemessenes Schutzniveau sicherstellen;
- innerhalb des jeweiligen geschützten Subnetzes besteht jeweils ein einheitliches Sicherheitsniveau;
- eine Kontrolle der verwaltungsinternen Verbindungen ist möglich, sofern die Kommunikation den durch dezentrale Firewalls geschützten Bereich überschreitet;
- auch ein gestaffeltes Firewall-System setzt eine definierte Sicherheitpolitik für das Gesamtnetz voraus; in diese müssen insbesondere die Anforderungen an einen zu garantierenden Grundschutz einfließen; darüber hinaus sind für die Subnetze gesonderte Sicherheitsanforderungen zu definieren;
- die Benutzerverwaltung kann weitgehend dezentralisiert werden. Allerdings sind einheitliche Regeln festzulegen, nach denen Benutzer das Recht haben, über die zentrale Firewall mit Systemen im Internet in Verbindung zu treten.

Für die dezentralen Firewalls bieten sich prinzipiell die gleichen Mechanismen wie bei einer zentralen Firewall an. Die Kombination zentraler und dezentraler Schutzmechanismen erlaubt die Realisierung des Prinzips eines autonomen Schutzes; bei sorgfältiger Konfiguration bleiben besonders geschützte Subnetze auch dann gesichert, wenn die zentrale Firewall durch einen Eindringling überwunden wurde.

Mit gestaffelten Firewalls kann – anders als bei zentralen Lösungen – das datenschutzrechtlich bedeutsame Prinzip der informationellen Gewaltenteilung abgebildet werden, mit dem es nicht zu vereinbaren wäre, wenn die Verwaltung als informatorisches Ganzes betrachtet würde. Die Teilnetze können sowohl gegen Angriffe von außen – aus dem Internet – als auch untereinander abgeschottet werden.

Da gestaffelte Lösungen besser als ausschließlich zentrale Firewalls die Anforderungen der Benutzer abbilden können, ist auch die Gefahr der Umgehung der kontrollierten Schnittstellen durch Schaffung wilder Internetzugänge geringer. Zudem würden sich

die Folgen derartiger Verstöße gegen die festgelegte Sicherheitspolitik besser isolieren lassen.

Auch gestaffelte Firewalls sind mit einem insgesamt hohen Administrations- und Pflegeaufwand verbunden, der jedoch auf die zentrale Firewall und jeweiligen Bereiche verteilt ist. Die Festlegung der individuellen Benutzerrechte kann dabei im wesentlichen den anwendernäheren dezentralen Firewalls zugeordnet werden.

Anlage 1: Dienste im Internet

Das Internet ist ein weltumspannender Zusammenschluß vieler lokaler Computernetze. Die Zahl der Benutzer wird auf etwa 40 Millionen geschätzt (Stand: Ende 1995). Bisher wurde das Internet hauptsächlich von wissenschaftlichen Einrichtungen wie Universitäten genutzt. Inzwischen hat sich der Nutzerkreis ausgeweitet, und es ist eine fortschreitende Nutzung für kommerzielle Zwecke zu beobachten. Der Datenübertragung im Internet liegen die einheitlichen TCP/IP-Protokolle (Transmission Control Protocol/Internet Protocol) zugrunde.

Jeder Rechner im Internet erhält eine eindeutige numerische Adresse, die IP-Adresse. Die zu übertragenden Daten werden in Pakete zerlegt, die u. a. mit der Absender- und der Empfänger-IP-Adresse versehen werden. Die Datenpakete werden über zumeist eine Vielzahl von Zwischenstationen weitergeleitet, die den Weg zum Zielrechner aufgrund der Adreßinformationen bestimmen (Routing). Die Zwischenstationen tauschen die Daten über Wähl- oder Standverbindungen im Telefonnetz (per Kabel oder Satellit) aus.

Die wichtigsten Dienste, die das Internet bietet, werden im folgenden beschrieben.

E-Mail:

Electronic Mail (kurz E-Mail) ist der am weitesten verbreitete Internet-Dienst. E-Mail ermöglicht das Verschicken von „elektronischen Briefen" zwischen mehreren Computerbenutzern. Die Nachrichten können aus Texten, Programmen, Grafiken oder Tönen bestehen. Sender und Empfänger müssen jeweils eine eindeutige E-Mail-Adresse besitzen (Form: Name@Anschrift), die ähnlich der postalischen Anschrift funktioniert. Um E-Mails in andere Datennetze zu verschicken oder von dort zu empfangen, werden Gateways benötigt, die den Übergang von einem System zum anderen handhaben. E-Mail kann außerdem für eine indirekte Inanspruchnahme von anderen Diensten (z. B. FTP, WWW) genutzt werden.

Usenet-News:

Öffentliche Nachrichten werden im Internet in thematisch gegliederten Diskussionsforen (Newsgroups) ausgetauscht. Dieser News-Dienst wird auch als Usenet (Kurzform von Users' Network) bezeichnet. Er gleicht einer riesigen Zeitung mit Fachartikeln, Leserbriefen und Kleinanzeigen. Zur Zeit gibt es etwa 10 000 verschiedene Newsgroups, in denen pro Monat rund 3,2 Millionen Artikel mit einem Datenvolumen von ca. 14 GB geschrieben werden (Stand: August 1995). Die Artikel werden auf zentralen Rechnern (Newsservern) in Datenbanken gehalten; der Zugriff erfolgt über Newsreader-Programme.

Telnet:

Mit Hilfe von Telnet ist es möglich, auf einem entfernten Rechner eine Terminalsitzung aufzubauen (Remote Login) und textorientierte Anwendungen zu nutzen. Dazu benötigt man einen Account (Nutzerkennung und Paßwort) oder einen öffentlichen Zugang auf dem entfernten Rechner. Über Telnet sind zum Beispiel Informationssysteme wie Datenbanken oder Bibliotheken zu nutzen. Telnet wird ebenfalls häufig für die Fernwartung von Rechnern eingesetzt.

FTP:

FTP steht für File Transfer Protocol und dient dem Übertragen von Dateien zwischen Rechnern mit Hilfe eines normierten Befehlssatzes. Auf dem eigenen Rechner läuft der FTP-Client, der die Befehle an den entfernten FTP-Server weiterleitet. Voraussetzung für die Nutzung sind Accounts auf beiden Rechnern oder eine öffentliche Zugriffsmöglichkeit auf dem FTP-Server durch „Anonymous FTP", wodurch ein eingeschränkter Zugriff auf bestimmte Dateien des entfernten Rechners ermöglicht werden kann. Weltweit gibt es Tausende Anonymous-FTP-Server, die Programme, Texte, Grafiken oder Tondateien bereithalten.

Archie:

Archie ist ein mächtiger Dienst für die weltweite Suche nach Dateien auf FTP-Servern. Der Zugriff erfolgt über Telnet, E-Mail oder einen eigenen Archie-Client. Als Suchergebnis liefert Archie entweder Server-, Verzeichnis- und Dateinamen oder eine Kurzbeschreibung zu gesuchten Dateien.

WWW:

Der jüngste Internet-Dienst WWW (World Wide Web) kann nahezu alle anderen Dienste integrieren. Durch einen multimediafähigen Hypertext-Mechanismus wird eine einfache Bedienbarkeit erreicht. Der Kommunikation zwischen dem WWW-Client und dem WWW-Server, der die multimedialen Daten anbietet, liegt das Protokoll HTTP (HyperText Transport Protocol) zugrunde. Die WWW-Dokumente werden mit der Definitionssprache HTML (HyperText Markup Language) erstellt. Für die Generierung interaktiver WWW-Seiten können CGI (Common Gateway Interface)-Skripte installiert werden.

Gopher:

Gopher ist ein menü-orientiertes Werkzeug zur Recherche, das unabhängig davon eingesetzt werden kann, auf welchem Rechner die gesuchten Informationen zu finden sind, in welchem Format sie vorliegen und welche Zugriffsmöglichkeiten (FTP, Telnet, WAIS usw.) existieren. Jeder Gopher-Server ist öffentlich zugänglich. Benutzer können mit

ihrem Gopher-Client nur lesend auf die angebotenen Daten zugreifen. Gopher ist im WWW integriert.

WAIS:

WAIS (Wide Area Information Server) ermöglicht eine Volltextsuche in einer Vielzahl von Datenbanken ohne Kenntnis komplizierter Abfragesprachen. WAIS-Abfragen können mit Telnet, E-Mail, einem eigenen WAIS-Client oder über WWW durchgeführt werden.

Finger:

Finger ist ein Werkzeug zur Suche nach Informationen über Personen und Rechner, die an der Kommunikation im Internet beteiligt sind. Es können sowohl personenbezogene Daten (Name, E-Mail-Adresse, Telefonnummer, Arbeitszeit, öffentliche Schlüssel usw.) als auch sicherheitsrelevante Informationen über angeschlossene Rechner in Erfahrung gebracht werden.

WhoIs:

WhoIs wurde speziell zur Recherche nach personenbezogenen Daten von im Internet registrierten Nutzern entwickelt. Das Vorhaben, eine Datenbank mit weltweit allen Internet-Nutzern aufzubauen, konnte nicht realisiert werden. Zur Zeit existiert eine Vielzahl von einzelnen WhoIs-Servern, auf die mit Telnet oder mit besonderer Client-Software zugegriffen werden kann.

Anlage 22 (zu 9.1.1)

**Arbeitskreis „Technische und organisatorische Datenschutzfragen"
der Konferenz der Datenschutzbeauftragten des Bundes und der Länder:**

Anforderungen zur informationstechnischen Sicherheit bei Chipkarten

I. Einleitung

Chipkarten sind miniaturisierte IT-Komponenten, meist in der genormten Größe einer Kreditkarte. Sie haben Eingang ins tägliche Leben gefunden, gewinnen zunehmend an gesellschaftlicher Bedeutung und bedürfen aus der Sicht des Datenschutzes zur Wahrung der informationellen Selbstbestimmung und der informationstechnischen Sicherheit größter Aufmerksamkeit.

Die derzeit bekannteste Chipkarten-Anwendung ist die Telefonkarte, die ein Guthaben enthält, das beim Gebrauch der Chipkarte in einem Kartentelefon reduziert wird, bis das Konto erschöpft ist und die Chipkarte unbrauchbar wird. Ebenfalls allgemein bekannt ist die Krankenversichertenkarte (KVK), die lediglich einen gesetzlich vorgegebenen Inhalt hat und zur Identifizierung des Patienten sowie zur Abrechnung ärztlicher Leistungen verwendet wird. Sie ist ein Beispiel für eine Chipkarte, die lediglich die dem Versicherten erkennbare Oberfläche einer umfassenden IT-Infrastruktur ist. Was unterhalb dieser Oberfläche geschieht, ist für die Betroffenen nicht transparent.

Weitere neue Anwendungsbereiche von Chipkarten sind derzeit in der Diskussion bzw. in der Erprobung, z. B.:

- die Chipkarte im bargeldlosen Zahlungsverkehr
- Gesundheits- oder Patientenchipkarten zur Speicherung und Übermittlung medizinischer Daten.

Von der Technik her sind reine Speicherchipkarten zur Aufnahme von Daten (meist in Halbleiter-Technologie oder optischer Speichertechnik) von solchen Karten zu unterscheiden, in die Mikroprozessoren und speichernde Bauteile integriert sind. Solche Prozessorchipkarten sind als Kleinstcomputer ohne Mensch-Maschine-Schnittstelle anzusehen. Ihre Verwendung bedarf also zusätzlicher technischer Systeme zum Lesen der gespeicherten Daten, zum Aktivieren der Funktionen der Mikroprozessoren und zum Beschreiben der Speicher.

Systeme zur Erschließung der Funktionen von Chipkarten werden im folgenden Chipkartenbasierte Dienstleistungssysteme (CDLS) genannt. Beispiele für solche Systeme sind:

- Öffentliches Telefon-Kartenterminal
- Funktelefon (Handy)
- PC mit externem Kartenterminal oder integriertem Kartenleser
- Laptop mit PCMCIA-Kartenleser
- Geldausgabeautomat
- Point-of-Sale-Kartenterminal (POS-Kartenterminal)
- Versicherten-Kartenterminal in seiner Standalone-Ausführung (ohne PC-Anschluß)
- Kontoauzugsdrucker
- Airline-Checkin-Terminal
- Customer-Service-Terminal
- Fahrschein-/Parkticket-Terminal

Sicherheitsbetrachtungen zum Einsatz von Chipkarten müssen deshalb auch die Sicherheit dieser Infrastrukturen einbeziehen.

Wichtige Funktionalitäten der Chipkarten sind:

- Chipkarten als Speicher von Daten, die hinsichtlich ihrer Vertraulichkeit und/oder Integrität hohen Schutzbedarf aufweisen (z. B. Kontodaten, medizinische Individualdaten, Personalausweisdaten, Führerscheindaten);
- Chipkarten als Mittel zur Authentisierung ihres Trägers für die Gewährung des Zugriffs auf sicherheitsrelevante Daten und Funktionen (Kontoverfügungen, Änderung medizinischer Individualdaten);
- Chipkarten als Mittel zur Signatur von Dokumenten (Verträge, Willenserklärungen, Befunde etc.);
- Chipkarten als Träger elektronischer Geldbörsen.

Die weiteren Ausführungen dieses Papiers beschränken sich auf die für die Sicherheit der Informationstechnik relevanten Merkmale und Anforderungen an Chipkarten, sowohl in ihrer Funktion als Instrumente zur Herstellung von Sicherheit als auch als sicherheitsbedürftige IT-Komponenten.

Obwohl – wie die Krankenversichertenkarte zeigt – auch Speicherchipkarten datenschutzrechtlich relevant sind, beschränken sich die weiteren Ausführungen auf Prozessorchipkarten. Diese haben in Zukunft sowohl hinsichtlich ihrer Verbreitung und Anwendungen als auch in Hinblick auf datenschutzrechtliche Chancen und Risiken eine größere datenschutzrechtliche Bedeutung.

II. Empfehlungen zum Einsatz von Chipkarten

Für den datenschutzgerechten Einsatz von Chipkarten ist eine konsequente und überzeugende Sicherungstechnologie erforderlich. Datensicherungsmaß-

nahmen müssen in ihrer Gesamtheit einen hinreichenden Schutz der Daten vor Mißbrauch gewährleisten. Dabei ist von folgenden Gefahren auszugehen:

- unbefugte Preisgabe von Informationen (Verlust der **Vertraulichkeit**);
- unbefugte Veränderung von Informationen (Verlust der **Integrität**);
- unbefugte Vorenthaltung von Informationen oder Betriebsmitteln (Verlust der **Verfügbarkeit**);
- unbefugte Änderung identifizierender Angaben (Verlust der **Authentität**).

Diese Gefahren sind sowohl dann zu betrachten, wenn die Daten auf der Chipkarte gespeichert werden, als auch dann, wenn sie in einer externen Datenbank gespeichert werden, die durch Chipkarten erschlossen wird.

Vor der Entscheidung über den sicherheitsrelevanten Einsatz von Chipkarten-Anwendungen sollte eine projektbezogene Technikfolgenabschätzung durchgeführt werden, so wie dies Artikel 20 der EU-Datenschutzrichtlinie als Vorabkontrolle fordert. Zur Auswahl geeigneter und angemessener Sicherungsmaßnahmen ist eine systematische Einschätzung der Gefahren für das informationelle Selbstbestimmungsrecht und das Recht auf kommunikative Selbstbestimmung vorzunehmen und sind Lösungsvorschläge für eine Sicherungstechnologie zu erarbeiten.

Die Auseinandersetzung mit dem Phänomen „Chipkarte" zwingt zur Differenzierung zwischen den technischen Systemen und den Applikationen, die sich dieser Systeme bedienen, und der Chipkarte selbst. Genausowenig wie es „die" Chipkarte gibt, genausowenig kann man von „der" Chipkartenanwendung sprechen. Würde man datenschutzrechtliche und sicherheitstechnische Schlußfolgerungen ausschließlich aus einer der vielen Kombinationsmöglichkeiten ziehen, wäre eine Allgemeinverbindlichkeit der Aussagen bzw. Anforderungen nicht zu erreichen. Konkrete Rechtsprobleme und Risiken lassen sich nur mit einem Bezug zu bestimmten inhaltlichen und technischen Rahmenbedingungen aufzeigen. Die geplanten Gesundheits- und Patientenchipkartensysteme sind insoweit geeignete Beispiele.

Notwendig erscheint auch eine dauernde Bereitschaft, die schnell fortschreitende technologische Weiterentwicklung aufmerksam zu begleiten und bei Bedarf steuernd einzugreifen, denn die datenschutztechnischen Fragestellungen werden umso komplexer, je weiter sich die Chipkartentechnologie entwickelt.

Künftige neue Anwendungen werden sich tendenziell der Prozessorchipkartentechnologie bedienen. Prozessorchipkarten sind miniaturisierte Computer, die allerdings nicht über eigene Mensch-Maschine-Schnittstellen verfügen. Diese werden über CDLS realisiert. Datenschutzrechtliche Anforderungen erstrekken sich hier neben den CDLS auch auf die Rahmenbedingungen bei der Herstellung, bei der Initialisierung, beim Versand und bei der Ersatzbeschaffung von Chipkarten in Fällen des Verlustes oder der Zerstörung einschließlich des „Ungültigkeitsmanagements". Die Hersteller bieten Chipkarten an, deren Leistungsfähigkeit und Funktionsweise diesbezüglich zum Teil sehr unterschiedlich ist. Eine Standardisierung wäre auch aus datenschutzrechtlicher Sicht in diesem Bereich dringend zu empfehlen.

Das Sicherungskonzept für Chipkarten sollte folgende Mindestanforderungen erfüllen, wenn Schutzbedarf besteht:

1. Grundschutzmaßnahmen
   - Ausstattung des Kartenkörpers mit fälschungssicheren Authentisierungsmerkmalen wie z. B. Unterschrift, Foto, Hologramme.
   - Steuerung der Zugriffs- und Nutzungsberechtigungen durch die Chipkarte selbst.
   - Realisierung aktiver und passiver Sicherheitsmechanismen gegen eine unbefugte Analyse der Chip-Inhalte sowie der chipintegrierten Sicherheitsfunktionen.
   - Benutzung allgemein anerkannter, veröffentlichter Algorithmen für Verschlüsselungs- und Signaturfunktionen sowie zur Generierung von Zufallszahlen.
   - Sicherung der Kommunikation zwischen der Chipkarte, dem CDLS und dem ggf. im Hintergrund wirkenden System durch kryptographische Maßnahmen.
   - Sicherung unterschiedlicher Chipkartenanwendungen auf einer Chipkarte durch gegenseitige Abschottung.
   - Durchführung einer gegenseitigen Authentisierung von Chipkarte und CDLS mit dem Challenge-Response-Verfahren.
2. Erweiterte Sicherungsmaßnahmen
   - Realisierung weiterer „aktiver" Sicherheitsfunktionen des Betriebssystems wie „Secure Messaging", I/O-Kontrolle aller Schnittstellen, Interferenzfreiheit der einzelnen Anwendungen, Verzicht auf Trace- und Debug-Funktionen und dergleichen. Zur Sicherung von Transaktionen oder zur Rekonstruktion nicht korrekt abgelaufener Transaktionen kann ein Logging vorhanden sein.
   - Auslagerung von Teilen der Sicherheitsfunktionen des Betriebssystems in dynamisch bei der Initialisierung bzw. Personalisierung zuladbare Tabellen, damit der Chipkartenhersteller nicht über ein „Gesamtwissen" verfügt.
3. Grundsätzlich sollte zunächst die Möglichkeit in Betracht gezogen werden, daß bei der Chipkartenbenutzung Anonymität gewahrt bleiben kann. Ist dies nicht möglich, sollten Wahlmöglichkeiten anonymer Alternativen geschaffen werden.
4. Der Chipkarteninhaber bzw. die Betroffenen sollten die Möglichkeit erhalten, auf neutralen, zertifizierten Systemumgebungen die Dateninhalte und Funktionalitäten ihrer Chipkarten einzusehen (Gebot der Transparenz).

5. Die gesamte Infrastruktur ist zu dokumentieren und die Produktion, die Initialisierung und der Versand der Chipkarten zu überwachen.
6. Für die gesamte Infrastruktur ist ein Mindestschutzniveau vorzuschreiben, das bei unbefugten Handlungen das Strafrecht anwendbar macht.
7. Alle Systemkomponenten datenschutzrelevanter Chipkartenanwendungen sind auf der Basis der Grundsätze ordnungsgemäßer Datenverarbeitung zu evaluieren.
8. Für die Informationsstrukturen sind zu Echtheits- und Gültigkeitsüberprüfungen (z. B. Abgleich gegen Sperr- und Gültigkeitsdateien) Kontrollmöglichkeiten zu schaffen.
9. Sicherheitsrelevante Karten (z.B. Bankkarten) sollten über den gesamten Lebenszyklus der Karte kryptographisch gesichert sein.

III. Technische Grundlagen

III.1 Hardware der Chipkarten

Chipkarten gibt es in vielfältigen Bauformen, Funktionsweisen und Funktionsspektren.

Man unterscheidet Chipkarten hinsichtlich der

- Art der Datenübertragung bei der Interaktion mit der Außenwelt:
  - kontaktbehaftet oder
  - kontaktlos über elektromagnetische Felder (bestimmte kontaktlose Karten können auch über eine Entfernung von mehreren Metern von einem CDLS gelesen werden);
- Art der in der Karte bereitgestellten IT-Ressourcen:
  - reine Speicherchipkarten mit nicht flüchtigem Speicher (z.B. Identifikationskarten),
  - intelligente Speicherchipkarten mit EPROM (z. B. Telefonkarte) oder EEPROM (z. B. Krankenversichertenkarten
  - Prozessorchipkarten mit EEPROM, RAM, ROM und CPU
  - Prozessorchipkarten mit Coprozessor für die Abwicklung kryptografischer Verfahren (Krypto-Coprozessor).
- Art der Anwendung:
  - elektronischer Zahlungsverkehr (Elektronische Geldbörse),
  - Wegwerfkarten (Telefonkarte),
  - wiederaufladbare Karten (z. B. Chipkarten im öffentlichen Personennahverkehr),
  - multifunktionale wiederaufladbare Chipkarten (z. B. unterschiedliche „Geldbörsen auf einer Chipkarte)
  - Berechtigungskarten (z. B. Mobiltelefone, Betriebsausweise)

Der Mikroprozessor einer Chipkarte leistet derzeit ca. 1 Million Befehle pro Sekunde. Direktzugriffsspeicher (RAM) erreichen eine Kapazität von 512 Byte, Festwertspeicher (ROM) für das Betriebssystem erreichen derzeit eine Kapazität von 16 KB, der elektrisch löschbare, programmierbare Festwertspeicher (EEPROM) mit der Kapazität von 16 KB erlaubt die Installation einer kleinen Datenbank. Im Vergleich dazu leisten Mikroprozessoren heute üblicherweise eingesetzter PCs ca. 100–150 Millionen Befehle pro Sekunde und arbeiten mit RAM-Speichern von 8–32 MB.

III.2 Chipkarten-Betriebssysteme

Prozessorchipkarten verfügen über einen nicht überschreibbaren Speicherbereich, der keine Änderungen und somit auch keine Manipulationen ermöglicht.

In diesem „Read-Only-Memory" (ROM) befindet sich das Betriebssystem einer Chipkarte. Für Chipkarten-Betriebssysteme existiert u.a. die Normen aus der Serie ISO/IEC 7816, in der die Befehle solcher Systeme beschrieben werden. Die Chipkarten-Betriebssysteme nutzen diese Befehle in unterschiedlicher Weise, d. h. nicht jedes Betriebssystem unterstützt jedes Kommando oder jede Option eines Kommandos. Auch weisen fast alle Chipkarten-Betriebssysteme zusätzliche herstellerspezifische Kommandos auf. Die Chipkarten-Betriebssysteme ermöglichen die multifunktionale Nutzung von Chipkarten, können also mehrere unterschiedliche Anwendungen unterstützen.

Die folgende Darstellung wird an den internationalen Standard angelehnt:

III.2.1 Filesystem

Die Dateien des Betriebssystems sind hierarchisch organisiert. Den Ursprung des Dateisystems bildet das Master File (MF). Auf der MF-Ebene können Daten vorhanden sein, die von allen Anwendungen der Chipkarte gemeinsam genutzt werden (z. B. Daten über den Karteninhaber, Seriennummer, Schlüssel). Sie sind in der Regel in Elementary Files (EF) abgelegt.

Daneben gibt es auch sog. Dedicated Files (DF), die mit ihren untergeordneten EFs und ihren Funktionen die Anwendungen in einer Karte repräsentieren. Für jedes DF können separate Sicherheitsfunktionen definiert werden. Die DFs einer Chipkarte sind physikalisch und logisch voneinander getrennt, können aber auf die Daten auf der MF-Ebene zugreifen.

EFs können dem Betriebssystem zugeordnet sein und damit Daten enthalten, die das Betriebssystem nutzt, z.B. anwendungsbezogene Paßwörter, Schlüssel und andere Zugriffsattribute zu Nutzdaten. Ein direkter Zugriff mittels des CDLS ist nicht möglich.

Sie können aber auch die Nutzdaten einer Anwendung enthalten, die ggfs. erst nach einer Authentisierung unter Berücksichtigung von Sicherheitsattributen gelesen und/oder verändert werden. Es gibt unterschiedliche Dateistrukturen für EFs: Sie können Records mit fester (linear fixed) oder variabler (linear variable) Länge enthalten, können eine Ringstruktur mit fester Länge (cyclic) haben, können jedoch auch

eine amorphe, d. h. vom Benutzer frei wählbare Struktur (transparent) aufweisen, auf denen auf Daten byte- oder blockweise zugegriffen werden kann.

III.2.2 Authentisierung

Die Authentisierungstechniken zwischen Chipkarte und einer externen Einheit werden in der Norm ISO/IEC 9798-2 beschrieben. Es wird dabei zwischen interner Authentisierung, bei der sich die Chipkarte gegenüber der externen Einheit authentisiert und externer Authentisierung, bei der sich die externe Einheit gegenüber der Chipkarte authentisiert unterschieden. Die gegenseitige Authentisierung ist in Vorbereitung.

Neben diversen Befehlen zum Lesen, Schreiben und Löschen (jeweils nach der Authentisierung) von Files sowie zur Auswahl von zu bearbeitenden Files definiert ISO 7816-4 einige Kommandos, die für die Implementation von Sicherheitsfunktionalitäten bedeutsam sind:

- VERIFY zur Benutzerauthentisierung mit einer PIN. Dies kann eine auf MF-Ebene gespeicherte globale PIN oder eine DF-spezifische anwendungsbezogene PIN sein. Der Befehl überträgt die vom Nutzer eingegebene PIN und – falls erforderlich – die Nummer der zu überprüfenden PIN an die Karte. Diese vergleicht die eingegebene PIN mit dem gespeicherten Referenzwert. Ein Erfolg wird durch Senden des Status „OK" angezeigt, ansonsten ein interner Fehlversuchszähler dekrementiert und als Status „nicht OK" übertragen. Bei Zählerstand 0 wird die Anwendung der Applikation, die die PIN benutzt, blockiert. Bei einigen Betriebssystemen kann die Blockierung durch Eingabe eines Personal Unblocking Key (PUK) aufgehoben werden, der ebenfalls durch einen Fehlerzähler geschützt ist.
- INTERNAL AUTHENTICATE löst eine interne Authentisierung aus. Dazu erhält die Chipkarte den Schlüsselbezeichner des ausgewählten EF und Authentisierungsdaten (Zufallszahl). Die Chipkarte verschlüsselt dann die Zufallszahlen mit dem Schlüssel des ausgewählten EF und sendet das Chiffrat zurück. Die prüfende Einheit (z. B. das CDLS oder eine Patientenkarte) entschlüsselt und prüft die Übereinstimmung der Zufallszahlen.
- EXTERNAL AUTHENTICATE löst die externe Authentisierung aus. Dazu wird mit dem Befehl GET CHALLENGE eine Zufallszahl von der Chipkarte gefordert, die an die zu authentisierende Instanz übergeben wird. Diese verschlüsselt sie und sendet das Ergebnis zusammen mit der Nummer des zu verwendenden Schlüssels an die Karte zurück. Dann entschlüsselt die Karte die Zufallszahl mit dem Schlüssel der angegebenen Schlüsselnummer. Bei Übereinstimmung wird die zu authentisierende Instanz als authentisch anerkannt.

Weitere Sicherheitsfunktionen werden derzeit in ISO 7816-8 spezifiziert. Von besonderer Bedeutung ist hierbei das Kommando PERFORM SECURITY OPERATION, mit dem folgende Sicherheitsoperationen ausgeführt werden können:

- COMPUTE DIGITAL SIGNATURE
- VERIFY DIGITAL SIGNATURE
- VERIFY CERTIFICATE
- HASH
- COMPUTE CRYPTOGRAPHIC CHECKSUM
- VERIFY CRYPTOGRAPHIC CHECKSUM
- ENCIPHER
- DECIPHER.

In ISO 7816-7 sind außerdem spezielle Sicherheitsfunktionen beschrieben, die sich auf Chipkarten mit einer sog. SCQL-Datenbank (Structured Card Query Language) beziehen.

III.3 Chipkartenbasierte Dienstleistungssysteme (CDLS)

Wie in der Einleitung kurz dargestellt, sind Chipkarten nicht als isolierte Träger von Risiken zu betrachten, wenn es um Fragen ihrer IT-Sicherheit geht. Aufwendige sicherheitstechnische Maßnahmen an und in der Chipkarte können durch unsichere Systemumgebungen bei der weiteren Verwendung der Daten konterkariert werden.

Wenn zum Beispiel das System eines zugriffsberechtigten Arztes nicht den erforderlichen Schutz bietet, können die Schutzmaßnahmen der Karte umgangen werden. Der Schutz der Chipkarte gegen unbefugte Manipulationen ist weitgehend wertlos, wenn beim elektronischen Zahlungsverkehr das POS-Terminal leicht manipuliert werden kann. Jedoch sieht ISO/IEC 7816 Schutzmechanismen vor, die bei richtiger Anwendung mit vertretbarem Aufwand nicht umgangen werden können.

Hier sollen jedoch nur für solche Komponenten Sicherheitsbetrachtungen angestellt werden, die chipkartenspezifisch sind. Solange die Chipkarten keine eigenen Mensch-Maschine-Schnittstellen enthalten, sind für die Erschließung der Chipkarteninhalte und -funktionen Systeme notwendig, mit denen die Chipkarten gelesen und beschrieben werden können. Auch wenn es einmal möglich sein wird, direkt mit der Chipkarte zu kommunizieren, z. B. über Sensorfelder, werden CDLS kaum entbehrlich sein, denn sie stellen zumindest die Schnittstelle zu jenen Nutzern dar, die mit dem Inhaber der Karte nicht identisch sind. CDLS können eigene Verarbeitungskapazitäten bieten und auch die Verbindung zu anderen Systemteilen herstellen.

Bisher sind für alle Chipkarten-Anwendungen (Telefonkarten, Krankenversichertenkarten, Sicherungskarten für Mobiltelefone usw.) spezielle CDLS entwickelt und eingesetzt worden. Soweit erkennbar, werden universell einsetzbare CDLS bisher nicht auf dem Markt angeboten. Im Gesundheitswesen werden derzeit CDLS eingesetzt, deren Verwendung auf die Kommunikation mit der Krankenversicherungskarte eingeschränkt wurde. Da sich weitergehende Anwendungen abzeichnen, wurde eine Spezifikatione für multifunktionale CDLS angefertigt, die von einem Arbeitskreis der Arbeitsgemeinschaft „Karten im Gesundheitswesen" und der Gesellschaft für

Mathematik und Datenverarbeitung (GMD) herausgegeben worden ist.

Dieser Spezifikation liegt folgende Konzeption zugrunde:

- Die CDLS sind transparent für jeden Dialog zwischen einem Anwendungsprogramm und einer Chipkarte, sofern dieser Dialog über eine genormte Schnittstelle geführt wird. Damit ist ihre Anwendung auch außerhalb des Gesundheitswesens möglich.
- Allerdings ist die Option, ein universell einsetzbares CDLS zu schaffen, aus pragmatischen Erwägungen heraus relativiert worden. Von den nach ISO 7816-3 zulässigen Optionen für die Übertragungsparameter wird nur ein Teil als obligatorisch gefordert. Dies entspricht der Politik des Kreditkartensektors, die zulässigen Lösungen enger zu fassen als das Spektrum der Optionen. Der Spezifikation entsprechende CDLS können sowohl mit synchronen Chipkarten wie die Krankenversicherungskarte als auch mit Prozessor-Chipkarten kommunizieren, die ein standardisiertes Übertragungsprotokoll unterstützen.
- Es können anwendungsspezifische Funktionen im CDLS realisiert werden, die dann nicht dem Anwendungsprogramm überlassen werden, solange nicht andere Vorkehrungen zum Schutz der Karte vor unbefugten oder durch Fehlfunktionen ausgelösten schreibenden Zugriffen getroffen sind. So ist z. B. ein Modul zur Verarbeitung der Versichertenkarte gem. § 291 SGB V für Gesundheitskarten-Terminal spezifiziert worden.
- Es können je nach Anwendung weitere anwendungsspezifische Module definiert werden, die periphere Geräte steuern. So wurde für die Gesundheitschipkarten ein Modul definiert, das einen Drucker steuert, damit Ärzte ohne IT-Einsatz die Kartensysteme zumindest für die Übertragung des Inhalts der Versichertenkarte auf die Belege der vertragsärztlichen Versorgung nutzen können. Das Druckmodul mit der parallelen Schnittstelle ist optional zu realisieren.
- Eine Download-Funktion erlaubt die Behebung von Softwarefehlern und ggf. im gewissen Umfang einen Upgrade von Leistungen.
- Die Spezifikation gilt für kontaktbehaftete Chipkarten nach ISO 7816 in 5-Volt-Technologie. Kontaktlose Chipkarten und kontaktbehaftete Chipkarten in 3-Volt-Technologie sollen einbezogen werden, wenn die Normung Klarheit geschaffen hat. Das gleiche gilt für eine Erweiterung von Standards für die Nutzung der Kontakte und für höhere als derzeit spezifizierte Übertragungsraten.
- Das Anwendungssystem in einem PC wird auf eine anwendungsunabhängige Schnittstelle für die Integration der Chipkartentechnik aufgesetzt.
- CDLS als separate Endgeräte können zusätzlich mit folgenden Optionen ausgestattet sein:
  - Display und/oder Tastatur,
  - mehrere Kontaktiereinheiten für eine Chipkarte im Normalformat gem. ISO-IEC 7816-2 oder im Plug-in-Format.

IV. Sicherheitstechnische Gestaltungsspielräume

Für die Entwicklung sicherer Chipkartenanwendungen gibt es eine Vielzahl von Ansatzpunkten, die je nach den in einer anwendungsspezifischen Sicherheitspolitik definierten Anforderungen zur Verbesserung der Sicherheit mit gewissen Spielräumen ausgenutzt werden können. In diesem abschließenden Kapitel geht es einerseits darum, diese sicherheitstechnischen Gestaltungsspielräume darzustellen und andererseits die Empfehlungen der Datenschutzbeauftragten zur Ausschöpfung dieser Spielräume hervorzuheben.

IV.1. Allgemeine Anforderungen

Wie bereits einleitend dargestellt sind Chipkarten als miniaturisierte Computer anzusehen, die (noch) nicht über eigene Mensch-Maschine-Schnittstellen verfügen. Daraus ergeben sich folgende Konsequenzen:

- Chipkarten sind leicht transportable Rechner. Die besonderen Bedrohungen der IT-Sicherheit, die z.B. bei anderen transportablen Rechnern (Laptops, Notebooks, . . .) berücksichtigten werden müssen, existieren in ähnlicher Weise auch für Chipkarten.
- Die Interaktion zwischen Mensch und Chipkarte bedarf zwischengeschalteter technischer Systeme (CDLS), die ebenfalls besonders zu sichern sind. Eine Chipkarte bildet zusammen mit dem CDLS ein vollständiges Rechnersystem mit Ein- und Ausgabekomponente. Die Evaluation der richtigen Funktionsweise setzt voraus, daß dabei alle Systemkomponenten einbezogen sind.
- Speicher- und Prozessorkapazitäten bilden Schranken für Sicherheitsfunktionen. Die technische Entwicklung dürfte diese Engpässe bald beseitigen. Heutige Betrachtungen müssen sie jedoch noch berücksichtigen.

Allgemein sind an die Sicherheitsfunktionen folgende Anforderungen zu stellen:

- Zugriffs- und Nutzungsberechtigungen sollten soweit möglich von der Chipkarte selbst geprüft und gesteuert werden.
- In Anwendungen sollten sich alle beteiligten Rechner (incl. Chipkarten) gegenseitig authentifizieren. Die Authentifizierung des Benutzers hat gegenüber der Chipkarte zu erfolgen, wobei für die Zukunft angestrebt werden sollte, daß dies in sicherer Umgebung oder ohne zwischengeschaltete Systeme erfolgen kann. Dies würde eine autonome Stromversorgung der Chipkarte und geeignete Mensch-Maschine-Schnittstellen voraussetzen (z. B. Sensorfelder für biometrische Merkmale).
- Es muß grundsätzlich ein Mindestschutz vorhanden sein, mit dem die in § 202a Abs. 1 StGB geforderte „besondere Sicherung gegen unberechtigten Zugang" realisiert wird, um bei unbefugter Nutzung einer Chipkarte das Strafrecht anwendbar zu machen.

IV.2. Hardwarebezogene Maßnahmen zur IT-Sicherheit bei Chipkarten

IV.2.1 Herstellung, Initialisierung und Versand von Chipkarten

Sicherheitserwägungen greifen bereits bei der Herstellung, Initialisierung und dem Versand von Chipkarten. Dabei müssen

- die Produktion der Prozessoren und Chipkarten,
- die Produktion und das Laden von Software,
- das Erzeugen der Schlüssel,
- das Laden der Schlüssel in die Sicherheitsmodule (Internal Elemetary Files),
- das Laden von Hersteller- und Transportschlüssel für die spätere Initialisierung und
- der Versand der Chipkarten und Transportschlüssel an den Empfänger

durch entsprechende technische und organisatorische Maßnahmen abgesichert werden.

IV.2.2 Sicherheitsmerkmale des Kartenkörpers

Zur Unterstützung der Authentifizierung des Karteninhabers gegenüber der Chipkarte und damit des Nachweises, daß die Chipkarte

- zur jeweiligen Anwendung gehört und
- die die Karte vorlegende Person die Karte rechtmäßig nutzt,

sollte der Kartenkörper mit Sicherheitsmerkmalen ausgestattet sein, die der Sensibilität angemessen sind:

- Aufdruck
- Hologramm
- Unterschrift des Besitzers (nur bei nicht anonymen Anwendungen)
- Foto des Besitzers (nur bei nicht anonymen Anwendungen)
- aufgebrachtes Echtheitsmerkmal
- Multiple Laser Image (durch Lasergravur auf der Chipkarte aufgebrachte hologrammähnliches Kippbild mit kartenindividuellen Informationen).

Dabei ist allerdings zu berücksichtigen, daß es Sicherheitsmerkmale gibt, die z.B. bei anonymen Chipkartenanwendungen (z.B. anonyme Zahlungsverfahren) die Anonymität aufheben würden und daher dabei nicht verwendet werden können.

IV.2.3 Sicherheitsmechanismen der Chip-Hardware

Sicherheitsmechanismen der Chip-Hardware richten sich vor allem gegen die Analyse der Chip-Inhalte und -Sicherheitssysteme mit Hilfe von Spezialgeräten, z. B. durch Abtragen dünner Chipschichten. Dabei kann unterschieden werden zwischen passiven Mechanismen, bei denen eine bestimmte Bauweise des Chips die Schutzfunktionen ergibt, und aktiven Mechanismen, die auf äußere Eingriffe passend reagieren und ggfs. den Chip zerstören.

Passive Mechanismen:

- Es gibt von außen keine direkte Verbindung zu den Funktionseinheiten. Ein Testmodus, der eventuell später nicht mehr erlaubte Zugriffe auf den Speicher ermöglicht, muß irreversibel auf den Benutzermodus geschaltet werden können.
- Interne Busse werden nicht nach außen geführt.
- Der Datenfluß auf den Bussen wird mit Scrambling geschützt.
- Der ROM befindet sich in den unteren Halbleiterschichten, um eine optische Analyse zu verhindern.
- Gegen das Abtasten von Ladungspotentialen erfolgt eine Metallisierung des gesamten Chips.
- Die Chipnummern werden eindeutig vergeben (werden u. U. von den Anwendungen benötigt).

Aktive Mechanismen:

- Es wird eine Passivierungsschicht aufgebracht, deren Entfernen einen Interrupt auslöst, der die Ausführung der Software unterbindet, sowie Schlüssel und andere sicherheitsrelevante Daten löscht.
- Es erfolgt eine Spannungsüberwachung. Wenn der Spannungswert den zulässigen Bereich über- oder unterschreitet, wird die weitere Ausführung von Prozessorbefehlen unterbunden.
- Den gleichen Zweck verfolgt die Taktüberwachung. Es werden damit Angriffe erschwert, mit denen die Abarbeitung einzelner Befehle analysiert werden soll.
- Es erfolgt eine Power-On-Erkennung, um bei Reset einen definierten Zustand herzustellen.

IV.3. Softwarebezogene Maßnahmen zur IT-Sicherheit bei Chipkarten

IV.3.1 Basisalgorithmen für Schutzfunktionen der Software

Die Schutzfunktionen der Chipkarten-Software basieren auf den bekannten und teilweise standardisierten Algorithmen zur Verschlüsselung, Signatur und Generierung von Zufallszahlen.

Dazu gehören symmetrische Verschlüsselungsalgorithmen wie DES, Triple-DES, IDEA und SC85 und asymmetrische Verfahren wie RSA, Signieralgorithmen wie DSS und RSA mit RipeMD160, Einwegfunktionen zur Berechnung des MAC und für das Hashing wie SHA und RipeMD160 sowie Zufallszahlengeneratoren.

IV.3.2 Schutzfunktionalitäten und -mechanismen des Betriebssystems

Zunächst sollte sichergestellt sein, daß sich nicht alle Teile des Betriebssystems im ROM befinden, damit der Chiphersteller nicht über das ganze Wissen über die Sicherung der Chipkarte verfügt. Wesentliche Teile des Betriebssystems können bei der späteren Initialisierung über entsprechend authentisierte CDLS dynamisch aus Tabellen geladen werden.

Darüber hinaus sollte das Betriebssystem in folgender Weise Sicherheit „erzeugen:

a) Die Identifizierung und Authentifizierung des Benutzers erfolgt mittels PIN oder mit biometrischen Verfahren.

   Üblicherweise erfolgt die Prüfung einer PIN. Zwar können die normale Forderungen zur Paßwortverwaltung bei Rechnern nicht voll auf Chipkarten übertragen werden, jedoch sollte die PIN-Länge je nach Sensibilität mindestens 4 oder mehr Stellen betragen, die Anzahl der Fehlversuche begrenzt sein, die Möglichkeit bestehen, die PIN zu ändern und eine Freischaltung der Karte auch mittels Personal Unblocking Key (PUK) in Abhängigkeit von der Anwendung ermöglicht werden.

   Biometrische Verfahren erfassen Fingerabdrücke, Augenhintergründe, Handgeometrien, Sprachmerkmale oder Unterschriftsdynamiken, verformeln sie und übertragen das Ergebnis zur Überprüfung auf die Chipkarte.

b) Es erfolgt eine Zugriffskontrolle mit einer Rechteverwaltung, wobei die Zugriffsrechte an die einzelnen Dateien geknüpft werden. Den Dateien sind Sicherheitsattribute zugeordnet, mit denen festgelegt wird, ob die Dateien (Daten) gelesen, kopiert, beschrieben, gelöscht, gesperrt oder freigegeben werden dürfen.

c) Wenn anderen Personen als dem Karteninhaber Zugriffsmöglichkeiten auf die Chipkarte gewährt werden sollen, erfolgt dies im Rahmen einer Programm-Programm-Kommunikation mit einem anderen Rechner oder einer anderen Karte (z. B. mit einer Professional Card). Der Rechner bzw. die andere Karte muß authentifiziert werden.

   Die Rechnerauthentifizierung wird meist nach einem auf DES basierenden Challenge-Response-Verfahren vorgenommen.

   Nach dem gleichen Schema verläuft die gegenseitige Authentifizierung von Chipkarte und Professional Card. Beide Benutzer müssen ihre Chipkarte aktivieren. Dann erfolgt die Authentifizierung zwischen den beiden Karten, wobei das CDLS die Daten transparent weiterleitet.

d) Zum Schutz gegen Ausforschung und Manipulation erfolgt eine sichere Datenübertragung zwischen Chipkarte und CDLS („Secure Messaging").

e) Auf Opto-Hybridkarten können die Daten auf der optischen Fläche verschlüsselt abgelegt werden. Die Entschlüsselung kann mit Hilfe des Prozessors erfolgen, der die Schlüssel verwaltet.

f) Das Betriebssystem führt eine I/O-Kontrolle aller Schnittstellen gegen unerlaubte Zugriffe durch.

g) Die Interferenzfreiheit der einzelnen Anwendungen wird gewährleistet, d. h. eine gegenseitige unerwünschte Beeinflussung der Anwendungen wird ausgeschlossen.

h) Trace- und Debugfunktionen sind nicht verfügbar.

i) Beim Initialisieren des Betriebssystems werden RAM und EEPROM geprüft.

j) Fehleingaben werden abgefangen.

k) Der Befehlsumfang wird auf die notwendigen Befehle reduziert. Funktionalitäten, die nicht zugelassen werden sollen, werden vom Betriebssystem unterbunden.

l) Die Dateiorganisation, Header und Speicherbereiche im EEPROM werden durch Prüfsummen abgesichert.

m) Das Betriebssystem sieht die Möglichkeit vor, die Chipkarte durch Löschung zu deaktivieren (etwa nach Ablauf einer Gültigkeitsdauer), jedoch verhindert es die mißbräuchliche Deaktivierung.

IV.3.3 Die Sicherheit der Anwendung

Die Betrachtung der Sicherheit bei der Anwendung von Chipkarten setzt die ganzheitliche Betrachtung der Kommunikation zwischen Chipkarten, CDLS und im Hintergrund wirkenden Systemen voraus. Die Kommunikation zwischen den einzelnen Systemen und Systembestandteilen ist ebenfalls mit kryptographischen Methoden zu sichern:

- Zur Unterstützung der Sicherheit der Kommunikation dienen Funktionen des Chipkarten-Betriebssystems zur gegenseitigen Authentifizierung von Chipkarten und Rechnern, zur sicheren Datenübertragung und zum Signieren und Verschlüsseln (siehe IV.3.2. c), d)).

- Gegen die unberechtigte Nutzung der Daten auf der Chipkarte muß eine Zugriffskontrolle erfolgen, die auf einer sicheren Identifikation und Authentifizierung der Benutzer beruht (siehe IV.3.2 a), b)).

Darüber hinaus sind die folgenden für die Sicherheit der Anwendung bedeutsamen Maßnahmen zu berücksichtigen:

- Den Dateien auf der Chipkarte sind Befehle zuzuordnen, die mit ihnen ausgeführt werden können. Die Ausführung anderer Befehle ist zu unterbinden.

- Zugriffe auf geschützte Datenbereiche und Veränderungen der Daten sollten protokolliert werden – vorzugsweise auf der Chipkarte. Die Anwendung muß die Auswertung der Protokolldaten unterstützen.

- Bedarfsweise sollten Überprüfungen durch Abgleich mit Hintergrundsystemen erfolgen, z. B. die Erkennung gesperrter Karten durch Abgleich mit Sperrdateien, Feststellung von Betragslimits im chipkartengestützten Zahlungsverkehr.

- Die eindeutige Nummer des Chips schützt vor der Erstellung von Dubletten.

Bei den letzten beiden Spiegelstrichen muß allerdings berücksichtigt werden, daß mit solchen Maßnahmen bei anonymen Systemen unter Umständen die Anonymität gefährdet sein kann. Es kann nicht immer ausgeschlossen werden, daß anonyme Chipkarten einzelnen Nutzern zugeordnet werden, wenn die Identifizierung der Karte möglich ist.

IV.4. Risiken und Anforderungen bei chipkartenbasierten Dienstleistungssystemen (CDLS)

Zwar bilden – wie oben festgestellt – Chipkarten und CDLS erst zusammen ein vollwertiges Rechensystem, jedoch befinden sich beide Komponenten in der Regel in unterschiedlicher Verfügungsgewalt, die Karte in der des Inhabers und das CDLS in der von Anwendern. Denkbar ist auch, daß bei Inhabern und Anwendern unterschiedliche Vorstellungen und Interessen mit der Nutzung verbunden werden. Wesentliche Teile der unabdingbaren Sicherheitsmechanismen der Karte können daher konterkariert werden, indem die Steuerungssoftware des CDLS verändert oder die Hardware des CDLS manipuliert wird. Eine Zertifizierung von CDLS kann sich daher nur auf unveränderliche Teile beziehen.

Wenn eine Chipkarte in ein CDLS eingeführt wird, gibt der Inhaber die Verfügungsgewalt über die Software auf der Karte und die ihn betreffenden Datenbestände auf. Eine unbefugte Veränderung der Software muß daher technisch verhindert werden.

Allerdings sind die Datenbestände grundsätzlich variabel. Sie können daher benutzt werden, über das CDLS Daten abzulegen, die für den Karteninhaber verdeckt sind und nur mit bestimmten Codes gelesen werden können (verdeckte Kanäle). Dies eröffnet Möglichkeiten für unbefugtes oder gar kriminelles Handeln.

Der Karteninhaber sollte daher nicht nur die Möglichkeit haben, sich den Inhalt der gespeicherten Daten anzeigen zu lassen, sondern die tatsächlichen Funktionen z. B. auf neutralen CDLS testen zu können. Wegen der u. U. unterschiedlichen Interessenlagen (z. B. in wirtschaftlichen Beziehungen) ist die Prüfung der korrekten Funktion der Software sowie umgekehrt des Ausschlusses ungewollter Funktionen im realisierbaren Rahmen zu ermöglichen.

Manipulationen an der Hardware und der Eingabesteuerungssoftware der CDLS können auch dazu führen, daß die geheimen oder unverfälschbaren Authentifizierungsmerkmale (PIN, biometrische Merkmale) bei der Authentifizierung des Kartenbesitzers in das CDLS übertragen und so Dritten bekannt werden.

Es sind daher folgende Sicherheitsanforderungen an CDLS zu stellen:

- Die CDLS müssen über mechanisch gesicherte Gehäuse verfügen, damit eine Hardware-Manipulation verhindert oder erschwert bzw. erkennbar wird.
- Sicherheitsmodule, die die für die vertrauliche Kommunikation mit Chipkarten und die gegenseitigen Authentifizierungen erforderlichen Hauptschlüssel enthalten, sind mechanisch (zum Beispiel durch Vergießung in Epoxidharz) und elektrisch gegen vielfältige Angriffsformen besonders abzusichern. Jeder Angriff auf das Sicherheitsmodul muß zum Löschen aller Schlüssel im Sicherheitsmodul führen. Dies setzt auch voraus, daß das Sicherheitsmodul weitgehend von der Stromversorgung des CDLS autark sein muß.
- Die CDLS müssen alle automatisch prüfbaren Sicherheitsmerkmale des Kartenkörpers prüfen können, müssen demzufolge also über die entsprechenden Sensoren verfügen (siehe IV.2.2).
- Sofern die Kommunikation zwischen Chipkarte und CDLS nicht durch kryptographische Verfahren gegen Abhören und Manipulation gesichert wird, ist das Abhören der Kommunikation durch mechanische Maßnahmen (sog. Shutter zum Abschneiden aller manipulativ mit der Karte in das CDLS eingebrachten Drähte) zu verhindern.

Als besonders angriffsgefährdet sind CDLS vom Typ „PC mit Kartenterminal" anzusehen, sofern sie nicht in manipulationsgeschützten Umgebungen eingesetzt werden. Erhöhte Schutzfunktionen werden hier als notwendig angesehen. Die bisherigen Spezifikationen für die CDLS lassen nicht erkennen, daß Maßnahmen gegen Penetrationsversuche aus der IT-Umgebung der Chipkartenanwendung im CDLS ergriffen werden können. Es fehlt daher an einem schlüssigen Sicherheitskonzept für das Zusammenspiel zwischen dem Betriebssystem und den Applikationen der (übergeordneten) IT-Umgebung und dem Betriebssystem und den Applikationen des Systems Chipkarte/CDLS.

Abkürzungsverzeichnis

CDLS	Chipkartenbasiertes Dienstleistungssystem
CPU	Central Processing Unit (Zentraleinheit)
DES	Symmetrischer Verschlüsselungsalgorithmus (Data Encryption Standard)
DF	Dedicated File
DSS	Signieralgorithmus (Digital Signature Standard)
EEPROM	Electrically Erasable Programmable Read Only Memory (elektrisch löschbarer, programmierbarer Festwertspeicher)
EF	Elementary File
EPROM	Erasable Programmable Read Only Memory (löschbarer, programmierbarer Festwertspeicher)
IDEA	Symmetrischer Verschlüsselungsalgorithmus
IEC	International Electrotechnical Commission
ISO	International Standardisation Organisation
IT	Informationstechnik

KB	Kilobyte
KT	Kartenterminal
KVK	Krankenversicherungskarte
MAC	Message Authentication Code
MB	Megabyte
MF	Masterfile
PC	Personal Computer
PIN	Persönliche Identifikations-Nummer
PUK	Personal Unblocking Key
RAM	Random Access Memory (Direktzugriffsspeicher)
RipeMD160	Hash-Algorithmus
ROM	Read Only Memory (Festwertspeicher)
RSA	Asymmetrischer Verschlüsselungsalgorithmus (Rivest- Shamir-Adleman)
SC 85	Symmetrischer Verschlüsselungsalgorithmus
SGB V	Sozialgesetzbuch V (Gesetzliche Krankenversicherung)
SHA	Secure Hash-Algorithmus

Literaturangaben

Das Papier basiert in wesentlichen Teilen auf dem Buch

Rankl, W.; Effing, W.: Handbuch der Chipkarten, Aufbau – Funktionsweise – Einsatz, München, Wien: Carl Hanser-Verlag, 1995

Ferner wurden verwendet:

Giesecke & Devirent GmbH (Hrsg.): Referenz-Handbuch STARCOS S 1.1, Januar 1995

Krummeck, G.; König, R.: Chipkarten im Gesundheitswesen – Technikfolgen-Abschätzung zur Sicherheit in der Informationstechnik, BSI-Schriftenreihe zur Informationstechnik, 1994

Zur ergänzenden Lektüre wird empfohlen:

Aberer, Karl: ISO/IEC 7816-8 SCQL-Database: Technik- und Mutzungsmöglichkeiten, in: Struif, B. (Hrsg.): Tagungsband des 6. GMD-Smart Card Workshops, GMD, 1996

Bachmeier, Roland: Chipkarten und Datenschutz, in: Struif, B. (Hrsg.): Tagungsband des 5. GMD-Smart Card Workshops, GMD, 1995

Ferreira, Malzahn, Quisquater, Wille: A High Performance Third Generation Crypto Card, in: Glade, Reimer, Struiff: Digitale Signatur und sicherheitssensitive Anwendungen, Vieweg

Fumy: Authentifizierung und Schlüsselmanagement, in: Struif, B. (Hrsg.): Tagungsband des 5. GMD-Smart Card Workshops, GMD, 1995

Hamann, Hirsch: Chipkarten-IC's – die richtige Lösung für sicherheitssensitive Anwendungen, in: Glade, Reimer, Struif: Digitale Signatur und sicherheitssensitive Anwendungen, Vieweg

Horster, Lender: Hybride Opto-Chip-Karten, in: Struif, B. (Hrsg.): Tagungsband des 5. GMD-Smart Card Workshops, 1995

Kruse, Peuckert: Chipkarte und Sicherheit; DuD 3/95, S. 142ff

Kruse: Sicherheitszertifikate für Chipkarten

Normann, Ute: Telefonkarten-Chip und Sicherheit, in Struif, B. (Hrsg.): Tagungsband des 6. GMD-Smart Card Workshops, GMD, 1996

SmartsCards – eine neue Dimension in der Informationstechnik, Der GMD-Spiegel 1/92, GMD, 1992

Struif, B.: Chipkarten – State of the Art, Tutorium „Verläßliche Informationssysteme", anläßlich der Fachtagung VIS 1991

Struif, B.: Neue Smart Card-Features aus Normensicht, in: Struif, B. (Hrsg.): Tagungsband des 6. GMD-Smart Card Workshops, 1996

Weikmann: Die neue Generation von Chipkarten-Mikrocontrollern, in: Glade, Reimer, Struiff: Digitale Signatur und sicherheitssensitive Anwendungen, Vieweg

Anlage 23 (zu Nr. 9.2.2)

10 Thesen der Arbeitsgemeinschaft „Karten im Gesundheitswesen"

Präambel

Karten im Gesundheitswesen mit medizinischen Inhalten sollen die Information der Ärzte in allen Leistungsbereichen über die von ihnen betreuten Patienten verbessern helfen. Die Karten sollen der Optimierung der Patientenversorgung, insbesondere im Notfall dienen.

Die Teilnahme an einem Kartenverfahren mit medizinischen Inhalten ist freiwillig und setzt die Aufklärung des Patienten voraus. Die Aufklärung des Patienten umfaßt: Zweck, Art, Umfang und Beteiligte des Chipkartenverfahrens sowie die Benennung der Zugriffsberechtigten.

1. Voraussetzung für jede Art von Kommunikation ist die Verständigung in **einer** Sprache (ICD, ICPM, EDTA, INN etc.).
2. Die Dokumentation aller **essentiellen** Daten und relevanten Informationen in Krankenakten und Karteien muß (zur problemlosen Übertragung) auch dieser Forderung unterworfen werden.
3. Die Forderung nach einer standardisierten Dokumentation betrifft sowohl den Inhalt als auch die Sequenz der dokumentationswürdigen Inhalte der essentiellen Daten („Minimum standard data set").
4. Notfalldaten sind von anwendungsspezifischen Anamnese-, Befund- und Behandlungsdaten getrennt zu präsentieren, weil deren schneller Kenntnisnahme höchste Priorität einzuräumen ist.
5. Die einheitliche Präsentation aller Notfalldaten ist – unabhängig von der Art der (Zwischen-) Speicherung – deswegen zu fordern, weil das schnelle (intuitive) Wiederauffinden der Informationen Priorität besitzt.
6. Verlaufsdaten, beispielsweise Meßdaten (Blutdruck, Zuckerwerte, Laborwerte u. a.) sind in einem getrennten Kompartment zu hinterlegen.
7. Der Patient ist Herr seiner Daten. Das bedeutet, daß ihm bei Freiwilligkeit der Teilnahme an einem Kartenprojekt das Recht der **vollständigen** Einsichtnahme, der notwendigen Ergänzung oder Löschung von Daten eingeräumt werden muß.
8. Der aufgeklärte Patient hat das Recht, zu entscheiden, welche seiner medizinischen Daten in die Karte aufgenommen werden und wem er die Daten im Einzelfall zugänglich macht.
9. Angaben des Patienten (Anamnese) oder seiner Angehörigen müssen als solche gekennzeichnet werden und sich von „erhobenen Befunden" Dritter (Ärzte, Assistenzberufe) unterscheiden lassen. Nur **gesicherte** Befunde werden dokumentiert.
10. Eine Protokollpflicht beim (Ein-)Lesen (Übernahme), Schreiben und Löschen von Daten ist unverzichtbar.

Anlage 24 (zu Nr. 10.4.15)

Der Bundesbeauftragte für den Datenschutz

Geschäftszeichen (bei Antwort bitte angeben)
VI – 191/52

☎ (02 28)
8 19 95 –

Datum
20. Dezember 1997

Der Bundesbeauftragte für den Datenschutz, Postf. 20 01 12, 53131 Bonn

An die
obersten Bundesbehörden

lt. Verteiler

Betr.: **Datenschutzprobleme in Telekommunikationsanlagen**

Bezug: Mein Schreiben vom 27. Dezember 1993 – VI – 191 / 52 –

Bereits mit o. g. Schreiben hatte ich auf einige Leistungsmerkmale moderner Telekommunikationsanlagen (TK-Anlagen) hingewiesen, deren Nutzung oft sehr hilfreich ist, die aber auch Datenschutzprobleme mit sich bringen.

Darüber hinaus sind mir durch Eingaben auf weitere Probleme bekannt geworden, auf die ich Ihre Aufmerksamkeit lenken möchte.

1. **„Anrufliste"**

Neuere TK-Anlagen besitzen – zum Teil nur für bestimmte Endgeräte – das Leistungsmerkmale „Anrufliste": Bei einem bestimmten Teilnehmer angekommene, nicht entgegengenommen Anrufe werden – hinsichtlich Datum, Uhrzeit, Rufnummer des Anrufers – zur Nutzung durch den Angerufenen automatisch in einer „Anrufliste" gespeichert. Dabei wird die Rufnummer des Anrufers nur angezeigt, wenn dieser entweder von einem ISDN-Anschluß aus angerufen hat oder aber von einem analogen Anschluß des sog. „T-Net" – der Anrufer also an eine digitale Vermittlungsstelle angeschlossen ist – und von der Telekom die Anzeige seiner Rufnummer beim Angerufenen verlangt hat.

Die „Anrufliste" wird von vielen gern genutzt, denn nach ihrem Aufruf ist der Rückruf zu einem der Anrufer mit lediglich einem Knopfdruck – zumeist der Wahlwiederholungstaste – möglich.

Anrufer, die dies alles nicht wissen, sind allerdings häufig über einen solchen Rückruf („Sie stehen in meiner Anrufliste!") sehr verwundert oder auch verärgert, nämlich dann, wenn sie dem Angerufenen z. B. die eigene Rufnummer nicht mitteilen wollten.

Der Eintrag eines Anrufes in die Anrufliste erfolgt nur, wenn der Anrufer das Leistungsmerkmal der Rufnummernübermittlung besitzt. Dieses Leistungsmerkmal kann für eine TK-Anlage an dieser selbst unterdrückt werden, für ISDN-Einzelanschlüsse durch die Telekom. Soll darauf jedoch nicht verzichtet werden, empfehle ich dringend, alle Nutzer der TK-Anlage sowohl über die Rufnummernübermittlung als auch über die Anrufliste zu informieren und diese Information in angemessenen Zeitabständen zu wiederholen.

Auch in der Dienstvereinbarung mit dem Personalrat über die Nutzung der TK-Anlage sollte ein entsprechender Hinweis enthalten sein.

2. **Anzeige der zuletzt gewählten Rufnummer**

Sowohl für Endgeräte von TK-Anlagen als auch bei modernen Telefonen an Einzelanschlüssen wird die zuletzt gewählte Rufnummer zumeist gespeichert, damit sie – z. B., falls der Anrufer nicht erreicht werden konnte – für die Funktion „Wahlwiederholung" genutzt werden kann.

Bei manchen TK-Anlagen wird durch die Vorwahl einer sog. PIN (personal identification number) ein danach gewähltes Gespräch als Privatgespräch gekennzeichnet.

Einige Endgeräte, aber auch manche TK-Anlagen, speichern aber nicht nur die zuletzt eingegebene *Telefonnummer* einer gewünschten Verbindung, sondern *alle* eingegebenen Ziffern – auch die PIN und die Nummer zum Aufschließen des „elektronischen Telefonschlosses". Dadurch können PIN und „Schloßnummer" durch Betätigung der Wahlwiederholtaste abgerufen und somit auch ausgespäht und unbefugt genutzt werden.

Ich empfehle insoweit eine Prüfung der bei Ihnen eingesetzten Technik sowie der Möglichkeit, die genannten Schwachstellen zu beheben. In jedem Fall erscheint auch hier ein Hinweis an alle Nutzer der TK-Anlage sowie in der Dienstvereinbarung mit dem Personalrat unerläßlich.

Im Auftrag

Anlage 25 (zu Nr. 28.1)

Anforderungen an die datenschutzgerechte Gestaltung von Systemen zur Automatischen Gebührenerhebung

Vorbemerkung

Die Darstellung ist auf Prepaid-Verfahren beschränkt, weil nach dem derzeitigen Stand nur diese Verfahren eine umfassende sichere Anonymisierung ermöglichen.

Allgemeine Anforderungen

- Die einzusetzende Technik ist so zu gestalten, daß nicht mehr Daten erfaßt und gespeichert werden können, als planmäßig vorgesehen ist, und Daten nur dann erfaßt und gespeichert werden, wenn die dafür festgelegten Bedingungen erfüllt sind.
- Das System muß so zuverlässig sein, daß auftretende Störungen und Fehler stets rechtzeitig erkannt werden. Diese müssen, soweit sie nicht vom Benutzer (Fahrer und/oder Halter des Fahrzeugs) zu vertreten sind, zu Lasten des Betreibers gehen. Diese Risikoverteilung ist geboten, weil der Benutzer keinen Einfluß auf die Systemgestaltung hat.
- Entsprechend den heutigen technischen Möglichkeiten ist die Sicherheit durch technische Vorkehrungen wie kryptographische Verschlüsselung (durch zertifizierte/gesiegelte Geräte) und digitale Signaturen zu gewährleisten, so daß die Protokollierung einzelner Nutzungen oder Zahlungen als überflüssig zu vermeiden ist. Insbesondere sind
  - die Verrechnungen zwischen dem Betreiber des AGE-Systems und dem Betreiber der gebührenpflichtigen Strecke sowie dem Emittenten des Zahlungsmittels so zu gestalten, daß Einzeldaten von Benutzern auch nicht zu Kontrollen der Korrektheit dieser Verrechnungen benötigt werden, und
  - die Abbuchungen von im voraus geleisteten Zahlungen ohne zentral (oder beim Emittenten) geführte Schattenkonten durchzuführen. Eventuell für erforderlich gehaltene Abstimmkreise sind so groß zu bilden und in einer Weise zu kontrollieren, daß die Buchungen nicht einzelnen Karten oder Benutzerkonten zugeordnet werden können und auch kein routing einer Karte bei einer konkreten Fahrt begünstigen.
- Protokolle über die Kommunikation zwischen dem Fahrzeug (einschließlich dessen AGE-Installation) und den straßenseitigen oder anderen Teilen des Systems dürfen nicht über das Ende einer Verbindung hinaus gespeichert werden. Eventuell anfallende Entgelte für die Kommunikationsdienste dürfen nicht individuell (dem Benutzer) zugerechnet, sondern nur pauschal oder aufgrund von Summenfortschreibungen dem Betreiber des AGE-Systems in Rechnung gestellt werden.
- Die Verteilung der Daten auf die im Fahrzeug fest installierten Geräte und die Karte(n) des Fahrers hat sich an den Interessen von Haltern und Fahrern zu orientieren. Hier können auch Wahlmöglichkeiten geboten werden, um unterschiedlichen Konstellationen Rechnung zu tragen.
- Das verfügbare Guthaben auf dem eingesetzten Zahlungsmittel sollte im Fahrzeug erkennbar sein.
- Wenn keine allgemeine Börse, sondern eine spezielle vorbezahlte AGE-Karte eingesetzt wird, muß der Inhaber einer Karte die Möglichkeit haben, sich anonym und ohne Angabe eines Grundes das Guthaben (ganz oder teilweise) erstatten zu lassen. Das verlangt wirksame technische Sicherungen gegen Manipulationen.
- Wenn im Rahmen einer abgestuften Reaktion auf Fälle von Nicht- oder Falschzahlen z. B. beim ersten „Fall" nur ein Hinweis an den Halter des Fahrzeugs erfolgt und zur Erkennung von Wiederholungsfällen eine Speicherung von Daten vorgesehen wird, so sind vertretbar kurze Löschungsfristen festzulegen. Außerdem ist zu bestimmen, was als Fall in diesem Sinne angesehen wird und was zu einem Fall als Wiederholungsfall gilt. Es ist zu gewährleisten, daß die jeweils Betroffenen über die Speicherung und deren Wirkung informiert sind.
- Die Tarifierung und die Informationsmöglichkeiten für den Fahrer sind so zu gestalten, daß er vor Antritt einer Fahrt die voraussichtlich zu zahlenden Gebühren und damit seinen Bedarf an Zahlungsmitteln abschätzen kann.
- Damit z. B. kein Unbefugter die Existenz einer Kontrollstelle mit Erfolg vortäuschen kann, müssen die zwischen dem Fahrzeug und dem System auszutauschenden Nachrichten mit technischen Mitteln gegen Fälschen und Verfälschen gesichert sein. Sonst würde ein nicht akzeptabler Zwang zur Protokollierung von Nachrichten entstehen, um mögliche Fälschungen durch nachträgliche Vergleiche erkennen zu können.

Zahlungen und Quittungen

- Die Daten, die ein Fahrzeug im Rahmen einer planmäßigen Zahlung sendet, müssen so beschaffen sein, daß
  - daraus kein Rückschluß auf das Fahrzeug möglich ist,
  - daraus keine Verknüpfung zu anderen Zahlungsdaten desselben Fahrzeugs oder zu den Kontrolldaten einer anderen Zahlung hergestellt werden kann und
  - im Prepaid-Verfahren das Zahlungsmittel nicht erkannt oder wiedererkannt werden kann.

- Wenn aus kommunikationstechnischen Gründen Identifikatoren während der Kommunikation benötigt werden, so dürfen auch diese kein Erkennen oder Wiedererkennen ermöglichen.
- Wenn die von einem Fahrzeug gesendeten Zahlungsdaten u. a. die Tarifklasse des Fahrzeugs und den Emittenten des Zahlungsmittels erkennen lassen, könnte man je nach den Umständen durch den Vergleich von Zahlungsdaten, die an hintereinander liegenden Mautstellen zu aufeinander folgenden Zeitpunkten empfangen wurden, mit mehr oder minder hoher Sicherheit Routen einzelner Fahrzeuge erkennen. Um dies zu vermeiden, müssen derartige Daten über einzelne Zahlungen im System unverzüglich weiterverarbeitet (z. B. auf Emittentenkonten gebucht und statistisch ausgewertet) und danach sofort gelöscht werden.
- Wenn das Fahrzeug Zahlungsdaten gesendet hat, die als falsch oder unplausibel erkannt werden, so muß unverzüglich dieser Fehler dem Fahrzeug signalisiert werden, um den Fahrer auf die Notwendigkeit der Abhilfe hinzuweisen.
- Der im Fahrzeug verfügbare Quittungsdatensatz zu einer Zahlung muß auch im Streitfall ohne Ergänzungen oder Vergleiche mit anderen Daten als Beweis dafür genügen, daß diese Zahlung für dieses Fahrzeug (einschl. Zeit und Grund) geleistet wurde. Ein entsprechender Einzelausdruck muß möglich sein. Diese Quittungsdatensätze müssen einzeln ausgedruckt und einzeln gelöscht werden können.
- Sollen fällige Zahlungen nicht einzeln, sondern zusammengefaßt geleistet werden, so müssen ein selbständiger Quittungsdatensatz für jeden Einzelposten und eine Sammelquittung für die Zahlung im Fahrzeug verfügbar sein.
- Wenn der im Fahrzeug verfügbare Quittungsdatensatz nur dann erzeugt wird, wenn von außen eine Nachricht darüber, daß die im Rahmen der Zahlung vom Fahrzeug gesendeten Daten angekommen und akzeptiert sind, gesendet und im Fahrzeug richtig empfangen wurde, so muß eine im Fahrzeug zu erzeugende Ersatzquittung für die Fälle vorgesehen werden, in denen das Fahrzeug den Betrag intern abgebucht und die Daten gesendet, aber die Nachricht von außen nicht (nicht verarbeitbar) erhalten hat. Diese Ersatzquittung muß bei einer Kontrolle als gültig angesehen werden, solange keine Anhaltspunkte für eine Manipulation bestehen.

Kontrollen

- Das Kontrollsystem darf nur dem Zweck dienen, einen möglichst hohen Anteil von Fahrten mit korrekter Zahlung zu erzielen. Dafür sind Stichproben an wechselnden Orten ausreichend, deren Dichte (relative Häufigkeit) nicht größer als erforderlich sein darf, um das richtige Zahlen auf Dauer billiger zu machen als das Nicht- oder Falschzahlen. Eine darüber hinausgehende oder gar flächendeckende Installation von Fahrzeugerkennungs- und -registrierungsgeräten, die nicht wirksam gegen die Änderung der Betriebsart auf „Vollerfassung aller Fahrzeuge" (also auch derer, für die richtig gezahlt wurde) gesichert werden können, würde einen nicht vertretbaren Überwachungsdruck schaffen.
- Kontrollen dürfen nur dann erfolgen, wenn durch eine gleichzeitige Prüfung der Funktion des Systems gewährleistet ist, daß Nicht- oder Falschzahlen nur vom Benutzer verursacht sein kann oder von ihm zu vertreten ist.
- Bei Kontrollen dürfen nur Daten zur letzten geleisteten Zahlung verlangt werden. Keine durchgreifenden Bedenken bestehen dagegen, daß in den Fällen, in denen die nachzuweisende Zahlung nicht geleistet wurde, Daten zur letzten tatsächlich geleisteten Zahlung vom Fahrzeug gesendet und vom System verarbeitet werden.
- Die bei einer Kontrolle vom Fahrzeug zu sendenden Kontrolldaten dürfen – außer Sicherungsdaten ohne weiteren Informationsgehalt – nur Angaben über Betrag, Zeit und Grund der Zahlung (Erhebungsstelle und Tarifmerkmale) enthalten und soweit für das Kontrollverfahren erforderlich – Identifikationsdaten des Fahrzeugs. Diese Identifikationsdaten sollten nicht geeignet sein, den Halter des Fahrzeugs zu ermitteln. Die Kontrolldaten dürfen über die Kontrolle eines Fahrzeuges hinaus nur gespeichert werden, wenn tatsächliche Anhaltspunkte dafür bestehen, daß für dieses Fahrzeug nicht oder nicht richtig gezahlt wurde, und nur in diesen Fällen dürfen weitere Daten, z. B. zur Ermittlung des Halters, aus dem Kontrollvorgang gespeichert werden.
- Um dem Fahrer eine Funktionskontrolle zu ermöglichen, sollen bei jeder Kontrolle sowohl das Stattfinden als auch der Erfolg oder Mißerfolg so signalisiert werden, daß diese Ereignisse im Fahrzeug bemerkbar sind. Darüber hinaus soll der Mißerfolg bei einer Kontrolle dem Fahrer möglichst sofort auch so angezeigt werden, daß er das auch ohne Funktionieren der entsprechenden Installationen im Fahrzeug bemerken kann.
- Wenn der Halter in einem Fall des Nicht- oder Falschzahlens in Anspruch genommen werden soll, so ist er unverzüglich über diesen Fall zu unterrichten. Soweit er seine Meldepflichten erfüllt und seine aktuelle Anschrift deshalb verfügbar ist, kann ein entsprechendes Schreiben z. B. mit e-Post innerhalb weniger Minuten bei der Post eingeliefert werden. Ohne vom Halter zu vertretenden Grund dürfen die vorzugebenden Ausschlußfristen nicht wesentlich länger sein.

Anlage 26 (zu Nr. 33.3)

Arbeitskreis „Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder:

Orientierungshilfe

„Datenschutzrechtliche Aspekte beim Einsatz optischer Datenspeicherung"

Die optische Datenspeicherung entwickelt sich in zunehmendem Maße zu einer Alternative für herkömmliche Datenträger- und Speicherungsmedien wie Magnetplatte, Diskette und Magnetband. Der Begriff der „optischen Datenspeicherung" ist abgeleitet vom zugrundeliegenden Aufzeichnungsverfahren mit Hilfe eines Laserstrahls. Auch bei der optischen Datenspeicherung können ähnlich wie bei der Mikroverfilmung – dem ältesten optischen Aufzeichnungsverfahren – Papierdokumente, Bilder und Graphiken optisch erfaßt, gespeichert und durch automatisierte Verfahren ausgewertet werden. Es kann daher nicht überraschen, daß auch für die optische Datenspeicherung Anwendungsmöglichkeiten einer papierlosen Datenverarbeitung und einer aktenlosen Verwaltung überlegt und erprobt werden.

Der Arbeitskreis „Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat die datenschutzrechtlichen Aspekte einer Verarbeitung und Archivierung mit optischen Datenspeichern untersucht und Empfehlungen für einen datenschutzgerechten Einsatz dieser neuen Medien erarbeitet, die im folgenden dargestellt sind.

Empfehlungen zum Einsatz optischer Datenspeicherung

Beim Einsatz der optischen Datenspeicherung ist zu unterscheiden zwischen Datenträgern die nur einmal beschreibbar, aber beliebig oft lesbar sind (z. B. CD-ROM, WORM, MO als WORM) und anderen Datenträgern, die mehrfach beschreibbar und lesbar sind (z. B. MO).

Aufgrund der fehlenden Löschbarkeit von Daten bei den nur einmal beschreibbaren, optischen Datenträgern und unter Berücksichtigung der Löschungs-, Sperrungs- und Berichtigungsvorschriften der Datenschutzgesetze des Bundes und der Länder ist nach folgenden Regeln zu verfahren:

1) Grundsätzlich sind wiederbeschreibbare, optische Datenträger einzusetzen. Diese können wie Magnetplatten behandelt werden.

2) Es können optische Datenträger verwendet werden, die nur einmal beschreibbar sind, wenn die gesetzlichen Regelungen es zulassen, daß an Stelle der Berichtigung oder Löschung von Daten eine Sperrung tritt. Die Sperren sind dabei besonders zu kennzeichnen. Spätestens nach dem vollständigen Beschreiben des Datenträgers sind die Datenbestände durch Umkopieren auf einen neuen Datenträger zu bereinigen. Der Ursprungsdatenträger ist unverzüglich und vollständig zu löschen, wozu der Datenträger vernichtet werden muß.

3) Werden Daten gesichert oder langfristig archiviert, können ebenfalls optische Datenträger verwandt werden, die nur einmal beschreibbar sind. Dabei sollten möglichst nur Daten mit gleichen Löschungsfristen auf dem gleichen Datenträger abgelegt werden.

4) Sind Daten auf einem nur einmal beschreibbaren Datenträger zu löschen oder zu berichtigen, muß unter Verwendung des alten Datenträgers ein neuer Datenträger beschrieben werden, der die zu löschenden Daten nicht mehr enthält. Der ursprüngliche Datenträger ist unverzüglich und vollständig zu löschen, wozu der Datenträger vernichtet werden muß.

5) Das vollständige Löschen von Daten auf einem nur einmal beschreibbaren, optischen Datenträger (d. h. dessen Vernichtung) ist mit angemessenen technisch-organisatorischen Maßnahmen unter Beachtung der DIN 32757 vorzunehmen. Dazu sind Verfahren wie Ätzen, Einschmelzen, Verbrennen, Zerkratzen oder Schreddern unter Berücksichtigung von Sicherheits- und Umweltverträglichkeitsaspekten anzuwenden.

Erläuterung der Abkürzungen:

- CD-ROM = **C**ompact-**D**isk-**R**ead-**O**nly-**M**emory (im Preßverfahren erstellter bzw. einmal beschreibbarer und mehrfach lesbarer, optischer Datenträger im CD-Format)
- WORM = **W**rite **O**nce **R**ead **M**any (einmal beschreibbarer und mehrfach lesbarer, optischer Datenträger)
- MO = **M**agnetic-**O**ptical (optischer Datenträger auf der Basis magnetischer Beschichtung), als
  - WORM-MO (nur einmal beschreibbar, mehrfach lesbar) und als
  - ROD-MO (Rewritable Optical Disc, mehrfach wiederbeschreib- und lesbar)

Sachverhalt

Zur Technik der optischen Speicherung

Bei der optischen Speicherung unterscheidet man derzeit zwischen CD-ähnlichen Datenträgern und einer Speicherung auf magnetisch-optischer Basis; weitere Techniken werden erprobt, sind aber noch nicht marktreif.

Bei CD-ähnlichen Datenträgern gibt es folgende Formen:

- **CD-ROM** (Compact Disc Read Only Memory) in den Formen:
- CD-DA (Digital-Audio), gemeinsamer Standard der Firmen Philips und Sony von 1982 für Ton-Aufzeichnung: „Red book", maximal 99 logische Stücke (Tracks = 1 Lied), die wieder in Sektoren von 1/75 Sekunden aufgeteilt sind, max. 74 Minuten Musik, 5¼ Zoll
- CD-Standard der Firmen Philips und Sony von 1985 für Programme, Texte und Grafiken: Norm: ISO 9660, „Yellow-book", 5¼ Zoll, 15 % der Nutzdaten sind für Zwecke der Fehlererkennung und -korrektur reserviert, in den Varianten: Mode 1 = max. 682 MB, Mode 2 = max. 778 MB
- CD-ROM/XA (1991, XA = Extended Architecture), 5¼ Zoll, Daten, Ton-, Bild- und Videodaten auf getrennten Spuren, analog der Photo-CD der Fa. Kodak von 1992, Aufzeichnung von Einzelbildern, zum Abspielen ist ein spezieller JPEG-Dekoder (JPEG = Joint Photographic Expert Group) erforderlich, der die komprimierten Daten auswertet,
- CD-Video (bis zu 72 Minuten Videofilme), in den beiden Varianten:
  - CD-I (1988, Fa. Philips, Compact Disc Interaktive, für Interaktion bei Multimedia-Anwendungen, Norm: „Green-book", entspricht Mode 2 des „Yellow-book", der um Audio und Video ergänzt wurde),
  - CD-DV (1993, Compact Disc Digital Video) zum Abspielen der Filme ist ein spezieller MPEG (= Motion Picture Expert Group)-Dekoder erforderlich, der die komprimierten Daten auswertet
- CD-R (CD-Recordable) beschreibbare CD, Norm „Orange-book", max. 60 Minuten als Tonträger

und CD-ROM-Sonderformen wie:

- Mega-CD (Spiele und Sound, Fa. Sega)
- CD-TV (Commodore Dynamic Total Vision, eine Norm der Fa. Commodore; ähnlich CD-I).
- EB-ROM (Sony 1990, Electronic Book Read Only Memory, 3¼ Zoll-Minidisk, ca. 200 MB).

Neue Entwicklungen bei CD-Datenträgern sind:

- Pippin-CD-ROM der Fa. Apple für Multimedia (Video, Interactive) und Spiele
- CD-Plus (Norm „Blue-Book") CD der Firmen Sony und Philips gemeinsam mit 3M, Ricoh, Mitsumi, Acer, Alps, Aztech, Teac, Wearnes Technologies, Nokia „Multimedia-CD" (MMCD), Einführung geplant 1996, 3,7 GB Daten, High-Density-CD, 5¼ Zoll, 135 Minuten Video mit MPEG-2-Dekodierung, CD-Audio-Daten und CD-ROM-Daten auf einer Scheibe (Musik, Standbilder, Videoclips, Liedtexte) Kapazitätsverdopplung durch 2. Schicht (1. Schicht transparent) auf der gleichen Seite möglich
- CD der Firma Matsushita (mit Töchtern JVC, Toshiba, Thomson, Telefunken, Saba, Nordmende) mit Hitachi, MCA, Pioneer, Thomson Multimedia und Film- und Medienkonzern Time Warner „SD-DVD = Super Density Digital Video Disc", 4,8 GB Daten, Super-Density-Standard, 5¼ Zoll, 142 Minuten Video mit MPEG-2-Dekodierung, mit möglicher Kapazitätsverdopplung durch 2. CD-ROM mit Schicht auf der Rückseite (Sandwich), Markteinführung noch offen

Alle diese genannten Speicherungsverfahren arbeiten mit einer schallplattenähnlichen Produktionstechnik (Herstellung einer Masterplatte, Erzeugung von vielen Kopien im Plattenpreßverfahren), deren Produkte in der Regel vom Anwender nur gelesen werden. Am Markt sind inzwischen allerdings auch Geräte verfügbar, die die individuelle Erstellung von CD-ROM's erlauben (Preis der Laufwerke ca. 2 000 DM); bei der Photo-CD ist dies selbstverständlich.

Bei magnetisch-optischen Datenträgern gibt es derzeit folgende Formen:

- **WORM** (Write Once Read Many, Norm: ISO 9171-1/-2 bei 5¼ Zoll,
  CD 13403/CCS-Speicherung oder WI 1.23.02.2/SSF-Speicherung bei 12 Zoll,
  DIS 10885 bei 14 Zoll, Norm: „Orange-book") mit einmaliger Datenspeicherung (ablativ, bubble/pit, melted alloy, phase change) und beliebig häufiger Lesemöglichkeit (Hard-WORM)
- **WO-Disc** (MO = mit magneto-optische Speicherung, Norm: ISO 10090 bzw. ECMA 154 oder ECMA 201 bei 3½ Zoll, Orange-Book) als:
  - **WORM-MO**: hier wird durch eine Plattenmarkierung der WORM-Status dokumentiert und durch Firmware (firmenspezifische Soft- oder Hardware-Programme im Laufwerk zur Sicherstellung der Basis-Funktionen) ein Wiederbeschreiben verhindert (Soft-WORM)
  - **ROD-MO** (Rewritable Optical Disc): d. h. eine mehrfach wiederbeschreibbare optische Disk. Diese erscheint aufgrund der beliebigen Beschreibbarkeit für eine gesicherte Langzeitarchivierung nicht geeignet und dürfte eher als Konkurrenz zu magnetischen Laufwerken (Magnetplatten, -disketten, -bänder, oder -kassetten) anzusehen sein; eine neuere Variante ist die Mini-Disk der Fa. Sony zur Aufzeichnung von Audio-Daten,
  - **WORM-MO** nach Norm ISO 11560 oder ECMA 153 bei 5¼ Zoll,
  - **Mini-Disc** (MD-Data) Sony, 2½ Zoll, ca. 140 MB, Transferrate ca. 150 KB/s, ca. 70 Minuten Musik, Texte, Grafiken, Tabellen, 3 Formate: ROM, mehrfach beschreibbar, hybride Aufzeichnung.

Neuere Entwicklungen

Es gibt auch neuere Entwicklungen, die nicht auf Magnetisierung sondern Phasenwechseltechnik basieren, aber noch nicht als Standard eingeführt sind:

- SD-CD „Super-Densitiy-CD", wiederbeschreibbare optische Disk der Fa. Toshiba mit Hitachi, Matsuhita, MCA, Pioneer, Thomson Multimedia und Film- und Medienkonzern Time Warner, 3½ Zoll, 2 Platten in Sandwich-Bauweise á 650 MB = 1,3 GB, 5 mm Dicke, max. 40 Minuten Video mit MPEG-2-Dekodierung, durch Phasenwechseltechnik (PD = Phasewriter Dual) wird Kunststoff als Trägermaterial von amorphem (nichtspiegelnd) in kristallinen Zustand (reflektierend) umgeschaltet und umgekehrt, keine Magnetisierung, hohe Transferrate von 9,8 bis 16,4 Megabit/s, Laufwerk mit 26 mm Bauhöhe auch für Laptops geeignet; nach gleicher Technik sind auch 5 Zoll Disks mit ca. 12 GB geplant.

Optische Datenträger gibt es in den Formaten 2 Zoll, 2½ Zoll, 3¼ Zoll, 3½ Zoll, 5¼ Zoll, 12 Zoll und 14 Zoll. Die Kapazitäten reichen derzeit von ca. 0,2 bis ca. 10 Giga-Bytes = Millarden Zeichen pro Medium. Die Daten können entweder als CI- (Coded Information-, aus EDV-Systemen) oder als NCI- (Non Coded Information-; Bitmap = grafische Bildpunktinformationen von Seiten über Scanner eingelesen) Dokumente abgelegt sein. Pro Giga-Byte sind damit bei NCI-Dokumenten ca. 20 000 DIN-A4-Seiten und bei CI-Dokumenten ca. 400 000 DIN-A4-Seiten gespeichert.

Datenschutzprobleme bei der optischen Datenspeicherung

Bei der Verarbeitung personenbezogener Daten sind die verfassungsrechtlichen Grundsätze der Verhältnismäßigkeit, Erforderlichkeit, Zweckbindung und informationellen Gewaltenteilung zu beachten, unabhängig davon, auf welche Weise (Akte, Kartei, Datei, Groß-DV, Mehrplatzsystem, PC usw.) die Datenverarbeitung geschieht. Beim Einsatz moderner Informations- und Kommunikations-Technologie sind insbesondere die materiellen Zweck- und Aufbewahrungsbestimmungen der Datenverarbeitung durch technische Maßnahmen zu gewährleisten. Auch die Betroffenenrechte der Datenschutzvorschriften – z. B. die Ansprüche auf Akteneinsicht, die Rechte auf Auskunft, Berichtigung und Löschung – müssen zu jeder Zeit erfüllbar sein.

Insbesondere die Löschungspflicht der Datenschutzgesetze könnte der optischen Datenspeicherung entgegenstehen. Während bei mehrfach beschreibbaren, magnetisch-optischen Systemen die technischen Möglichkeiten mit denen der herkömmlichen Magnetplatten bzw. -disketten weitgehend übereinstimmen, ist das Löschen von Daten bei CD-ROM- bzw. WORM-Datenträgern nicht ohne weiteres erfüllbar.

Das Bundesdatenschutzgesetz und die meisten Landesdatenschutzgesetze definieren das Löschen als „das Unkenntlichmachen gespeicherter Daten" (die entsprechende Formulierung im Berliner DSG lautet: „Beseitigen"). Personenbezogene Daten werden dann als unkenntlich angenommen, wenn die Informationen nicht länger aus den ursprünglich gespeicherten Daten gewonnen werden können.

Auernhammer führt aus, „. . . daß die Löschung, da sie eine Beseitigung der Daten bewirkt, im Gegensatz zur Sperrung einen absoluten Nutzungsausschluß zur Folge hat." (Auernhammer, Kommentar zum BDSG, 3. Auflage 1993, § 20, Rdnr. 13).

Simitis, Dammann u. a., Kommentar zum BDSG, 4. Aufl. 92, äußern sich wie folgt:

„Der Begriff **Unkenntlichmachen** trifft auf jede Handlung zu, die irreversibel bewirkt, daß eine Information nicht länger aus gespeicherten Daten gewonnen werden kann" (§ 3, Rdnr. 180). „Um eine Gefährdung der Rechte der Betroffenen zu vermeiden, sind in diesem Fall an die Unmöglichkeit *(der Wiedergewinnung)* strenge Anforderungen zu stellen. Die schlichte Aufwand-Zweck-Relation des § 9 und die Unverhältnismäßigkeit im Sinne der Anonymisierungsdefinition des Abs. 7 genügen nicht" (§ 3, Rdnr. 187). „Um ein Löschungsgebot zu erfüllen, genügt es nicht, die Datenorganisation so zu verändern, daß ein **gezielter Zugriff** auf die betreffenden Daten ausgeschlossen wird" (§ 3, Rdnr. 188). Die Löschung soll im Gegensatz zur Sperrung die Information zum Verschwinden bringen, nicht nur ihre Verwertbarkeit einschränken. „Unkenntlich (und damit gelöscht) sind Daten nur dann, wenn die Kenntnisnahme ihres Informationsgehalts . . . **unmöglich** ist" (§ 3, Rdnr. 189).

Schaffland/Wiltfang, Kommentar zum BDSG, Stand: Februar 95, definieren wie folgt:

„Unter Löschen von Daten ist das Unkenntlichmachen der gespeicherten Daten zu verstehen. Dies kann dadurch erfolgen, daß der Datenträger (z. B. Karteikarten, Lochkarten) vernichtet oder daß die Daten neu (mit anderen Daten) überschrieben werden (z. B. Magnetband). Jedenfalls dürfen die Daten, die zu löschen sind, nicht mehr lesbar sein."

Bergmann/Möhrle/Herb, Kommentar zum BDSG, Stand: März 1994, definieren zu § 3 in Rdnr. 99 wie folgt:

„Durch das Löschen werden Daten unkenntlich gemacht, so daß eine weitere Verarbeitung nicht mehr möglich ist."

Und in Rdnr. 100: „Löschen verlangt das tatsächliche Unkenntlichmachen der Daten (physisches Löschen) Sie dürfen nicht mehr lesbar sein . . .".

Und weiter in Rdnr. 105: „Die Auslagerung von Datenbeständen, andere organisatorische oder technische Maßnahmen, die verhindern, daß Daten verarbeitet oder genutzt werden können, reichen nicht aus. Diese Daten stehen weiterhin zur Verfügung und können zumindest von DV-Fachleuten wieder aktiviert werden."

Nach § 20 Abs. 3 Nr. 3 und § 35 Abs. 3 Nr. 3 BDSG kann an die Stelle der „Löschung" eine „Sperrung" treten, wenn „eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist". Hierin könnte eine Rechtsgrundlage für den Einsatz neuerer technischer Lösungen, wie z. B. die optische Datenspeicherung,

gesehen werden (vgl. Auernhammer, Kommentar zum BDSG, 3. Aufl. 1993, §20, Rdnr. 27). Nur wenige Landesdatenschutzgesetze lassen derzeit eine ähnliche Lösung zu (z. B. die Länder Brandenburg, Rheinland-Pfalz, Sachsen, Sachsen-Anhalt und Thüringen).

Ein weiteres Datenschutzproblem kann bei der optischen Datenspeicherung dann entstehen, wenn auf die Aufbewahrung von Originaldokumenten in Verfahrensakten verzichtet und an deren Stelle ausschließlich eine digitale Aktenführung treten soll. Dabei kann es Probleme bezüglich der gerichtsverwertbaren Reproduktion von Akten geben. Gesetzliche Regelungen, die klarstellen, ob bei optischer Datenspeicherung auf einen Aktennachweis in Papierform verzichtet werden kann, fehlen weitestgehend. Die Forderung des Papieraktenrückhalts läßt sich nicht allgemein begründen, sondern ist differenziert für jedes einzelne Rechtsgebiet zu untersuchen und an anderer Stelle auszuführen.

Löschung von Informationen bei CD-ROM bzw. WORM

Nach derzeitigem Stand der überwiegenden Zahl der Landesdatenschutzgesetze bestehen bezüglich der Löschung von Datensätzen bei CD-ROM- bzw. WORM-Datenträgern erhebliche datenschutzrechtliche Bedenken, da den Forderungen nach Löschung personenbezogener Daten, wenn ihre Speicherung unzulässig ist oder ihre Kenntnis für die speichernde Stelle zur Aufgabenerfüllung nicht mehr erforderlich ist oder eine Löschung im Rahmen der Berichtigung erforderlich ist, nicht ausreichend Rechnung getragen wird.

Bei CD-ROM- bzw. WORM-Systemen kann die Löschung von Daten aufgrund der technischen Spezifikationen nur durch Löschen von Verweisdaten erfolgen, die in den separat betriebenen, den Zugriff steuernden EDV-Systemen in einem Datenverwaltungssystem gehalten werden. In der aktuellen Indexdatei bzw. Datenbank sind dann die alten Verweise auf die zu löschende Information nicht mehr enthalten (Logische Löschung), obwohl die Nutzdaten auf dem optischen Speichersystem noch physikalisch und im Volltext vorhanden sind. Ohne die Kenntnis dieser Verweisdaten sind die auf der CD-ROM bzw. WORM (gestreut) abgelegten Nutzinformationen nicht gezielt verwertbar.

In einigen Archivierungsystemen werden diese Verweisdaten in der jeweils aktuellen Form für eventuelle Notfall-Restaurierungen ebenfalls auf dem optischen Datenträger abgelegt, so daß mit Hilfe älterer Verweisdaten die nur logisch gelöschten Nutzdaten für einen potentiellen Angreifer leicht lesbar sein könnten.

Das Sperren von Einzeldaten oder Datensätzen kann durch das Setzen und Abfragen von entsprechenden Kennzeichen in den separat geführten Verweisdaten vorgenommen werden.

Aufgrund der oben genannten Definitionen und ihrer Auslegungen und unter Berücksichtigung der technischen Gegebenheiten ist bei einer Nutzung von CD-ROM- bzw. WORM-Datenträgern eine faktische Löschung nicht möglich, da lediglich durch Software (Verweisdaten), die geändert werden kann, der Zugriff auf die auf der CD-ROM bzw. WORM weiterhin vollständig vorhandenen Daten unterbunden (logische Löschung) ist. Es ist zudem denkbar, daß u. a. der Anbieter der CD-ROM- bzw. WORM-Platte und des Laufwerks über das Wissen und die Möglichkeit verfügt, auf derart „logisch" gelöschte Daten zuzugreifen.

Die gesetzlichen Berichtigungs- und Löschungsansprüche von Betroffenen können bei CD-ROM- bzw. WORM-Speicherung dadurch gelöst werden, daß unverzüglich ein neuer Datenträger aus dem alten erzeugt wird, wobei nur noch die gültigen Daten übernommen und die Daten auf dem ursprünglichen Datenträger gelöscht werden.

Eine vollständige Löschung der auf CD-ROM- bzw. WORM-Platten enthaltenen Informationen ist derzeit nur möglich durch Zerstörung der Speicherfläche (Ätzen, Zerkratzen) oder durch physikalische Vernichtung des gesamten Datenträgers (Einschmelzen, Verbrennen, Schreddern); analog der Behandlung von Magnetdatenträgern und Mikrofilmen. Die Grundsätze der DIN 32757 „Vernichtung von Informationsträgern" können nicht ohne weiteres übernommen werden, da diese Speichermedien bisher unübliche, hochkapazitäre Datenablagen bieten (ca. 1 000 Seiten pro Quadratzentimeter, ca. 300 000 Schreibmaschinenseiten bei einer WORM mit 5¼ Zoll = 12 Zentimeter-Durchmesser) und eine damit verbundene Gefahr der Entwendung bzw. Wiedergewinnung höchst umfangreicher und sensibler Datenbestände besteht. Es muß mit der Möglichkeit gerechnet werden, daß eine Rekonstruktion erfolgen kann.

Nach Aussage der Fa. Siemens als Anbieter optischer Speichersysteme ist es bei WORM-Datenträgern mit besonderem Aufwand möglich, den durch Firmware gesicherten Schreibschutz belegter Bereiche (sogenannter „Blank-Check") zu umgehen und beschriebene Bereiche nachträglich zu überschreiben (wird aber nicht softwaremäßig unterstützt). Eine Veränderung der vorhandenen Daten ist dabei allerdings nicht möglich. Systembedingt gilt der überschriebene Bereich als zerstört und die Neuinformation wird in einen Ersatzspurbereich übernommen, der nur über eine beschränkte Kapazität (ca. 1 MB) verfügt. Nach relativ geringen Änderungen würde dieser Bereich überlaufen und eine weitere Ablage auf dem Datenträger verhindern. Diese Umgehungsmöglichkeit auch im positiven Sinne zu nutzen, um Daten zu löschen, ist aus diesen Gründen nicht sinnvoll. Eine diesbezügliche Forderung zur Realisierung in der Software würde die Änderung internationaler Normen erfordern.

Anlage 27

Der Bundesbeauftragte für den Datenschutz
Dr. Jacob
Tel. 0228/81995-0
Fax 0228/81995-50
X.400: C=de;A=bund400; P=bfd;S=post stelle
Riemenschneiderstr. 11
53175 Bonn
Leitender Beamter
Dir Bachmeier
Zentrale Aufgaben
OARn Schumacher
Presse und Öffentlichkeitsarbeit
OAR Czepluch
Haushalt, Organisation, Innerer Dienst
I
Grundsatzangelegenheiten
Internationales
nicht-öffentl. Bereich
Meldewesen
MinR Dr. Dammann
II
Rechtswesen
Finanzen
Arbeitsverwaltung
Verteidigung
Zivildienst
Auswärtiger Dienst
MinR Dr.Au
III
Sozialwesen
Personalwesen
MinR Spickschen
IV
Wirtschaft und Verkehr
Multimedia
Forschung
Statistik
Archivwesen
Post
Umweltangelegenheiten
MinR Dr. Schmidt
V
Polizei
Nachrichtendienste
MinR Dr. von Pommer Esche
VI
Informationstechnik
Telekommunikation
Datensicherung
MinR Alke
VII
Allgemeine innere Verwaltung
Strafrecht
Aufarbeitung der Mfs-Unterlagen
MinR Ottermann

Sachregister

Abkürzungsverzeichnis

3-S-Konzept	Service, Sicherheit und Sauberkeit im Bahnhofsbereich
AA	Auswärtiges Amt
AAÜG	Anspruchs- und Anwartschaftsüberführungsgesetz
ABl	Amtsblatt der Europäischen Gemeinschaften
ADV	Automatisierte Datenverarbeitung
AFG	Arbeitsförderungsgesetz
AFIS	Automatisiertes Fingerabdruck-Identifizierungssystem
AFRG	Arbeitsförderungs-Reformgesetz
AG	Aktiengesellschaft
AGE	Automatisische Gebührenerhebung
AL Z	Leiter der Zentralabteilung
AMD	Arbeitsmedizinischer Dienst
AO	Abgabenordnung
AOK	Allgemeine Ortskrankenkasse
APC	Arbeitsplatzcomputer
APL	Anschlußpunkt des Liniennetzes
ARGUS	Ausfuhrkontrollsystem für Erstattungswaren auf der Basis von Risikoanalysen
AZR-VV	Allgemeine-Verwaltungsvorschrift des BMI zum AZR-Gesetz und zur AZRG-Durchführungsverordnung
ASYLON	Asyl-online
AsylVfG	Asylverfahrensgesetz
AtomG	Atomgesetz
AuslG	Ausländergesetz
AVS	Automatisiertes Vollstreckungssystem
AWG	Außenwirtschaftsgesetz
AZR	Ausländerzentralregister
AZR-Gesetz	Ausländerzentralregister-Gesetz
AZRG-DV	Verordnung zur Durchführung des Ausländerzentralregistergesetzes
BA	Bundesanstalt für Arbeit
BAB	Bundesautobahn
BAfAM	Bundesanstalt für Arbeitsmedizin
BAFl	Bundesamt für die Anerkennung ausländischer Flüchtlinge
BAföG	Bundesausbildungsförderungsgesetz
Bahn-BKK	Bahnbetriebskrankenkasse
BAN	Bundesgrenzschutzaktennachweis
BAPT	Bundesamt für Post und Telekommunikation
BauStatG	Gesetz über die Durchführung von Statistiken der Bautätigkeit und die Fortschreibung des Gebäudebestandes
BAV	Bundesaufsichtsamt für das Versicherungswesen
BAZ	Bundesamt für den Zivildienst
BBG	Bundesbeamtengesetz
BBKK	Bundesbahnbetriebskrankenkasse
BBN	Bundesbehördennetz
BDSG	Bundesdatenschutzgesetz
BfA	Bundesversicherungsanstalt für Angestellte
BfD	Bundesbeauftragter für den Datenschutz
BfS	Bundesamt für Strahlenschutz
BfV	Bundesamt für Verfassungsschutz
BGBl	Bundesgesetzblatt
BGS	Bundesgrenzschutz
BGSG	Bundesgrenzschutzgesetz
BIOS	Basic Input Output System
Bit	Binary Digit
BK	Bundeskanzleramt
BK-DOK	Berufskrankheiten-Dokumentation
BKA	Bundeskriminalamt
BKAG	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten

BKK	Betriebskrankenkasse
BMA	Bundesministerium für Arbeit und Sozialordnung
BMBau	Bundesministerium für Raumordnung, Bauwesen und Städtebau
BMBF	Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie
BMF	Bundesministerium der Finanzen
BMFSFJ	Bundesministerium für Frauen, Senioren, Familie und Jugend
BMG	Bundesministerium für Gesundheit
BMI	Bundesministerium des Innern
BMJ	Bundesministerium der Justiz
BMPT	Bundesministerium für Post und Telekommunikation
BMU	Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit
BMV	Bundesministerium für Verkehr
BMVg	Bundesministerium der Verteidigung
BMWi	Bundesministerium für Wirtschaft
BND	Bundesnachrichtendienst
BNDG	Gesetz über den Bundesnachrichtendienst
BOS	Behörden und Organisationen mit Sicherheitsaufgaben
BPersVG	Bundespersonalvertretungsgesetz
BPräsA	Bundespräsidialamt
BR-Drs.	Bundesrats-Drucksache
BSHG	Bundessozialhilfegesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BStU	Bundesbeauftragter für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR
BT-Drs.	Bundestags-Drucksache
Btx	Bildschirmtext
BVA	Bundesverwaltungsamt
BVerfG	Bundesverfassungsgericht
BVerfGE	Bundesverfassungsgerichtsentscheidung
BVerfSchG	Bundesverfassungsschutzgesetz
BVerfSchGE	Bundesverfassungsschutzgesetz-Entwurf
BVerwG	Bundesverwaltungsgericht
BVFG	Bundesvertriebenengesetz
BVG	Bundesverfassungsgericht
BZR	Bundeszentralregister
BZRG	Bundeszentralregistergesetz
C.SIS	technische Unterstützungseinheit des Schengener Informationssystems
CCITT	Comité Consultatif International Télégraphique et Téléphonique
CD-ROM	Compact Disc – Read Only Memory
CIS	Zollinformationssystem (Customs Information System)
CNIL	Commission Nationale de l'Informatique et des Libertés
DASPO-T	DV-gestütztes Arbeitssystem für Personal- und Organisationsstellen für den Bereich Telekom
Datex-J	data exchange – Jedermann (ältere Bezeichnung des T-Online-Dienstes der Telekom AG)
Datex-P	data exchange – packet (paketvermittelndes Datennetz der Telekom AG)
DDR	Deutsche Demokratische Republik
DIN	Deutsches Institut für Normung
DNA	Desoxyribonoclein acid (acid = Säure)
DRK	Deutsches Rotes Kreuz
DSB	Datenschutzbeauftragter
Dv/dv	Datenverarbeitung
E-Mail	Electronic Mail
EAGFL	Europäischer Ausrichtungs- und Garantiefonds für die Landwirtschaft
EDE	Europäische Drogeneinheit
EDS	Europäische Drogenstelle
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
EG-AH-G	EG-Amtshilfe-Gesetz
EG-Vertrag	Vertrag zur Gründung der Europäischen Gemeinschaft
EheSchlRG	Gesetz zur Neuordnung des Eheschließungsrechts
EIS	Europäisches Informationssystem
EPR	Elektronisches Personenregister

EStG	Einkommensteuergesetz
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EURATOM	Europäische Atomenergie-Gemeinschaft
EURODAC	Europäisches daktyloskopisches System
EUROPOL	Zentrales Europäisches Kriminalpolizeiamt
EUROSTAT	Statistisches Amt der Europäischen Gemeinschaft
EUV	Vertrag über die Europäische Union
EVÜ	Einzelverbindungsübersicht
EWG	Europäische Wirtschaftsgemeinschaft
FAG	Fernmeldeanlagengesetz
FKTO	Fernmeldekontonummer
FVG	Finanzverwaltungsgesetz
G 10	Gesetz zu Artikel 10 GG
G 7	Gruppe der 7 größten Industrienationen
GAN	Datei Grenzaktennachweis
GG	Grundgesetz
ggf.	gegebenenfalls
GKI	Gemeinsame Kontrollinstanz
GKV	Gesetzliche Krankenversicherung
GmbH	Gesellschaft mit beschränkter Haftung
GMD	Gesellschaft für Mathematik und Datenverarbeitung
GÜG	Grundstoffüberwachungsgesetz
GÜS	Grundstoff-Überwachungs-Stelle
GVG	Gerichtsverfassungsgesetz
GwG	Geldwäschegesetz
HP	Health Professional
HPC	Health Professional Card
HVBG	Hauptverband der gewerblichen Berufsgenossenschaften
i. d. R.	in der Regel
i. S. d.	im Sinne des
i. V. m.	in Verbindung mit
ICD-10	International Classification of Diseases – 10th Revision
IKPO	Internationale Kriminalpolizei-Organisation
ILAN	Internetworking Local Area Network
IMK	Innenministerkonferenz
INPOL	Informationssystem der Polizei
InVeKoS	Integriertes Verwaltungs- und Kontrollsystem
INZOLL	Informationssystem für den Zollfahndungsdienst
IRENE	Irrégularités, Enquêtes, Exploitation (Übersetzung: Unregelmäßigkeiten, Ermittlungen, Auswertung)
ISDN	Integrated Services Digital Network
ISO	International Standard Organisation
IT	Informationstechnik
ITSEC	Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik
IuKDG	Informations- und Kommunikationsdienstegesetz (Entwurf)
IVBB	Informationsverbund Berlin–Bonn
IVS	Informationsverarbeitungsservice
JuMiG	Justizmitteilungsgesetz
JVA	Justizvollzugsanstalt
KBA	Kraftfahrt-Bundesamt
KBSt	Koordinierungs- und Beratungsstelle der Bundesregierung für Infromationstechnik in der Bundesverwaltung
KBV	Kassenärztliche Bundesvereinigung
Kbyte	Kilobyte
KONTES-ANDI	Kundenorientierte Neugestaltung des Telekomservices – Anmeldedienste
KONTES-BUDI	Kundenorientierte Neugestaltung des Telekomservices – Buchdienste
KSD/IA	Koordingungsstelle Schengen/Dublin – Internationale Aufgaben
KVK	Krankenversicherungskarte
KZBV	Kassenzahnärztliche Bundesvereinigung
LAN	Local Area Network
LBA	Luftfahrt-Bundesamt

LfD	Landesbeauftragter für den Datenschutz
lit.	Litera = Buchstabe
LuftVG	Luftverkehrsgesetz
MAD	Militärischer Abschirmdienst
MADG	Gesetz über den MAD
MdK	Medizinischer Dienst für die Bereiche der Bahnbetriebskrankenkasse und der Betriebskrankenkassen des Bundesverkehrsministeriums
MfS	Ministerium für Staatssicherheit/Amt für nationale Sicherheit (der ehemaligen DDR)
MHSAV	Message-Handling System Auslands-Vertretungen
MKT	Multifunktionales Kartenterminal
MOE-Staaten	mittel- und osteuropäische Staaten
MRRG	Melderechtsrahmengesetz
MV	Mitteilungsverordnung
n. F.	neue Fassung
NADIS	Nachrichtendienstliches Informationssystem
NADIS-PZD	Personenzentraldatei im NADIS
NJW	Neue Juristische Wochenzeitschrift
NVA	Nationale Volksarmee
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OWi	Ordnungswidrigkeit
PC	Personalcomputer
PD-DSV	Postdienst-Datenschutzverordnung
PDS	Partei des Demokratischen Sozialismus
PDSV	Postdienstunternehmen-Datenschutzverordnung
PDV	Polizei-Dienstvorschrift
PE	Personalressorts
PIN	persönliche Identifikationsnummer
PROFIT	Prüfungsorientierte Form der Informationstechnik
PStÄndG	Gesetz zur Änderung des Personenstandsgesetzes
PStG	Personenstandgesetz
PTNeuOG	Gesetz zur Neuordnung des Postwesens und der Telekommunikation (Postneuordnungsgesetz)
PTRegG	Gesetz über die Regulierung der Telekommunikation und des Postwesens
RBKK	Reichsbahnbetriebskrankenkasse
RV-Nr.	Rentenversicherungsnummer
RVO	Reichsversicherungsordnung
s. o.	siehe oben
s. u.	siehe unten
SCHUFA	Schutzgemeinschaft für allgemeine Kreditsicherung
SchwbG	Schwerbehindertengesetz
SDAG	Sowjetisch-Deutsche Aktiengesellschaft
SDÜ	Schengener Durchführungsübereinkommen
SED	Sozialistische Einheitspartei Deutschlands
SEED	System for the Exchange of Excise Data
SGB	Sozialgesetzbuch
SGB I	Sozialgesetzbuch Erstes Buch (Allgemeiner Teil)
SGB IV	Sozialgesetzbuch Viertes Buch (Gemeinsame Vorschriften für die Sozialversicherung)
SGB V	Sozialgesetzbuch Fünftes Buch (Gesetzliche Krankenversicherung)
SGB VI	Sozialgesetzbuch Sechstes Buch (Gesetzliche Rentenversicherung)
SGB VII	Sozialgesetzbuch Siebentes Buch (Gesetzliche Unfallversicherung)
SGB VIII	Sozialgesetzbuch Achtes Buch (Kinder- und Jugendhilfe)
SGB X	Sozialgesetzbuch Zehntes Buch (Verwaltungsverfahren)
SGB XI	Sozialgesetzbuch Elftes Buch (soziale Pflegeversicherung)
SIRENE	Supplementary Information Request for National Entry
SIS	Schengener Informationssystem
SMBG	Süddeutsche Metallberufsgenossenschaft
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
StrEG	Gesetz über die Entschädigung für Strafverfolgungsmaßnahmen
StUG	Gesetz über die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (Stasi-Unterlagen-Gesetz)

StUGÄndG	Änderungsgesetz zum Stasi-Unterlagen-Gesetz
StVÄG	Strafverfahrensänderungsgesetz
SÜG	Sicherheitsüberprüfungsgesetz
T&T	Tracking and Tracing
TAE	Telekommunikatons-Anschlußeinheit
TB	Tätigkeitsbericht*)
TDDSG	Teledienstedatenschutzgesetz (Entwurf)
TDG	Teledienstegesetz
TDSV	Telekom-Datenschutzverordnung
TIBIS	Telekom integrierendes Büroinformationssystem
TIDSV	Telekommunikations- und Informationsdienstunternehmen-Datenschutzverordnung
TK	Telekommunikation
TK-Anlagen	Telekommunikationsanlagen
TKG	Telekommunikationsgesetz
TKV	Telekommunikations-Kundenschutzverordnung
TLG	Treuhand Liegenschaftsgesellschaft
TOS-AV	Telekom Operator Service-Auslandsvermittlung
TPG	Transplantationsgesetz
Ü 1	einfache Sicherheitsüberprüfung
Ü 2	erweiterte Sicherheitsüberprüfung
Ü 3	erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen
u. U.	unter Umständen
UCLAF	Betrugsbekämpfungseinheit der Europäischen Kommission
UDSV	Teledienst-Unternehmen-Datenschutzverordnung
VBG	Verwaltungs-Berufsgenossenschaft
VdAK	Verband der Angestellten Krankenkassen
VDR	Verband Deutscher Rentenversicherungsträger
VGH	Verwaltungsgerichtshof
VNP	Vorgangsnachweis Personen
VNS	Vorgangsnachweisdatei
VT-BS	Vertriebsteams für Behörden mit Sicherheitsaufgaben
VZR	Verkehrszentralregister
WDO	Wehrdisziplinarordnung
WpHG	Wertpapierhandelsgesetz
WWW	World Wide Web
z. Z.	zur Zeit
ZDG	Zivildienstgesetz
ZEB	Zentralstelle Betrugsbekämpfung
Zeus	Zeiterfassungssystem
ZIS	Zollinformationssystem
ZKA	Zollkriminalamt
ZStV	Zentrales Staatsanwaltschaftliches Verfahrensregister

*) Erster Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 8/2460
Zweiter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 8/3570
Dritter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 9/93
Vierter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 9/1243
Fünfter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 9/2386
Sechster Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 10/877
Siebenter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 10/2777
Achter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 10/4690
Neunter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 10/6816
Zehnter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 11/1693
Elfter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 11/3932
Zwölfter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 11/6458
13. Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 12/553
14. Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 12/4805
15. Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 13/1150

Ich bitte den 16. Tätigkeitsbericht 1995–1996

als Diskette ☐

als CD-ROM ☐

an folgende Anschrift zu senden:

_____

_____

_____

_____

_____

Druck: Bonner Universitäts-Buchdruckerei, 53113 Bonn
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 13 20, 53003 Bonn, Telefon: 02 28/3 82 08 40, Telefax: 02 28/3 82 08 44
ISSN 0722-8333